6759-W1-NA

User Manual

VER: 1.0

Contents

1 Safety Precautions 1
2 Overview 2
2.1 Application 2
2.2 Features 3
2.3 Standards Compatibility and Compliance 4
3 Hardware Description and Installation 5
3.1 Hardware Description 5
3.1.1 Front Panel 5
3.1.2 Rear Panel and Side Panel 7
3.2 Hardware Installation 8
3.2.1 Choosing the Best Location for Wireless Operation 8
3.2.2 Connecting the Device 8
4 PC Network Configuration and Login 10
4.1 PC Network Configuration 10
4.2 Logging In to the DSL Router 12
5 Web-Based Management 13
5.1 Device Information 13
5.1.1 Summary 14
5.1.2 WAN 15
5.1.3 Statistics 16
5.1.4 LAN 16
5.1.5 WAN Service 16
5.1.6 xTM 17
5.1.7 xDSL 17
5.1.8 Route 20
5.1.9 ARP 21
5.1.10 DHCP 21
5.2 Advanced Setup 21
5.2.1 Layer2 Interface 22
5.2.2 WAN Service 26
5.2.3 3G WAN Service 51
5.2.4 LAN Configuration 55

5.2.5 NAT 61
5.2.6 Security 64
5.2.7 Parental Control 64
5.2.8 Quality of Service 64
5.2.9 Routing 64
5.2.10 DNS 64
5.2.11 DSL 64
5.2.12 UPnP 64
5.2.13 DNS Proxy 64
5.2.14 Print Server 64
5.2.15 DLNA 64
5.2.16 Packet Acceleration 64
5.2.17 Storage Service 64
5.2.18 Interface Grouping 64
5.2.19 IP Tunnel 64
5.2.20 IPSec 64
5.2.21 Certificate 64
5.2.22 Power Management 64
5.2.23 Multicast 64
5.3 Wireless 64
5.3.1 Security 64
5.3.2 MAC Filter 64
5.3.3 Wireless Bridge 64
5.3.4 Advanced Settings 64
5.3.5 Station Info 64
5.4 Voice 64
5.4.1 VoIP Status 64
5.4.2 SIP Basic Setting 64
5.4.3 SIP Advanced Setting 64
5.4.4 SIP Extra Setting 64
5.4.5 SIP Debug Setting 64
5.4.6 VoIP Functionality 64
5.5 Diagnostics 64
5.5.1 Diagnostics 64

5.5.2 Fault Management 64
5.6 Management 64
5.6.1 Settings 64
5.6.2 System Log 64
5.6.3 SNMP Agent 64
5.6.4 TR-69 Client 64
5.6.5 Internet Time 64
5.6.6 Access Control 64
5.6.7 Update Software 64
5.6.8 Reboot 64
6 Q&A 64

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: 6RTDL01B67X9. If requested, this number must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11.

REN (RINGER EQUIVALENT NUMBERS) STATEMENT

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

ATTACHMENT LIMITATIONS STATEMENT

Notice: This equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment with the Industry Canada certification number. The Department does not guarantee the equipment will operate to the user's satisfaction. Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together.

This precaution may be particularly important in rural areas.

Caution:

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

IC Statement

This product meets the applicable Industry Canada technical specifications. / Le présent matériel est conforme aux specifications techniques applicables d'Industrie Canada.

The Ringer Equivalence Number (REN) is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five. / L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

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 xDSL Router integrates wireless LAN, USB, and VoIP service into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11b/802.11g/802.11n wireless network. The Router combines high-speed xDSL Internet connection, Ethernet uplink, 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 supports 3G WAN service.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The xDSL connection is made using ordinary telephone line with standard connectors. You can connect the Ethernet interface of WAN to Internet with Ethernet cable for ETH uplink. 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
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming
- Voice over IP (VoIP)
- USB storage

- 3G WAN service

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 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates, compatible with IEEE 802.11b/g/n
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Packet Transfer Mode (PTM)
- Ethernet (ETH) Transfer Mode
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Command line interface (CLI)
  - TR-069 WAN management protocol
  - Simple Network Management Protocol (SNMP)
- 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+)
- ITU G.993.1 (VDSL)
- ITU G993.2 (VDSL2)
- 3G (WCDMA, CDMA2000, TD-SCDMA)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- RFC3261 (SIP for VoIP)

3 Hardware Description and Installation

Note:

The figures in this document are for reference only.

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	The device is powered on and the device operates normally.
		Blink	The software is upgrading.
		Off	The device is powered off.
	Red	On	The device is initiating.
		Blink	The software is upgrading.
DSL	Green	On	DSL link has established.
		Blink	The DSL line is training.
		Off	Device is powered off.
Internet	Green	On	Internet is synchronized successfully in the route mode.
		Blink	Internet data is being transmitted.
		Off	Ethernet interface is disconnected.
	Red	On	Authentication has failed.
LAN 1/2/3/4	Green	On	The Ethernet interface is connected.
		Blink	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet interface is disconnected.
USB1/2	Green	On	The connection of 3G or USB flash disk has

Indicator	Color	Status	Description
			established.
		Blink	Data is being transmitted.
		Off	No signal is detected.
WLAN	Green	On	WLAN is enabled.
		Blink	Data is being transmitted through the wireless interface.
		Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blink	Negotiation is in progress under Wi-Fi Protected Setup.
		Off	Wi-Fi Protected Setup is disabled.
TEL1/2	Green	Off	No FXS signal is detected.
		Blink	The user data is passing through FXS port.
		On	The FXS interface is ready to work.
PSTN	Green	Off	No PSTN signal is detected.
		Blink	The user data is passing through FXO port.
		On	The FXO interface is ready to work.

3.1.2 Rear Panel and Side Panel

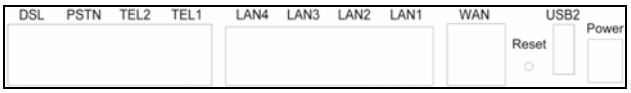


Figure 2 Rear panel

Figure 3 Side panel

The following table describes the interfaces and the buttons.

Interface	Description
DSL	RJ-11 port. Connect the router to DSL connector or splitter through telephone cable.
PSTN	RJ-11 FXO port. Connect the router to the PSTN line with telephone cable.
TEL1/2	RJ-11 FXS port, using the telephone cable to connect the telephone set.
LAN 4~1	RJ-45 port, for connecting the router to a PC or another network device.
WAN	For connecting Ethernet cable to provide Ethernet uplink.
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.
USB1/2	USB port, for connecting the 3G network card or other USB storage devices.
Power	Power interface, for connecting the power adapter.

Interface	Description
On/Off	Power switch.
WLAN	WLAN switch, for enabling or disabling the WLAN function.
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.

⚠ Precautions:

*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.*

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

Step 1 Connect the **DSL** port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable; and connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

- **Line**: Connect to a wall phone jack (RJ-11 jack)
- **Modem**: Connect to the Line interface of the router
- **Phone**: Connect to a telephone set

Step 2 Connect the **LAN** port of the router to the network card of the PC through an Ethernet cable.

Step 3 Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** port of the router.

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

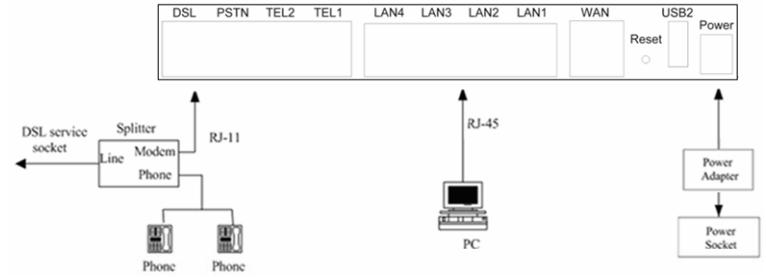


Figure 4 Connecting the DSL router

Note:

If you use 3G WAN service, connect the 3G USB data card to the **USB** port of the router.

If you use the Ethernet uplink, connect the WAN interface that is defined to the Internet with Ethernet cable.

The xDSL uplink, 3G WAN service, and Ethernet uplink can not coexist.

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.

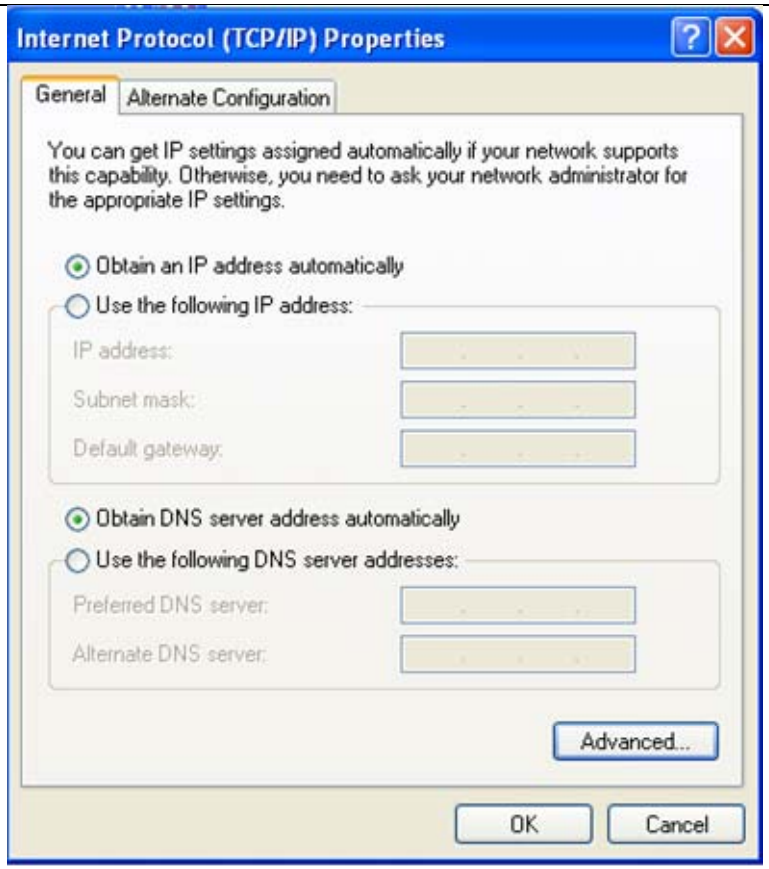


Figure 5 IP and DNS configuration

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

Step 1 Choose **Start** > **Control Panel** > **Network Connections**.

Step 2 Right-click the Ethernet connection icon and choose **Properties**.

Step 3 On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step 4 The **Internet Protocol (TCP/IP) Properties** window appears.

Step 5 Select the **Obtain an IP address automatically** radio button.

Step 6 Select the **Obtain DNS server address automatically** radio button.

Step 7 If you want to set the IP address and subnet mask manually, you can set the IP address and subnet mask of the computer to **192.168.1.x** and **255.255.255.0** respectively. The range for x is from 2 to 254.

Step 8 Click **OK** to save the settings.

4.2 Logging In to the DSL Router

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

Step 1 Open a Web browser on your computer.

Step 2 Enter ***http://192.168.1.1*** (the default IP address of the DSL router) in the address bar. The login page appears.

Step 3 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.

Step 4 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.

Figure 6 Login page

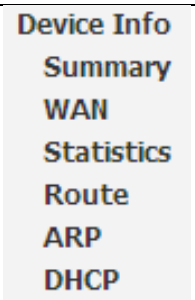
After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system

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.

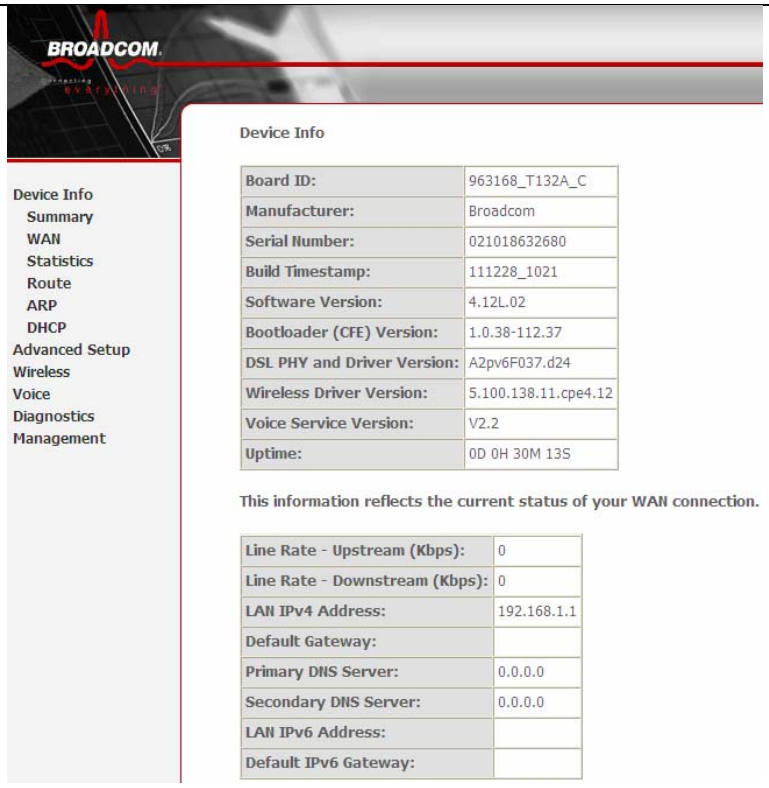
5.1 Device Information

Choose **Device Info**, and the submenus of **Device Info** are shown as below:



5.1.1 Summary

Choose **Device Info > Summary**, and the following page appears.



This page displays the device information such as the board ID, software version, and the information of your WAN connection such as the upstream rate and the LAN address.

5.1.2 WAN

Choose **Device Info > WAN** and the following page appears.

WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Connected Time
ppp0.1	pppoe_0_1_1	PPPoE	Disabled	Disabled	Enabled	Enabled	Unconfigured	0.0.0.0		/

This page displays the information of the WAN interface, such as the connection status, and the IP address.

5.1.3 Statistics

5.1.4 LAN

Choose **Device Info > Statistics > LAN** and the following page appears.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	9300	65	0	0
eth1	74561	738	0	0	945911	1155	0	0
eth2	0	0	0	0	9300	65	0	0
eth3	0	0	0	0	9300	65	0	0
wlan	0	0	0	0	5822	43	0	0

Reset Statistics

In this page, you can view the statistical information about the recevied and transmitted data packets of the Ethernet and wireless interfaces.

Click **Reset Statistics** to restore the values to zero and recount them.

5.1.5 WAN Service

Choose **Device Info > Statistics > WAN Service** and the following page appears.

Statistics -- WAN

Interface	Description	Connected Time	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0.1	pppoe_0_1_1	/	0	0	0	0	0	0	0	0

Reset Statistics

In this page, you can view the statistical information about the recevied and transmitted data packets of the WAN interface.
Click **Reset Statistics** to restore the values to zero and recount them.

5.1.6 xTM

Choose **Device Info > Statistics > xTM** and the following page appears.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

Reset

In this page, you can view the statistical information about the recevied and transmitted data packets at the xTM interfaces.
Click the **Reset** button to restore the values to zero and recount them.

5.1.7 xDSL

Choose **Device Info > Statistics** > **xDSL** and the following page appears.

Statistics -- xDSL

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test Reset Statistics

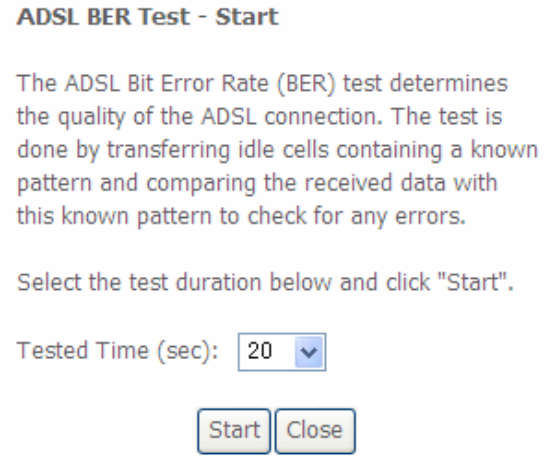
In this page, you can view the statistical information about the recevied and transmitted data packets of the xDSL interfaces.

Click **xDSL BER Test** to test the xDSL Bit Error Rate.

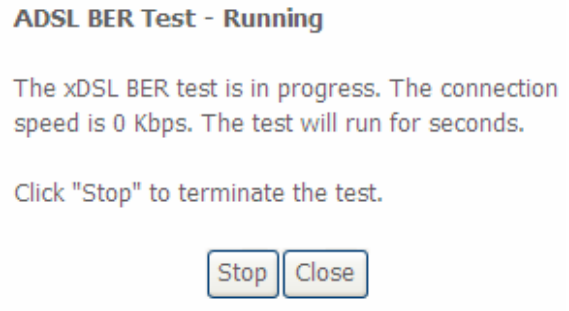
Click **Reset Statistics** to restore the values to zero and recount them.

xDSL BER Test

Click **xDSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows:



The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time in the drop-down list and click **Start**. The following pages appear.



When the ADSL BER test completes, the following page appears.

ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x000000001B69B580
Total Error Bits:	0x0000000000000000
Error Ratio:	0.00e+00

Close

Note:

If the BER reaches e-5, you cannot access the Internet.

5.1.8 Route

Choose **Device Info > Route** and the following page appears.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

Destination	Destination	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

In this page, you can view the route table information.

5.1.9 ARP

Choose **Device Info > ARP** and the following page appears.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.25	Complete	00:1d:0f:19:91:c1	br0

In this page, you can view the MAC address and IP address information of the device connected to the router.

5.1.10 DHCP

Choose **Device Info > DHCP** and the following page appears.

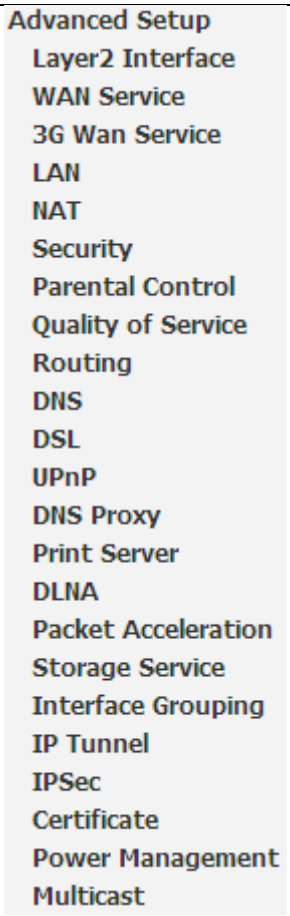
Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
gjdoc-d0cf4a448	08:00:27:75:75:2c	192.168.1.2	22 hours, 10 minutes, 8 seconds

In this page, you can view the host name, the IP address assigned by the DHCP server, the MAC address this is corresponding to the IP address, and the DHCP lease time.

5.2 Advanced Setup

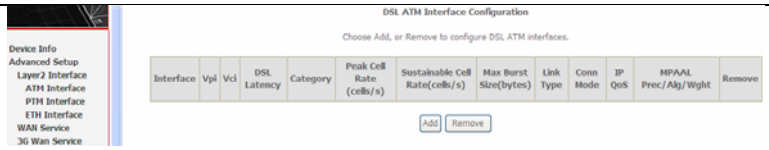
Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown as below:



5.2.1 Layer2 Interface

5.2.1.1 ATM Interface

Choose **Advanced Setup** > **Layer2 Interface > ATM Interface** . In this page, you can add or remove to configure DSL ATM Interfaces.



Click **Add** to add ATM Interface and the following page appears.

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: 0 [0-255]

VCI: 35 [32-65535]

Select DSL Latency

☑ Path0 (Fast)

☐ Path1 (Interleaved)

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

◉ EoA

○ PPPoA

○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence as the Default Queue

◉ Weighted Round Robin

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

VC WRR Weight: 1 [1-63]

VC Precedence: 8 [1-8] (lower value, higher priority)

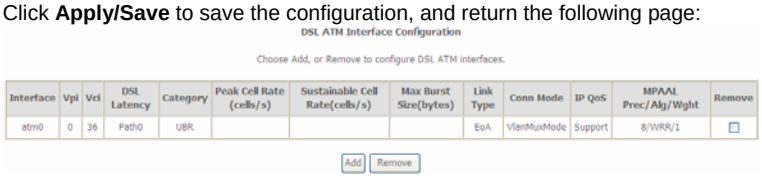
Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

Back Apply/Save

In this page, you can enter this PVC (VPI and VCI) value, and select DSL link type (EoA is for PPPoE, IPoE, and Bridge.), encapsulation mode, service category.

- **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).
- **DSL Link Type**: EoA (it is for PPPoE, IPoE, and Bridge), PPPoA, or IPoA
- **Encapsulation Mode**: LLC/SNAP-BRIDGING, or VC/MUX
- **Service Category:** UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR.
- **Select Scheduler for Queues of Equal Precedence as the Default Queue**: Weighted Round Robin or Weighted Fair Queuing.

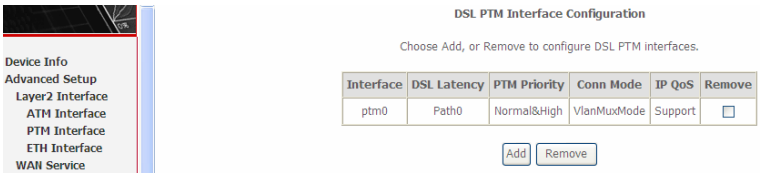
Click **Apply/Save** to save the configuration, and return the following page:



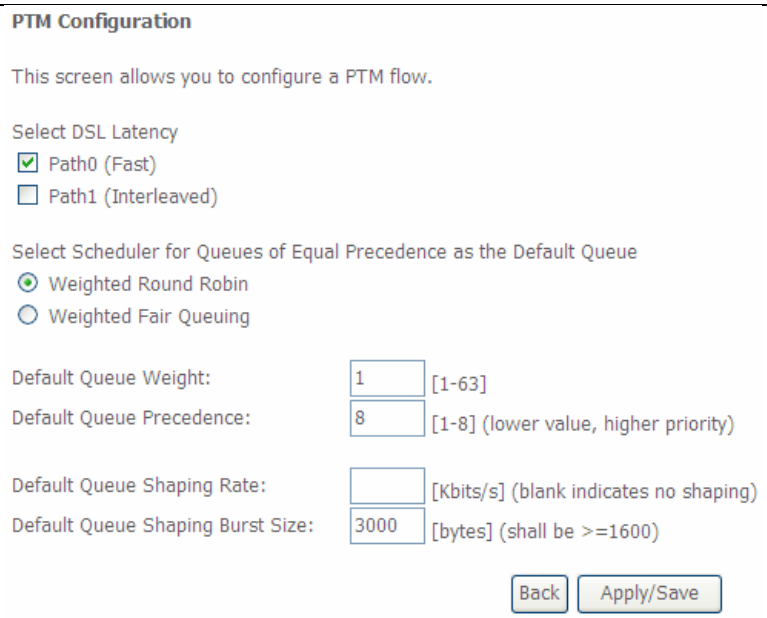
If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

5.2.1.2 PTM Interface

Choose **Advanced Setup** > **Layer2 Interface > PTM Interface**, and the following page appears. In this page, you can add or remove to configure PTM WAN Interfaces.



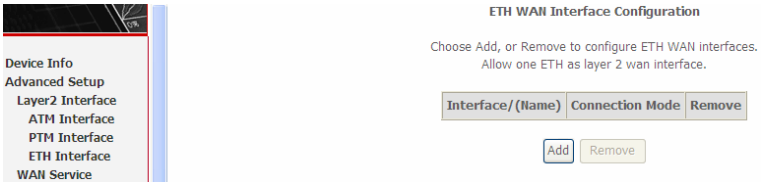
Click **Add** and the following page appears.



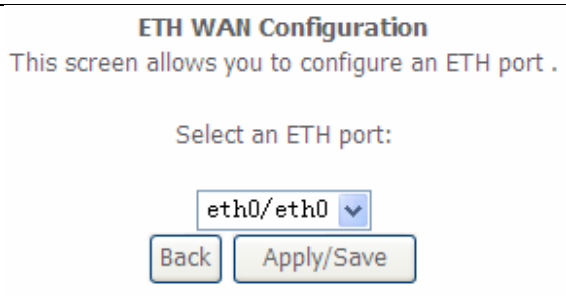
In this page, you can select scheduler for queues of equal precedence and enter the queue value. Click **Apply/Save** to save configuration.

5.2.1.3 ETH Interface

Choose **Advanced Setup** > **Layer2 Interface > ETH Interface**, and the following page appears. In this page, you can add or remove to configure ETH WAN Interfaces.



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



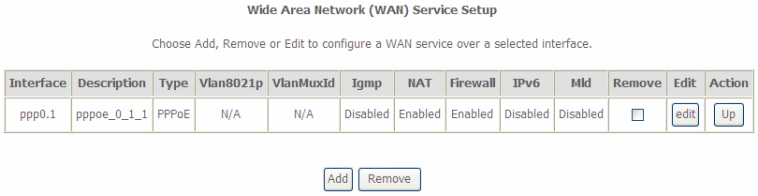
In this page, you can select a ETH port. Click **Apply/Save** to save configuration.

Note:

If ETH Interface is selected, there are two WAN service types (PPPoE and IPoE).

5.2.2 WAN Service

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



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

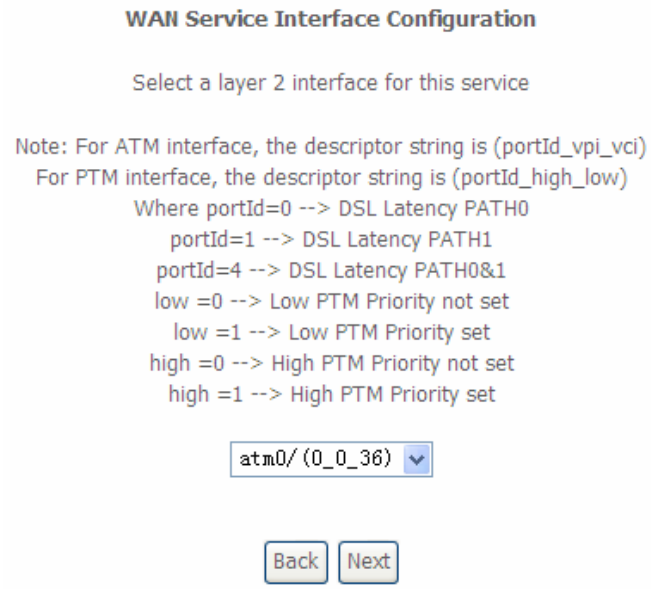
Note:

If PTM Interface is selected, there are three WAN service types: PPP over Ethernet (PPPoE), IP over Ethernet, Bridging. And the corresponding configurations of PTM WAN service are same as the configurations of ATM WAN service.

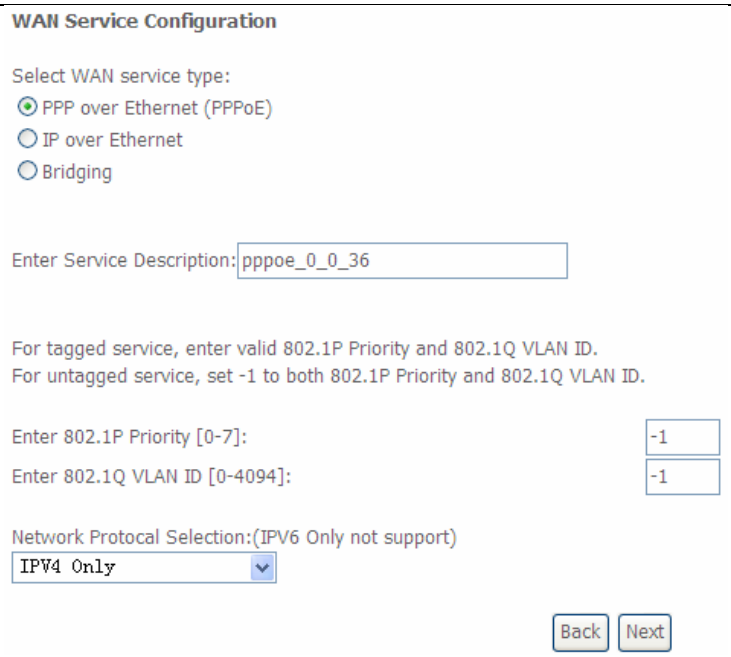
5.2.2.1 Adding a PPPoE WAN Service

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

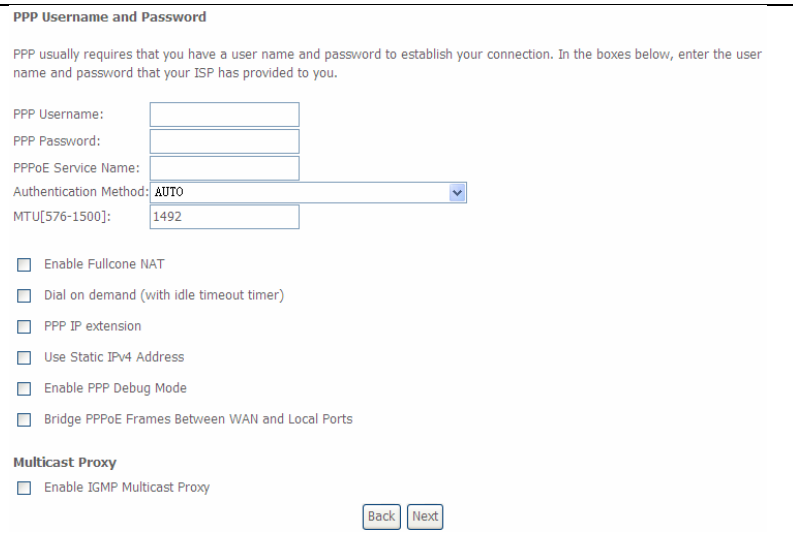
Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM or PTM interface for this WAN service.)



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.



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



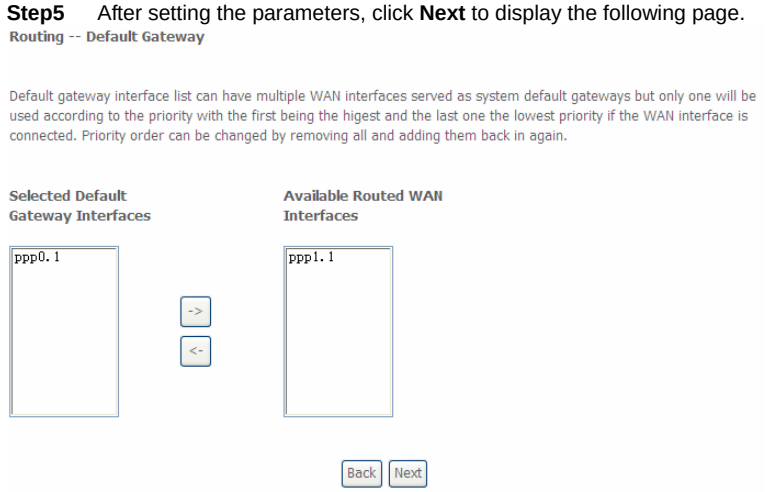
Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **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.



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

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces | Available WAN Interfaces

ppp0.1 | -> <- | ppp1.1

Back Next

Step7 In this page, you can obtain the DNS server addresses from the selected WAN interface. Click **Next**, and the following page appears.

WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

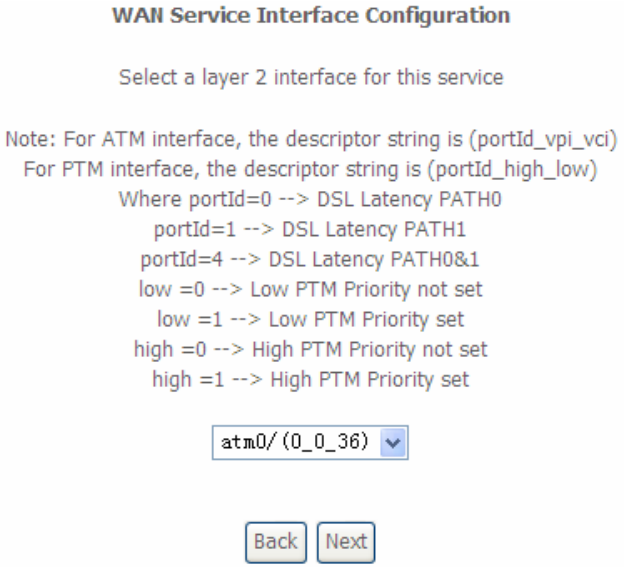
Back Apply/Save

Step8 In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings.

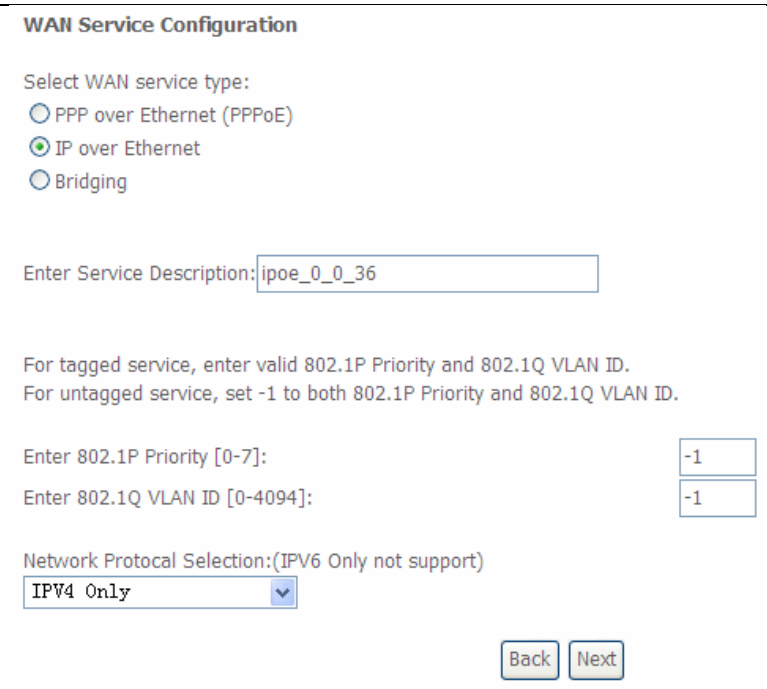
5.2.2.2 Adding a MER (IPoE) WAN service

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

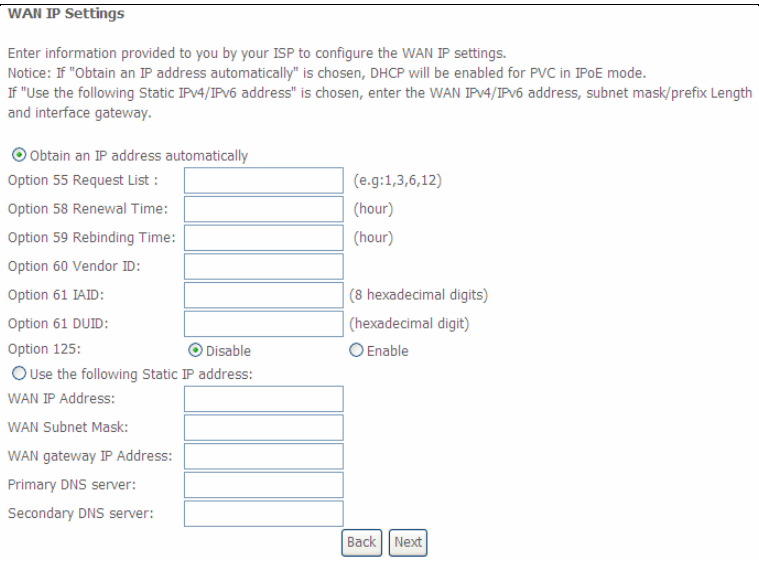
Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM or PTM interface for this WAN service.)



Step2 Select an ATM Interface, and then click **Next** to display the following page.



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



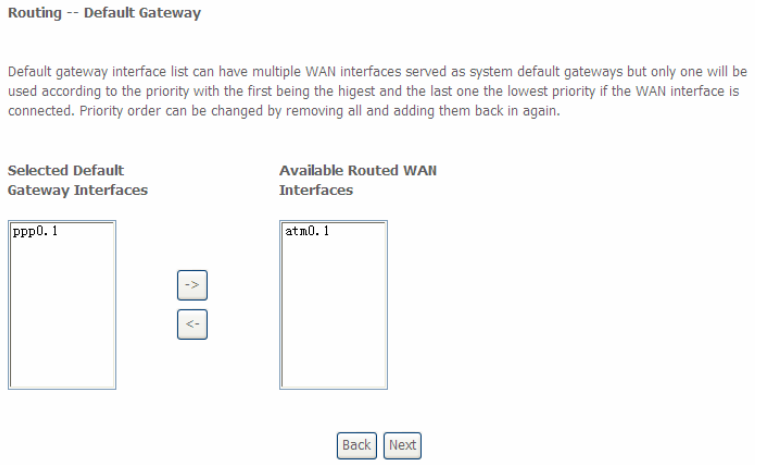
Step4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

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.*

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.



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

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces | Available WAN Interfaces

ppp0.1 | -> <- | atm0.1

Back Next

Step7 In this page, you can obtain the DNS server addresses from the selected WAN interface. 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:	IPoE
NAT:	Disabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

Back Apply/Save

Step8 In this page, it displays the information about the IPoE settngs.Click **Apply/Save** to save and apply the settings.

5.2.2.3 Adding a PPPoA WAN service

This section describes the steps for adding the PPPoA WAN 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.

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: 0 [0-255]

VCI: 37 [32-65535]

Select DSL Latency

☑ Path0 (Fast)

☐ Path1 (Interleaved)

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

○ EoA

◉ PPPoA

○ IPoA

Encapsulation Mode: VC/MUX

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence as the Default Queue

◉ Weighted Round Robin

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

VC WRR Weight: 1 [1-63]

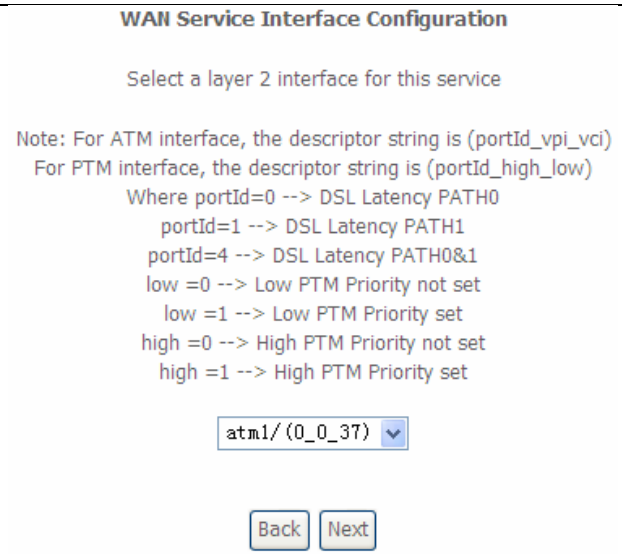
VC Precedence: 8 [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

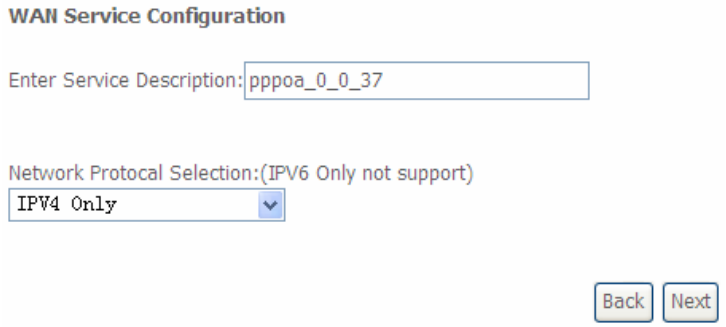
Back Apply/Save

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.

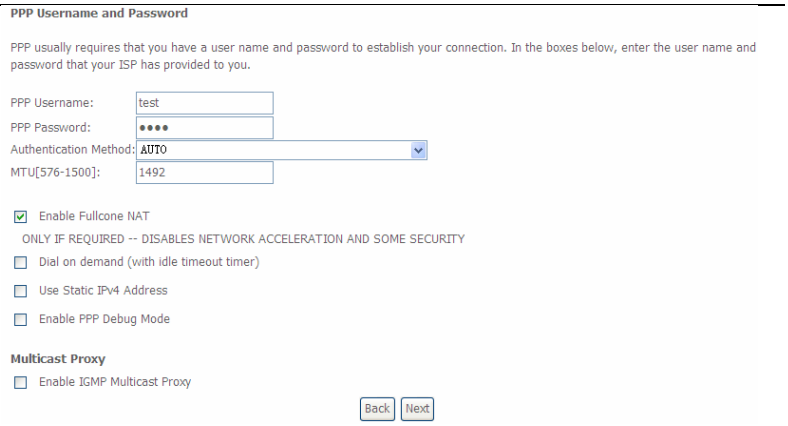
Step3 Choose **WAN Service** and click **Add** to display the following page.



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



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

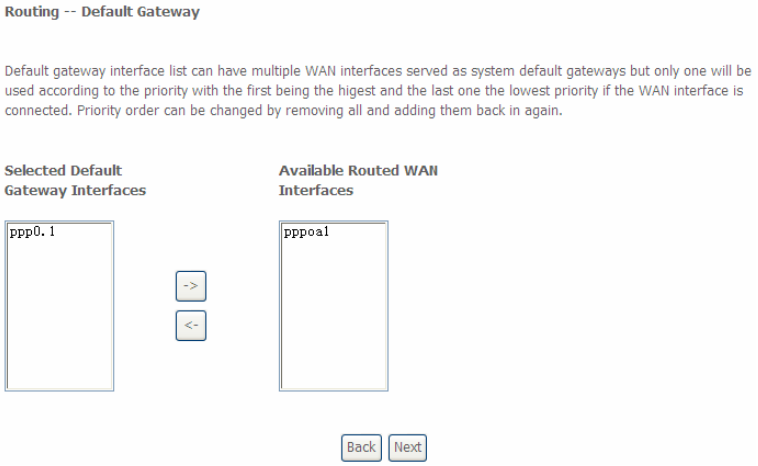


- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:**. NAT is one where all requests from the same 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.
- **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 PPPoA

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.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.

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.



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

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces | Available WAN Interfaces

ppp0.1 | -> <- | pppoa1

Back Next

Step8 In this page, you can obtain the DNS server addresses from the selected WAN interface. 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:	PPPoA
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

Back Apply/Save

Step9 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.

5.2.2.4 Adding an IPoA WAN service

This section describes the steps for adding the IPoA WAN 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 IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: 0 [0-255]

VCI: 38 [32-65535]

Select DSL Latency

☑ Path0 (Fast)

☐ Path1 (Interleaved)

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

○ EoA

○ PPPoA

◉ IPoA

Encapsulation Mode: LLC/SNAP-ROUTING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence as the Default Queue

◉ Weighted Round Robin

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

VC WRR Weight: 1 [1-63]

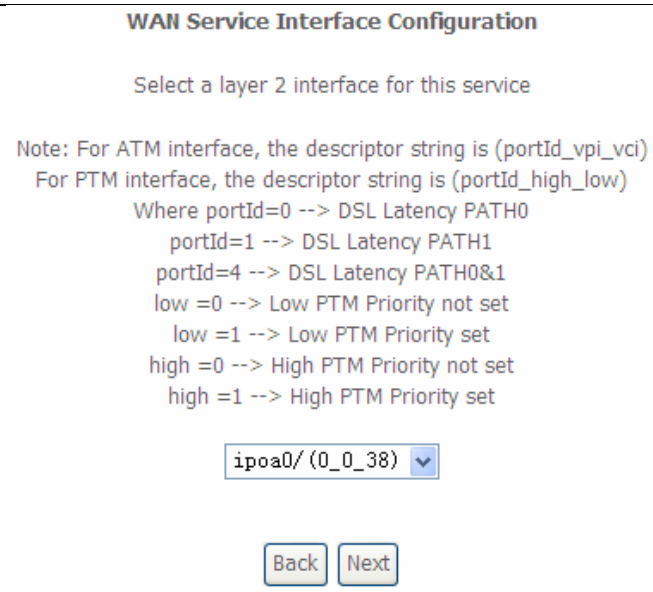
VC Precedence: 8 [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

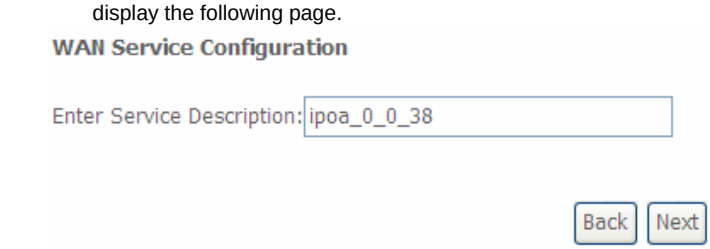
Back Apply/Save

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 save the settings.

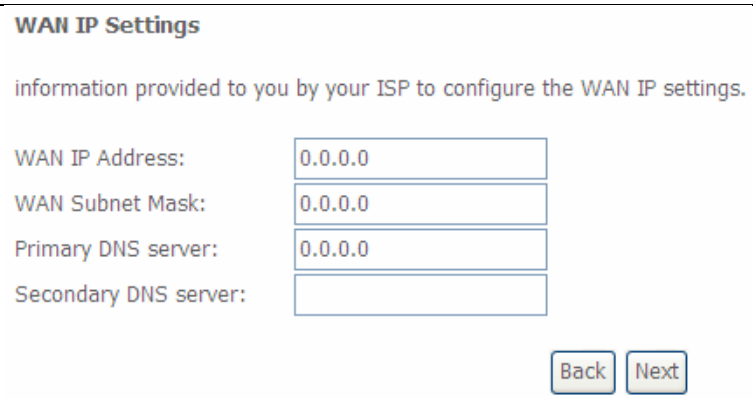
Step3 Choose **WAN Service** and click **Add** to display the following page.



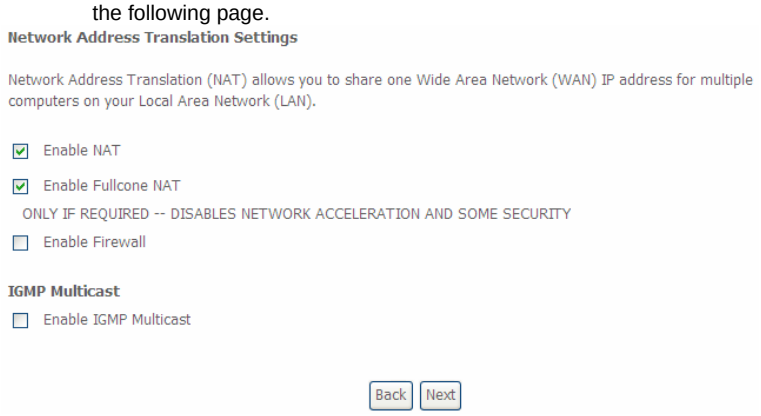
Step4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.



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



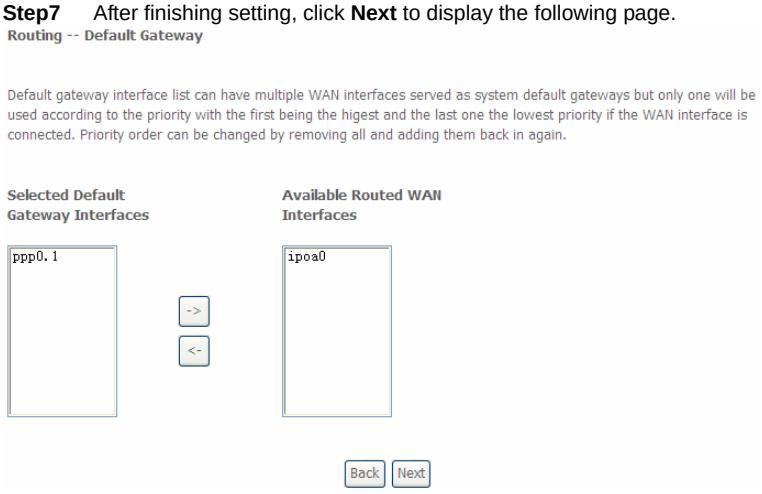
Step6 In this page, enter the WAN IP address, the WAN subnet mask, and primary DNS server provided by your ISP and then click **Next** to display the following page.



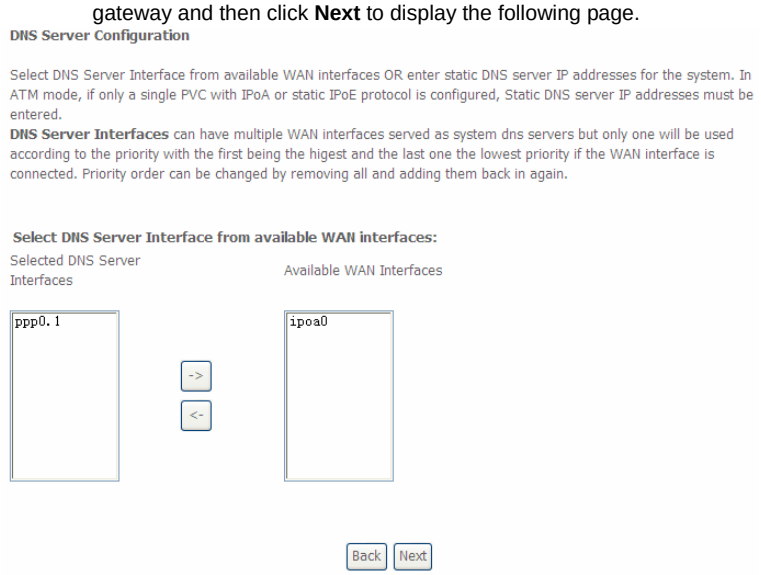
In this page, Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

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.

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



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



Step9 In this page, you can obtain the DNS server addresses from the selected WAN interface. 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:	IPoA
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

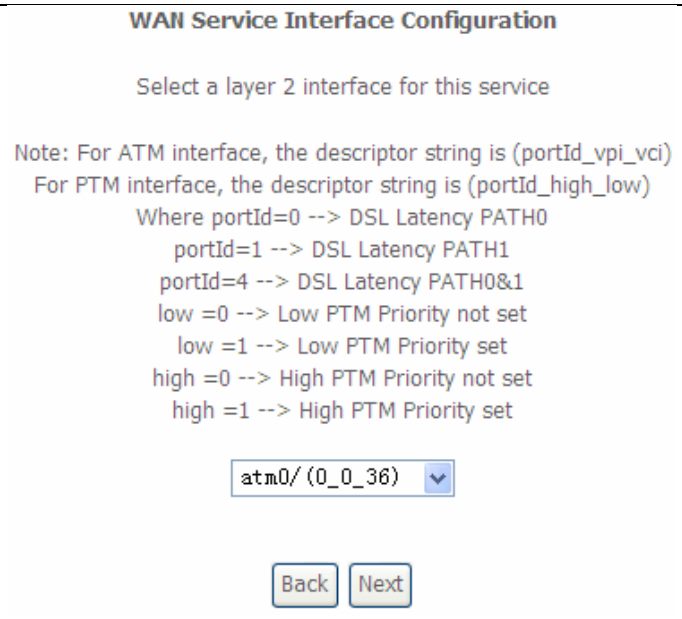
Back Apply/Save

Step10 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.

5.2.2.5 Adding a Bridge WAN service

This section describes the steps for adding the Bridge WAN 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 or PTM interface for this WAN service.) Click the **Add** button to display the following page.



Step2 Select the proper ATM Interface and then click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:

- ○ PPP over Ethernet (PPPoE)
- ○ IP over Ethernet
- ◉ Bridging

Enter Service Description: br_0_0_36

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Back Next

Step3 In this page, you can select the WAN service type, and modify the service description for this service. 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:	Enabled
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

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

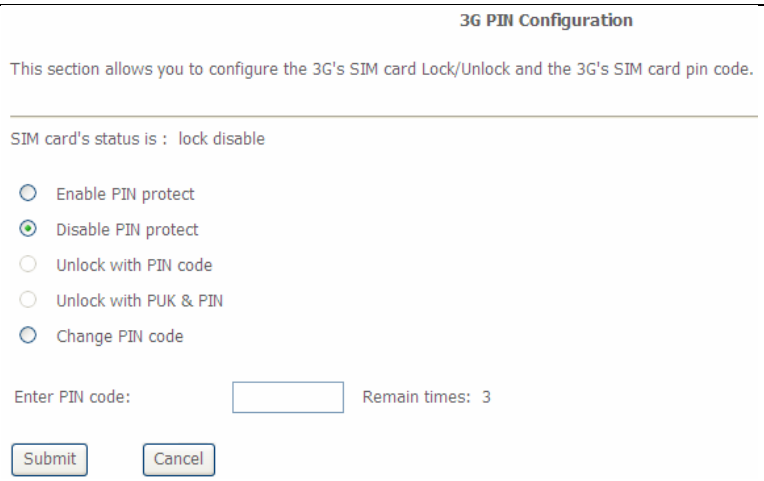
5.2.3 3G WAN Service

Choose **Advanced Setup > 3G WAN Service** , and the following page appears.

This page is used to configure 3G connection. If you want to access the Internet through 3G connection, a 3G network card is required. Connect the 3G network card to the USB interface of the Router.

- **Information**: Click it to display the information of the 3G network card.
- **Pin Manage**: Click it to configure the 3G PIN.
- **Upload Driver**: For a un-support USB dongle, click it to upload the new driver for supporting the USB. The driver is a text file.

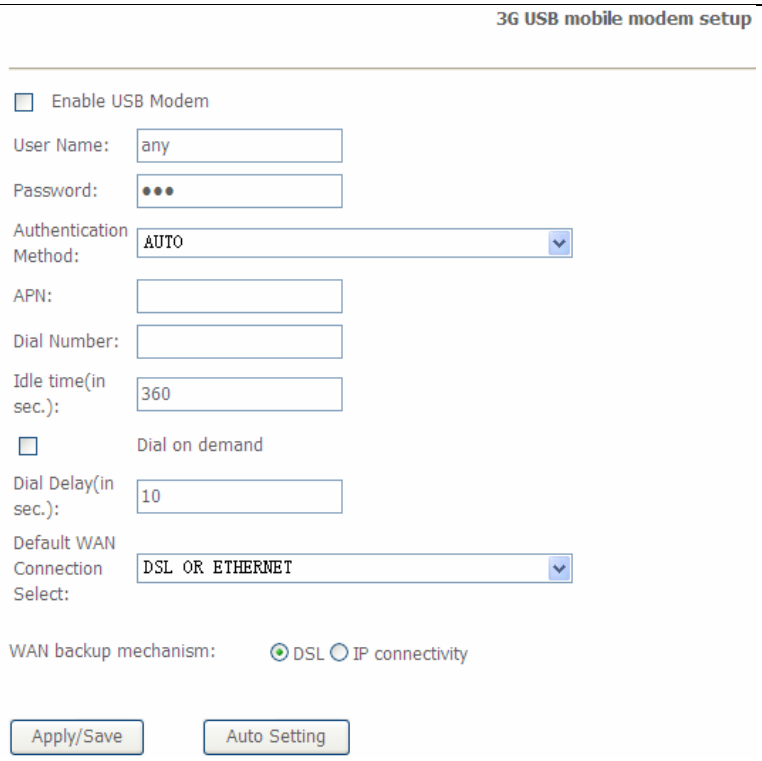
Click **Pin Manage,** and the following page appears.



- **Enable PIN protect**: If you enable it, you need to enter the PIN code when rebooting or inserting the card to the USB interface.
- **Unlock with PIN code**: If you disable it, you need to enter PIN code when using 3G.
- **Unlock with PUK & PIN**: If you disable it, you need to enter PUK code when failing to enter the PIN code for 3 times.
- **Change PIN code**: Choose it to change the PIN code.

After proper settings, click **Submit** to take the settings in to effect.

Click **Add** in the **WAN Service For 3G Moblie Setup** to display the following page.



In this page, you are allowed to configure the settings of the 3G USB modem.

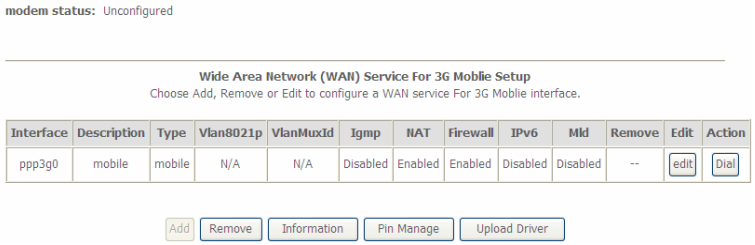
- **Enable USB Modem:** If you want to access the Internet through the 3G network card, you must enable the USB modem.
- **User Name:** Username provided by your 3G ISP.
- **Password:** Password provided by your 3G ISP.
- **Authentication Method:** Select a proper authentication method in the drop-down list. You can select Auto, PAP, CHAP, or MSCHAP.
- **APN:** APN (Access Point Name) is used to identify the service type. Enter the APN provided by your 3G ISP.
- **Dial Number:** Enter the dial number provided by your 3G ISP.

- **Idle time (in sec.):** If no traffic for the preset time, the 3G will disconnect automatically.
- **Net Select:** Select the 3G network that is available.You may select EVDO, WCDMA, CDMA2000, TD-SCDMA, GSM, or Auto.
- **Dial on demand**: Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the 3G connection. Once it detects the flow (like access to a webpage), the modem restarts the 3G dialup.
- **Dail Delay (in sec.)**: The 3G delays dial after the DSL is disconnected.
- **Default WAN Connection Select**: You can select DSL or 3G from the drop-down list.
- **WAN back mechanism**: The 3G connection is backup for the DSL connection.
  - **DSL**: If the DSL is disconnected, the 3G starts to dial.
  - **IP connectivity**: If the system fails to ping the specified IP address, the 3G starts to dial.

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

You may also click the **auto setting** button to automatically configure the 3G connection.

After clicking the **Apply/Save** button, the following page appears.



If the 3G network card is installed, you may click the button on the **Action** column to establish or disconnect the 3G connection.

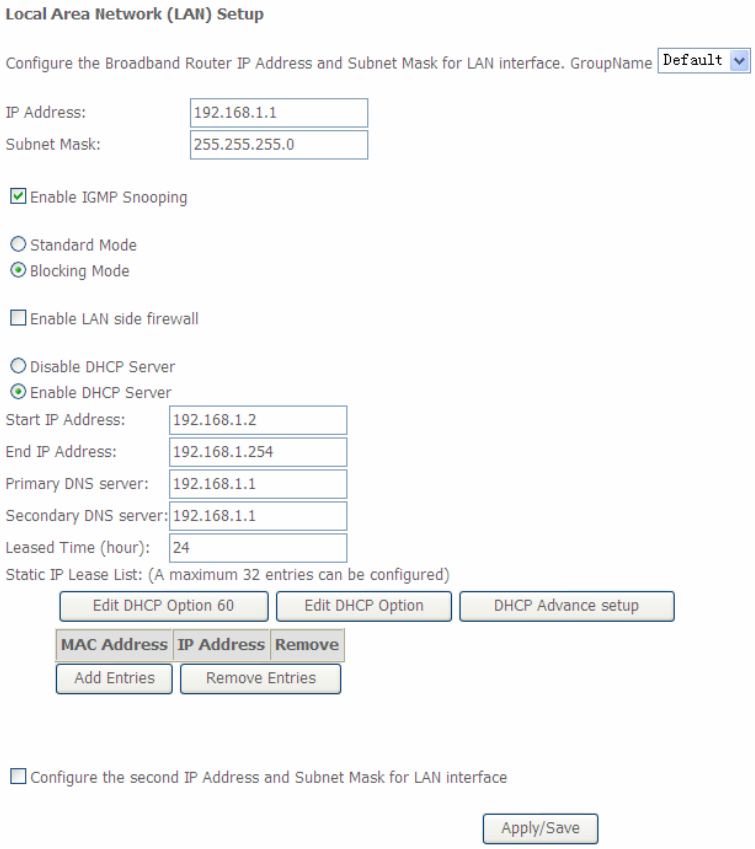
Note:

When there is no DSL WAN connection, insert the 3G network card, and then system will perform dial-up automatically. If the DSL WAN connection and the 3G connection coexist, the DSL WAN connection takes priority over the 3G

connection. When the DSL WAN connection starts to perform dial-up, the 3G connection will be disconnected. If the DSL WAN connection has established, you may manually to perform 3G dial-up, and then the DSL WAN connection will be disconnected.

5.2.4 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

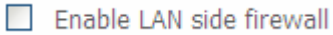
In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1.

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.

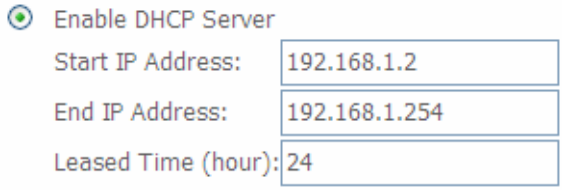
Enabling the LAN Side Firewall

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.

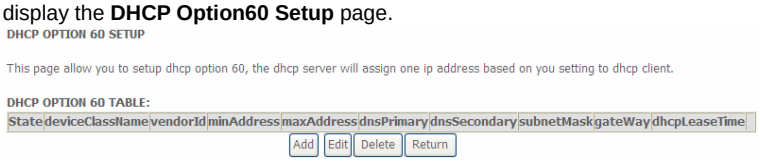
Configuring the DHCP Server



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 Option60

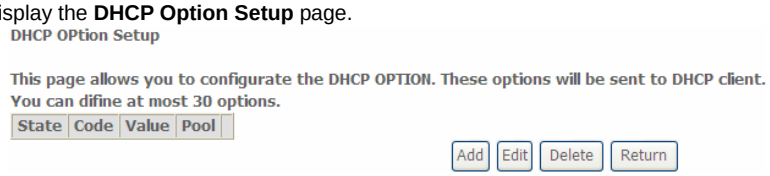
Click the **Edit DHCP Option60** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option60 Setup** page.



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

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.

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.

DHCP Advance Setup

This page allows you to enable or disable dhcp for every lan interface.
You must enable **lan ports**.

State	Interface
☑	eth0
☑	eth1
☑	eth2
☑	eth3
☑	eth4
☑	wl0
☑	wl0.1
☑	wl0.2
☑	wl0.3

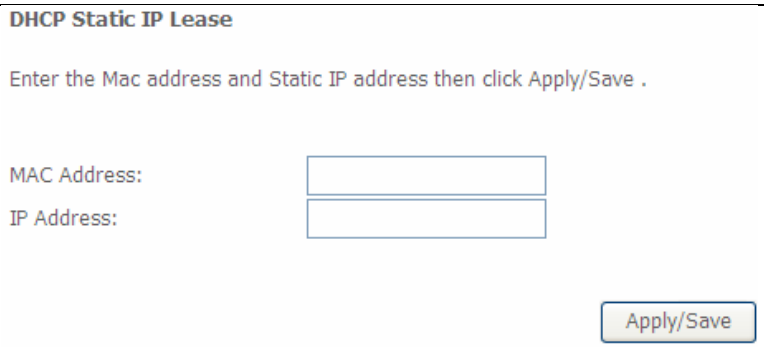
Configuring the DHCP Static IP Lease List

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.

MAC Address	IP Address	Remove

Add Entries Remove Entries

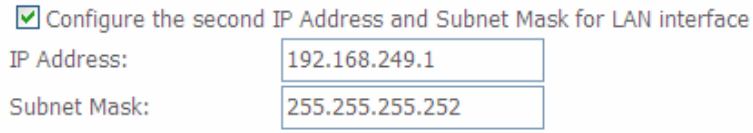
Click the **Add Entries** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Static IP Lease** page.



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

5.2.4.1 IPv6 Auto-configuration

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

IPv6 LAN Auto Configuration

Note:

1: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".

2: Unique local address must start with "fd". The prefix and the address must be in same network.

☐ **Enable Unique Local Addresses And Prefix Advertisement**

○ Randomly Generate

○ Statically Configure

Address: (e.g: fd80::1/64)

Prefix: (e.g: fd80::/64)

Preferred Life Time (hour):

Valid Life Time (hour):

IPv6 LAN Applications

☑ Enable DHCPv6 Server and RADVD

◉ Stateless

○ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour): 24

☑ Enable MLD Snooping

○ Standard Mode

◉ Blocking Mode

Save/Apply

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.

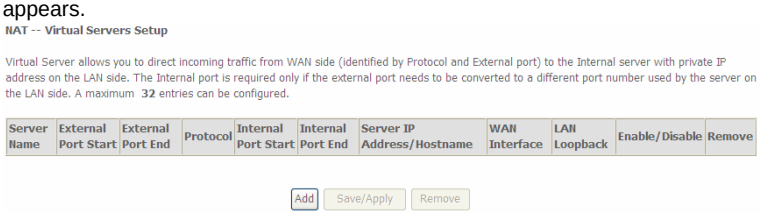
After finishing setting, click the **Save/Apply** button to apply the settings.

5.2.5 NAT

5.2.5.1 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.

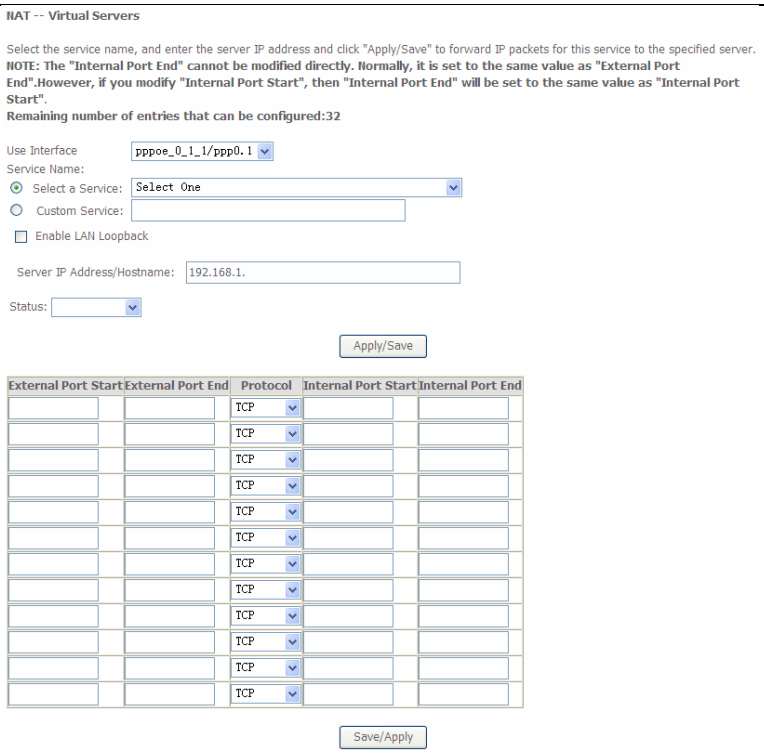
Choose **Advanced Setup > NAT > Virtual Servers**, and the following page appears.



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

5.2.5.2 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.

NAT -- Port Triggering Setup

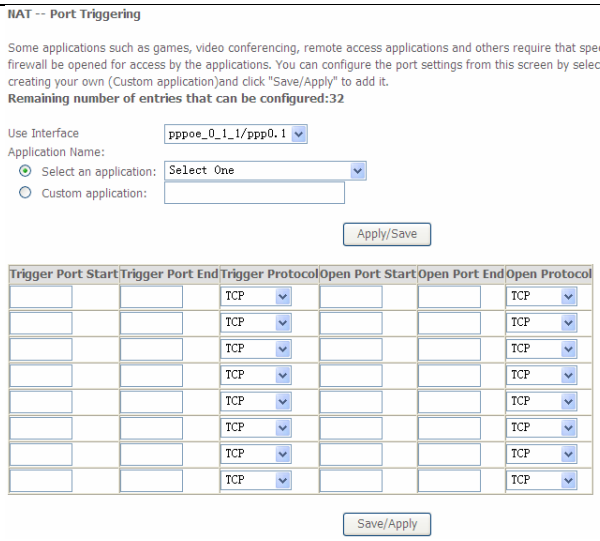
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum **32** entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Add Remove

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

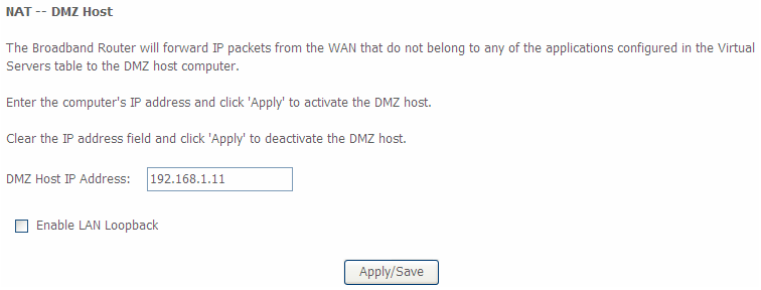
Note:

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.

5.2.5.3 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.

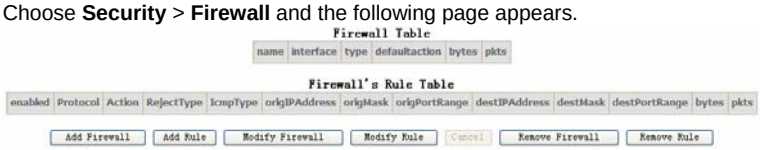
After finishing the settings, click the **Apply/Save** button to apply the settings.

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.

5.2.6 Security

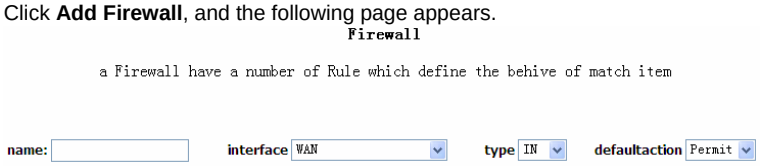
Firewall

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



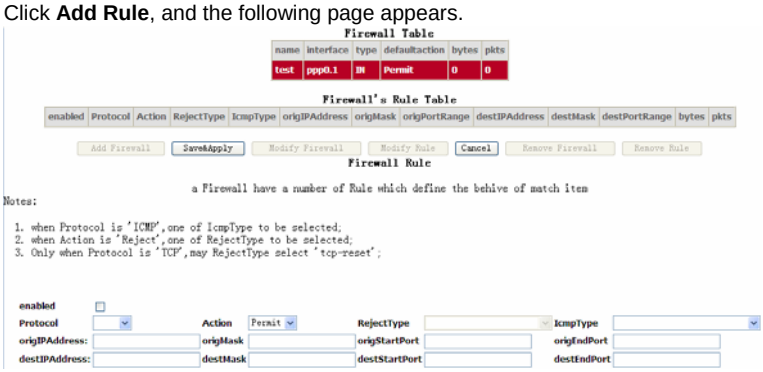
Click **Modify Firewall** or **Remove Firewall** to modify or remove the firewall. And click **Modify Rule** or **Remove Rule** to modify or remove the rule.

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



- **name**: The name of firewall.
- **interface**: You can select **LAN** or **WAN** from the drop-down list.
- **type**: You can select **IN** or **OUT** from the drop-down list.
- **defaultaction**: You can select **Permit** or **Drop** from the drop-down list.

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



- **enabled**: Select the check box to enable the firewall rule.
- **Protocol**: You can select **UDP**, **TCP**, or **ICMP** from the drop-down list.
- **Action**: You can select **Permit**, **Drop**, or **Reject** from the drop-down list.
- **RejectType**: You can select the reject type, when you select **Reject** as the action.
- **IcmpType**: You can select the type of ICMP packet, when you select ICMP as the protocol.
- **origIPAddress**: The original IP address.
- **origMask**: The original subnet mask.
- **origStartPort**: The original start port.
- **origEndPort**: The original end port.

- **destIPAddress**: The destination IP address.
- **destMask**: The destination subnet mask.
- **destStartPort**: The destination start port.
- **destEndPort**: The destination end port.

After finishing setting, click **Save&Apply** to save and activate the rule.

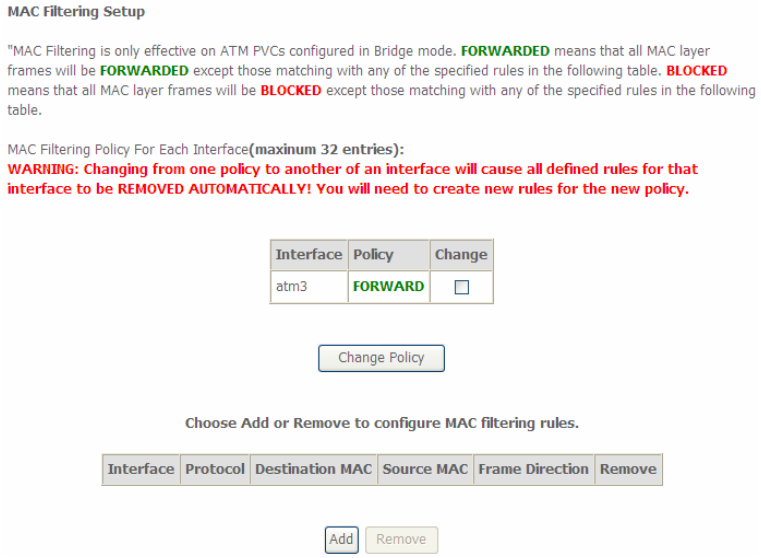
MAC Filtering Setup

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:

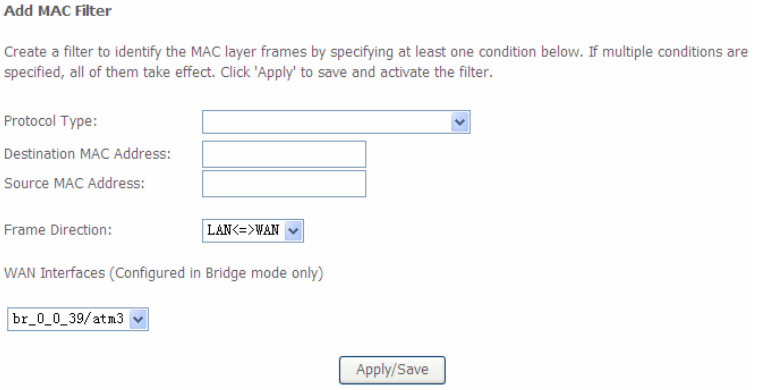
MAC filtering is only effective on ATM PVCs configured in bridge mode.

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.



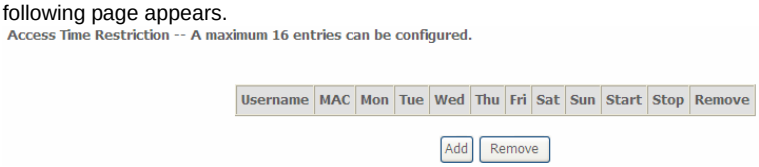
- **Protocol Type**: Select the proper protocol type.
- **Destination MAC Address**: Enter the destination MAC address.
- **Source MAC Address**: Enter the source MAC address.
- **Frame Direction**: The direction of transmission frame.
- **WAN Interface (Configured in bridge mode only)**: Select the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

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

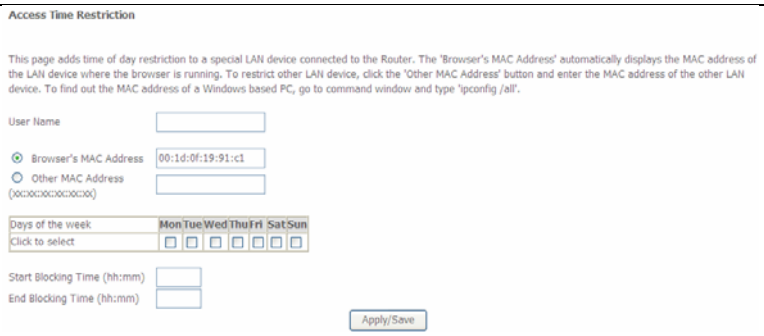
5.2.7 Parental Control

Time Restriction

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



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

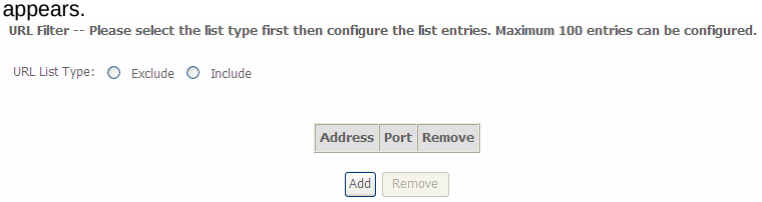


This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, se the user name and configure the time settings.

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

Url Filter

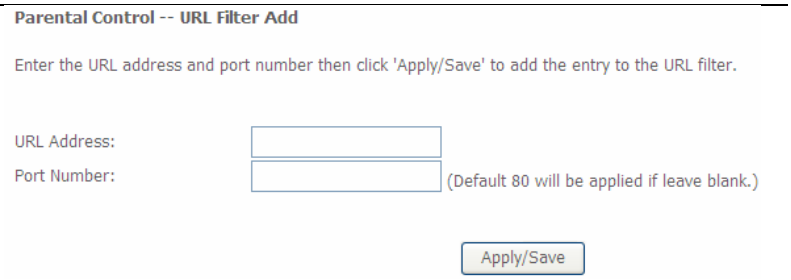
Click **Advanced Setup** > **Parental Contr**ol > **Url Filter**, and the following page appears.



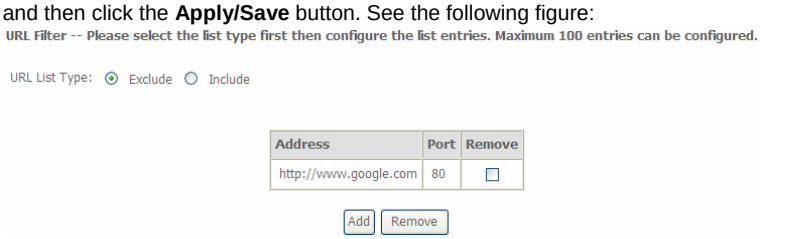
Thisp age is used to prevent the LAN users from accessing some Websites in the WAN.

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 the URLs in the list.

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



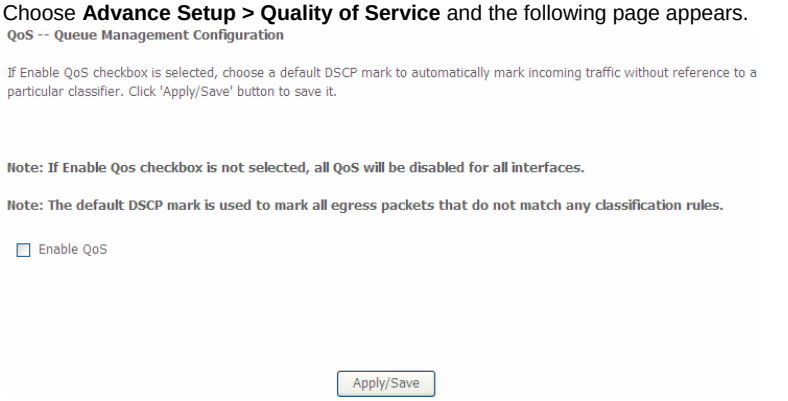
In this page, enter the URL address and its corresponding port number. For example, enter the URL address ***http://www.google.com*** and the port number **80**, and then click the **Apply/Save** button. See the following figure:



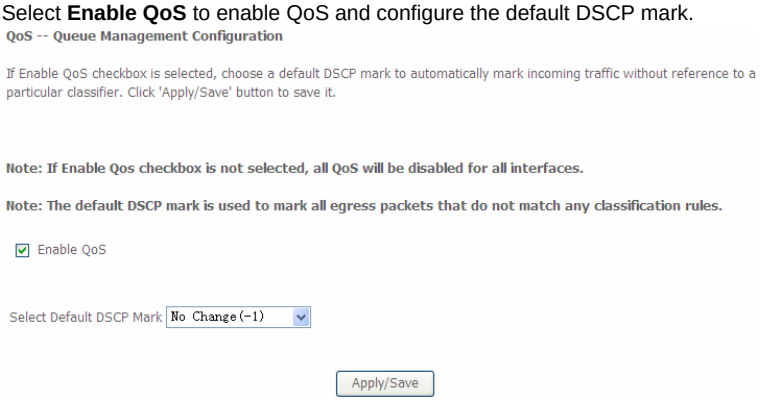
5.2.8 Quality of Service

Enabling QoS

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 finishing 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 Configuration

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

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 3 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate (bits/s)	Burst Size (bytes)	Enable	Remove
WMM Voice Priority	1	wl0	0	1/SP					Enabled	
WMM Voice Priority	2	wl0	0	2/SP					Enabled	
WMM Video Priority	3	wl0	0	3/SP					Enabled	
WMM Video Priority	4	wl0	0	4/SP					Enabled	
WMM Best Effort	5	wl0	0	5/SP					Enabled	
WMM Background	6	wl0	0	6/SP					Enabled	
WMM Background	7	wl0	0	7/SP					Enabled	
WMM Best Effort	8	wl0	0	8/SP					Enabled	
Default Queue	34	ptm0	1	8/WRR/1	Path0	Low			☐	

Add Enable Remove

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

Note:

The lower integer value for precedence indicates the higher priority.

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

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: Disable

Interface:

Apply/Save

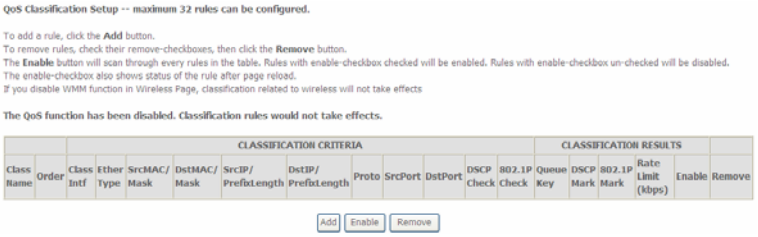
- **Name:** Enter the name of QoS queue.

- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

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

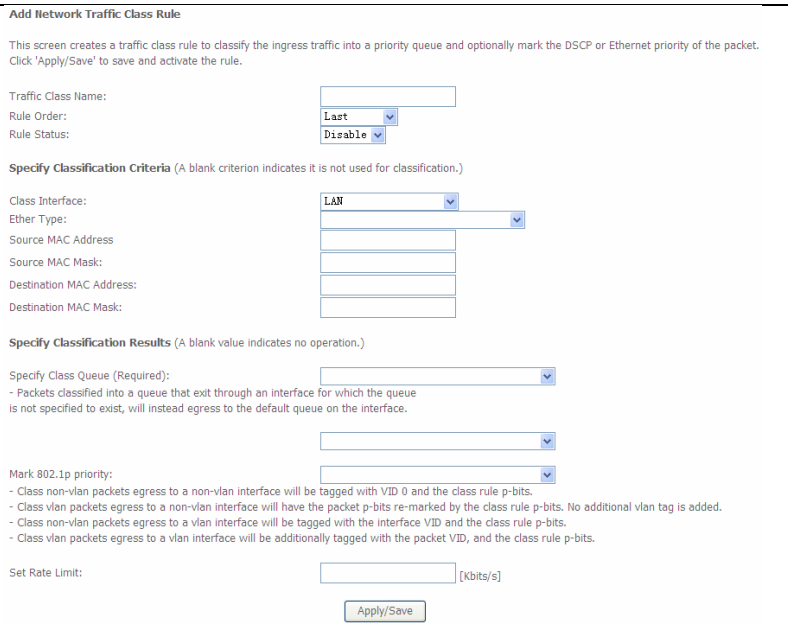
QoS Classification

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.

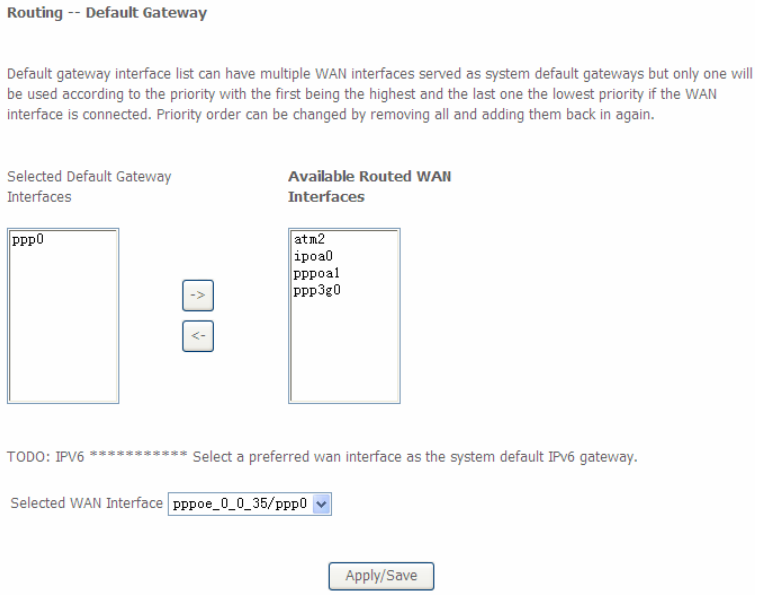
Click the **Add** button to display the following page.



5.2.9 Routing

Default Gateway

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



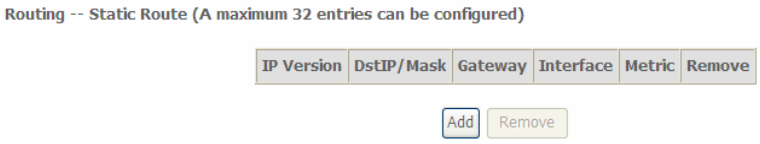
In this page, you can modify the default gateway settings.

Select a proper WAN interface in the drop-down list of **Selected WAN Interface** as the system default gateway.

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

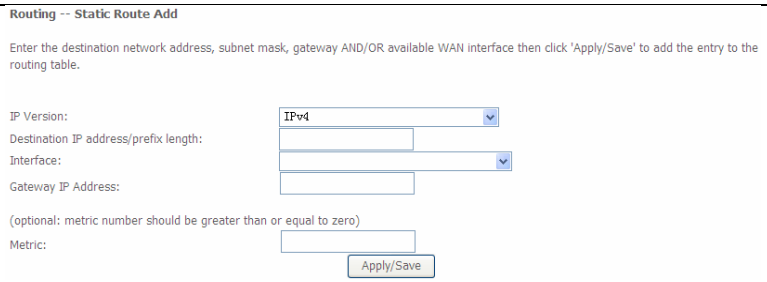
Static Route

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.

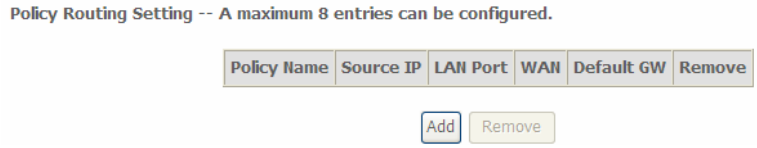


- **IP Version:** Select the IP version.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

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

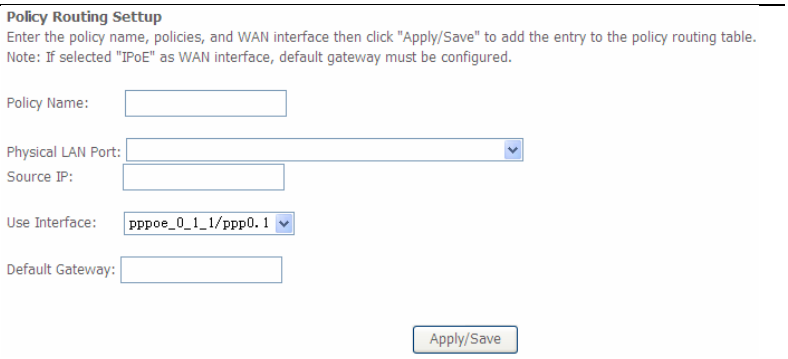
Policy Routing

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.

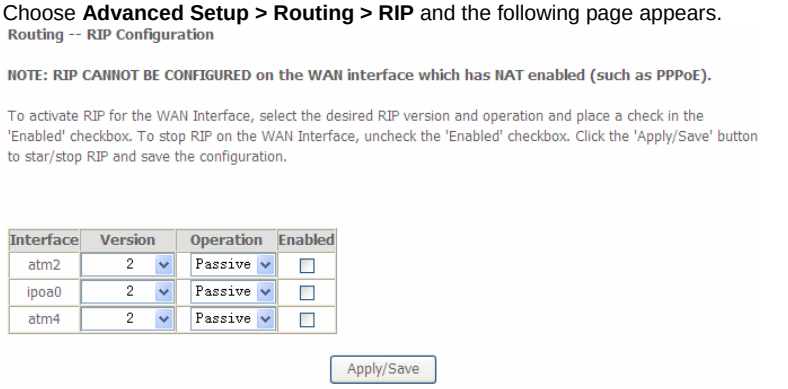


In this page, enter the policy name, source IP and default gateway, and select the physical LAN port and interface.

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

RIP

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



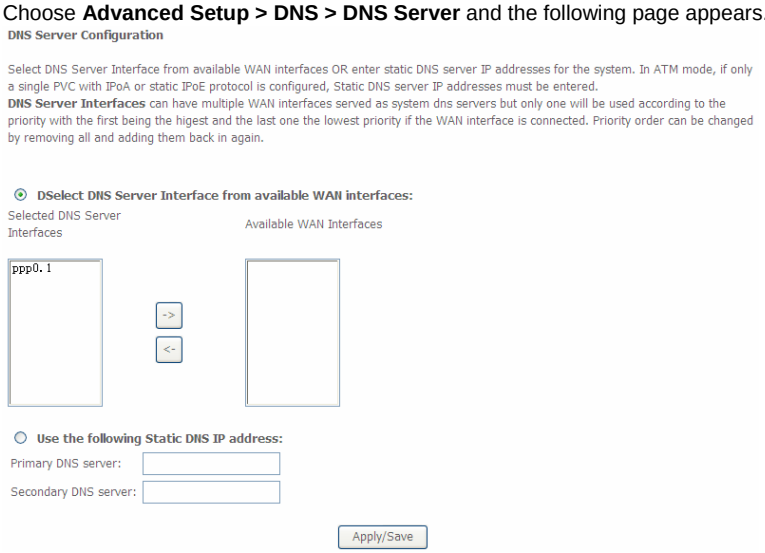
In this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

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

5.2.10 DNS

DNS Server

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



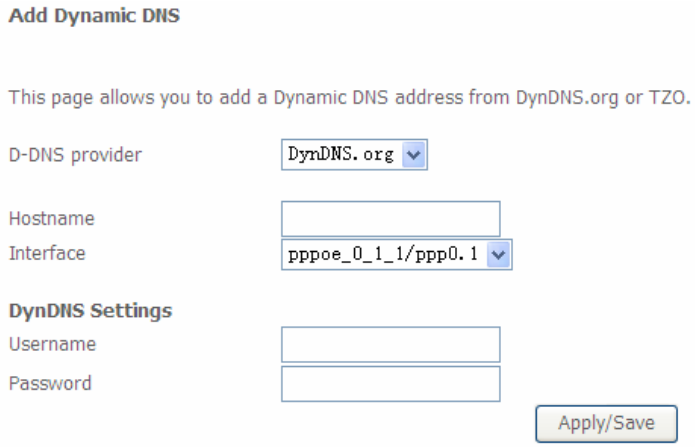
In this page, you can select a DNS server interface from the available interfaces, manually enter the DNS server addresses, or obtain the DNS address from a WAN interface.

After finishing 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.

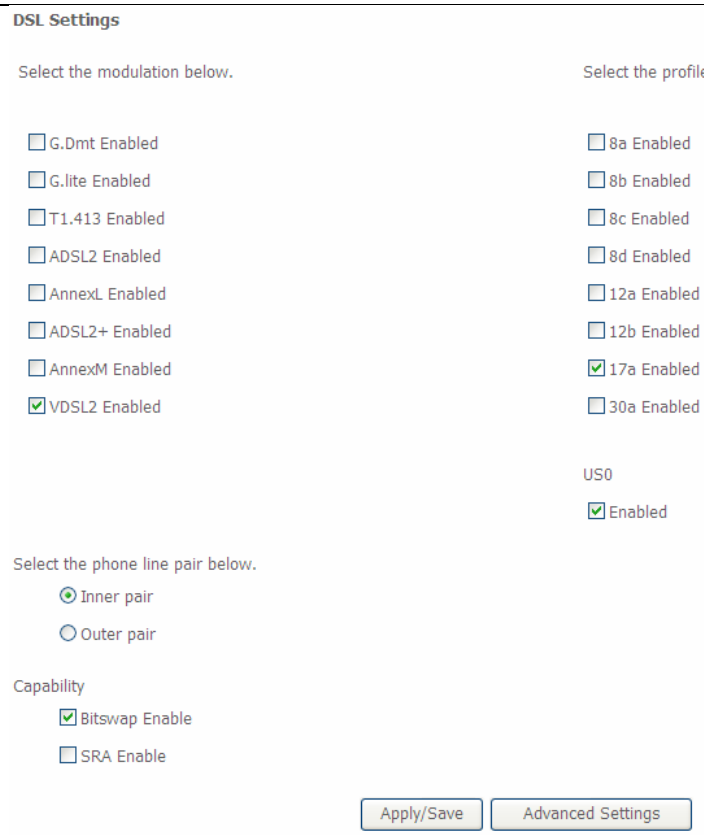


- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the DSL router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:**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

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

5.2.11 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. If you select **VDSL2 Enabled** check box, you can set the VDSL2 parameters on the right area.

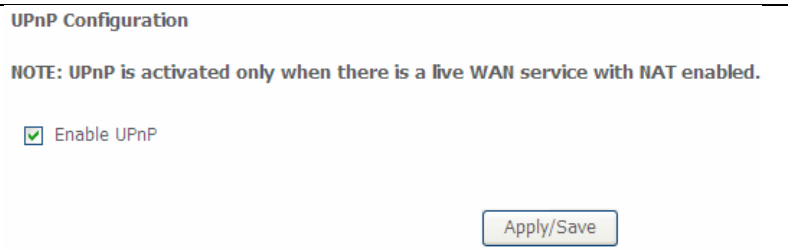


In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

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

5.2.12 UPnP

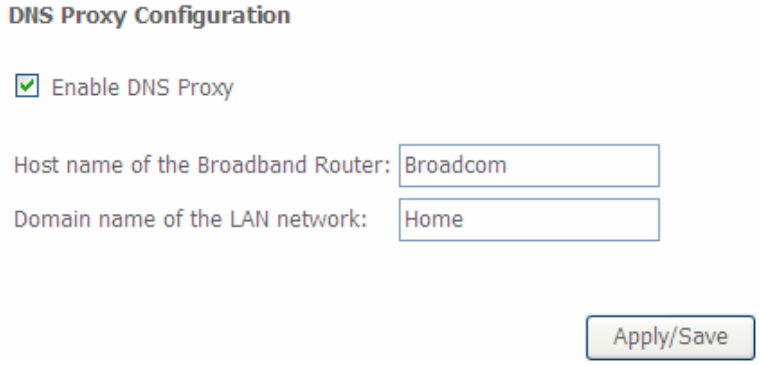
Choose **Advanced Setup > UPnP** and the following page appears.



In this page, you can enable or disable the UPnP function.
After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.13 DNS Proxy

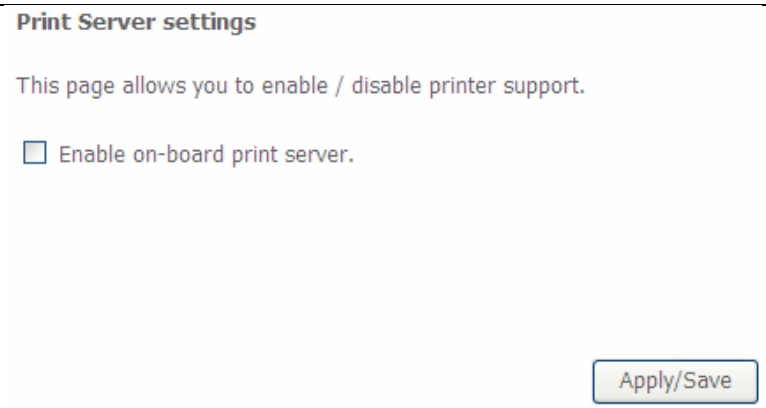
Choose **Advanced Setup > DNS Proxy** and the following page appears.



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.

5.2.14 Print Server

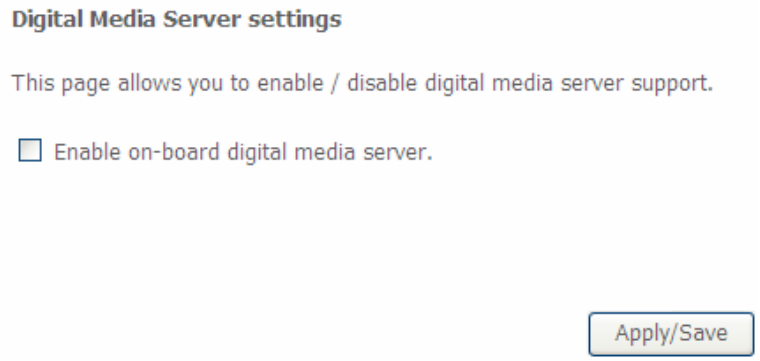
Choose **Advanced Setup > Printer Server** and the following page appears.



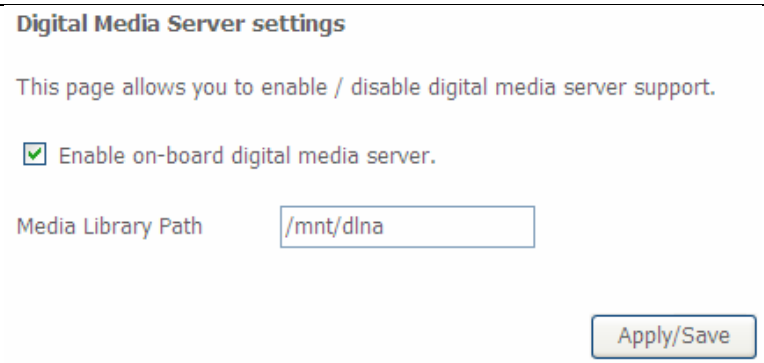
In this page, you can enable or disable the printer server.
After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.15 DLNA

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

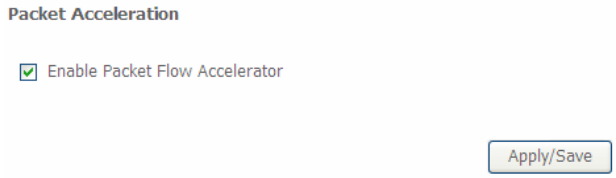


In this page, select the **Enable on-board digital media server** check box, and the following page appears. In this page, enter the media library path to run digital media server.



5.2.16 Packet Acceleration

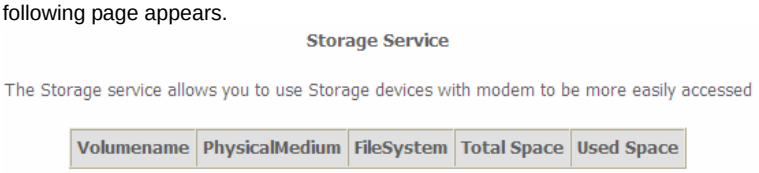
Choose **Advanced Setup > Packet Acceleration** and the following page appears. In this page, you can enable packet flow accelerator.



5.2.17 Storage Service

Storage Device Info

Choose **Advanced Setup** > **Storage Service** > **Storage Device Info** and the following page appears.



This page is used to display the information of the storage device that connects to the DSL router.

5.2.18 Interface Grouping

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

Interface Grouping -- A maximum 16 entries can be configured

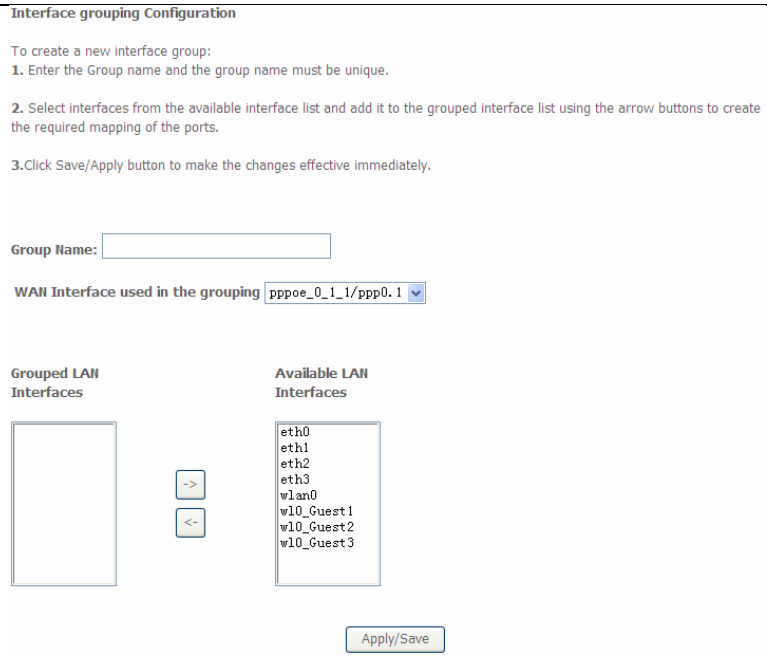
Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped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

Group Name	Remove	WAN Interface	LAN Interfaces
Default		ppp0.1	eth0
			eth1
			eth2
			eth3
			wlan0
			wl0_Guest1
			wl0_Guest2
			wl0_Guest3

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.



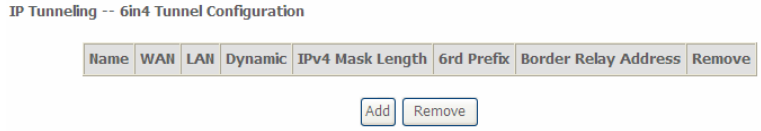
In this page, please follow the on-screen configuration steps to configure the parameters of the interface grouping.

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

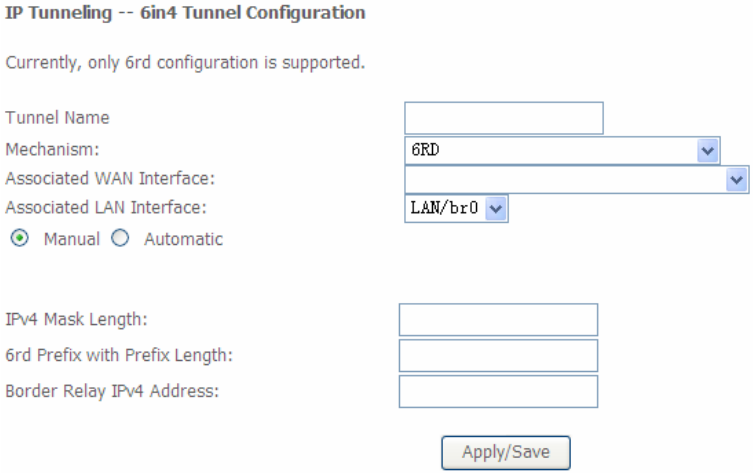
5.2.19 IP Tunnel

5.2.19.1 IPv6 in IPv4

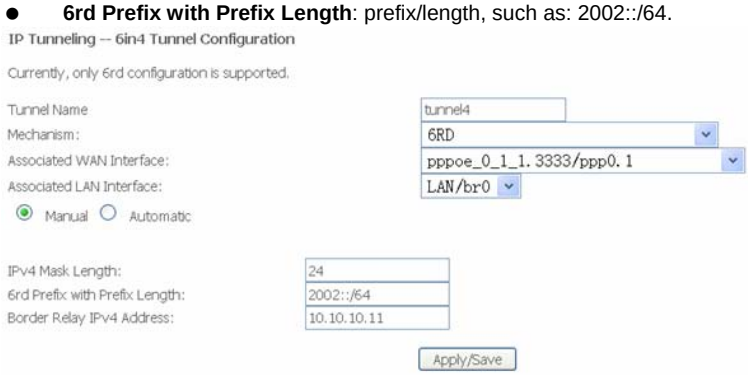
Choose **Advanced Setup > IP Tunnel** > **IPv6inIPv4** and the following page appears. The default value is IPv6 in IPv4 information.



Click **Add** and the following page appears. In this page, you can add a new tunnel.



- **IPv4 Mask Length**: The value is 0 ~ 32.
- **6rd Prefix with Prefix Length**: prefix/length, such as: 2002::/64.



After proper settings, click **Apply/Save** and the following page appears.

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
tunnel4	ppp0.1	br0	Static	24	2002::/64	10.10.10.11	☐

Remove

5.2.19.2 IPv4 in IPv6

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

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote IPv6 Address	Remove

Add Remove

Click **Add** and the following page appears. In this page, you can add a new tunnel of IPv4 in IPv6.

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name
Mechanism: DS-Lite
Associated WAN Interface:
Associated LAN Interface: LAN/br0
Manual Automatic

Remote IPv6 Address:

Apply/Save

5.2.20 IPSec

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

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
111	10.10.10.10	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	☐
222	20.20.20.20	192.168.1.2	192.168.3.0/255.255.255.0	☐
333	30.30.30.30	192.168.1.0/255.255.255.0	192.168.6.1	☐

Add Remove

In this page, you can add or remove the IPSec tunnel connections.
Click the **Add** button to display the following page.

IPSec Settings

IPSec Connection Name	new connection
Tunnel Mode	ESP
Remote IPSec Gateway Address (IPv4 address in dotted decimal)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

Apply/Save

In this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

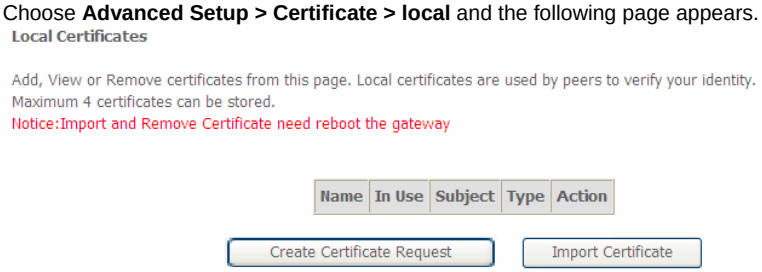
If you need to configure the advanced settings of this IPSec tunnel connection, please click the **Show Advanced Settings** button to display the other parameters.

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

5.2.21 Certificate

Local

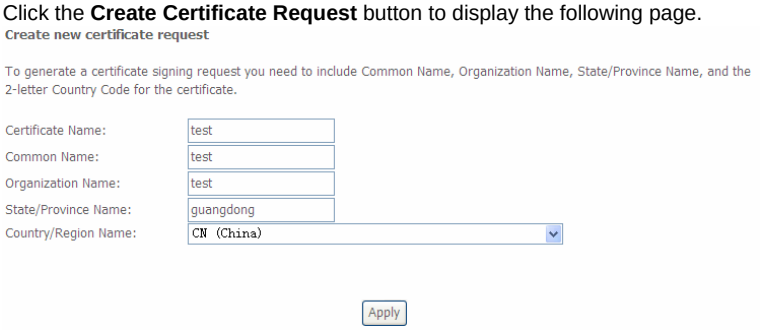
Choose **Advanced Setup > Certificate > local** and the following page appears.



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

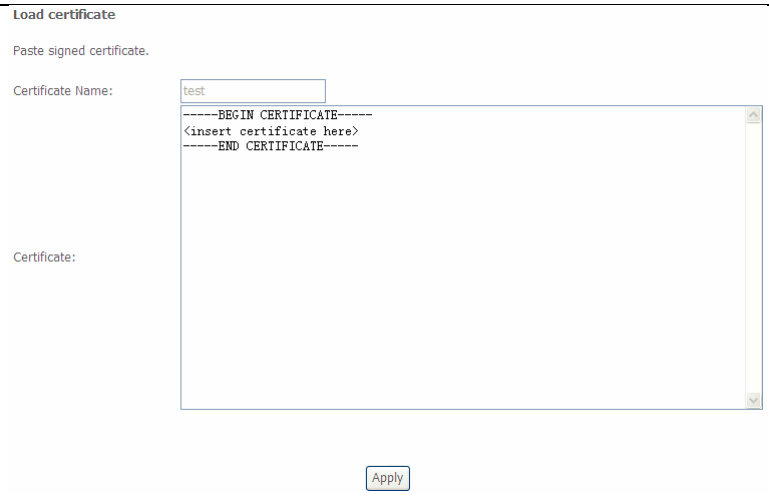
Certificate signing request

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

Name	test
Type	request
Subject	CN=test/O=test/ST=guangdong/C=CN
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBfjCB6AIBADA/MQ0wCwYDVQQDEwR0ZXN0MQ0wCwYDVQQKEwR0ZXN0MRIwEAYD VQQIEwlndWFuZ2RvbmcxCzAJBgNVBAYTAkN0MIGfMA0GCSqGSIb3DQEBAQUAA4GN ADCBiQKBgQClNyqBx3gtIp16ufx+Rh00WH2Q67+fy36IUhbSEG1kNkdEMhaUN0b4 isL66+xXP+Gu+gEs+pgQ4aAoXjvY4k0ZskhKJTD6r4lzvIhnTfb4nNKz0H+nQkUT 1RGjAGDTefaXSRemVshjF7CZtovHHICu5/XhDKfFGvrtP7tKnUidNwIDAQABoAAw DQYJKoZIhvcNAQEEBQADgYEAL9VxsVI2XLDPYNxAlE6QiiSVRQg2Z/GiirG7BZ+6 bK2VleuqO1GFQvkzrNEqAO4DcAb+qkI2JBp6KqotucVYRHfvHf//naGM5lpxH8wN YLw9+2L+DYCaSN6P4b3Gfa6qvfo6xqiRmqA31XvFW1uIldhw9VaUbsl3jDZj7x0f QFk= -----END CERTIFICATE REQUEST-----

Back | Load Signed Certificate

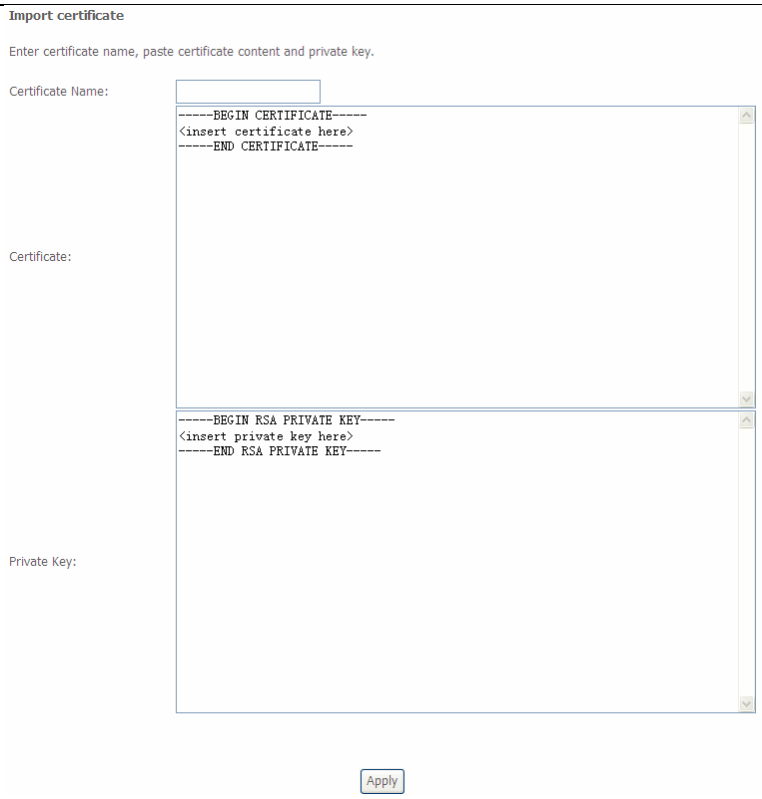
The certificate request needs to be submitted to a certificate authority, which will sign the request. Then the signed certificate needs to be loaded to the DSL router. Click **Load Signed Certificate** in this page, and the following page appears.



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

- **Importing an Existing Local Certificate**

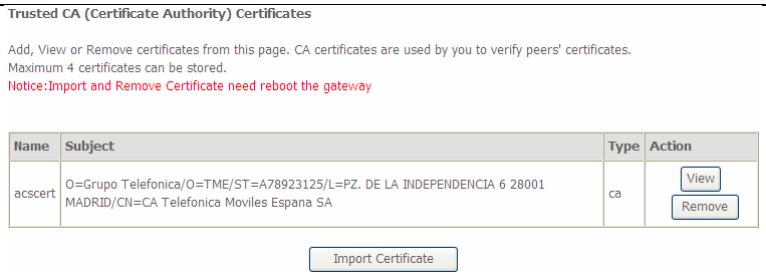
To import an existing certificate, click the **Import Certificate** button to display the following page.



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.



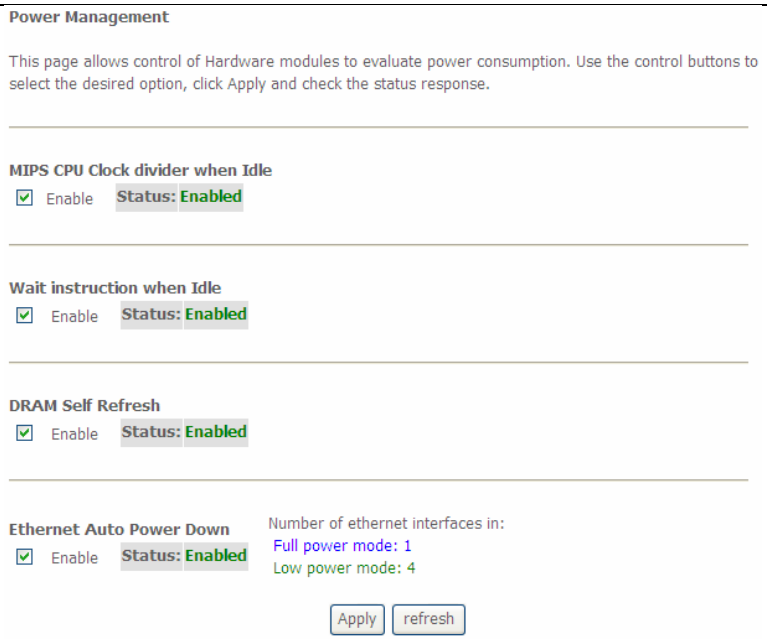
In this page, you may import or remove a CA certificate.

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.

5.2.22 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.

5.2.23 Multicast

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

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Data Sources (for IGMPv3):	10
Fast Leave Enable:	☑
Mebership Join Immediate (IPTV):	☐

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

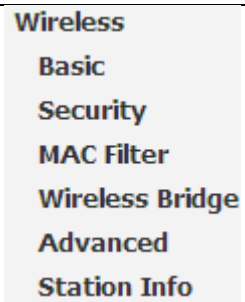
Default Version:	2
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Data Sources (for mldv2):	10
Fast Leave Enable:	☑

Apply/Save

In this page, you can configure the multicast parameters.
After finishing setting, click **Apply/Save** to save and apply the settings.

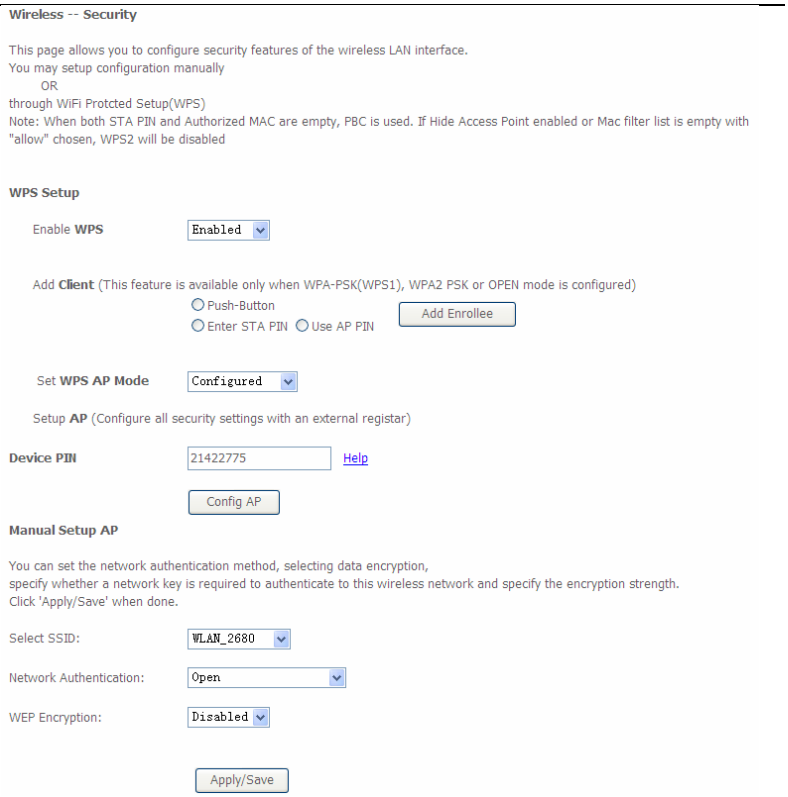
5.3 Wireless

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



5.3.1 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:

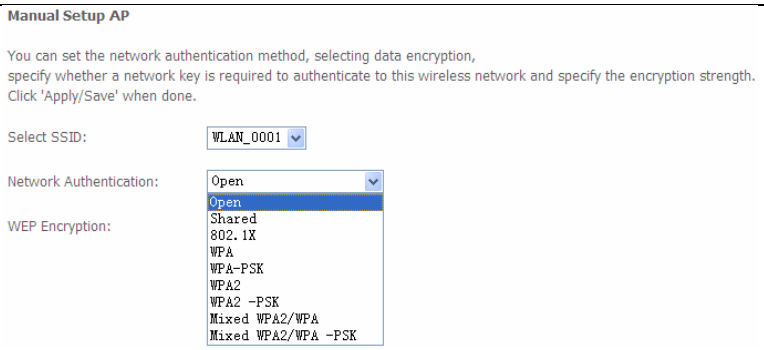
- PIN entry, a mandatory method of setup for all WPS certified devices.
  - **Enter STA PIN**: If you select it, you need to enter the station PIN from client.
  - **Use AP PIN**: The PIN is generated by AP.
- Push button configuration (PBC), an actual push button on the hardware or through a simulated 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*)

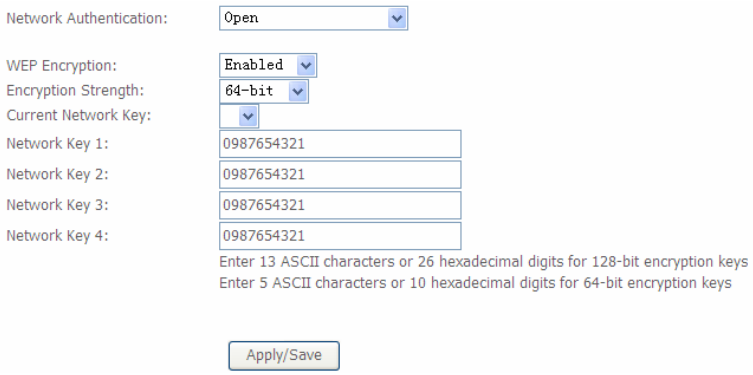
In order to use the push-button for WPS authentication, you must ensure that the network card support the function. if it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function.

- **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.

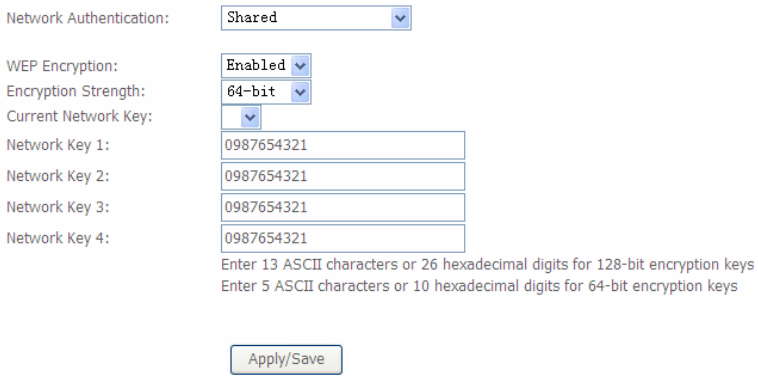


- Open Mode



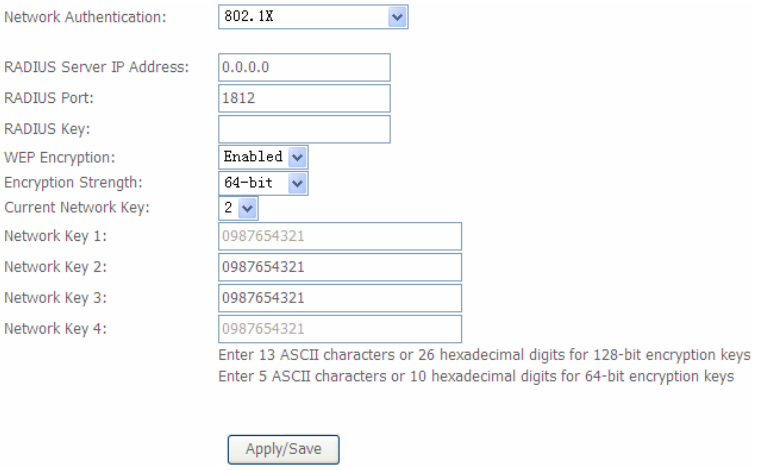
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the Open mode.
- **WEP Encryption:** Enable or disable WEP encryption. After enabling this function, you can set the encryption strength, current network key, and network keys.
- **Encryption 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



The parameters' description of shared mode, please refer to the **Open Mode**.

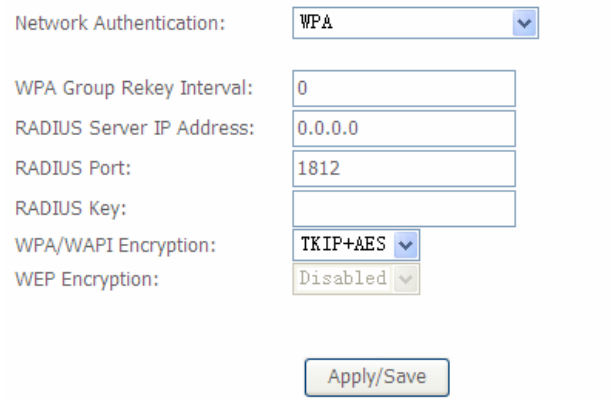
- 802.1x



- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the 802.1X in the drop-down list.

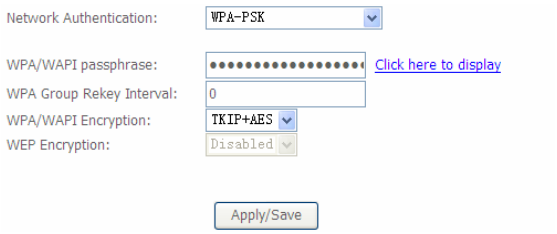
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS 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



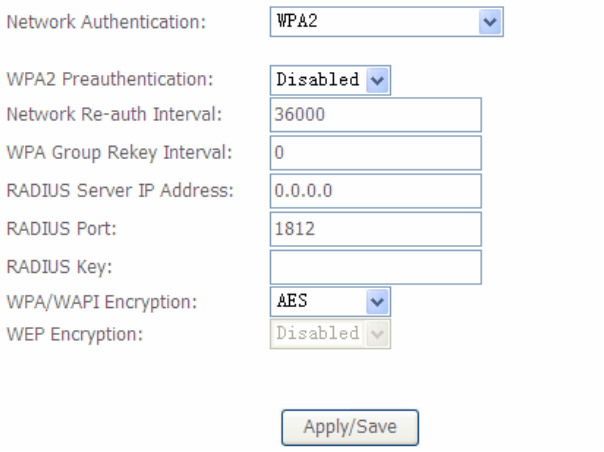
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate 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.

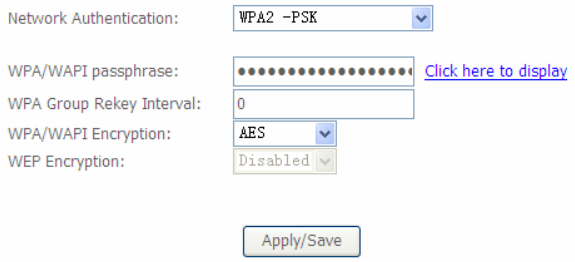
- WPA2 Mode



- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA2 mode.

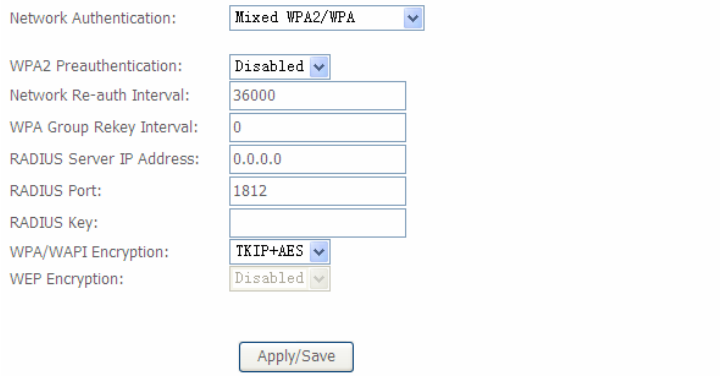
- **WPA2 Preauthentication:** Enable or disable pre-authentication.
- **Network Re-auth Interval:** Set the network re-auth interval.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used 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.

- WPA2-PSK



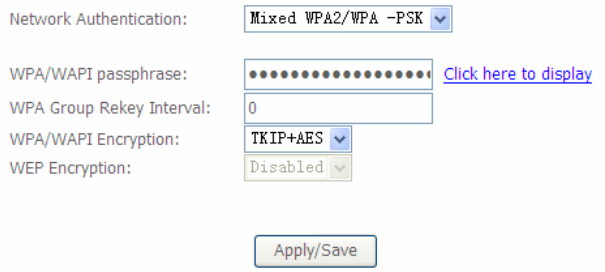
The parameters' description of WPA2-PSK mode, please refer to the **WPA-PSK mode**.

- Mixed WPA2/WPA



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

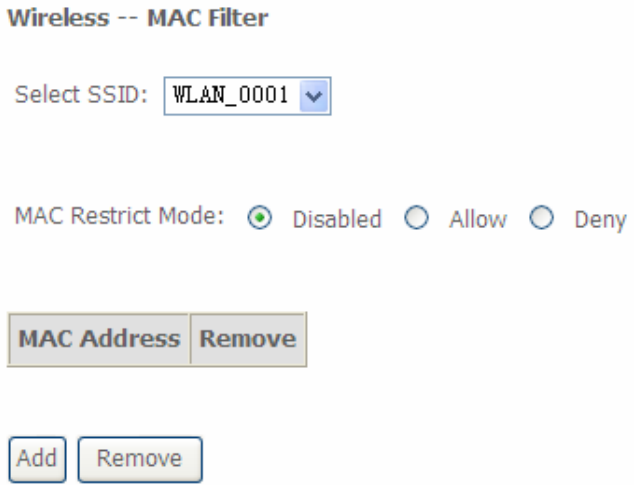
- Mixed WPA2/WPA-PSK



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

5.3.2 MAC Filter

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



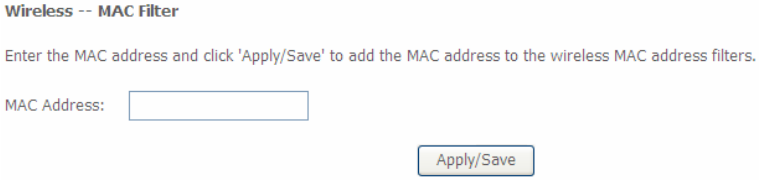
This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

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.

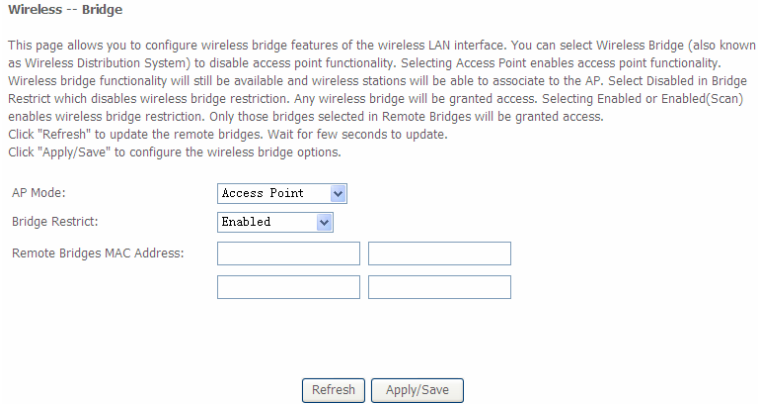
Click the **Add** button to display the following page.



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.

5.3.3 Wireless Bridge

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



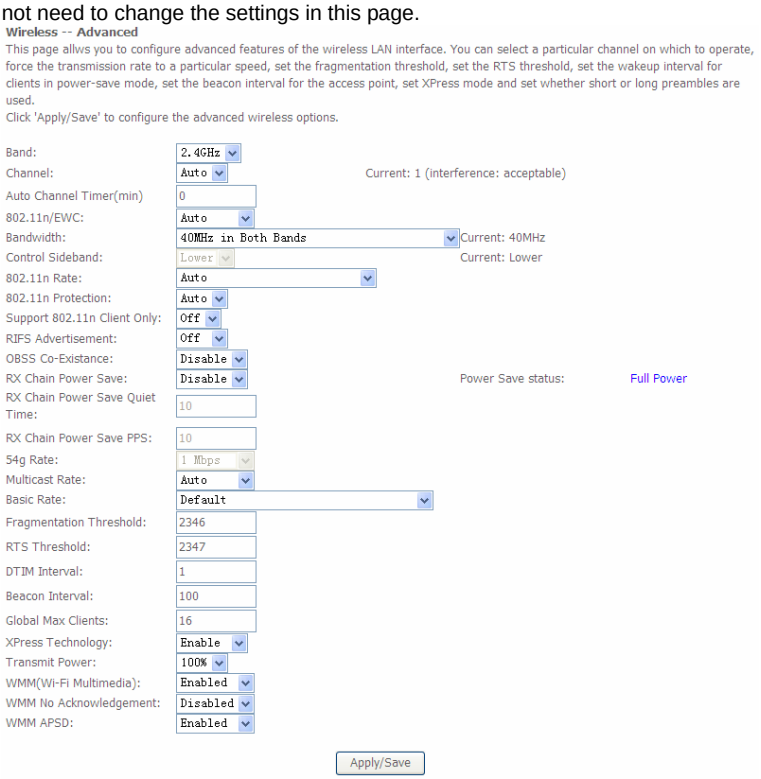
This page allows you to configure the wireless bridge features of the wireless LAN interface.

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

5.3.4 Advanced Settings

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:** 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. You can select **20MHz in 2.4G Band**, **40MHz in 2.4G Band**
- **Control Sideband:** If you select **20MHz in 2.4G Band** or **40MHz in 2.4G Band**, the service of control sideband does not work. When you select **40MHz in 2.4G Band in 2.4G Band** as the bandwidth, the following page appears. Then you can select **Lower** or **Upper** as the value of sideband. As the control sideband, when you select **Lower**, the channel is 1~7. When you select **Upper**, the channel is 5~11.

- **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.
- **WMM (Wi-Fi Multimedia):** Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
- **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
- **WMM APSD:** APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

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.

5.3.5 Station Info

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

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
(null)			WLAN_28EE	wl0

Refresh

This page shows the authenticated wireless stations and their status.

5.4 Voice

Choose **Voice** and the submenus of **Voice** are shown as below.

Voice
- VoIP Status
- SIP Basic Setting
- SIP Advanced Setting
- SIP Extra Setting
- SIP Debug Setting

5.4.1 VoIP Status

Choose **Voice** > **VoIP Status** and the **Voice Status** page appears. In the **Registration Status** field, **Up** means registered successfully, **Down** means unregistered, **Disable** means account is not enabled.

Voice -- Voice Status

Account denial will display "Disabled", registered successfully will display "Up", and unregistered will display "Down".

SIP Account	call time	User Accounts	Registration Status
1	0:00:00		Disabled
2	0:00:00		Disabled

5.4.2 SIP Basic Setting

Choose **Voice** > **SIP Basic Setting**, and the following page appears.

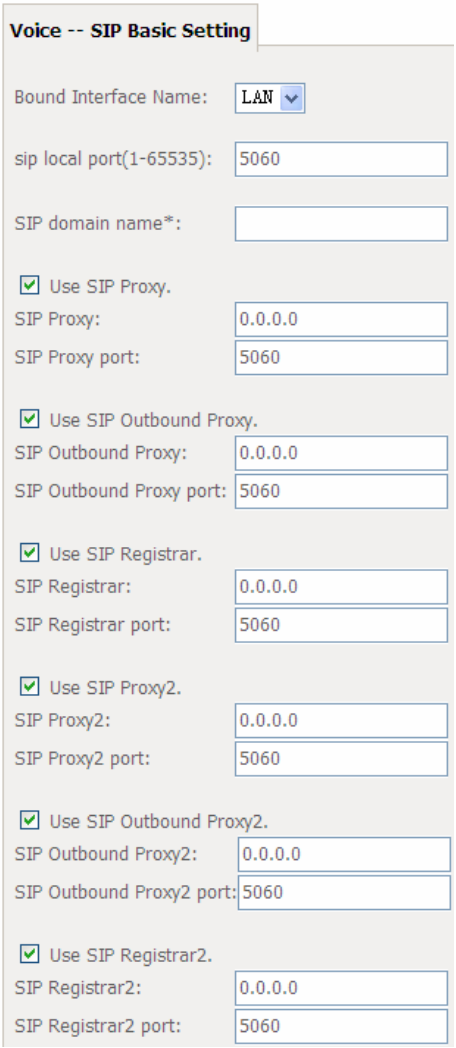


Figure 7 SIP Basic Setting – 1

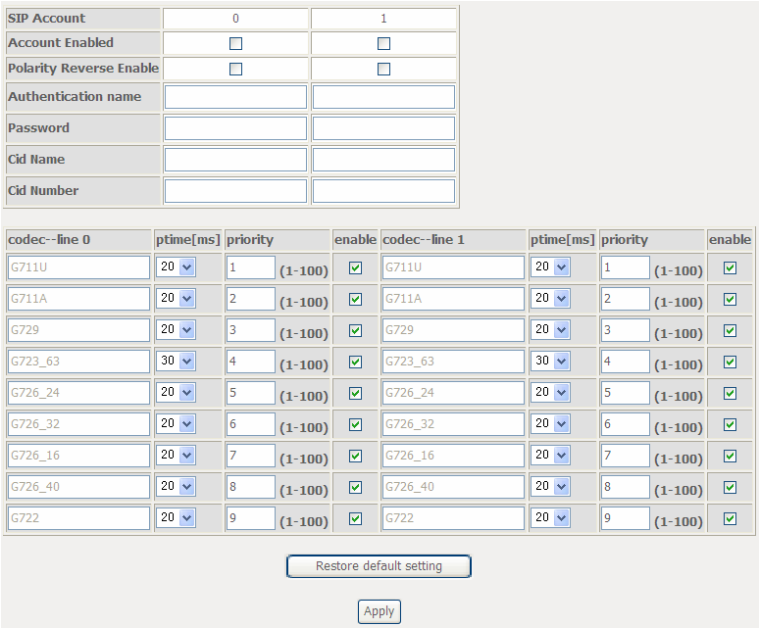
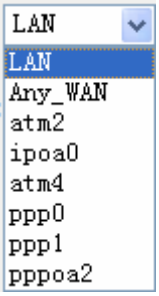


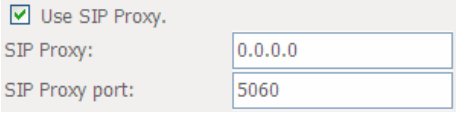
Figure 8 SIP Basic Setting - 2

- **Bound Interface Name:** you can select the bound interface name from the drop-down list.

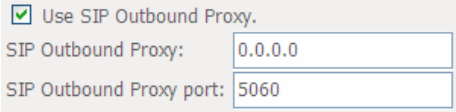


- **SIP Local Port**: Set the SIP local port of the gateway, the default value is **5060**. SIP local port is the SIP UA (user agent) port.

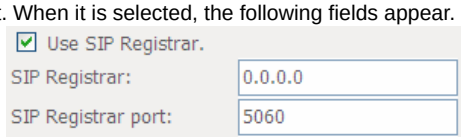
- **SIP domain name**: Enter the SIP domain name that you want to set.
- **Use SIP Proxy**: Select the checkbox of **Use SIP Proxy**, if your DSL router uses a SIP proxy. SIP proxy allows other parties to call DSL router through it. When it is selected, the following fields appear.



  - **SIP Proxy**: The IP address of the proxy.
  - **SIP Proxy port:** The port that this proxy is listening on. By default, the port value is **5060**.
- **Use SIP Outbound Proxy**: Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet. When it is selected, the following fields appear.



  - **SIP Outbound Proxy:** The IP address of the outbound proxy.
  - **SIP Outbound Proxy port:** The port that the outbound proxy is listening on. By default, the port value is **5060**.
- **Use SIP Registrar**: Select the checkbox of **Use SIP Registrar** to register with the proxy. You can register your user ID on the SIP registrar. SIP registrar works with SIP proxy, allowing other parties to call DSL router through it. When it is selected, the following fields appear.



  - **SIP Registrar:** The IP address of the SIP registrar.
  - **SIP Registrar port:** The port that SIP registrar is listening on. By default, the port value is **5060**.
- **Account Enabled:** If it is unselected, the corresponding account is disabled. You can not use it to initiate or accept any call.

- **Polarity Reverse Enable**: Enable or disable this function.
- **Authentication name**: Set the user name of authentication.
- **Password**: Set the password of authentication.
- **Cid Name**: User name. It is the Display Name.
- **Cid Number**: Set the caller number. It must be a number of 0~9.
- **ptime:** You can use it to set the packetization time (PT). The PT is the length of the digital voice segment that each packet holds. The default is **20** millisecond packets. If selecting 10 millisecond, packets improve the voice quality. Because of the packet loss, less information is lost, but more loads on the network traffic.
- **Priority**: The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the DSL router chooses the codec automatically.

After setting, click **Apply** to take the settings in to effect.

5.4.3 SIP Advanced Setting

Choose **Voice** > **SIP Advanced Setting**, and the following page appears.

Voice -- SIP Advanced Setting

Line	1	2
Call waiting	☑	☑
Unconditionally Call forwarding number		
Busy Call forwarding number		
No Answer Call forwarding number		
Options Time	0	0
Forward unconditionally	☑	☑
Forward on "busy"	☑	☑
Forward on "no answer"	☑	☑
MWI	☐	☐
Anonymous call blocking	☑	☑
Anonymous calling	☑	☑
DND	☑	☑
Enable Call Return	☑	☑

Figure 9 SIP Advanced Setting - 1

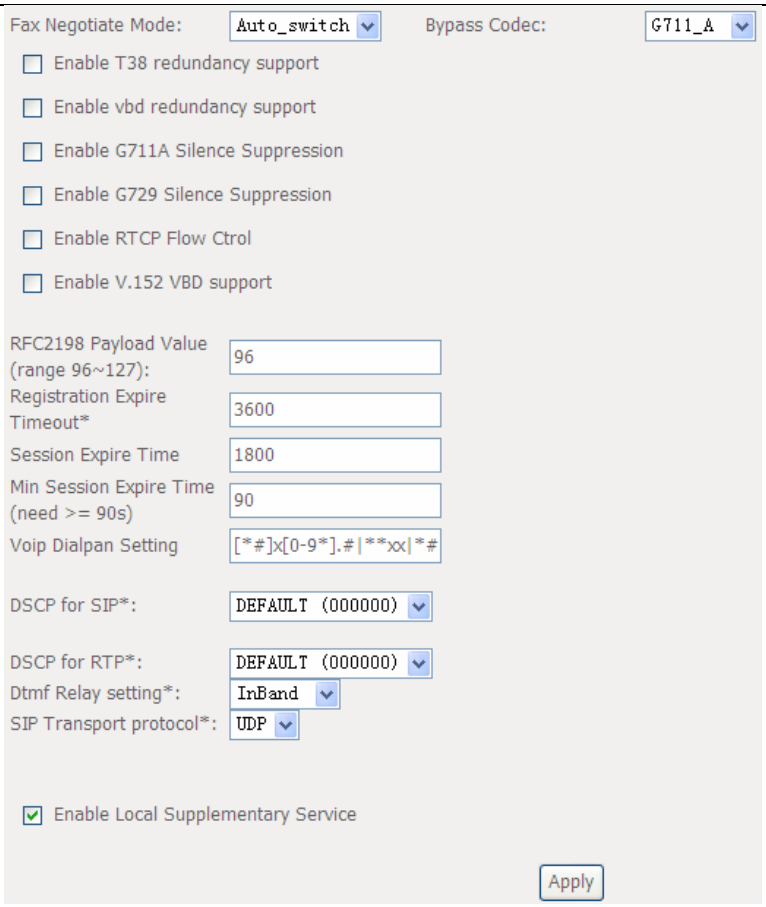


Figure 10 SIP Advanced Setting - 2

- **Line:** It displays the line you want to configure.
- **Call waiting**:

If call waiting is enabled on a line, you can hear the call waiting tone during a call, press **FLASH** on the phone to answer the second call. The first call is automatically placed on hold. To switch between calls, press **FLASH** again.

Select **Call waiting** to enable this feature.

Call forward feature settings (Busy or All) take priority over the call waiting feature. Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

- **Unconditionally Call forwarding number**: Enter the number that you want to set. It is the feature that forwards all incoming calls to an appointed number unconditionally.
- **Busy Call forwarding number**: Enter the number that you want to set. It is a feature that forwards all incoming calls to an appointed number when the line is busy.
- **No Answer Call forwarding number**: Enter the number that you want to set. It is a feature that forwards all incoming calls to an appointed number when the call is not answered.
- **Options Time**: Set the time interval for sending the Options message.
- **Forward unconditionally**: Select the check box to enable this function.
- **Forward on "busy"**: Select the check box to enable this function.
- **Forward on "no answer"**: Select the check box to enable this function.
- **MWI:** When selecting message waiting indicator (MWI), the DSL router sends a SIP SUBSCRIBE message to the proxy, asking for a notification when its voicemail status changes. When its status does change, the proxy send a NOTIFY message to the gateway, causing a MWI tone streamed to user's receiver.
- **Anonymous call blocking**

It is a feature that can block the anonymous call.

Select the checkbox of **Anonymous call blocking** to enable this feature. You can also dial ***77** to enable this feature. Dial ***87** to disable this feature.

- **Anonymous calling**

It is a feature that allows using anonymous name as a call number when calling out.

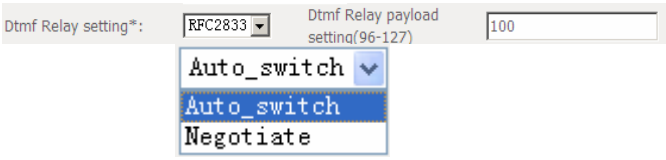
Select the checkbox of **Anonymous calling** to enable this feature. You can also dial ***68** to enable this feature. Dial ***82** to disable this feature.

- **DND**

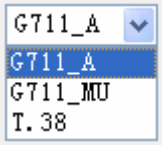
It is a feature to reject all incoming calls.

Select the checkbox of **DND** to enable this feature. You can also Dial ***78** to enable the feature.

- **Enable Call Return**: Select the check box to enable this function.
- **Fax Negotiate Mode**: You can select it from the drop-down list.



- **Bypass Codec**: You can select it from the drop-down list.



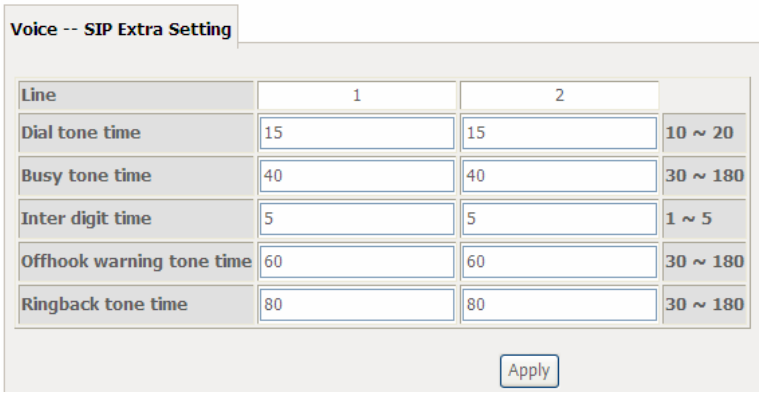
- **Enable T38 redundancy support:** Select the check box to enable this function.
- **Enable vbd redundancy support:** Select the check box to enable this function.
- **RFC2198 Payload Value (range 96~127):** Enter the RFC2198 payload value that the valid range is 96 ~ 127.
- **Registration Expire Timeout*:** Enter the registration expire timeout.
- **Session Expire Time:** The interval of dialog refreshing time.
- **Min Session Expire Time:** The minimum interval of dialog refreshing time.
- **VoIP DialPlan Setting**: Set the VoIP dial plan. If user-dialed number matches it, the number is processed by the DSL router immediately.
- **DSCP for SIP**: Set the DSCP for SIP. You can select it from the drop-down list.
- **DSCP for RTP**: Set the DSCP for RTP. You can select it from the drop-down list.
- **Dtmf Relay Setting**: Set DTMF transmit method, which can be following values:
  - **SIP Info:** Use SIP INFO message to transmit DTMF digits.
  - **RFC2833:** Use RTP packet to encapsulate DTMF events, as specified in RFC 2833.
  - **InBand:** DTMF events are mixed with user voice in RTP packet.

- **SIP Transport Protocol**: Select the transport protocol to use for SIP signaling. Note that the SIP proxy and registrar need to support the protocol you select.
- **Enable Local Supplementary Service**: Select the checkbox to enable the supplementary service settings by the telephone set. If you deselect the checkbox, the supplementary service can not be set by the telephone set.

After setting, click **Apply** to take the settings in to effect.

5.4.4 SIP Extra Setting

Choose **Voice** > **SIP Extra Setting**, and the following page appears.



Voice -- SIP Extra Setting

Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 5
Offhook warning tone time	60	60	30 ~ 180
Ringback tone time	80	80	30 ~ 180

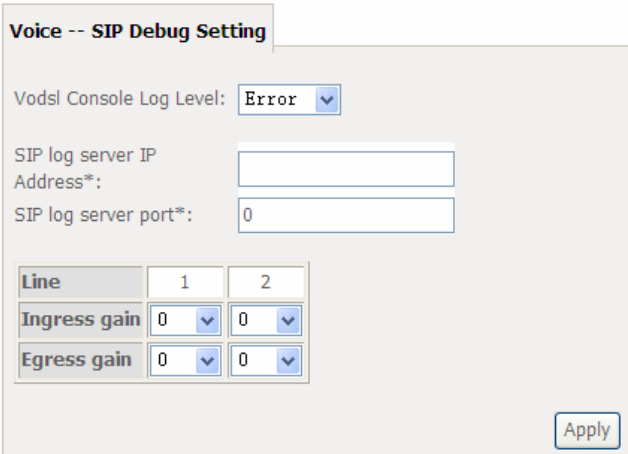
Apply

- **Dial tone time:** Dial tone duration.
- **Busy tone time:** Busy tone duration.
- **Inter digit time:** The valid range is 1 ~ 5.
- **Offhook warning tone time:** Offhook warning tone duration.
- **Ringback tone time:** Ringback tone duration.

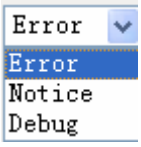
After setting, click **Apply** to take the settings in to effect.

5.4.5 SIP Debug Setting

Choose **Voice** > **SIP Debug Setting**, and the following page appears.



- **Vodsl Console Log Level**: Select it from the drop-down list.



- **SIP Log Server Settings**: Set SIP log server IP address and port, then the log message of the VoIP is sent to the device which IP address you set to. If you want use this function, both of the IP address and port must be set correctly.
- **Gain Settings**: Gain is a measure of the ability of a circuit (often an amplifier) to increase the power or amplitude of a signal. You can increase or decrease ingress gain and egress gain. The range of the value is from -14 to 6.

5.4.6 VoIP Functionality

This section describes how to use the VoIP function of the DSL router in more detail. Some features involve 2 or 3 parties. In that case, note that all 3 parties have to be successfully registered.

5.4.6.1 Registering

Before using any VoIP functions, the DSL router has to register itself to a registrar. The DSL router also has to be configured with a proxy, which relays VoIP signaling

to the next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

Step 1 Select the right interface to use for registering, depending on where proxy/registrar resides. If use WAN link, ensure that it is already up.

Step 2 Select the checkbox of **Use SIP Registrar**, and fill in the IP address and port with the right value.

Step 3 Fill the extension information: **Authentication name**, **Password**, **Cid Name** and **Cid Number**.

Step 4 Click **Apply** to take the settings into effect.

Step 5 **TEL** indicator of VoIP service should be on, indicating that SIP client is successfully registered.

5.4.6.2 Placing a Call

This section describes how to place a basic VoIP call.

(1) Pick up the receiver on the phone.
(2) Hear the dial-tone. Dial the extension of remote party.
(3) To end the dialing, wait for digit timeout, or just press # immediately.
(4) After the remote party answers the call, you are in voice connection.

5.4.6.3 Anonymous call

Anonymous call does not send the caller ID to the remote party. This is useful if you do not want others know whom you are.

(1) Enable **Anonymous calling** in the **Voice--SIP Advanced Setting** web page.
(2) Pick up the receiver on the phone.
(3) Dial ***68** to enable anonymous call.
(4) Hook on the receiver, and dial another extension as you like. Now your caller ID information is blocked.

5.4.6.4 Do Not Disturb (DND)

If DND is enabled, all incoming calls are rejected. DND is useful if you do not want others to disturb you.

(1) Enable **DND** in the **Voice--SIP Advanced Setting** web page.
(2) Pick up the receiver on the phone.
(3) Dial ***78** to enable DND.
(4) Hook on the phone. Now your phone rejects all incoming calls.
(5) Hook off again to disable the DND.

5.4.6.5 Call Return

For incoming calls, the DSL router remembers the number of calling party.

(1) Enable **Call Return** in the **Voice--SIP Advanced Setting** web page.
(2) Press ***69** to return a call.
(3) Now you can make the call as if you have dialed the whole number.

5.4.6.6 Call Hold

Call hold enable you to put a call to a pending state, and pick it up in future.

(1) Assuming you are in a voice connection, you can press **FLASH** to hold current call.
(2) Now you can call another party, or press **FLASH** again to return to first call.

5.4.6.7 Call Waiting

Call waiting allows third party to call in when you are in a voice connection.

(1) Enable **Call waiting** in the **Voice--SIP Advanced Setting** web page.
(2) Pick up the phone attached to the DSL router.
(3) Assuming you are in a voice connection. When another call comes in, the DSL router streams a call waiting tone to your phone, indicating another call is available.
(4) Press **FLASH** to switch to this call and the initial call put to hold automatically.
(5) Press **FLASH** multi-times to switch between these two calls back and forth.

5.4.6.8 Blind Transfer

Blind transfer transfers the current call to a third party blindly, regardless of whether the transfer is successfully or not.

(1) Assume you have already been in a voice connection.
(2) Press **FLASH** to hold the first party.
(3) Dial **#90** + third party number.
(4) Before the third party answering the call, hook on your phone.
(5) Now the first party takes over the call and he is in connection with the third party.

5.4.6.9 Consultative Transfer

Consultative transfer lets the third party answer the transferred call, and then hook on the transferring party. It' more gentle than blind transfer.

(1) Assume you have already been in a voice connection with a first party.

(2) Press **FLASH** to hold the first party.
(3) Dial **#91** + third party number.
(4) After the third party answering the call, hook on your phone.
(5) Now the first party takes over the call and he is in connection with the third party.

5.4.6.10 Call Forwarding No Answer

If this feature enabled, incoming calls are forwarded to third party when you does answer them. It involves in two steps: setting the forwarding number and enable the feature.

(1) Enable **Forward on "no answer"** in the **Voice--SIP Advanced Setting** web page.
(2) When our phone does not answer the incoming call, the call is forwarded.

5.4.6.11 Call Forwarding Busy

If this feature enabled, incoming calls will be forwarded to third party when you busy. It involves two steps: setting the forwarding number and enable the feature.

(1) Set **Busy Call forwarding number** and enable **Forward on "busy"** in the **Voice--SIP Advanced Setting** web page.
(2) When our phone is busy, this call can be forwarded.

5.4.6.12 Call Forwarding All

If this feature enabled, incoming calls are forwarded to third party without any reason. It involves in two steps: setting the forwarding number and enable the feature.

(1) Set **Unconditionally Call forwarding number** and **Forward unconditionally** in the **Voice--SIP Advanced Setting** web page.
(2) All incoming calls are forwarded to the third party.

5.4.6.13 Three-Way Conference

Three-way conference enables you to invite a third party to a call, and every person in the conference is able to hear others' voice.

(1) Assume you are in connection with a first party.
(2) Press **FALSH** to put the first party on-hold.
(3) Dial a third party.
(4) After the third party answers the call, press **FLASH** again to invite the first party.

(5) Now all three parties are in a three-way conference.

5.4.6.14 T38 Faxing

To make T38 faxing, enable T38 support on the Web. After that, connect a fax machine to a FXS port of the DSL router. Now you can use it as a normal phone, and it is able to send or receive fax to or from other fax machines on the VoIP network.

In the initial setup, faxing behaves like a normal call. After the DSL router detects the fax tone, it switch to T38 mode, and use it as the transmit approach.

5.4.6.15 Pass-Through Faxing

If T38 support is disabled, faxing uses normal voice codec as its coding approach. Therefore, this mode more like normal phone calls.

5.5 Diagnostics

5.5.1 Diagnostics

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

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 the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

pppoe_0_1_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your eth0 Connection:	FAIL	Help
Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	PASS	Help
Test your USB Connection:		Help
Test your Wireless Connection:	PASSFAILFAILFAIL	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

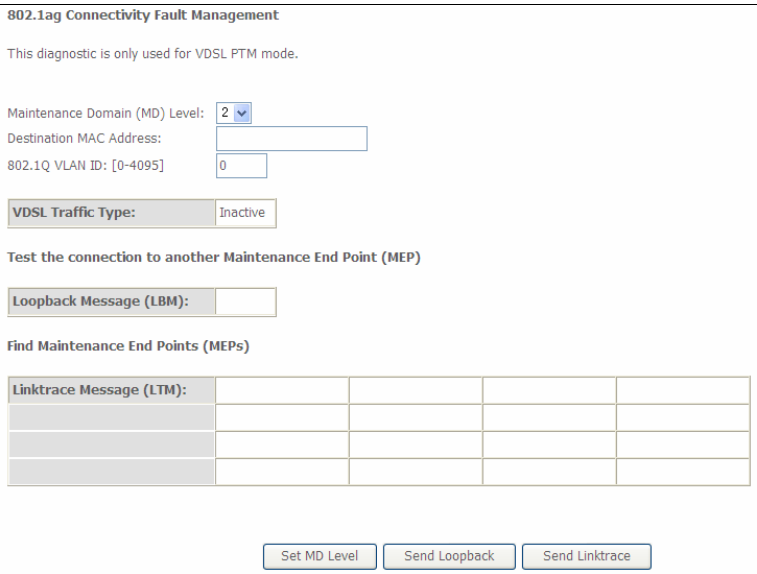
Test | Test With OAM F4

5.5.2 Fault Management

Note:

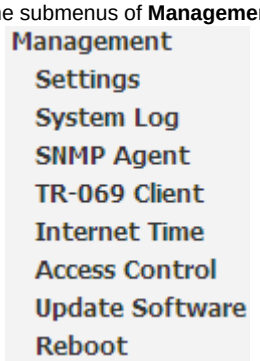
The **Fault Management is only available for VDSL PTM**

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



5.6 Management

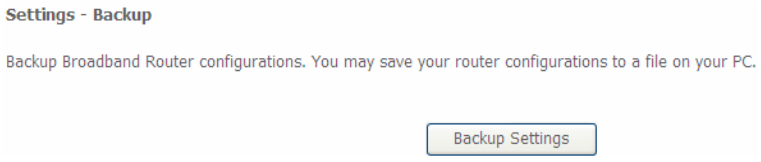
Choose **Management** and the submenus of **Management** are shown as below:



5.6.1 Settings

Backup

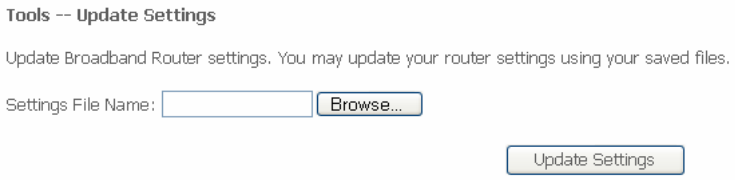
Choose **Management > Settings > Backup** to display the following page.



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.

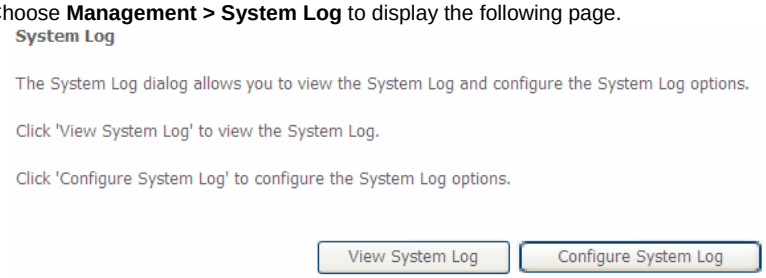
Restore Default

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

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

5.6.2 System Log

Choose **Management > System Log** to display the following page.



In this page, you are allowed to configure the system log and view the security log.

- **Configuring the System Log**

Click the **Configure System Log** button to display the following page.

In this page, you can set 3 types of system log modes, including **Local**, **Remote**, and **Both**.

- **Local:** When selecting **Local**, the events are recorded in the local memory.
- **Remote:** When selecting **Remote**, the events are sent to the specified IP address and UDP port of the remote system log server.
- **Both:** When selecting **Both**, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

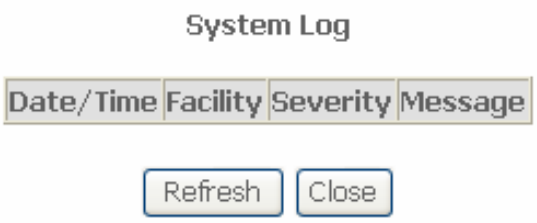
After finishing setting, click the **Apply/Save** button to save and apply the settings.

Note:

*If you want to log all the events, you need to select the **Debugging** log level.*

- **View System Log**

Click the **View System Log** button to display the following page.

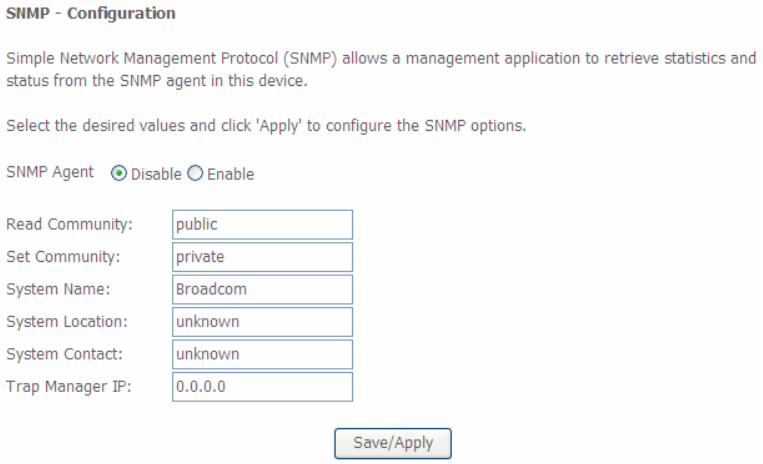


In this page, you can view the system log.

Click the **Refresh** button to refresh the system log. Click the **Close** button to exit.

5.6.3 SNMP Agent

Choose **Management > SNMP Agent**, and the following page appears.



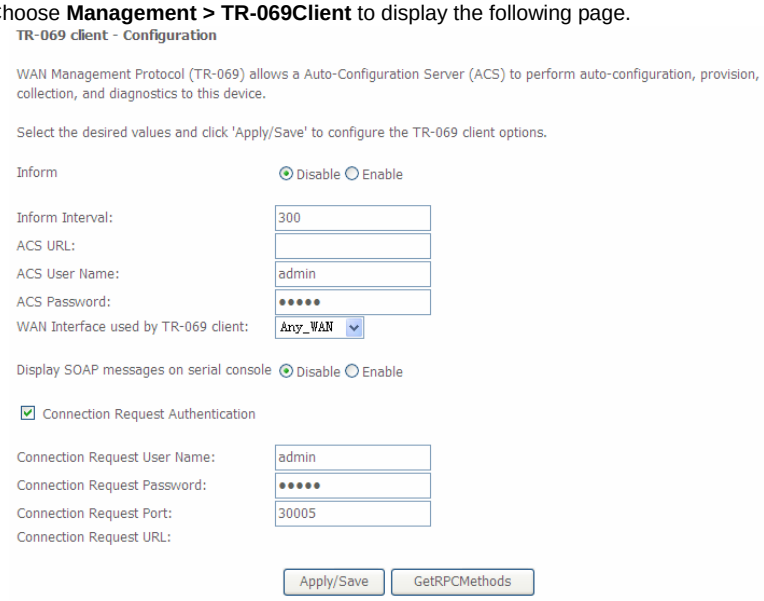
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

In this page, you may enable or disable the SNMP agent and set the parameters such as the read community, system name and trap manager IP.

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

5.6.4 TR-69 Client

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



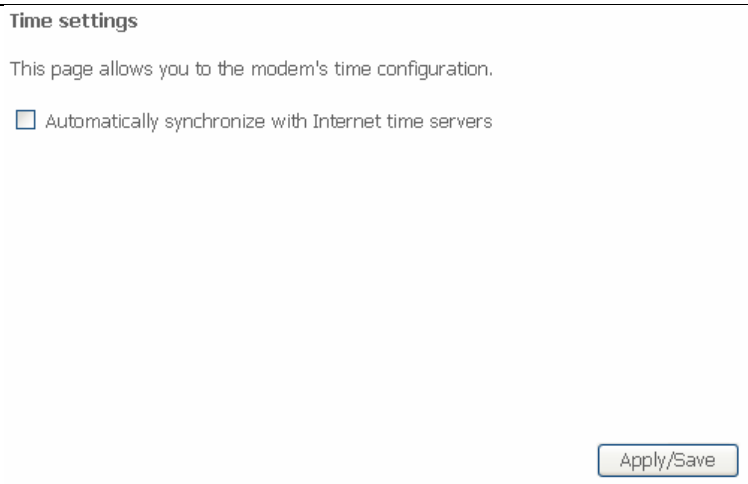
WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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

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

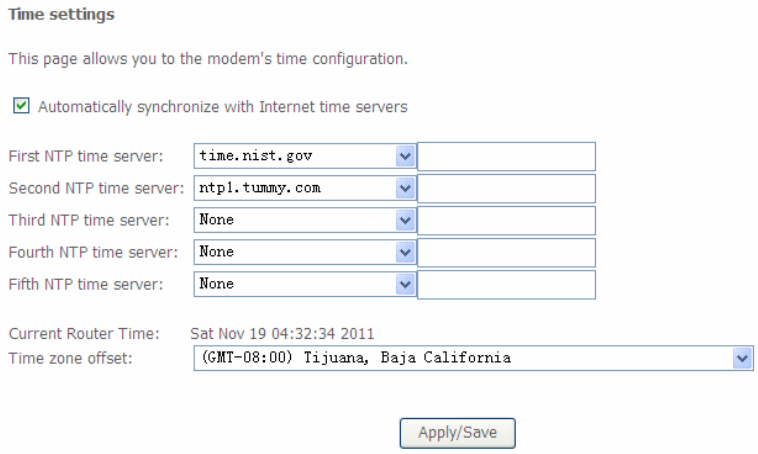
5.6.5 Internet Time

Choose **Management > Internet Time** to display the following page.



In this page, you may configure the router to synchronize its time with the Internet time servers.

After enabling **Automatically synchronize with Internet time servers**, the following page appears.

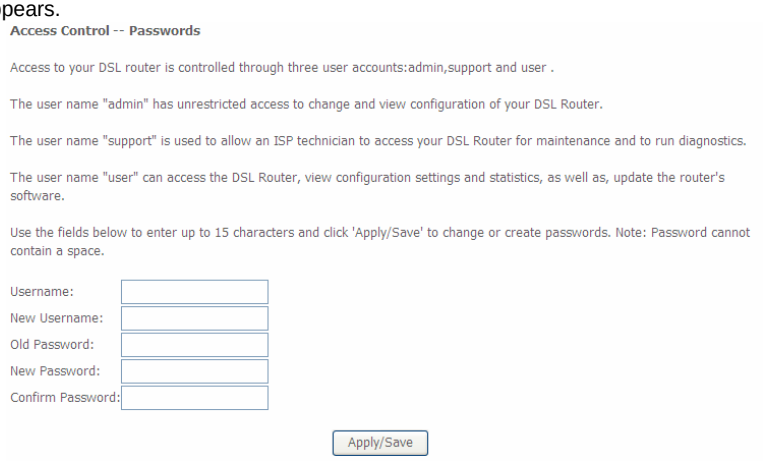


In this page, set the proper time servers, and then click the **Apply/Save** button to save and apply the settings.

5.6.6 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 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.

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

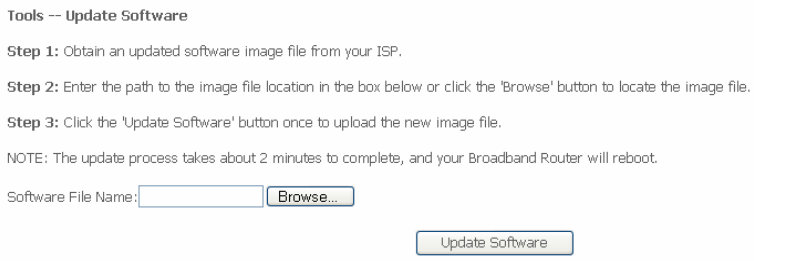
Services	LAN	WAN	Port
HTTP	☑ enable	☐ enable	80
TELNET	☑ enable	☐ enable	23
SSH	☐ enable	☐ enable	22
FTP	☑ enable	☐ enable	21
TFTP	☑ enable	☐ enable	69
ICMP	☑ enable	☐ enable	0
SNMP	☑ enable	☐ enable	161
SAMBA	☑ enable	☐ enable	445

Apply/Save

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.

5.6.7 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.

5.6.8 Reboot

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

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 **DSL** indicator is off?

A: Check the connection between the “DSL” port of router and the wall jack.

(4) **Q**: Why Internet access fails while the **DSL** 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**