MD1600

User Manual

VER: 1.0

Contents

Contents i
1 Safety Precautions 1
Default Safety Language in manual 2
2 Overview 3
2.1 Application 3
2.2 Features 4
2.3 Standards Compatibility and Compliance 5
3 Hardware Description and Installation 6
3.1 Hardware Description 6
3.1.1 Front Panel 6
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 9
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 13
5.1.2 WAN 14
5.1.3 Statistics 15
5.1.4 LAN 15
5.1.5 WAN Service 15
5.1.6 xTM 16
5.1.7 xDSL 16
5.1.8 Route 19
5.1.9 ARP 20
5.1.10 DHCP 20
5.2 Advanced Setup 20
5.2.1 Layer2 Interface 22
5.2.2 WAN Service 26

5.2.3 LAN Configuration 51
5.2.4 NAT 57
5.2.5 Security 61
5.2.6 Parental Control 64
5.2.7 Quality of Service 66
5.2.8 Routing 70
5.2.9 DNS 74
5.2.10 DSL 75
5.2.11 UPnP 76
5.2.12 DNS Proxy 77
5.2.13 Print Server 77
5.2.14 Packet Acceleration 78
5.2.15 Storage Service 78
5.2.16 Interface Grouping 79
5.2.17 IP Tunnel 80
5.2.18 IPSec 82
5.2.19 Certificate 84
5.2.20 Power Management 88
5.2.21 Multicast 89
5.3 Wireless 90
5.3.1 Basic Settings 91
5.3.2 Security 92
5.3.3 MAC Filter 100
5.3.4 Wireless Bridge 101
5.3.5 Advanced Settings 102
5.3.6 Station Info 105
5.4 Diagnostics 105
5.4.1 Diagnostics 105
5.5 Management 106
5.5.1 Settings 107
5.5.2 System Log 108
5.5.3 SNMP Agent 109
5.5.4 TR-69 Client 110
5.5.5 Internet Time 111
5.5.6 Access Control 113

5.5.7 Update Software.....114
5.5.8 Reboot.....115
6 Q&A.....116

.....116
7 Technical Support 117
We like to help. 117

1 Safety Precautions

NOTICE

This document contains proprietary information protected by copyright, and this Manual and all the accompanying hardware, software, and documentation are copyrighted. No part of this document may be photocopied or reproduced by mechanical, electronic, or other means in any form.

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

© Copyright 2017 MTRLC LLC

All rights reserved.

SAFETY PRECAUTIONS

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment. MOTOROLA and MTRLC assume no liability for damage caused by any improper use of the DSL router.

CAUTION:

- Place the device on a stable surface in its normal upright orientation.
- Do not use the DSL router outdoors.
- Keep the DSL router in an environment that is between 0°C and 40°C (between 32°F and 104°F).
- Do not place any object on top of the DSL router since this may cause overheating.
- Do not place the DSL router in a confined space that may cause overheating.
- Do not restrict the flow of air around the DSL router.
- Use only the telephone cord that is packed within the device package.
- Use only the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or power adapter wires. An overburden power outlet or damaged wires and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.

- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid placing the device in direct sunlight.
- Do not put this device close to a place where it is high moisture or wet. Do not spill any fluid on this device.

FCC Statement

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Class B Part 15 and Part 68 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: this equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: reorient or relocate the receiving antenna, increase the separation between the equipment and receiver, connect the equipment into an outlet on a circuit different from that to which the receiver is connected, and/or consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement: This equipment complies with radiation exposure limits and should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom case of this equipment is a label that contains, among other information, a product identifier in the format US: MTLDL01AMD1600 and REN: 0.1A for this equipment.

This equipment uses the following USOC jacks: RJ-11/RJ45/USB/Power Jacks!

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

REN (RINGER EQUIVALENT NUMBERS) STATEMENT

REN=0.1

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.

If this equipment MD1600 causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment MD1600, for repair or warranty information, please contact MTRLC LLC If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this MD1600 does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

~ Input supply voltage is from AC outlet (mains), disconnect device from outlet to remove power.

WEEE is a directive in the EU that designates safe and responsible collection, recycling, and recovery procedures for electronic waste.

MTRLC LLC
PO Box 121147
Boston, MA 02112-114

H Overview

The xDSL Router integrates wireless LAN, and USB storage into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11g/802.11b/802.11n wireless network. The Router combines high-speed xDSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Router connects to an Ethernet L computers via standard Ethernet ports. The xDSL connection is made usin ordinary telephone line with standard connectors. 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 Route the WAN interface.

1.1 Application

- Home gateway
- Wireless LAN
- SOHO
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming
- USB storage

1.2 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 xDSL 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
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- Print server
- Web filtering
- Management and control

  Web-based management (WBM)

  Command line interface (CLI)

  TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.

1.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)

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

Hardware Description and Installation

Note:

The figures in this document are for reference only.

2.1 Hardware Description

2.1.1 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.

Indicator	Color	Status	Description
		Off	The Ethernet interface is disconnected.
USB	Green	On	The connection of USB flash disk has 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.

2.1.2 Rear Panel and Side Panel

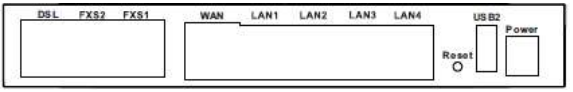


Figure 2 Rear panel

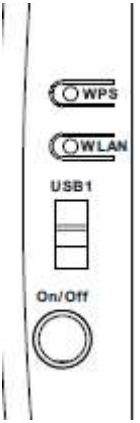


Figure 3 Side panel

The following table describes the interfaces or the buttons.

Interface	Description
DSL	RJ-11 port: Connect the router to DSL connector or splitter through telephone cable.
LAN 4~1	RJ-45 port, for connecting the router to a PC or another network device.
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.
USB	For connecting the USB storage devices.
Power	Power interface, for connecting the power adapter.
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.

⚠ **Warning:**

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

2.2 Hardware Installation

2.2.1 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.

2.2.2 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.

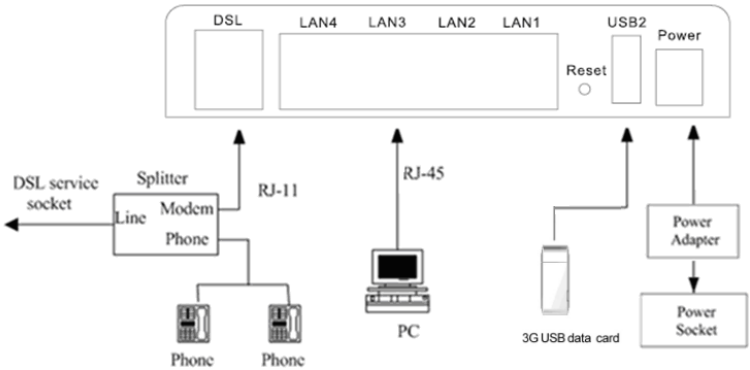


Figure 4 Connecting the DSL router

3 PC Network Configuration and Login

3.1 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.

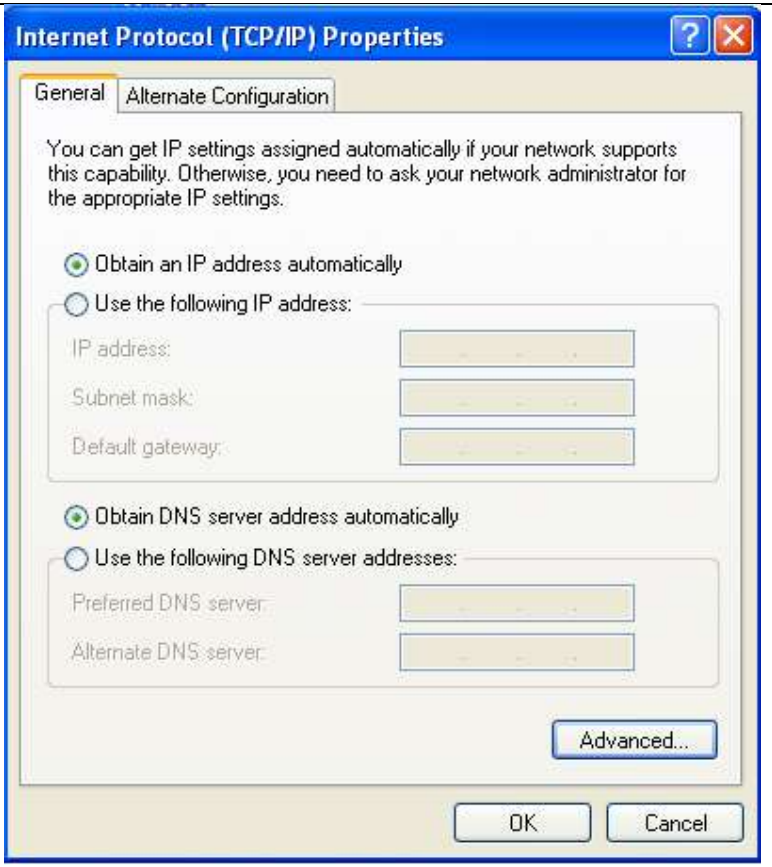


Figure 5 IP and DNS configuration

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

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

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

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

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

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

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

Click **OK** to save the settings.

3.2 Logging In to the DSL Router

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

Open a Web browser on your computer.

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

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.

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

Figure 6 Login page

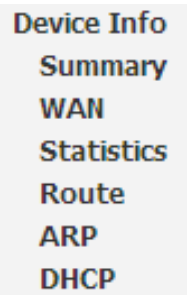
After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

4 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.

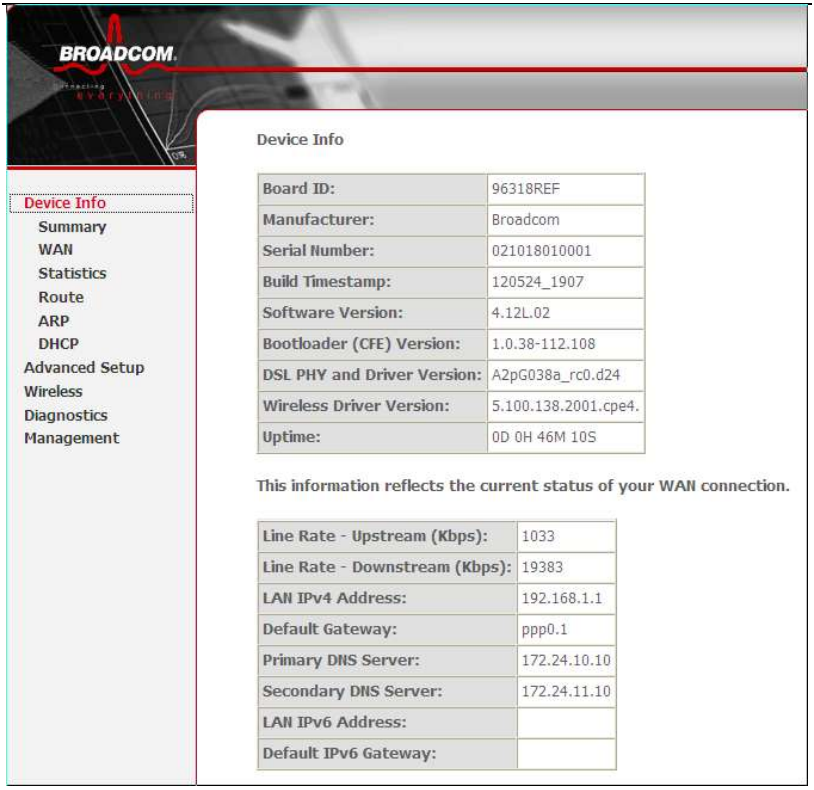
4.1 Device Information

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



4.1.1 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.

4.1.2 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.

4.1.3 Statistics

4.1.4 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.

4.1.5 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.

4.1.6 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.

4.1.7 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

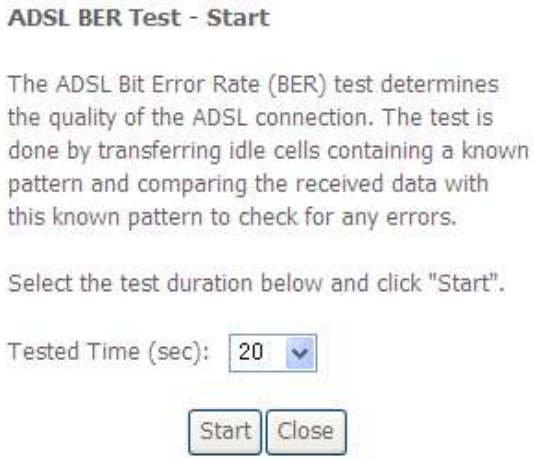
In this page, you can view the statistical information about the recevied and transmitted data packets of the xDSL interfaces.

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

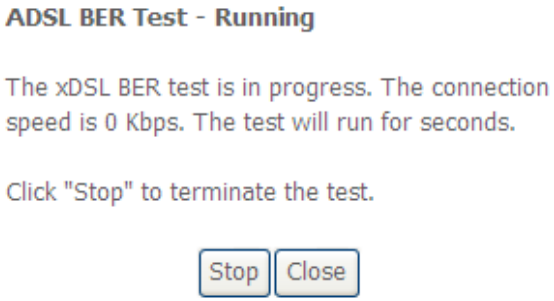
Click **Reset Statistics** to restore the values to zero and recount them.

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.

4.1.8 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.

4.1.9 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.

4.1.10 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.

4.2 Advanced Setup

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

Advanced Setup

- Layer2 Interface
- WAN Service
- 3G Wan Service
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnP
- DNS Proxy
- Print Server
- DLNA
- Packet Acceleration
- Storage Service
- Interface Grouping
- IP Tunnel
- IPSec
- Certificate
- Power Management
- Multicast

4.2.1 Layer2 Interface

4.2.1.1 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:

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	0	36	Path0	UBR				EoA	VlanMuxMode	Support	8/WRR/1	☐

Add Remove

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

4.2.1.2 PTM Interface

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

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

PTM Configuration

This screen allows you to configure a PTM connection.

Select DSL Latency
- [x] Path0 (Fast)
- [ ] Path1 (Interleaved)

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)
Default Queue Minimum Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Rate	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Burst Size:	3000	[bytes] (shall be >=1600)

Back Apply/Save

In this page, you can configuration the PTM interface Click Apply/Save.

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

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	☐

Add Remove

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

4.2.1.3 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.

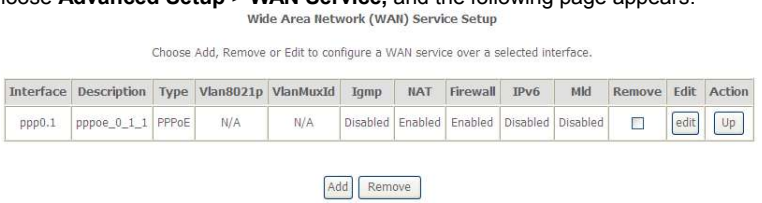
In this page, you can select a ETH port. Click **Apply/Save** to save configuration.

Note:

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

4.2.2 WAN Service

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



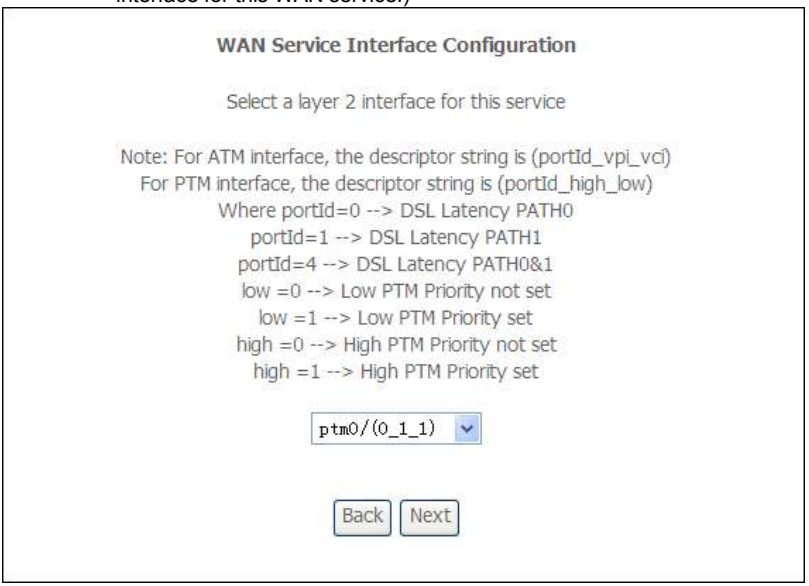
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit	Action
ppp0.1	pppoe_0_1_1	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up

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

4.2.2.1 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 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.

WAN Service Configuration

Select WAN service type:

- (•) PPP over Ethernet (PPPoE)
- ( ) IP over Ethernet
- ( ) Bridging

Enter Service Description: pppoe_0_1_1

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

Network Protocal Selection:

IPV4 Only

Back Next

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

PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

MTU[576-1500]: 1492

- [ ] Config KeepAlive
- [ ] Enable Fullcone NAT
- [ ] Dial on demand (with idle timeout timer)
- [ ] PPP IP extension
- [ ] Use Static IPv4 Address
- [ ] Enable PPP Debug Mode
- [ ] Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

- [ ] Enable IGMP Multicast Proxy

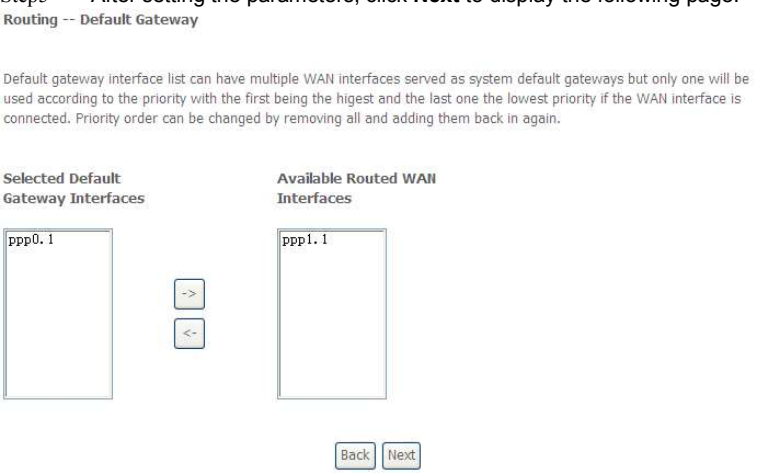
Back Next

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.

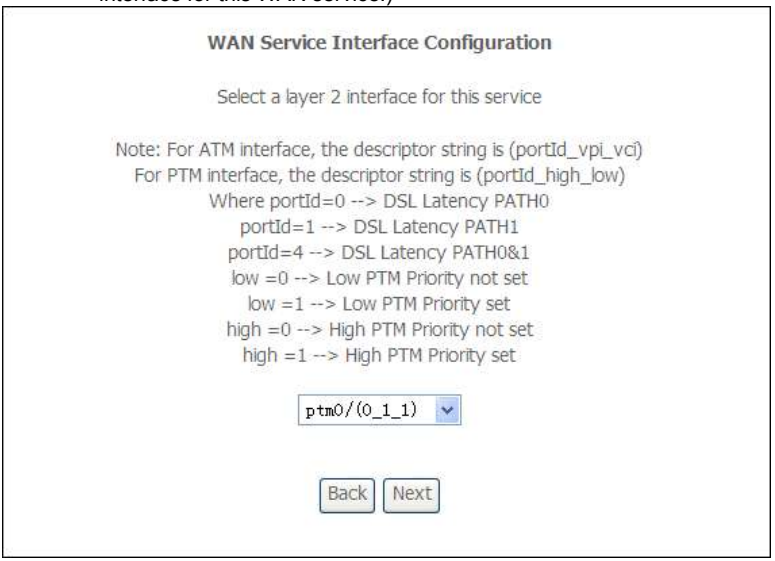
Back Apply/Save

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

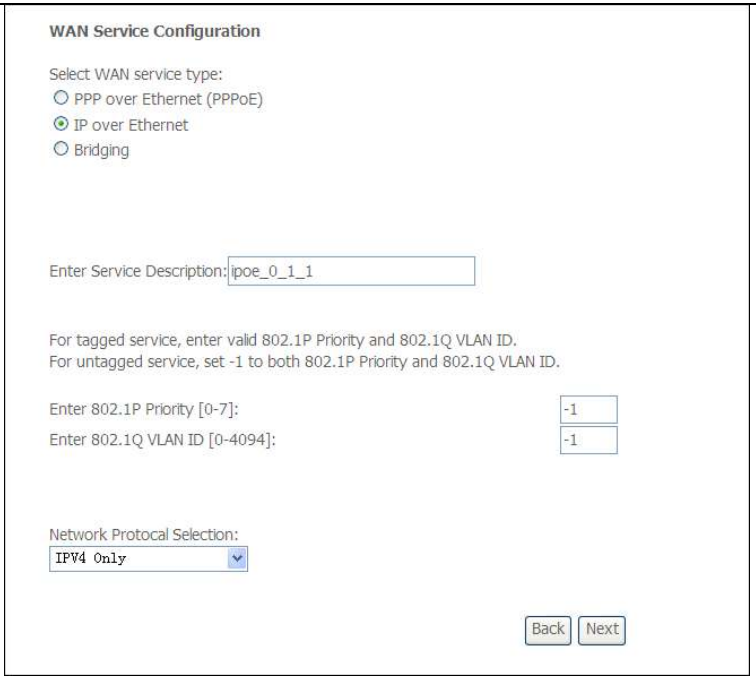
4.2.2.2 Adding a MER (IPoE) WAN service

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 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.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(hexadecimal digit)
Option 125:	Disable	Enable

Use the following Static IP address

WAN IP Address:	
WAN Subnet Mask:	
WAN gateway IP Address:	
Primary DNS server:	
Secondary DNS server:	

Back Next

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.*

Network Address Translation Settings

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

☐ Enable NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

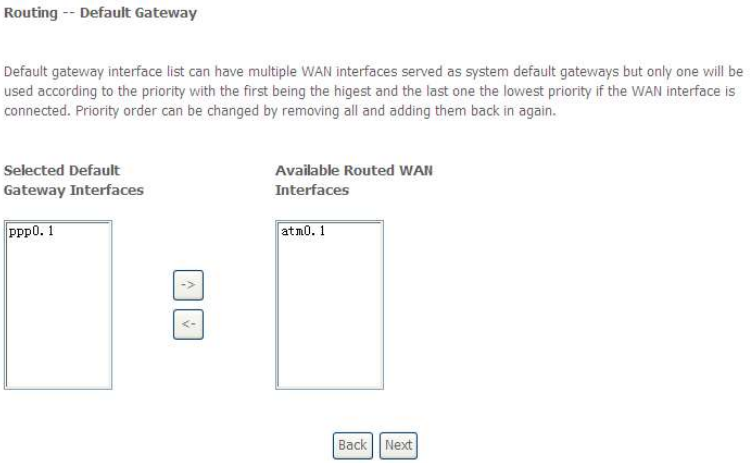
☑ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast

Back Next

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.

4.2.2.3 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.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm1/(0_0_37)

Back Next

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

WAN Service Configuration

Enter Service Description: pppoa_0_0_37

Network Protocal Selection:(IPV6 Only not support)

IPV4 Only

Back Next

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

PPP Username and Password

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

PPP Username: test
PPP Password: ••••
Authentication Method: AUTO
MTU[576-1500]: 1492

☑ Enable Fullcone NAT
ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY
☐ Dial on demand (with idle timeout timer)
☐ Use Static IPv4 Address
☐ Enable PPP Debug Mode

Multicast Proxy
☐ Enable IGMP Multicast Proxy

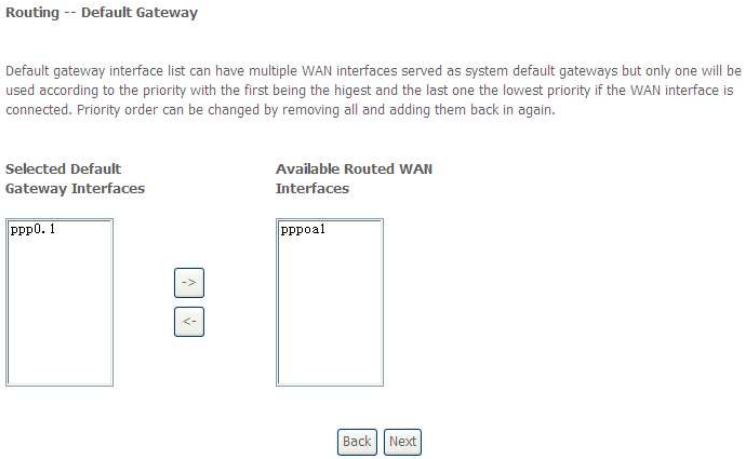
Back Next

- **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.

4.2.2.4 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.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ipoa0/(0_0_38)

Back Next

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

WAN Service Configuration

Enter Service Description: ipoa_0_0_38

Back Next

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

WAN IP Settings

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

WAN IP Address:	0.0.0.0
WAN Subnet Mask:	0.0.0.0
Primary DNS server:	0.0.0.0
Secondary DNS server:	

Back Next

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.

Network Address Translation Settings

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

☑ Enable NAT

☑ Enable Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

☐ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast

Back Next

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.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways 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.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	-> <-	ipoa0

Back Next

Step8 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	-> <-	ipoa0

Back Next

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.

4.2.2.5 Adding a Bridge WAN service

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

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 interface for this WAN service.) Click the **Add** button to display the following page.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm0/(0_0_36)

Back Next

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

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

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.

4.2.3 LAN Configuration

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

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

◉ Blocking Mode

☐ Enable LAN side firewall

○ Disable DHCP Server

◉ Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Primary DNS server: 192.168.1.1

Secondary DNS server: 192.168.1.1

Leased Time (hour): 24

Static IP Lease List: (A maximum 32 entries can be configured)

Edit DHCP Option 60 | Edit DHCP Option | DHCP Advance setup

MAC Address	IP Address	Remove

Add Entries | Remove Entries

☐ Configure the second IP Address and Subnet Mask for LAN interface

Apply/Save

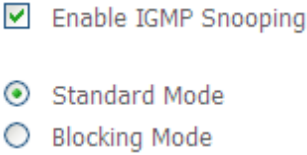
In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP option, configure the DHCP advanced setup and set the binding between a MAC address and an IP address.

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.

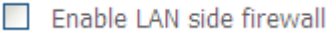
Enabling IGMP Snooping

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.



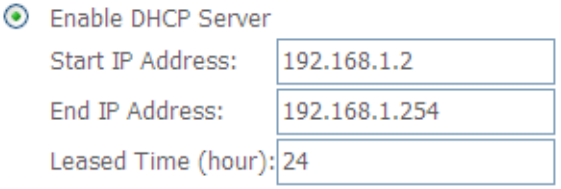
Enabling the LAN Side Firewall

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.

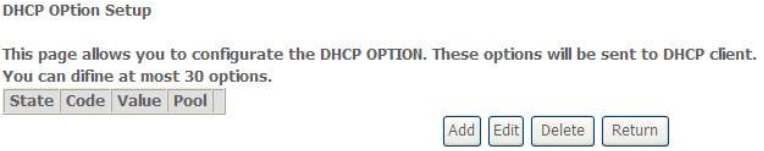
Editing the DHCP Option60

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.

DHCP Static IP Lease

Enter the Mac address and Static IP address then click Apply/Save .

MAC Address:

IP Address:

Apply/Save

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.

☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address: 192.168.249.1

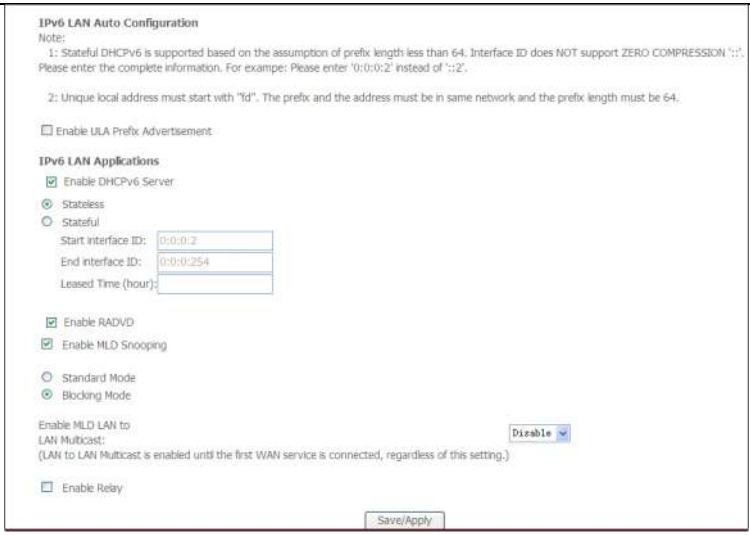
Subnet Mask: 255.255.255.252

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.

4.2.3.1 IPv6 Auto-configuration

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



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

- **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
- **Enable RADVD:** The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
- **Enable MLD Snooping**: Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

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

4.2.4 NAT

4.2.4.1 Virtual Servers

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

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

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum **32** entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address/Hostname	WAN Interface	LAN Loopback	Enable/Disable	Remove

Add Save/Apply Remove

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

To add a virtual server, do as follows:

Step 4 Click the **Add** button to display the following page.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured:32

Use Interface: pppoe_0_1_1/ppp0.1
Service Name:
Select a Service: Select One
Custom Service:
Enable LAN Loopback

Server IP Address/Hostname: 192.168.1.

Status:

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Save/Apply

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

4.2.4.2 Port Triggering

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

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

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.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Use Interface: pppoe_0_1_1/ppp0.1

Application Name:

- Select an application: Select One
- Custom application:

Apply/Save

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

- **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.

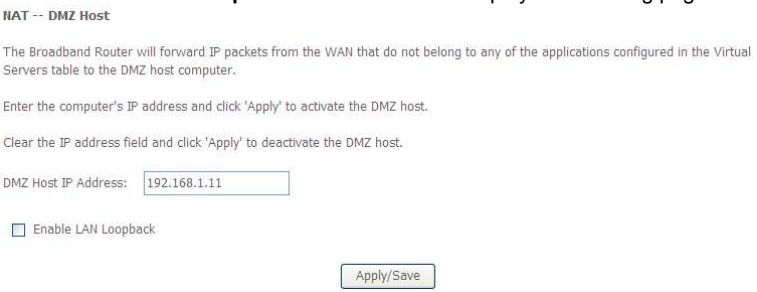
Note:

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.

4.2.4.3 DMZ Host

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

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



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

After 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.

4.2.5 Security

Firewall

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

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be**BLOCKED**by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

Add Remove

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.

Add IP Filter -- Outgoing

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

Filter Name:

IP Version: IPv4

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Apply/Save

- **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.

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.

MAC Filtering Setup

"MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface**(maxinum 32 entries):**

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm3	FORWARD	☐

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Add Remove

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.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_39/atm3

Apply/Save

- **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.

4.2.6 Parental Control

Time Restriction

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

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Add Remove

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.

Parental Control -- URL Filter Add

Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Apply/Save

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:

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
http://www.google.com	80	

Add Remove

4.2.7 Quality of Service

Enabling QoS

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

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

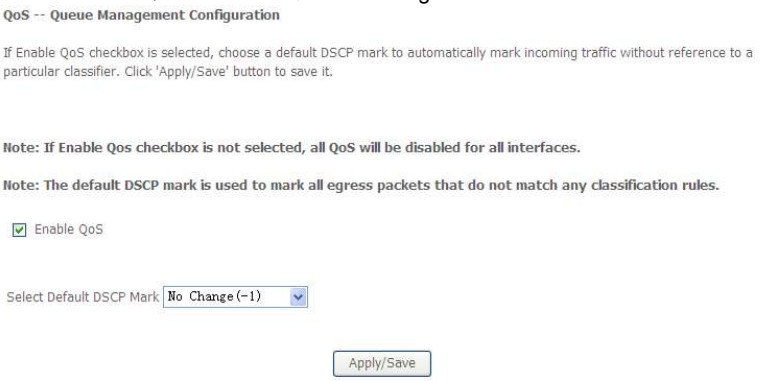
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Apply/Save

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.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the rule after page reload.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit (kbps)	Enable	Remove

Add Enable Remove

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

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

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:
Rule Order: Last
Rule Status: Disable

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface: LAN
Ether Type:
Source MAC Address
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):
- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark 802.1p priority:
- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

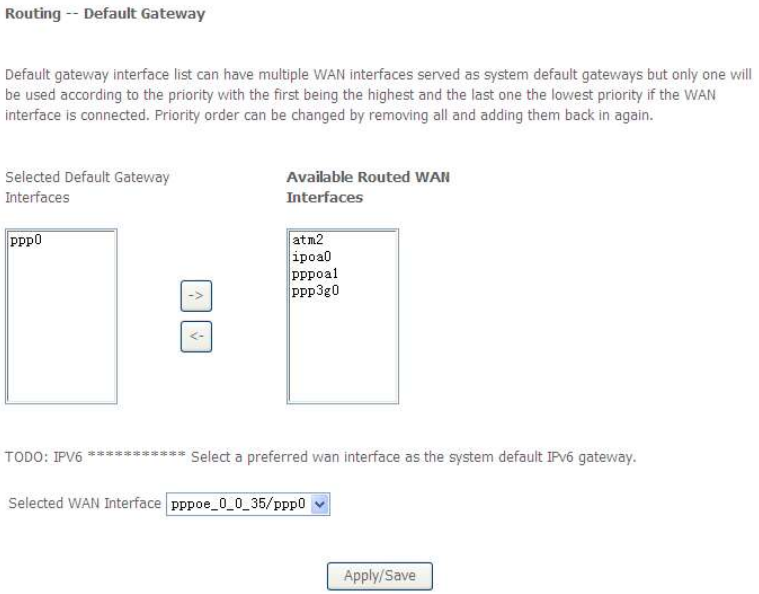
Set Rate Limit: [Kbits/s]

Apply/Save

4.2.8 Routing

Default Gateway

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



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

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

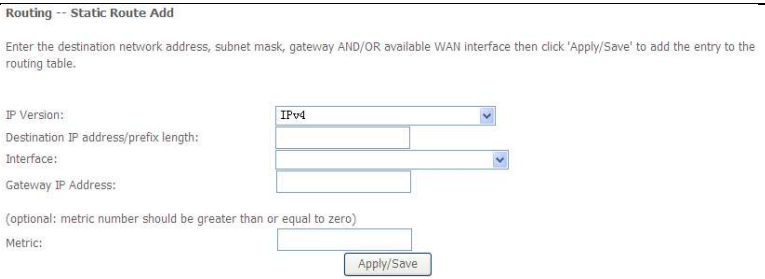
After finishing setting, click **Apply/Save** to save and apply the settings.

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.

Policy Routing Settup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface: pppoe_0_1_1/ppp0.1

Default Gateway:

Apply/Save

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.

Routing -- RIP Configuration

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

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

Interface	Version	Operation	Enabled
atm2	2	Passive	☐
ipoa0	2	Passive	☐
atm4	2	Passive	☐

Apply/Save

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.

4.2.9 DNS

DNS Server

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

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.

DSelect DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ppp0.1

Available WAN Interfaces

-> <-

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Apply/Save

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.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Add Remove

In this page, you are allowed to modify the DDNS settings.
Click the **Add** button to display the following page.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_1_1/ppp0.1

DynDNS Settings

Username:

Password:

Apply/Save

- **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.

4.2.10 DSL

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

DSL Settings

Select the modulation below.

- [x] G.Dmt Enabled
- [x] G.lite Enabled
- [x] T1.413 Enabled
- [x] ADSL2 Enabled
- [x] AnnexL Enabled
- [x] ADSL2+ Enabled
- [ ] AnnexM Enabled

Select the phone line pair below.

- (•) Inner pair
- ( ) Outer pair

Capability

- [x] Bitswap Enable
- [ ] SRA Enable

Apply/Save | Advanced Settings

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.

4.2.11 UPnP

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

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

- [x] Enable UPnP

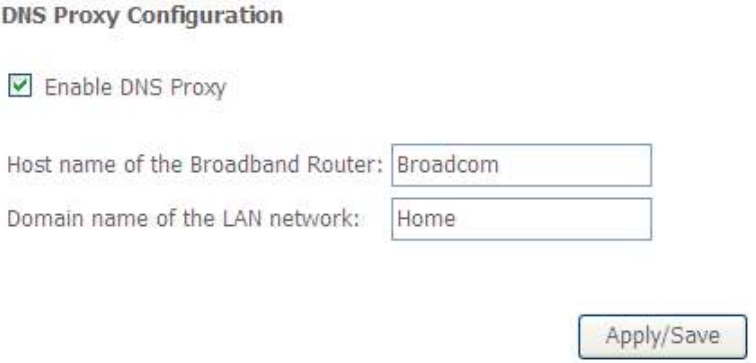
Apply/Save

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

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

4.2.12 DNS Proxy

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

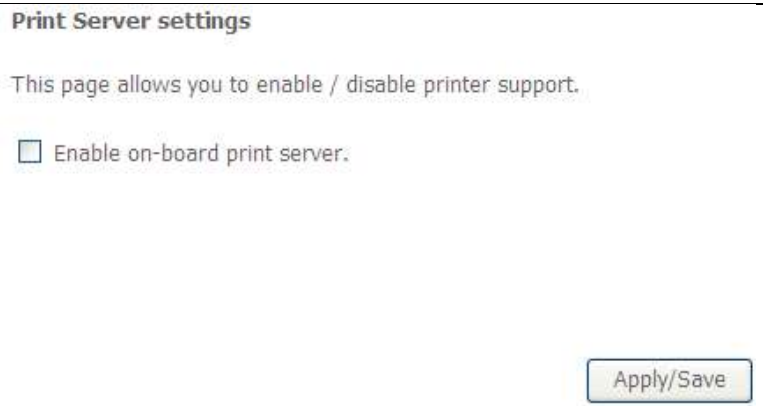


In this page, you can enable or disable the DNS proxy function.

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

4.2.13 Print Server

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



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

4.2.14 Packet Acceleration

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

4.2.15 Storage Service

Storage Device Info

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

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	PhysicalMedium	FileSystem	Total Space	Used Space

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

4.2.16 Interface Grouping

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

Interface Grouping -- A maximum 16 entries can be configured

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

Group Name	Remove	WAN Interface	LAN Interfaces
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.

Interface grouping Configuration

To create a new interface group:
1. Enter the Group name and the group name must be unique.

2. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.

3.Click Save/Apply button to make the changes effective immediately.

Group Name:

WAN Interface used in the grouping pppoe_0_1_1/ppp0.1

Grouped LAN Interfaces		Available LAN Interfaces
	->	eth0
	<-	eth1
		eth2
		eth3
		wlan0
		wl0_Guest1
		wl0_Guest2
		wl0_Guest3

Apply/Save

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.

4.2.17 IP Tunnel

4.2.17.1 IPv6 in IPv4

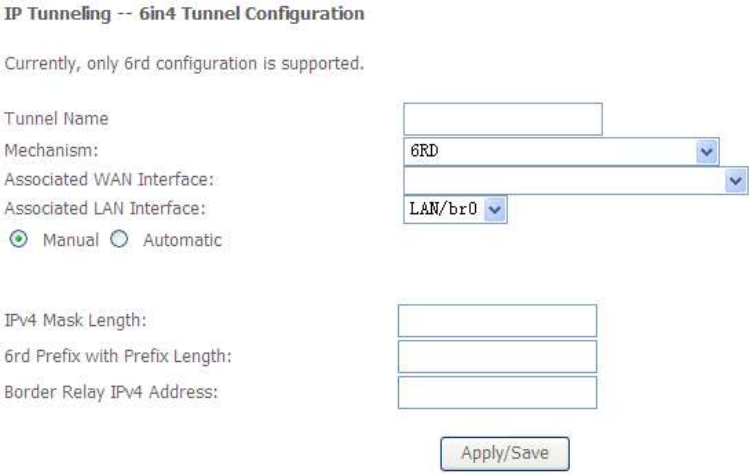
Choose **Advanced Setup > IP Tunnel** > **IPv6inIPv4** and the following page appears. The default value is IPv6 in IPv4 information.

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

Add Remove

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



4.2.17.2 IPv4 in IPv6

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

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

4.2.18 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.

4.2.19 Certificate

Local

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

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.
Notice:Import and Remove Certificate need reboot the gateway

Name	In Use	Subject	Type	Action

Create Certificate Request Import Certificate

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.

Create new certificate request

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

Certificate Name:	test
Common Name:	test
Organization Name:	test
State/Province Name:	guangdong
Country/Region Name:	CN (China)

Apply

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.

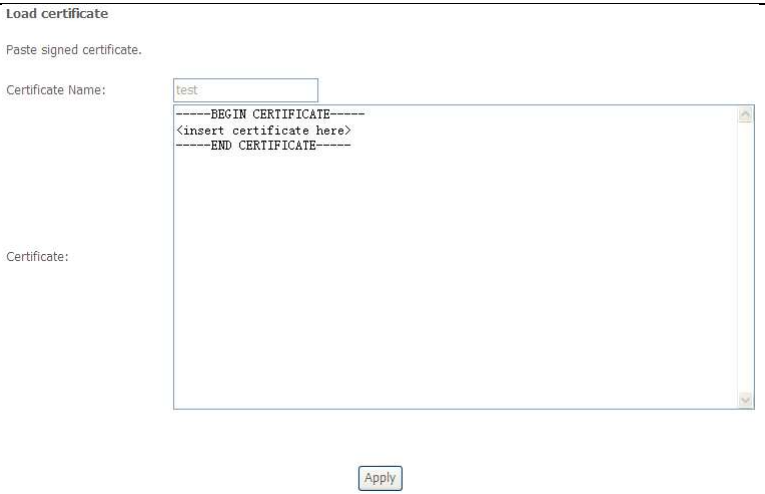
Certificate signing request

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+pgQ4aAoXjvY4k0ZskhKJTD6r4lzvIhnIfb4nNKz0H+nQkUT 1RGjAGDTefaXSRemVshjF7CZtovHHICu5/XhDKfFGvrtP7tKnUidNwIDAQABoAAw DQYJKoZIhvcNAQEEBQADgYEAL9VxsVI2XLDPYNxAlE6QiiSVRQg2Z/GiirG7BZ+6 bK2VleuqO1GFQvkzrNEqAO4DcAb+qkI2JBp6KqotucVYRHfvHf//naGM5lpxH8wN YLw9+2L+DYCaSN6P4b3Gfa6qvfo6xqiRmqA31XvFW1uIldhw9VaUbs13jDZj7x0f 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.

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

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

Private Key:

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

Apply

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.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.
Notice:Import and Remove Certificate need reboot the gateway

Name	Subject	Type	Action
acscert	O=Grupo Telefonica/O=TME/ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/CN=CA Telefonica Moviles Espana SA	ca	View Remove

Import Certificate

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

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

Import CA certificate

Enter certificate name and paste certificate content.
Notice: If certificate use for tr069, the Certificate Name must be "acscert"

Certificate Name:

Certificate:

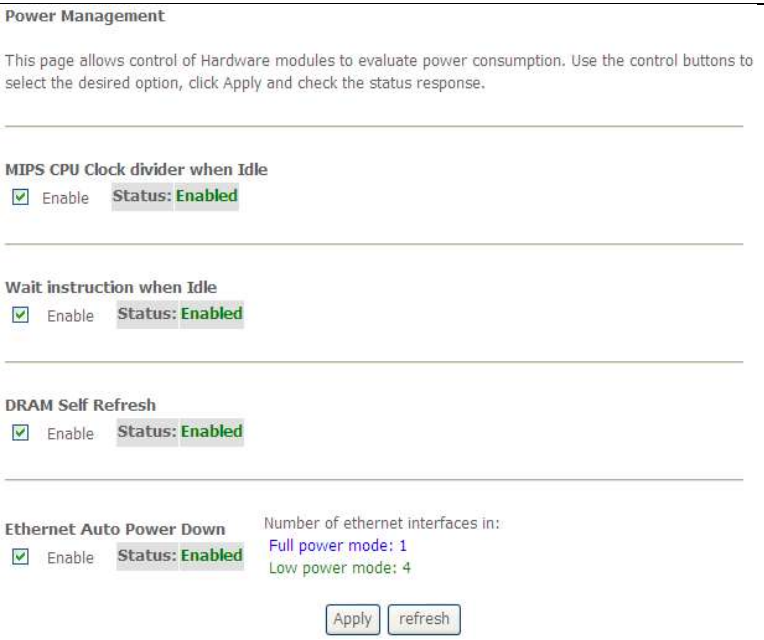
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Apply

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

4.2.20 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.

4.2.21 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.

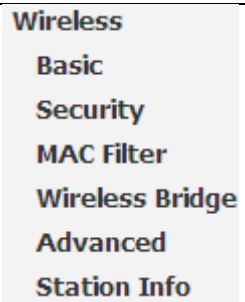
Default Version:	2
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Data Sources (for mldv2):	10
Fast Leave Enable:	☑

Apply/Save

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

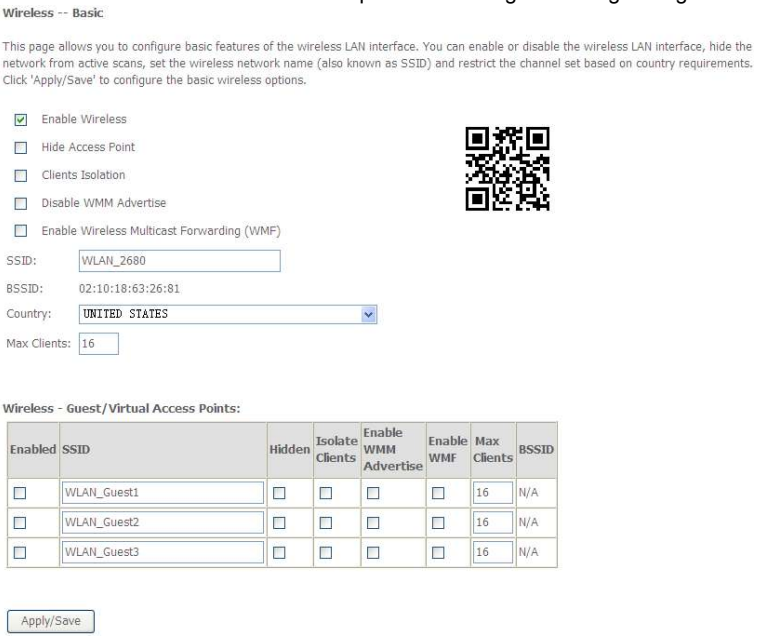
4.3 Wireless

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



4.3.1 Basic Settings

Choose **Wireless** > **Basic** to display the following page. In this page, the figure in the right area is 2-dimensional code. It includes the wireless SSID and password. You can obtain the wireless SSID and password through scanning this figure.



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

- **Enable Wireless:** Enable or disable the wireless function.
- **Hide Access Point:** if you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
- **Disable WMM Advertise:** After enabling this option, the transmission performance multimedia of the video data can be improved.
- **Enable Wireless Multicast Forwarding (WMF):** After enabling this option, the transmission quality of video service such as IPTV can be improved.
- **SSID**: For the security reason, you should change the default SSID to a unique name.
- **BSSID:** Display the MAC address of the wireless interface.
- **Country**: The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max vlaue, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

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

4.3.2 Security

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

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable **WPS** Enabled

Add **Client** (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Push-Button
Enter STA PIN Use AP PIN
Add Enrollee

Set **WPS AP Mode** Configured

Setup **AP** (Configure all security settings with an external registar)

Device PIN 21422775 Help

Config AP

Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click 'Apply/Save' when done.

Select SSID: WLAN_2680

Network Authentication: Open

WEP Encryption: Disabled

Apply/Save

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.

Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click 'Apply/Save' when done.

Select SSID: WLAN_0001

Network Authentication: Open

WEP Encryption:

Open
Shared
802.1X
WPA
WPA-PSK
WPA2
WPA2 -PSK
Mixed WPA2/WPA
Mixed WPA2/WPA -PSK

- Open Mode

Network Authentication: Open

WEP Encryption: Enabled
Encryption Strength: 64-bit
Current Network Key:
Network Key 1: 0987654321
Network Key 2: 0987654321
Network Key 3: 0987654321
Network Key 4: 0987654321

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

- **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

Network Authentication: Shared

WEP Encryption: Enabled
Encryption Strength: 64-bit
Current Network Key:
Network Key 1: 0987654321
Network Key 2: 0987654321
Network Key 3: 0987654321
Network Key 4: 0987654321

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

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

- 802.1x

Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:
WEP Encryption: Enabled
Encryption Strength: 64-bit
Current Network Key: 2
Network Key 1: 0987654321
Network Key 2: 0987654321
Network Key 3: 0987654321
Network Key 4: 0987654321

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

- **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

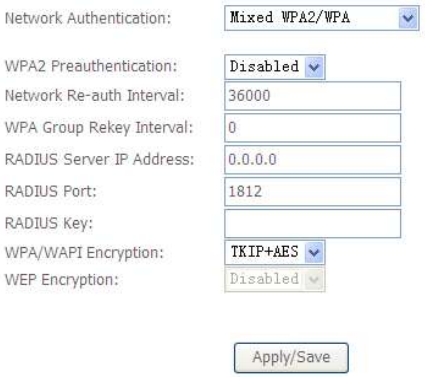
- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA2 mode.

- **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

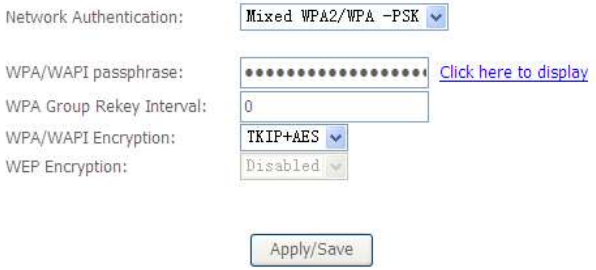
The parameters' description of WPA2-PSK mode, please refer to the **WPA-PSK mode**.

- 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**.

4.3.3 MAC Filter

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

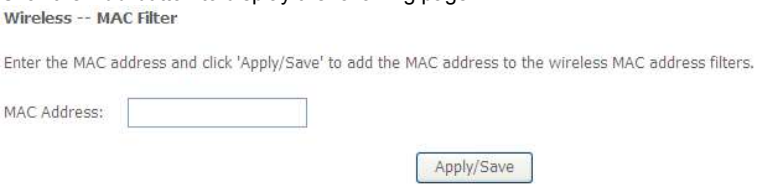
This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

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

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

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

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



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

4.3.4 Wireless Bridge

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

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode:	Access Point
Bridge Restrict:	Enabled
Remote Bridges MAC Address:	

Refresh Apply/Save

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.

4.3.5 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.

Wireless -- Advanced

This page allws you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

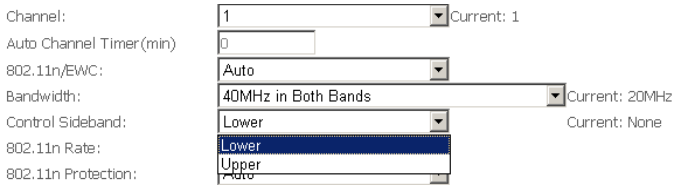
Click 'Apply/Save' to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	40MHz in Both Bands	Current: 40MHz
Control Sideband:	Lower	Current: Lower
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existance:	Disable	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress Technology:	Enable	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Apply/Save

- **Band:** You can select 2.4GHz or 5GHz.
- **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 Both Bands**, **20MHz in 2.4G Band and 40MHz in 5G Band**, or **40MHz in Both Bands.**
- **Control Sideband:** If you select **20MHz in Both Bands** or **20MHz in 2.4G Band and 40MHz in 5G Band**, the service of control sideband does not work. When you select **40MHz in Both Bands** 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.
- **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.

4.3.6 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.

4.4 Diagnostics

4.4.1 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

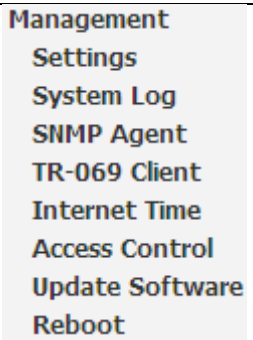
Test the connection to your Internet service provider

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

4.5 Management

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



4.5.1 Settings

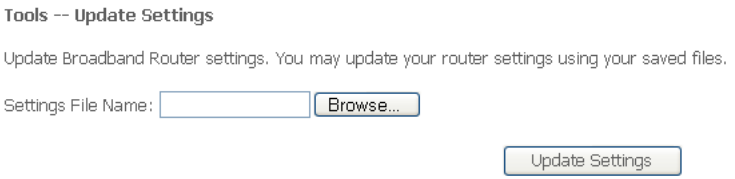
Backup

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.

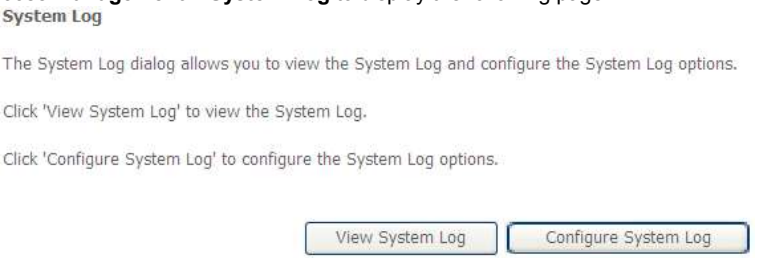
Restore Default

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.

4.5.2 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.

System Log

Date/Time	Facility	Severity	Message

Refresh Close

In this page, you can view the system log.

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

4.5.3 SNMP Agent

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

SNMP - Configuration

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

Select the desired values and click 'Apply' to configure the SNMP options.

SNMP Agent ◉ Disable ○ Enable

Read Community:	public
Set Community:	private
System Name:	Broadcom
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

Save/Apply

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.

4.5.4 TR-69 Client

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

TR-069 client - Configuration

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

Select the desired values and click 'Apply/Save' to configure the TR-069 client options.

Inform	Disable Enable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	Disable Enable
Connection Request Authentication	
Connection Request User Name:	admin
Connection Request Password:	•••••
Connection Request Port:	30005
Connection Request URL:	

Apply/Save GetRPCMethods

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.

4.5.5 Internet Time

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

Time settings

This page allows you to the modem's time configuration.

☐ Automatically synchronize with Internet time servers

Apply/Save

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.

Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server:	time.nist.gov	
Second NTP time server:	ntp1.tummy.com	
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Current Router Time: Sat Nov 19 04:32:34 2011

Time zone offset: (GMT-08:00) Tijuana, Baja California

Apply/Save

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

4.5.6 Access Control

Passwords

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

Access Control -- Passwords

Access to your DSL router is controlled through three user accounts:admin,support and user .

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 15 characters and click 'Apply/Save' to change or create passwords. Note: Password cannot contain a space.

Username:
New Username:
Old Password:
New Password:
Confirm Password:

Apply/Save

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.

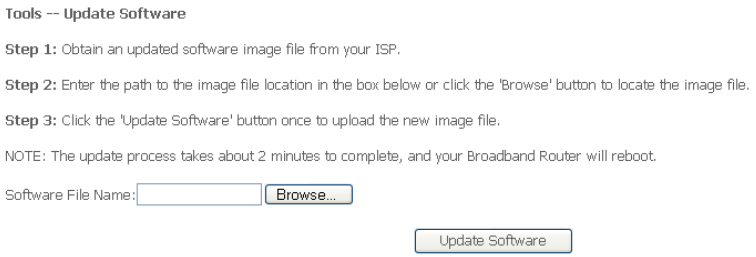
Services	LAN	WAN	Port
HTTP	☑ enable	☐ enable	80
TELNET	☑ enable	☐ enable	23
SSH	☐ enable	☐ enable	22
FTP	☑ enable	☐ enable	21
TFTP	☑ enable	☐ enable	69
ICMP	☑ enable	☐ enable	0
SNMP	☑ enable	☐ enable	161
SAMBA	☑ enable	☐ enable	445

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.

4.5.7 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.

4.5.8 Reboot

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

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

5 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**

6 Technical Support

We like to help.

Please visit our support Website or call our support specialists. Our Website has our Motorola Mentor information, and also provides returns and warranty information.

- **www.motorolanetwork.com/support**
- **Email: support@motorolanetwork.com**
- **Phone:**
- **In the US and most other countries:**
- **800-753-0797 or +1 617-753-0562**
- **UK: +44 800 023 9083**
- **Spain: +34 900 839 783**

Limited Warranty

MTRLC LLC warrants this product against defects in material and workmanship for a warranty period of 2 years. To read the full warranty, please go to **www.motorolanetwork.com/warranty**