ZHONE 6738

User Manual

VER: 1.0

Contents

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: 6RTDL01B6738. If requested, this number must be provided to the telephone company.
This equipment uses the following USOC jacks: RJ-11.

REN (RINGER EQUIVALENT NUMBERS) STATEMENT

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

ATTACHMENT LIMITATIONS STATEMENT

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

Caution:

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

IC Statement

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

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

1   Safety Precautions

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

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

1

2   Overview

The Zhone 6738 provides wireless LAN and USB services. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11b/802.11g/802.11n wireless network. The Router combines high-speed xDSL Internet connection, Ethernet uplink, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises. The Router supports 3G WAN service.

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

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

2.1   Application

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

2

- USB storage
- 3G WAN service

2.2 Features

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates, compatible with IEEE 802.11b/g/n
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Packet Transfer Mode (PTM)
- Ethernet (ETH) Transfer Mode
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Command line interface (CLI)

3

-     TR-069 WAN management protocol
-     Simple Network Management Protocol (SNMP)
● Remote update
● System statistics and monitoring
● DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.

2.3   Standards Compatibility and Compliance

● Support application level gateway (ALG)
● ITU G.992.1 (G.dmt)
● ITU G.992.2 (G.lite)
● ITU G.994.1 (G.hs)
● ITU G.992.3 (ADSL2)
● ITU G.992.5 (ADSL2+)
● ITU G.993.1 (VDSL)
● ITU G993.2 (VDSL2)
● 3G (WCDMA, CDMA2000, TD-SCDMA)
● ANSI T1.413 Issue 2
● IEEE 802.3
● IEEE 802.3u
● IEEE 802.11b
● IEEE 802.11g
● IEEE 802.11n

3   Hardware Description and Installation

📖 **Note:**

The figures in this document are for reference only.

3.1   Hardware Description

3.1.1   Front Panel
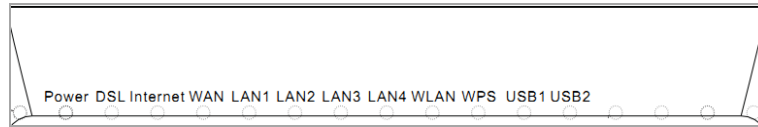
Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and the device operates normally.
		Off	The device is powered off.
	Red	On	The device is initiating.
		Blinking	The software is upgrading.
DSL	Green	On	DSL link has been established.
		Fast Blinking	The DSL line is training.
		Slow Blinking	DSL Link is turned off.
Internet	Green	On	The connection to the Internet has been established successfully in the routing pattern.
		Blinking	Internet data is being transmitted.
		Off	Ethernet interface is disconnected.
	Red	On	The Authentication is failed.
LAN	Green	On	The Ethernet link is connected.

| Indicator	Color	Status	Description
1/2/3/4		Blinking	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet link is disconnected.
WLAN	Green	On	The WLAN is enabled.
		Blinking	Data is being transmitted through the wireless interface.
		Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blinking	Negotiation is in progress under Wi-Fi Protected Setup.
		Off	Wi-Fi Protected Setup is disabled.
USB1/2	Green	On	The connection of 3G or USB flash disk has been established.
		Blinking	Data is being transmitted.
		Off	The connection of 3G or USB flash disk is not established.

3.1.2   Rear Panel and Side Panel
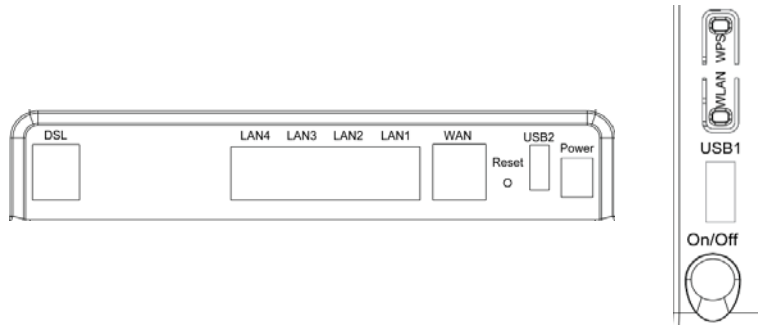
Figure 2 Rear panel

Figure 3 Side panel

The following table describes the interfaces and the buttons.

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

3.2   Hardware Installation

3.2.1 Choosing the Best Location for Wireless Operation

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

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

3.2.2 Connecting the Device

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

The spliiter has three ports:

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

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

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

The followig figure displays the connection of the DSL router, PC, and telephones.
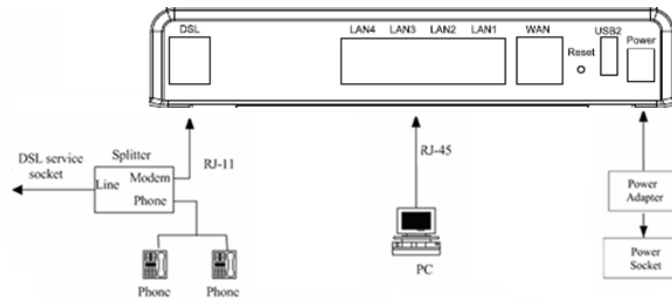
Figure 4 Connecting the DSL router

Note:

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

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

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

9

4 PC Network Configuration and Login

4.1 PC Network Configuration

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

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

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

Figure 5 IP and DNS configuration

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

Step 1   Choose **Start** > **Control Panel** > **Network Connections**.
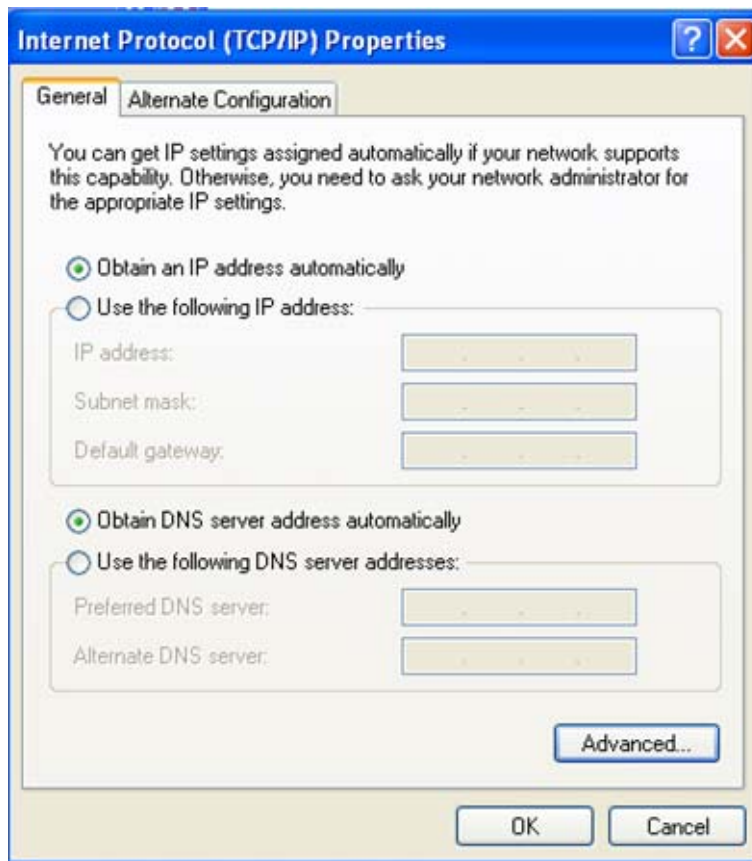
Step 2   Right-click the Ethernet connection icon and choose **Properties**.

11

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

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

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

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

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

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

4.2   Logging In to the DSL Router

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

Step 1   Open a Web browser on your computer.

Step 2   Go to *http://192.168.1.1* (the default IP address of the DSL router), and then the login page appears.

Step 3   Enter the user name and the password. The default username and password of the super user are **admin** and **admin******.(****** is the capital form of the last six digits of the MAC address pasted on the bottom pane of the modem.) The username and password of the common user are **user** and **user**. It is recommended to change these default values after logging in to the DSL router for the first time.

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

Figure 6 Login page

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

5 Web-Based Management

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

5.1 Device Information

Choose **Device Info**, and the submenu of **Device Info** is shown as below:

Device Info

Summary

WAN

Statistics

Route

ARP

DHCP

IGMP

5.1.1 Summary

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

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

5.1.2   WAN

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

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Connected Time	Action
atm0.1	br_0_8_35	Bridge	Disabled	Disabled	Disabled	Disabled	Unconfigured	0.0.0.0		/	
ppp0.2	pppoe_0_8_35	PPPoE	Disabled	Disabled	Enabled	Enabled	Unconfigured	0.0.0.0		/	

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

5.1.3 Statistics

5.1.4 LAN

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

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	1010073	7405	0	0	3333170	8333	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0
ETHWAN	0	0	0	0	0	0	0	0
wlan	54973	550	0	0	62056	443	0	0

Reset Statistics

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

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

5.1.5 WAN Service

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

16

Statistics -- WAN

Interface	Description	Connected Time	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0.1	br_0_8_35	/	0	0	0	0	0	0	0	0
ppp0.2	pppoe_0_8_35	/	0	0	0	0	0	0	0	0

Reset Statistics

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

5.1.6   xTM

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

Interface Statistics

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

Reset

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

5.1.7   xDSL

Choose **Device Info > Statistics** > **xDSL** and the following pages appear.

17

Statistics -- xDSL

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:	L3	
	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:		

Figure 7   xDSL-1

HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test   Reset Statistics

Figure 8 xDSL-2

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:

ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection.
The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): [20 ▼]

[Start] [Close]

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.

ADSL BER Test - Running

The xDSL BER test is in progress. The connection speed is 0 Kbps. The test will run for seconds.

Click "Stop" to terminate the test.

Stop   Close
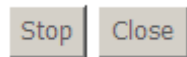
When the ADSL BER test completes, click **Stop**, the following page appears.

ADSL BER Test - Result

The ADSL BER test completed successfully.

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

Close

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

5.1.8   Route

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

Device Info -- Route

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

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

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

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

5.1.9 ARP

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

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	44:37:e6:99:43:25	br0

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

5.1.10 DHCP

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

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
dorman	00:21:6b:5e:e8:86	192.168.1.3	23 hours, 58 minutes, 5 seconds
android-3b434b30a83d3e58	30:39:26:e1:0f:e6	192.168.1.4	21 hours, 27 minutes, 34 seconds

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

5.1.11 IGMP

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

IGMP Info

Interface	State	Group Address

In this page, you can view the information of the interfaces which join in the multicast group. Group address is the IP address of the multicast group.

5.2 Quick Setup

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

24

Quick Setup

☐ Automatic Configuration

ATM PVC Configuration

VPI: [0-255]   ☐

VCI: [32-65535]   ☐

Encapsulation Mode: LLC/SNAP-BRIDGING ▼

WAN Service Configuration

Protocol: PPPoE ▼

PPP Configuration

PPP Username: ☐

PPP Password: ☐

☐ Use Static IP Address

Wireless SSID

SSID: ☐

Apply/Save

- **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).
- **Encapsulation Mode**: You can select **LLC/SNAP-BRIDGING** or **VC/MUX.**
- **Protocol**: You can select the following items from the drop-down list: **PPPoE**, **DHCP**, **PPPoA**, **IPoA** or **Bridge**.
- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Use Static IP 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.
- **SSID**: The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the router.

You can also check the checkbox of **Automatic Configuration**. Then **ATM PVC Configuration** and **WAN Service Configuration** can be configured automatically by system.

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

5.3 Advanced Setup

Choose **Advanced Setup** and the submenu of **Advanced Setup** is shown as below:

Advanced Setup
    Layer2 Interface
    WAN Service
    3G WAN Service
    Ethernet Mode
    LAN Configuration
    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

5.3.1 Layer2 Interface

ATM Interface

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

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

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

Add   Remove

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 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**: You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.

29

- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** from the drop-down lsit.
- **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.

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

PTM Interface

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

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove

Add   Remove

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

PTM Configuration

This screen allows you to configure a PTM flow.

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 Shaping Rate:		[Kbits/s] (blank indicates no shaping)
Default Queue Shaping Burst Size:	3000	[bytes] (shall be >=1600)

Back   Apply/Save

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

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.

ETH WAN Interface Configuration

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

Interface/(Name)	Connection Mode	Remove

Add   Remove

31

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

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

Note:

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

5.3.2 WAN Service

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

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

Note:

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

Adding a PPPoE WAN Service

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

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

<div align="center">

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_8_35)

Back   Next

</div>

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_8_35`

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:(IPV6 Only not support)
`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, enter the user name and password that your ISP has provided to you.

PPP Username: [   ]
PPP Password: [   ]
PPPoE Service Name: [   ]
Authentication Method: [AUTO   ▼]
MTU[576-1500]: [1400   ]

☑ Enable KeepAlive

KeepAliveTime[10-30]: [30   ] seconds
KeepAliveMaxFail[1-100]: [5   ] times
PPP Dial Up Delay Seconds [0-30]: [0   ]
(0 means random delay between 1-30 seconds)

☑ Limit Retry Time of PPP password on authentication error

Retry Time[0-100]: [3   ] times
NAT Public Ip Address(0.0.0.0 mean auto): [0.0.0.0   ]

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ Manual connect

☐ PPP IP extension

MAC Clone: [   ] [Clone the PC MAC Address]

☐ 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.
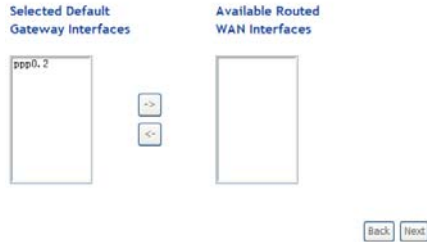
- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be **AUTO**, **PAP**, **CHAP** or **MSCHAP**. Usually, you can select AUTO.
- **MTU:** Maximum Transmission Unit. Sometimes you must modify this function to access network successfully.
- **NAT Public IP Address:** Transfer the IP address of the Lan port to the specified WAN IP address.
- **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.
- **MAC Clone:** Use the specified MAC address, click Clone the PC MAC address to get the specified MAC.
- **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.

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   Available Routed
Gateway Interfaces   WAN Interfaces

ppp0.2

->
<-

Back   Next

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
ppp0.2	-> <-	

[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:	Disabled
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]

38

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

Adding a MER (IPoE) WAN service

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

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

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
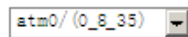portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm0/ (0_8_35)

Back   Next

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

39

WAN Service Configuration

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

Enter Service Description: | ipoe_0_8_35 |

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:(IPV6 Only not support)
| IPV4 Only ▼ |

Back Next

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 55 Request List :		(e.g:1,3,6,12)
Option 58 Renewal Time:		(hour)
Option 59 Rebinding Time:		(hour)
Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(hexadecimal digit)
Option 66:	◉ Disable	○ Enable
Option 121:	◉ Disable	○ Enable
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:
□ Enable MAC Clone

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.*

41

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).

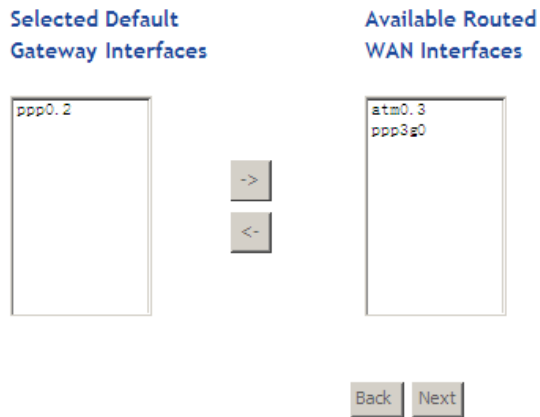☐ Enable NAT

NAT Public Ip Address(0.0.0.0 means auto): [0.0.0.0]

☐ 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.

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

ppp0.2

Available Routed WAN Interfaces

atm0.3
ppp3g0

->

<-

Back   Next

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   Available WAN
Interfaces   Interfaces

```
ppp0.2                       atm0.3
                             ppp3g0
```

`->`
`<-`

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:	Disabled
Firewall:	Disabled
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

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 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 setting, click the **Apply/Save** button to apply 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

atm1/ (0_0_37)

Back   Next

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

47

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: [   ]

PPP Password: [   ]

Authentication Method: [AUTO ▼]

MTU[576-1500]: [1400]

☑ Enable KeepAlive

KeepAliveTime[10-30]: [30]   seconds

KeepAliveMaxFail[1-100]: [5]   times

PPP Dial Up Delay Seconds [0-30]: [0]
(0 means random delay between 1-30 seconds)

☑ Limit Retry Time of PPP password on authentication error

Retry Time[0-100]: [3]   times

NAT Public Ip Address(0.0.0.0 mean auto): [0.0.0.0]

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ Manual connect

MAC Clone: [   ]   [Clone the PC MAC Address]

☐ Use Static IPv4 Address

☐ Enable PPP Debug Mode
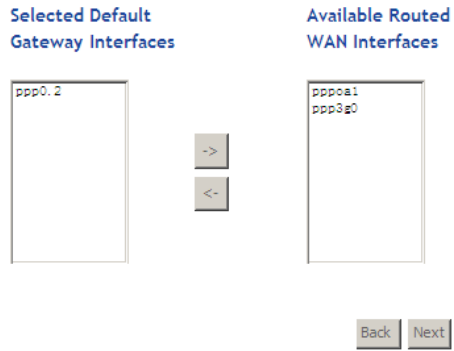
Multicast Proxy

☐ Enable IGMP Multicast Proxy

[Back] [Next]

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.

49

For the description of the field, please refer to the Step4 in **Adding a PPPoE WAN Service** of **WAN Service**.

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

ppp0.2		pppoa1
	->	ppp3g0
	<-	

Back   Next

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

ppp0.2		pppoa1
	->	ppp3g0
	<-	

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.

51

WAN Setup - Summary

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

Connection Type:	PPPoA
NAT:	Enabled
Full Cone NAT:	Disabled
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

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.

Adding a Bridge WAN

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

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

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_8_35)

Back   Next

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

WAN Service Configuration

Select WAN service type:

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

Enter Service Description: br_0_8_35

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

Enter 802.1P Priority [0-7]:   -1
Enter 802.1Q VLAN ID [0-4094]:   -1

Back   Next

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

WAN Setup - Summary

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

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

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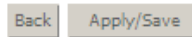
Back   Apply/Save

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

5.3.3 3G WAN Service

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

modem status NO USB CARD

Wide Area Network (WAN) Service For 3G Mobile Setup
Choose Add, Remove or Edit to configure a WAN service For 3G Mobile interface.
Help

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit	Action

Add   Remove   Information   Pin Manage   Upload Driver

55

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

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

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

3G USB mobile modem setup

☐ Enable USB Modem

User Name: `any`

Password: `•••`

Authentication Method: `AUTO`

APN: ` `

Dial Number: ` `

Idle time(in sec.): `360`

☐ Dial on demand

Dial Delay(in sec.): `10`

Default WAN Connection Select: `DSL OR ETHERNET`

WAN backup mechanism: ◉ DSL ○ IP connectivity

[Apply/Save] [Auto Setting]

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

- **Enable USB Modem:** If you want to access the Internet through the 3G network card, you must enable the USB modem.
- **User Name:** Username provided by your 3G ISP.
- **Password:** Password provided by your 3G ISP.
- **Authentication Method:** Select a proper authentication method in the drop - down list. You can select Auto, PAP, CHAP, or MSCHAP.

57

- **APN:** APN (Access Point Name) is used to identify the service type. Enter the APN provided by your 3G ISP.
- **Dial Number:** Enter the dial number provided by your 3G ISP.
- **Idle time (in sec.):** If no traffic for the preset time, the 3G will disconnect automatically.
- **Dial on demand**: Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the 3G connection. Once it detects the flow (like access to a webpage), the modem restarts the 3G dialup.
- **Dial Delay (in sec.)**: The 3G delays dial after the DSL is disconnected.
- **Default WAN Connection Select**: You can select DSL or ETHERNET or 3G from the drop-down list.
- **WAN back mechanism**: The 3G connection is the backup for the DSL connection.
    - **- DSL**: If the DSL is disconnected, the 3G starts to dial.
    - **- IP connectivity**: If the system fails to ping the specified IP address, the 3G starts to dial.

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

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

> **Note:**
>
> When there is no DSL WAN connection, insert the 3G network card, and then system will perform dial-up automatically. If the DSL WAN connection and the 3G connection coexist, the DSL WAN connection takes priority over the 3G connection. When the DSL WAN connection starts to perform dial-up, the 3G connection will be disconnected. If the DSL WAN connection has established, you may manually to perform 3G dial-up, and then the DSL WAN connection will be disconnected.

5.3.4   Ethernet Mode

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

58

Ethernet Speed Configuration

Port Name	Speed	Status
LAN1	Auto ▼	Disabled
LAN2	Auto ▼	Up
LAN3	Auto ▼	Disabled
LAN4	Auto ▼	Disabled
ETHWAN	Auto ▼	Disabled

Apply/Save

In this page, you can set speed of all the LAN and WAN interface. After setting, click Apply/Save to take the settings into effect.

5.3.5 LAN Configuration

5.3.5.1 IPv4 Configuration

Choose **Advanced Setup > LAN Configuration > IPv4 Configuration**, and the following page appears.

IPv4 Configuration

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

Group Name: 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.

- **IP Address:** You can modify the IP address of the LAN interface. The preset IP address is 192.168.1.1.
- **Subnet Mask:** Enter the subnet mask of this IP address. The preset subnet mask is 255.255.255.0.
- **Enable IGMP Snooping:** IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Only identified Multicast traffic will be forwarded to ports.
    - **Standard Mode**:
    - **Blocking Mode**:
- **Enable LAN side firewall:** Firewall can prevent unexpected traffic on the Internet from your host in the LAN.
- **Disable/Enable 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.
- **Start IP Address:** It specifies the first IP address.
- **End IP Address:** It specifies the last IP address.
- **Primary DNS server:** Enter the IP address of the primary DNS server.
- **Secondary DNS server:** Enter the IP address of the primary DNS server.
- **Lease Time (hour):** The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change. The default is 24 hours.

Editing the DHCP Option60

Click the **Edit DHCP Option60** button in the **IPv4 Configuration** page, the following page appears.

61

DHCP OPTION 60 SETUP

This page allow you to setup dhcp option 60, the dhcp server will assign one ip address based on you setting to dhcp client.

DHCP OPTION 60 TABLE:

State	deviceClassName	vendorId	minAddress	maxAddress	dnsPrimary	dnsSecondary	subnetMask	gateWay	dhcpLea

Add Edit Delete Return

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

Editing the DHCP Option

Click the **Edit DHCP Option** button in the **IPv4 Configuration** page, the following page appears.

DHCP OPtion Setup

This page allows you to configurate the DHCP OPTION. These options will be sent to DHCP client.
You can define at most 30 options.

State	Code	Value	Pool	

Add Edit Delete Return

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 **IPv4 Configuration** 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
☑	LAN1
☑	LAN2
☑	LAN3
☑	LAN4
☑	ETHWAN
☑	wl0_Guest1
☑	wl0_Guest2
☑	wl0_Guest3
☑	wlan0

Add Entries

Click the **Add Entries** button in the **IPv4 Configuration** page, the following page appears.

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: Enable this function, 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

Enter an IP address and a subnet mask for the LAN interface.
After finishing setting, click the **Apply/Save** button to apply the settings.

5.3.5.2   IPv6 Configuration

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

IPv6 Configuration
Note:
   1: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64.
Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.
For exampe: Please enter "0:0:0:2" instead of "::2".

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

☐ **Enable Unique Local Addresses And Prefix Advertisement**
○ Randomly Generate
○ Statically Configure
    Address: [＿＿＿＿＿＿] (e.g: fd80::1/64)
    Prefix: [＿＿＿＿＿＿] (e.g: fd80::/64)
    Preferred Life Time (hour): [＿＿＿＿＿＿]
    Valid Life Time (hour): [＿＿＿＿＿＿]

IPv6 LAN Applications
☑ Enable DHCPv6 Server and RADVD
◉ Stateless
○ Stateful
    Start interface ID: [0:0:0:2]
    End interface ID: [0:0:0:254]
    Leased Time (hour): [24]

☑ Enable MLD Snooping

○ Standard Mode
◉ Blocking Mode

[Save/Apply]

In this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.
● **Enable Unique Local Addresses and Prefix Advertisement:** Unique Local Addresses is used to control CPE in the LAN. Enable this function is to broadcast proxy prefix to the LAN. So the PC in this LAN can obtain the required information like gateway and DNS to generate global address to access the internet.

● **Enable DHCPv6 Server and RADVD:** 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. The router advertisement daemon (RADVD) is running Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.

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

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

5.3.5.3   LAN VLAN Setting

Click **Advanced Setup > LAN Configuration > LAN VLAN Setting**, and the following page appears.

In this page, you can set a VLAN for the specified LAN port, then bundle this LAN port with a certain WAN interface. The packet with configured VLAN value will be transmitted from the bundled WAN interface.

5.3.6 NAT

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 or 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.

Click Add button in this page and the following page appears.

NAT -- Virtual Servers

Select the service name, and enter the server IP address or hostname, 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_8_35/ppp0.2 ▾
Service Name:
⦿ Select a Service: Select One   ▾
○ Custom Service: [   ]
☐ Enable LAN Loopback

Server IP Address or 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.

68

- **Custom Server**: Enter a new service name to establish a user service type.
- **Server IP Address or Hostname**: Assign an IP address to virtual server.
- **Status**: You can choose **Enable** or **Disable** from the drop-down list.
- **External Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Protocol**: You may select **TCP/UDP**, **TCP** or **UDP** in the drop-down list.
- **Internal Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

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

Port Triggering

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

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

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

69

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_8_35/ppp0.2

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.

70

- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

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

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

DMZ Host

DMZ allows all the ports 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.

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP
Address:

☐ Enable LAN Loopback

Apply/Save

71

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.

ALG

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

ALG

Select the ALG below.

☑ SIP Enabled
☑ FTP Enabled
☑ H323 Enabled
☑ PPTP Enabled
☑ RTSP Enabled
☑ TFTP Enabled

Save/Apply

In this page, you can enable a variety of functions from the list.

5.3.7 Security

Firewall

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

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

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

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

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

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

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

MAC Filtering

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

Note:

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

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**(maximun 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_8_35/atm0.1

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 the settings, click **Apply/Save** to save and apply the filtering rules.

5.3.8 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.

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

User Name

○ Browser's MAC Address   44:37:e6:99:43:25

○ Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Apply/Save

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.

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

Add   Remove

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

78

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

5.3.9 Quality of Service

Choose **Advance Setup > Quality of Service**, select **Enable OoS** in this page 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

Select Default DSCP Mark No Change (-1) ▼

Apply/Save

In this page, you can configure the default DSCP mark. After setting, click **Apply/Save** to save and apply the settings.

Note:

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

QoS Queue

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	wlan0	0	1/SP					Enabled	
WMM Voice Priority	2	wlan0	0	2/SP					Enabled	
WMM Video Priority	3	wlan0	0	3/SP					Enabled	
WMM Video Priority	4	wlan0	0	4/SP					Enabled	
WMM Best Effort	5	wlan0	0	5/SP					Enabled	
WMM Background	6	wlan0	0	6/SP					Enabled	
WMM Background	7	wlan0	0	7/SP					Enabled	
WMM Best Effort	8	wlan0	0	8/SP					Enabled	
Default Queue	33	atm0	1	8/WRR/1	Path0				☐	

Add   Enable   Remove

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

Note:

81

The lower integer value for precedence indicates the higher priority.

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

- **Name:** Enter the name of QoS queue.
- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

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

QoS Classification

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

In this page, you can enable, add or remove a QoS classification rule.
Click the **Add** button to display the following page

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]

In this page, you can create a traffic class rule and mark the DSCP or Ethernet priority of the packet.
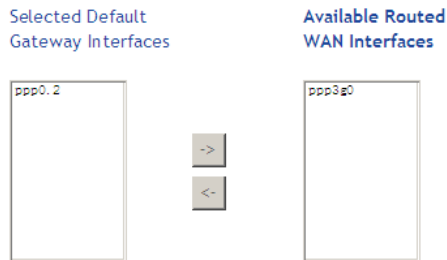
83

5.3.10 Routing

Default Gateway

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

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 highest 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   **Available Routed**
Gateway Interfaces   **WAN Interfaces**

ppp0.2   ppp3g0

->

<-

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

Selected WAN Interface   NO CONFIGURED INTERFACE

Apply/Save

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.

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/Mask	Gateway	Interface	Metric	Remove

Add   Remove

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

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

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.

IP Version:	IPv4
Destination IP address/prefix length:	
Interface:	
Gateway IP Address:	

(optional: metric number should be greater than or equal to zero)

Metric:	

Apply/Save

- **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.

85

Policy Routing

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

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

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

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

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

RIP

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

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
atm0.1	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 setting, click **Apply/Save** to save and apply the settings.

5.3.11　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	Available WAN Interfaces
ppp0.2	ppp3g0

->
<-

○ **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.

5.3.12   Dynamic DNS

Choose **Advanced Setup > 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_8_35/ppp0.2 ▼

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 for the packets to 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.

89

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

5.3.13 DSL

Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM. If you select **VDSL2 Enabled** check box, you can set the VDSL2 parameters on the right area.

90

DSL Settings

Select the modulation below.   Select the profile below.

☑ G.Dmt Enabled   ☑ 8a Enabled
☑ G.lite Enabled   ☑ 8b Enabled
☑ T1.413 Enabled   ☑ 8c Enabled
☑ ADSL2 Enabled   ☑ 8d Enabled
☑ AnnexL Enabled   ☑ 12a Enabled
☑ ADSL2+ Enabled   ☑ 12b Enabled
☐ AnnexM Enabled   ☑ 17a Enabled
☑ VDSL2 Enabled

                                               US0
                                               ☑ Enabled

Capability
        ☑ Bitswap Enable
        ☐ SRA Enable
        ☐ SESdrop Enabled
        ☐ PhyR Upstream Enabled
        ☑ PhyR Downstream Enabled

                    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.

5.3.14 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.

☑ Enable UPnP

Apply/Save

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

5.3.15 DNS Proxy

Basic Configuration

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

DNS Proxy Basic Configuration

☑ Enable DNS Proxy

Host name of the Broadband Router: Zhone

Domain name of the LAN network: Home

Apply/Save

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.

Server Configuration

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

In this page, you can add or remove a local host. Click **Add Local Host**, the following page appears.

In this page, you need to enter a domain name and IP address for the new local host.

5.3.16 Print Server

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

Print Server settings

This page allows you to enable / disable printer support.

☑ Enable on-board print server.

Printer name   [   ]
Make and model   [   ]
http://192.168.1.1:631/printers

Apply/Save

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

5.3.17   DLNA

Choose **Advanced Setup > DLNA** and enable the **on-board digital media server** function, the following page appears. In this page, enter the **media library path** to run digital media server.

Digital Media Server settings

This page allows you to enable / disable digital media server support.

☑ Enable on-board digital media server.

Interface Default ▼

Media Library Path /mnt/usb1_1

Apply/Save

5.3.18 Packet Acceleration

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

Packet Acceleration

☑ Enable Packet Flow Accelerator

Apply/Save

5.3.19 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.

User Accounts

Choose **Advanced Setup** > **Storage Service** > **User Accounts** and the following page appears.

Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	HomeDir	Remove

Add   Remove

In this page, you can add or remove a storage user account.
Click **Add,** and the following page appears.

96

Storage User Account Setup

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.
Username and Password must consists of [A-Z] or [a-z] or [0-9].

Username: [＿＿＿＿＿]
Password: [＿＿＿＿＿]
Confirm Password: [＿＿＿＿＿]
VolumeName: [＿＿＿＿＿]

[Apply/Save]

In this page, you can set the user name and password of the storage account and a volume name.

5.3.20 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		atm0.1	LAN1
		ppp0.2	LAN2
			LAN3
			LAN4
			ETHWAN
			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.

99

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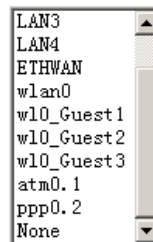
To create a new interface group:
1. Enter the Group name and the group name must be unique.

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: [   ]

Grouped LAN Interfaces   **Available LAN Interfaces**

```
LAN3
LAN4
ETHWAN
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3
atm0.1
ppp0.2
None
```

[->]
[<-]

[Apply/Save]

100

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

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

5.3.21 IP Tunnel

IPv6 in IPv4

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

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.

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name	
Mechanism:	6RD
Associated WAN Interface:	
Associated LAN Interface:	LAN/br0
⦿ Manual ○ Automatic	
IPv4 Mask Length:	
6rd Prefix with Prefix Length:	
Border Relay IPv4 Address:	

Apply/Save

101

● **IPv4 Mask Length**: The value is 0 ~ 32.

● **6rd Prefix with Prefix Length**: prefix/length, such as: 2002::/64.

Enter the field with proper parameters as follow for example:

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name	tunnel4
Mechanism:	6RD
Associated WAN Interface:	pppoe_0_1_1.3333/ppp0.1
Associated LAN Interface:	LAN/br0

◉ Manual ○ Automatic

IPv4 Mask Length:	24
6rd Prefix with Prefix Length:	2002::/64
Border Relay IPv4 Address:	10.10.10.11

Apply/Save

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

IP Tunneling -- 6in4 Tunnel Configuration

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

Remove

5.3.21.1   IPv4 in IPv6

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

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote IPv6 Address	Remove

Add   Remove

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

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

⦿ Manual ○ Automatic

Remote IPv6 Address:

Apply/Save

5.3.22   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

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, you can set the parameters such as the **IPSec connection name**, **tunnel mode**, and **remote IPSec gateway address**.

104

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

5.3.23 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:	guandong
Country/Region Name:	US (United States)

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=US
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBfjCB6AIBADA/MQ0wCwYDVQQDEwR0ZXN0MQ0wCwYDVQQKEwR0ZXN0MRIwEAYD VQQIEwlndWFuZ2RvbmcxCzAJBgNVBAYTA1VTMIGfMA0GCSqGSIb3DQEBAQUAA4GN ADCBiQKBgQDbC7FMcqcHRi/Lgs790b7hdM+DcO1zmJnOu11QTg2wIkJ9wU7IQsvZ qtb0Y2dTJSSNTxuLxKTtuLOImPu2vtEgxZ6IPjcIIsONtRJrOiOK7TX2YCYpQBMT nf5uIMfYog4W5r2Tfkeo3d1uabZdfoCa9vVi/g3zQ+cyHTvz6MoYkQIDAQABoAAw DQYJKoZIhvcNAQEEBQADgYEAQ+k7cNfMAFWsxSj2LGISpbOQ4rf5OONmLwN7n5Un wKW+ORp1S7n9ezUCJ2YwrPHLDKzOfEVO9RE/aDIOHB4ifZRCjpP879rFgT6c1tjo MGSct1Gzs0Z3uuOR9Q+wCKJchPv1OtI3HEfO/uFQYEnnLOgXjOomKkQTROLMrgWk JU4= -----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.

Load certificate

Paste signed certificate.

Certificate Name: test

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

Apply

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.

Load certificate

Paste signed certificate.

Certificate Name: test

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

Certificate:

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

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.

5.3.24   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.

Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle
☑ Enable   Status: Enabled

Wait instruction when Idle
☑ Enable   Status: Enabled

DRAM Self Refresh
☑ Enable   Status: Enabled

Ethernet Auto Power Down   Number of ethernet interfaces in:
☑ Enable   Status: Enabled   Full power mode: 6
                                     Low power mode: 4

Apply   refresh

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

5.3.25 Multicast

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

111

IGMP Configuration View

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:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☐
Mebership Join Immediate (IPTV):	☐

MLD Configuration View

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:	☑

In this page, you can configure the multicast parameters.

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

5.4 Wireless

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

Wireless

    Basic

    Security

    MAC Filter

    Wireless Bridge

    Advanced

    Station Info

5.4.1 Basic Settings

Choose **Wireless** > **Basic** to display the following page. In this page, the figure on 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.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click 'Apply/Save' to configure the basic wireless options.

☑ Enable Wireless
☐ Hide Access Point
☐ Clients Isolation
☐ Disable WMM Advertise
☐ Enable Wireless Multicast Forwarding (WMF)

SSID: Zhone010000

BSSID: 22:10:18:63:26:80

Country: UNITED STATES

Max Clients: 16

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Enable WMM Advertise	Enable WMF	Max Clients	BSSID
☐	WLAN_Guest1	☐	☐	☐	☐	16	N/A
☐	WLAN_Guest2	☐	☐	☐	☐	16	N/A
☐	WLAN_Guest3	☐	☐	☐	☐	16	N/A

Apply/Save

This page allows you to configure the basic features of the wireless LAN interface.
● **Enable Wireless:** Enable or disable the wireless function.
● **Hide Access Point:** if you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive scanning.

- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
- **Disable WMM Advertise:** After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
- **Enable Wireless Multicast Forwarding (WMF):** After enabling this option, the transmission quality of video service such as IPTV can be improved.
- **SSID**: For the security reason, you should change the default SSID to a unique name.
- **BSSID:** Display the MAC address of the wireless interface.
- **Country**: The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max vlaue, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

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

5.4.2   Security

Choose **Wireless** > **Security,** enable the WPS function in this page. The page is shown as the following figure appears. This page allows you to configure the security 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.

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   [16986640   ]   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: [Zhone010000 ▼]

Network Authentication: [Open   ▼]

WEP Encryption: [Disabled ▼]

                    [Apply/Save]

116

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

● **Push button**: An actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

● 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.

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.

● **Set WPS AP Mode:** You can choose **Configured** or **Unconfigured**.

● **Device PIN:** WPS has three access modes: Button, STA PIN and AP PIN. Device pin is the pin code of AP PIN.

● **Select SSID:** Select a SSID for configuring the security settings.

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

   - Open Mode: No password is needed for the SSID connection.
   - Shared Mode

117

Network Authentication: Shared

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

● **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.

- 802.1x

- **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

- **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

- **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

Network Authentication: WPA2

WPA2 Preauthentication: Disabled

Network Re-auth Interval: 36000

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Apply/Save

- **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

124

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

5.4.3   MAC Filter

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

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

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

There are three MAC restrict modes: **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.

Wireless -- MAC Filter

Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.

MAC Address: [   ]

Apply/Save

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

5.4.4   Wireless Bridge

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

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 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:

                                Apply/Save

This page allows you to configure the wireless bridge 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 the settings, click the **Apply/Save** button to save and apply the settings.

5.4.5 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.

127

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.

Field	Value	
Band:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz/40MHz	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

128

This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.

Note:

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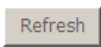
5.4.6   Station Info

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
00:26:5A:08:E3:25	Yes		Zhone010000	wl0

Refresh

This page shows the authenticated wireless stations and their status.

5.5   Diagnostics

5.5.1   Diagnostics

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

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

br_0_8_35 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Test With OAM F4" 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 LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your ETHWAN Connection:	FAIL	Help
Test your USB Connection:		Help
Test your Wireless Connection:	PASS	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

Next Connection

Test   Test With OAM F4

5.5.2　Fault Management

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

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

802.1ag Connectivity Fault Management

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:	2 ▾
Destination MAC Address:	
802.1Q VLAN ID: [0-4095]	0

VDSL Traffic Type:	Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):	

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

Set MD Level   Send Loopback   Send Linktrace

5.6   Management

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

Management

Settings

System Log

SNMP Agent

TR-069 Client

Internet Time

Access Control

Update Software

Reboot

Tools

5.6.1 Settings

Backup

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

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

☐ Backup configurations without user accounts and passwords information

Backup Settings

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

132

Update

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

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: [_____] Browse...

Update Settings

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

Restore Default

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

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Restore Default Settings

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

5.6.2   System Log

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

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click 'View System Log' to view the System Log.

Click 'Configure System Log' to configure the System Log options.

| View System Log | Configure System Log |

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.

System Log -- Configuration

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

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ⊙ Disable ○ Enable

Log Level: Debugging
Display Level: Error
Mode: Local
                Local
                Remote
                Both

                                    Apply/Save

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.

134

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

Note:

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

● **View System Log**

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

In this page, you can view the system log.

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

5.6.3 SNMP Agent

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

135

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.

5.6.4 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.

5.6.5 Internet Time

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

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

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

138

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 08:36:17 2011
Interval: Every 0 Minutes

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.

5.6.6 Access Control

Passwords

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

Access Control -- Passwords

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

    📖   **Note:**

       Password cannot contain a space.

Services Control

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
FILE SHARING	☑ enable	☐ enable	445

Apply/Save

In this page, you can enable or disable the different types of services.

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

IP Addresses

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

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ⊙ Disable ○ Enable

IP Address	Subnet Mask	Remove

Add   Remove

In the page, you can enable or disable the IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

5.6.7   Update Software

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

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

Step 3: Click the 'Update Software' button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: [_____] Browse...

Update Software

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

Note:
When software update is in progress, do not shut down the router. After software update completes, the router automatically reboots.
Please make sure that the new software for updating is correct, and do not use other software to update the router.

5.6.8   Reboot

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

Click the button below to reboot the router.

Reboot

In this page, click the **Reboot** button. You can reboot the button.

5.6.9　Tools

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

Ping and Trace Route

You can use ping and trace route in this page.

Please input the IP address and click "Ping" or "Trace Route".

IP Address: 　　　　　［　　　　　　　　　　　］

Ping　.　Trace Route

In this page, enter the IP address. The Ping package sent by the moderm would be transmitted to the IP address you entered here.you can view the Ping result by click **Ping**. If you click **Trace Route**, you can view the trace route result of moderm to specified IP address.

6   Q&A

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

   A: Check the following:

   ● The connection between the power adaptor and the power socket.

   ● The status of the power switch.

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

   A: Check the following:

   ● The connection between the ADSL router and your computer, hub, or switch.

   ● The running status of your PC, hub, or switch.

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

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

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

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

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

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

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

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

   ● User/password of super user: **admin**/**admin******** (****** is the capital form of the last six digits of the MAC address pasted on the bottom pane of the modem.)

   ● User/password of common user: **user**/**user**

145