HT-178 User Manual

VER: 1.0

Contents

1 Safety Precautions

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

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

2 Overview

The Router is designed to provide a simple and cost-effective Internet connection for a private Ethernet. The Router combines high-speed Internet connection, IP routing for the LAN connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The connection is made using ordinary telephone line with standard connectors. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

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

2.2 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
- 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 PPPoE sessions
- Support RIP v1 & RIP v2
- IP routing and bridging
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Universal plug-and-play(UPnP)
- Web filtering
- Management and control

Web-based management (WBM)

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u

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.

USB	Functions
Green	Device connected
Green blinking	DATA

Lan ports	Functions
Green	link/act
Green blinking	Blinking speed will adapt According to transferring DATA

SFP	Functions
Green	link/act

Wan ethernet	Functions
Green	link/act
Green blinking	Blinking speed will adapt According to transferring DATA

Internet	Functions
Green	Connected
Red	authentication failed/no asnwer from DHCP(connection without dialer)

FXS	Functions
Green	Line is registered
Green **Slow** blinking	Calling, Talking, Ringing

POWER	Functions
Green	Start complete
Red	In CFE mode

2.4G WIRELESS	Functions
Green	Function open
Green off	Function close
Green blinking	DATA

5G WIRELESS	Functions
Green	Function open
Green off	Function close
Green blinking	DATA

3.1.2 Rear Panel and Side Panel

Figure 2 Rear Panel

Figure 3 Side panel

The following table describes the interfaces or the buttons.

Interface	Description
LAN	RJ-45 port, for connecting the router to a PC or another network device.
USB3.0	Connect the devices to router through USB port.
WAN	Device management port
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.
Power	Power interface, for connecting the power adapter.
On/Off	Power switch.

Interface	Description
SFP	Insert SFP module to access network through fiber optic cable
WiFi	Wifi switch

⚠ **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.*

3.1.3 Connecting the Device

Step 1 Connect the **WAN** port of the router with a telephone cable.

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.

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 .
The IP address should be set 10.10.0.X.

4.2 Logging In to the Router

To log in to the Router, do as follows:

Open a Web browser on your computer.

Enter ***https://100.100.100.100*** (the default IP address of the Router) in the address bar. The login page appears.

Enter the the password. It should be the last six digits of SN

Figure 4 Login page

After logging in to the 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 Router, which allows you to configure and control all of Router features and system parameters in a user-friendly GUI.

5.1 Device Information

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

5.1.1 Summary

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

Device Info

Board ID:	BCM963178DVT_Hs
Model Name:	HT-178AX-V2-INT
MAC Address:	00:B8:C2:D8:0F:00
Serial Number:	HT123456789
Build Timestamp:	20230504_1422
Software Version:	2.0.0.9-HT-178AX-V2-OS-INT-debug
Bootloader Version:	U-Boot 2019.07
DSL PHY and Driver Version:	A2pv6L047f1.d27n
Wireless Driver Version:	17.10.188.75
Voice Service Version:	Voice
Uptime:	0D 0H 1M 47S
Certificate validity period:	**Jan 1 18:22:10 2033 GMT**

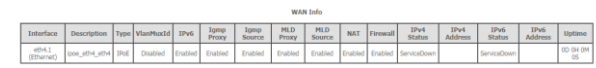
This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	100000
Line Rate - Downstream (Kbps):	100000
LAN IPv4 Address:	192.168.40.1
Default Gateway:	eth4.1 (Ethernet)
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	4.4.4.4
LAN IPv6 ULA Address:	
LAN IPv6 Global Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Mar 28 10:15:26 2024

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

5.1.2 WAN

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



WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Proxy	Igmp Source	MLD Proxy	MLD Source	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address	Uptime
eth4.1 (Ethernet)	ipoe_eth4_eth4	IPoE	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	ServiceDown		ServiceDown		0D 0H 0M 0S

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&WLAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	5091	29	0	0	4256	25	0	4	8494	118	0	0	8430	117	0	1
wl1.1	0	0	0	0	0	0	0	0	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 Ethernet.

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

5.1.5 WAN Service

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

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth4.1	cpe-ipintf-4	346165	2807	0	0	15941	94	2658	55	3220857	4616	0	0	648	8	4607	1

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. 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	Interface
100.100.100.0	0.0.0.0	255.255.255.0	U	0	eth4.1
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.

5.1.6 xTM

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

Interface Statistics

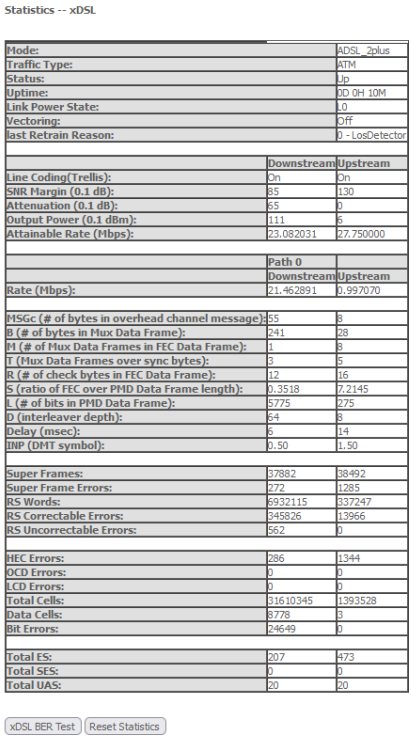
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
0	448539	742	0	5	1	0	0	0	0	8463

Reset

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

5.1.7 xDSL

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



Statistics -- xDSL

Mode:		ADSL_2plus
Traffic Type:		ATM
Status:		Up
Uptime:		0D 0H 10M
Link Power State:		L0
Vectoring:		Off
last Retrain Reason:		0 - LosDetector
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	85	130
Attenuation (0.1 dB):	65	0
Output Power (0.1 dBm):	111	6
Attainable Rate (Mbps):	23.082031	27.750000
	Path 0	
	Downstream	Upstream
Rate (Mbps):	21.462891	0.997070
MSGc (# of bytes in overhead channel message):	55	8
B (# of bytes in Mux Data Frame):	241	28
M (# of Mux Data Frames in FEC Data Frame):	1	8
T (Mux Data Frames over sync bytes):	3	5
R (# of check bytes in FEC Data Frame):	12	16
S (ratio of FEC over PMD Data Frame length):	0.3518	7.2145
L (# of bits in PMD Data Frame):	5775	275
D (interleaver depth):	64	8
Delay (msec):	6	14
INP (DMT symbol):	0.50	1.50
Super Frames:	37882	38492
Super Frame Errors:	272	1285
RS Words:	6932115	337247
RS Correctable Errors:	345826	13966
RS Uncorrectable Errors:	562	0
HEC Errors:	286	1344
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	31610345	1393528
Data Cells:	8778	3
Bit Errors:	24649	0
Total ES:	207	473
Total SES:	0	0
Total UAS:	20	20

xDSL BER Test | Reset Statistics

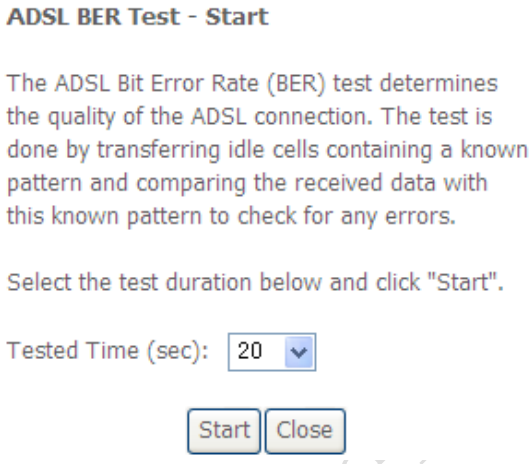
In this page, you can view the statistical information about the recevied and transmitted data packets of the xDSL interfaces.

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

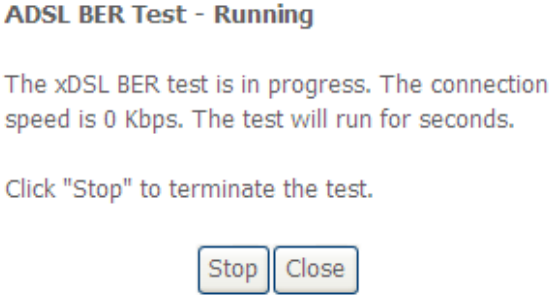
Click **Reset Statistics** to restore the values to zero and recount them.

xDSL BER Test

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



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



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

ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000001B69B580
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 ARP

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

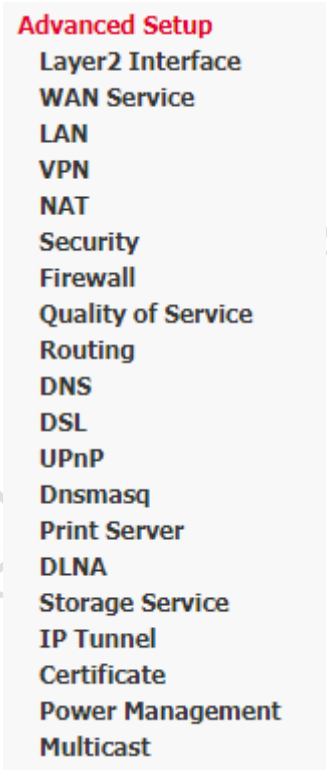
Device Info -- ARP

IP address	Flags	HW Address	Device
100.100.100.106	Complete	48:02:2a:f0:92:a3	eth4.1

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

5.2 Advanced Setup

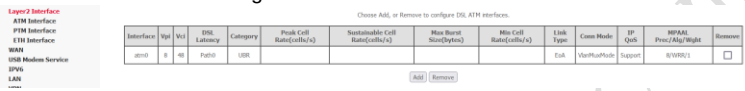
Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown as below:



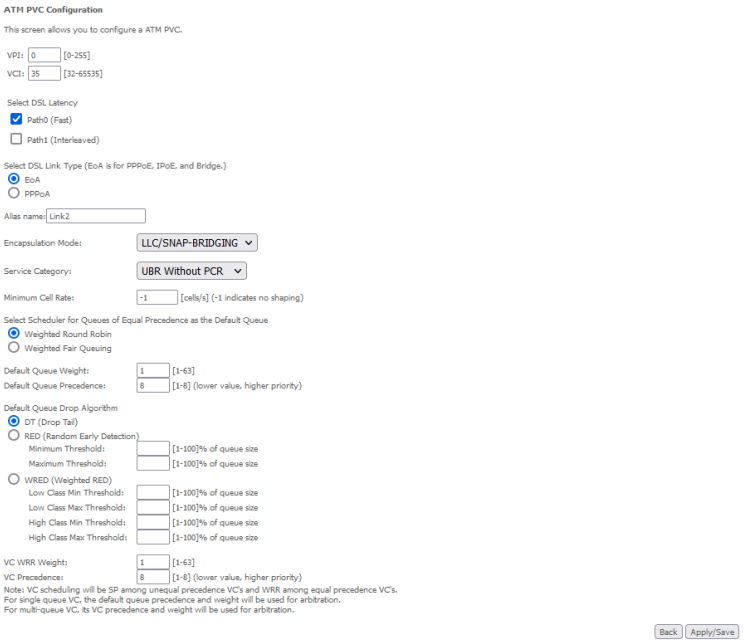
5.2.1 Layer2 Interface

5.2.1.1 ATM Interface

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



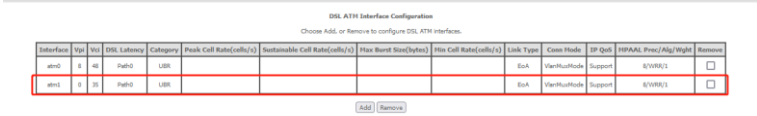
Click **Add** to add ATM Interface and the following page appears.



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

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **DSL Link Type**: EoA (it is for PPPoE, IPoE, and Bridge), PPPoA, or IPoA
- **Encapsulation Mode**: LLC/SNAP-BRIDGING, or VC/MUX
- **Service Category:** UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR.
- **Select Scheduler for Queues of Equal Precedence as the Default Queue**: Weighted Round Robin or Weighted Fair Queuing.

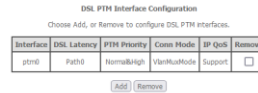
Click **Apply/Save** to save the configuration, and return the following page:



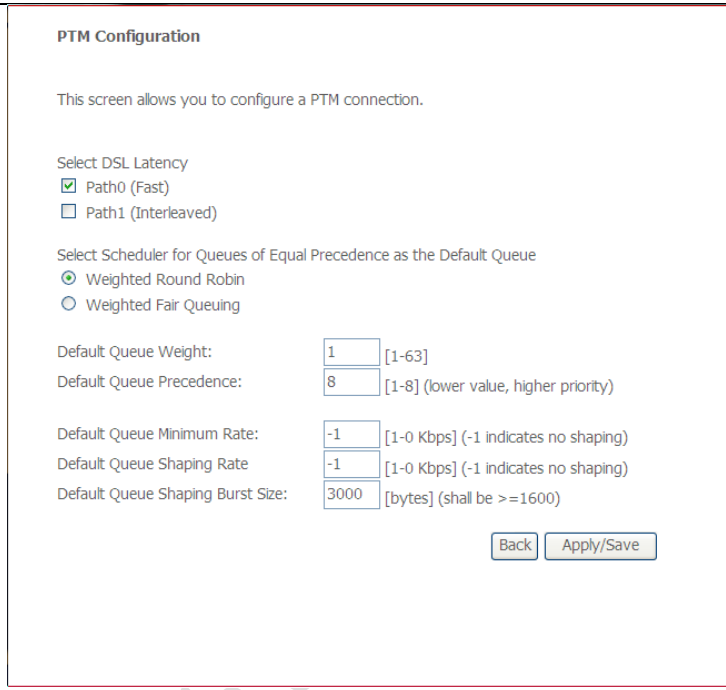
If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

5.2.1.2 PTM Interface

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

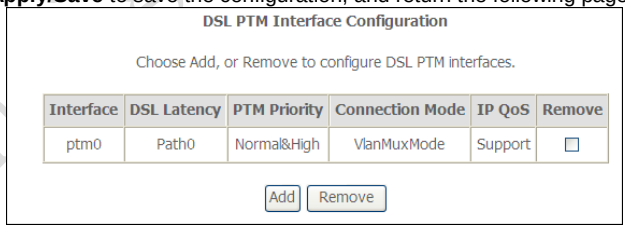


Click **Add** to add PTM Interface and the following page appears.



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

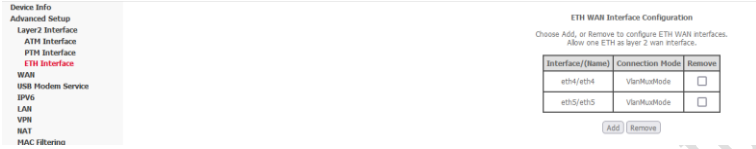
Click **Apply/Save** to save the configuration, and return the following page:



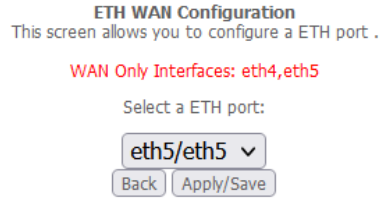
If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

5.2.1.3 ETH Interface

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

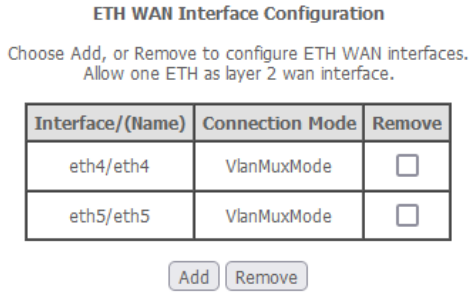


Click **Add** to add ETH Interface and the following page appears.



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

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



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

5.2.2 WAN Service

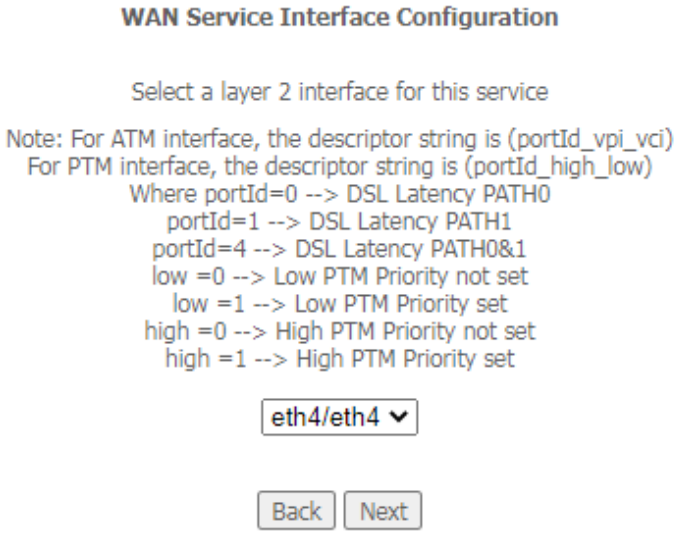
Choose **Advanced Setup** > **WAN Service,** and the following page appears.

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

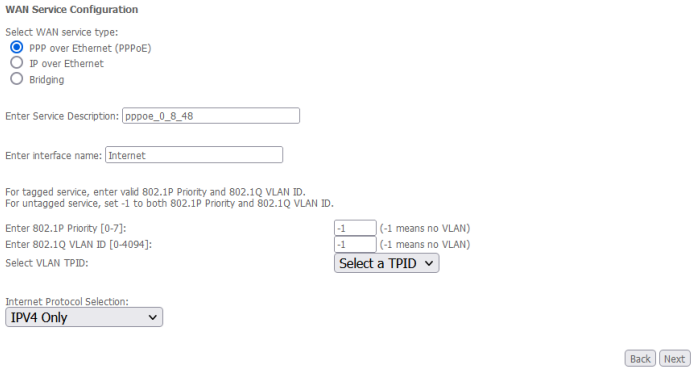
5.2.2.1 Adding a PPPoE WAN Service by GUI

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

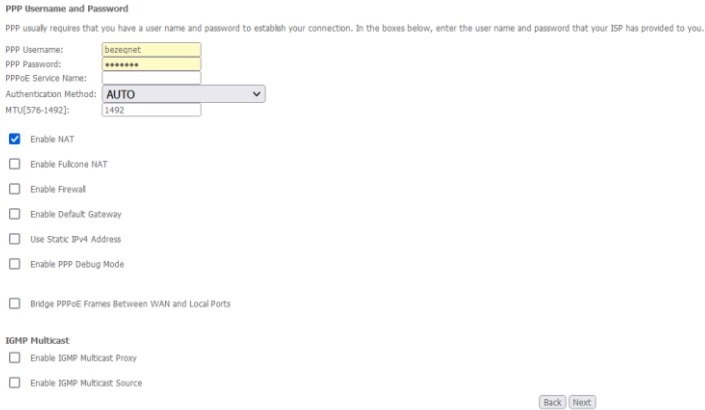
Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM interface for this WAN service.)



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



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

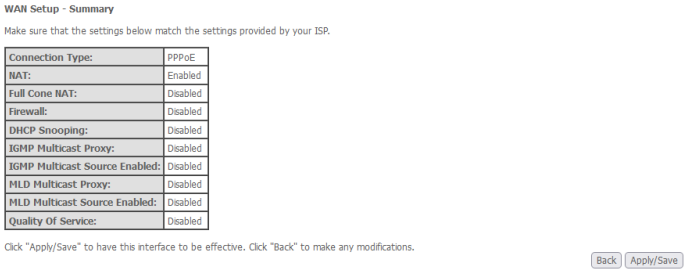


Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

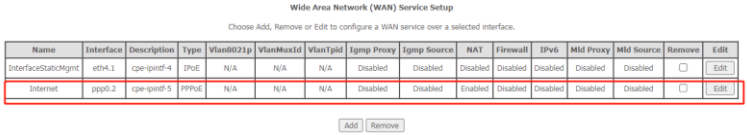
- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.

- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable 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.
- **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.
- **Enable Firewall :** Used to control whether remote access is allowed
- **Enable Default Gateway :** Set that wan connection as the default gateway
- **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.
- **Enable IGMP Multicast Source: i**f enable it, allow this interface accept the Multicast Source.

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



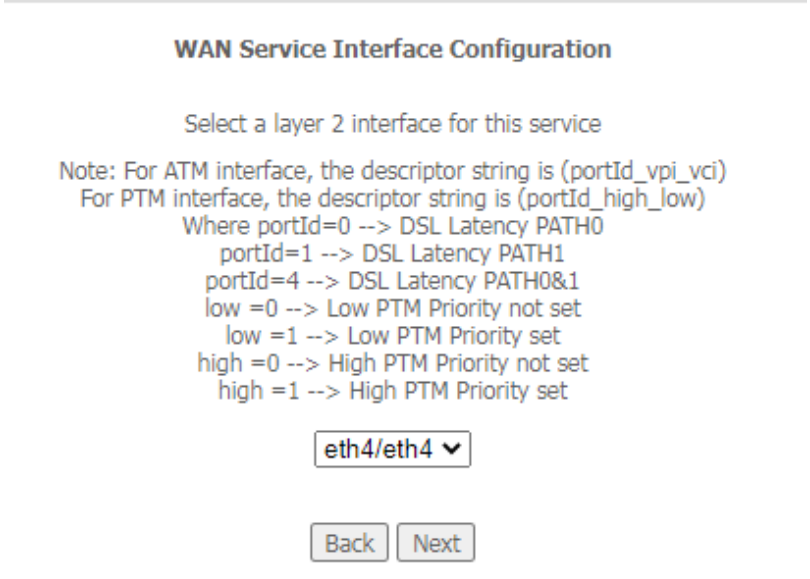
Step6 In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings.



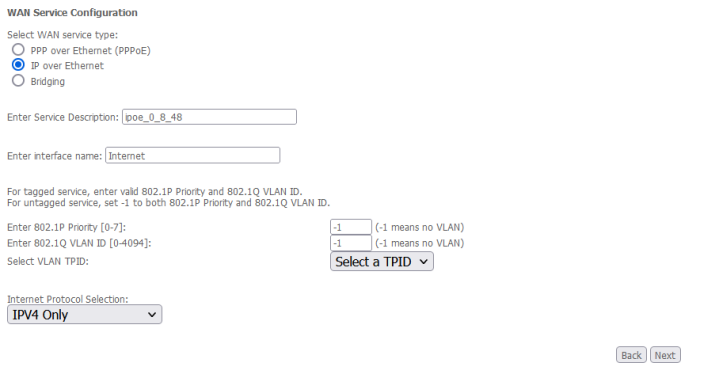
Adding a MER (IPoE) WAN service by GUI

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

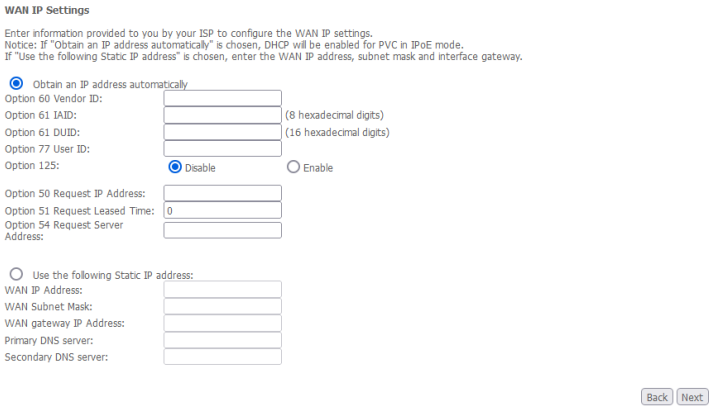
Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM interface for this WAN service.)



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



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



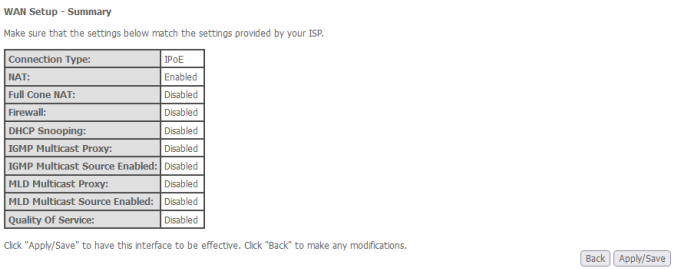
Step4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

Note:

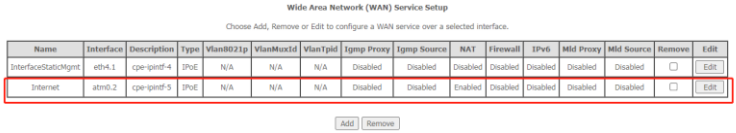
*If selecting **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.*

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

Step5 In this page, click **Next** to display the following page.



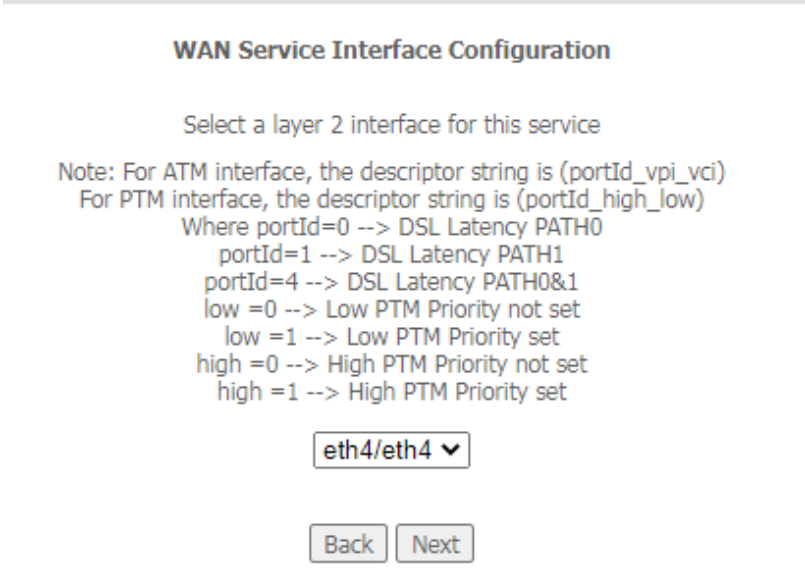
Step6 In this page, it displays the information about the IPoE settngs.Click **Apply/Save** to save and apply the setting.



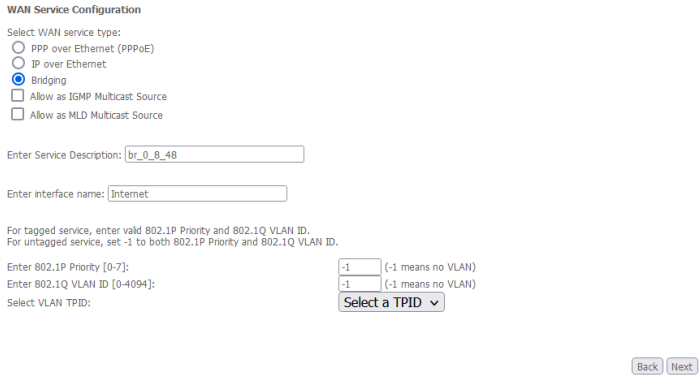
5.2.2.2 Adding a Bridge WAN service by GUI

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

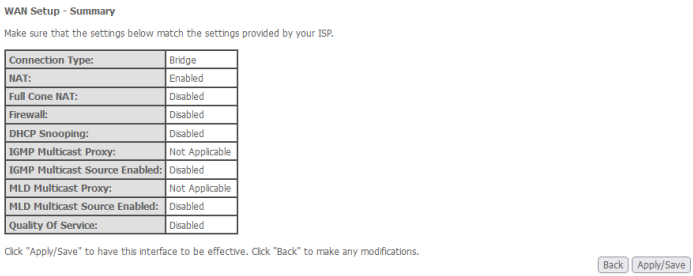
Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM interface for this WAN service.) Click the **Add** button to display the following page.



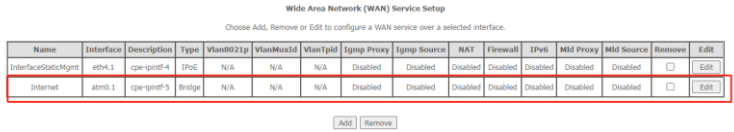
Step2 Select the proper ETH Interface and then click **Next** to display the following page.



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.



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



5.2.3 IPV6

Choose **Advanced Setup > IPV6**, and the following page appears.

In the **IPV6 enable or disable control setting** page, Click **Apply/Save** to save and apply the settings.

5.2.4 LAN Configuration

5.2.4.1 IPv4 Autoconfiguration

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

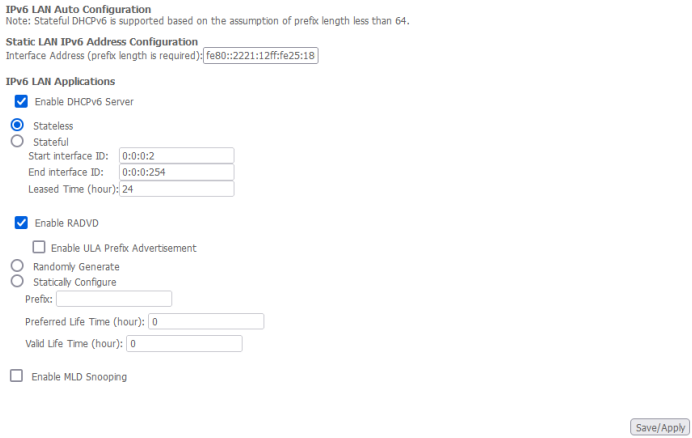
Local Area Network (LAN)

LAN IP:	10.10.0.138
LAN mask:	255.255.255.0
Start IP Address:	10.10.0.1
End IP Address:	10.10.0.64
Primary DNS server:	10.10.0.138
Secondary DNS server:	0.0.0.0
Leased Time (secends):	86400

In this page, only show the settings. User can't config it.

5.2.4.2 IPv6 Autoconfiguration

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



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

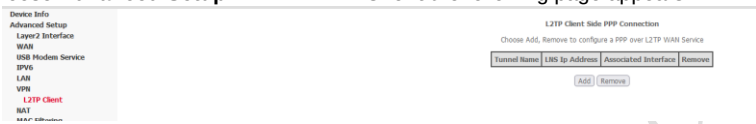
- **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
- **Enable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

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

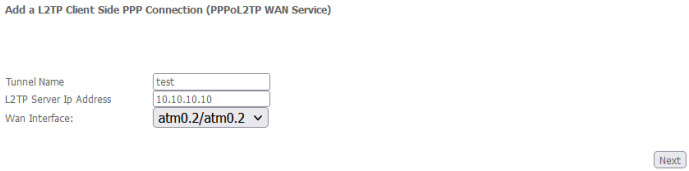
5.2.5 VPN

5.2.5.1 L2TP Client

Choose **Advanced Setup >VPN> L2TP Client** the following page appears.



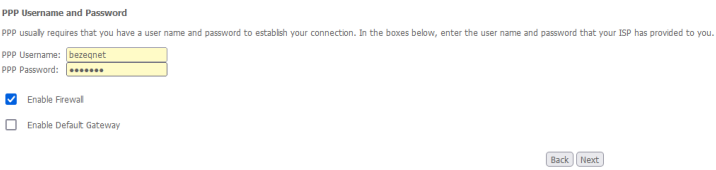
Step1 In the **L2TP Client Side PPP Connection** page.Cick the **Add** button to display the following page.



Step2 In this page, you can modify the **Tunnel Name**, **L2TP Server Ip Address**, **Wan Interface**.

- **Tunnel Name:** The name of the Tunnel
- **L2TP Server Ip Address:** Set the address of the L2TP server.
- **Wan Interface**: Select an existing wan connection, and then build an L2TP channel on this wan connection.

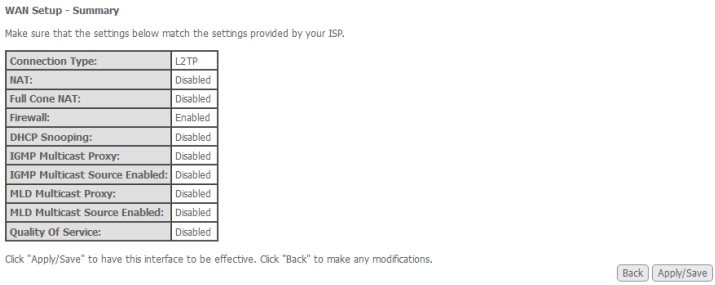
Step3 After setting the parameters, click **Next** to display the following page.



Step4 In this page, you can modify the **PPP Username**, **PPP Password**, **Enable Firewall, Enable Default Gateway**.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Enable Firewall :** Used to control whether remote access is allowed
- **Enable Default Gateway :** Set that wan connection as the default gateway

Step5 After setting the parameters, 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:	L2TP
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
DHCP Snooping:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

Back Apply/Save

Step6 In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings.

5.2.6 NAT

5.2.6.1 Port Forwarding

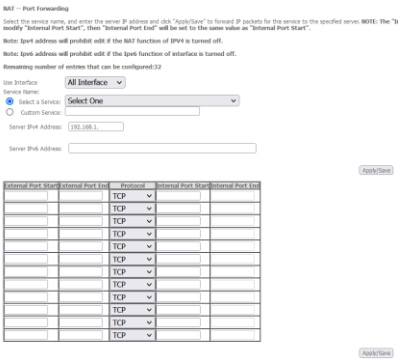
Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The Port Forwarding can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Choose **Advanced Setup > NAT > Port Forwarding**, and the following page appears.

In this page, you are allowed to add or remove a Port Forwarding entry.

To add a Port Forwarding, do as follows:

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



- **Use interface**: Select an interface that you want to configure.
- **Select a Service**: Select a proper service in the drop-down list.
- **Custom Server**: Enter a new service name to establish a user service type.
- **Server IPv4 Address**: Assign an IP address to virtual server.
- **Server IPv6 Address**: Assign an IP address to virtual server.

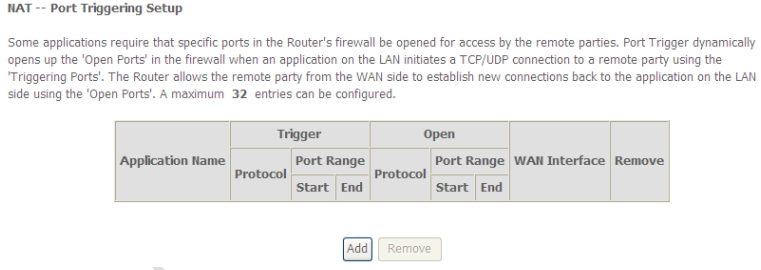
- **External Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Protocol**: You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

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

5.2.6.2 Port Triggering

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

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


NAT -- Port Triggering Setup

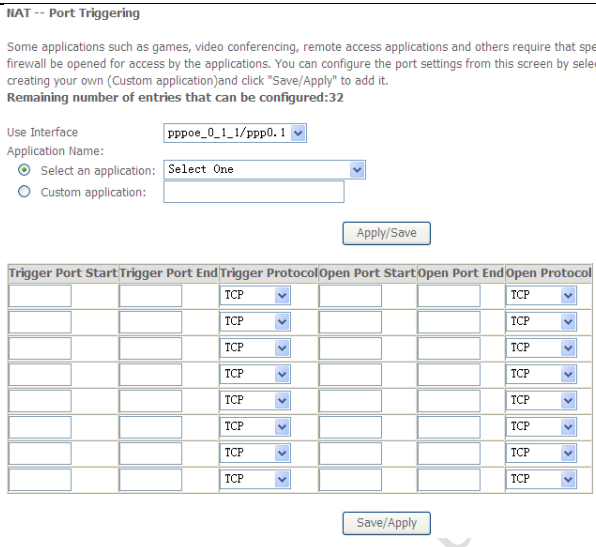
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router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

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

Add Remove

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

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



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

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

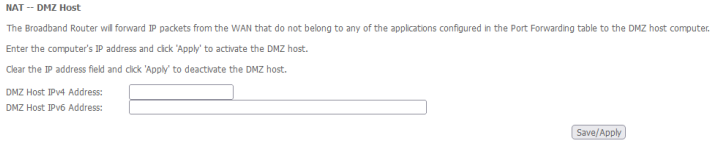
Note:

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

5.2.6.3 DMZ Host

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

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



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

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

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

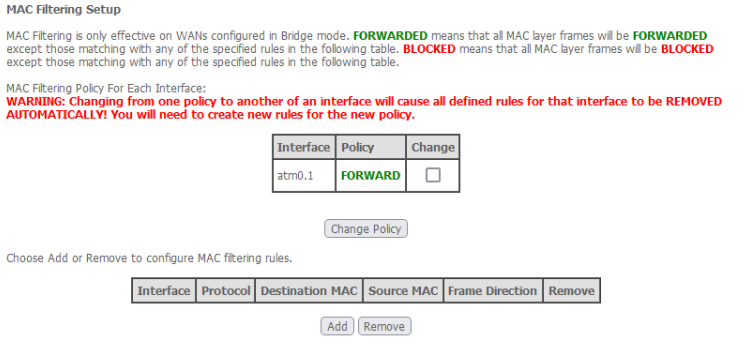
5.2.7 MAC Filtering

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 Router serves as a firewall that works at layer 2.

Note:

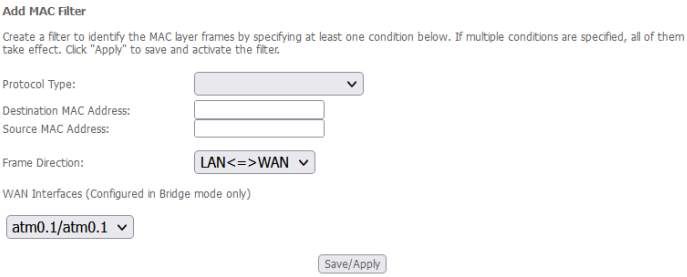
MAC filtering is only effective on ATM PVCs configured in bridge mode.

Choose **Advanced Setup** > **MAC Filtering** and the following page appears.



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

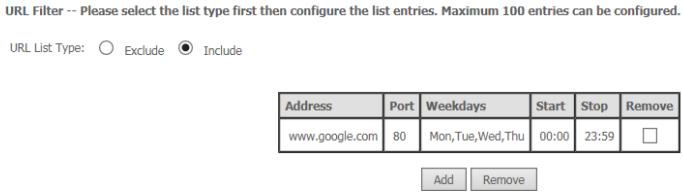
Click the **Add** button to display the following page.



- **Protocol Type**: Select the proper protocol type.
- **Destination MAC Address**: Enter the destination MAC address.
- **Source MAC Address**: Enter the source MAC address.
- **Frame Direction**: The direction of transmission frame.

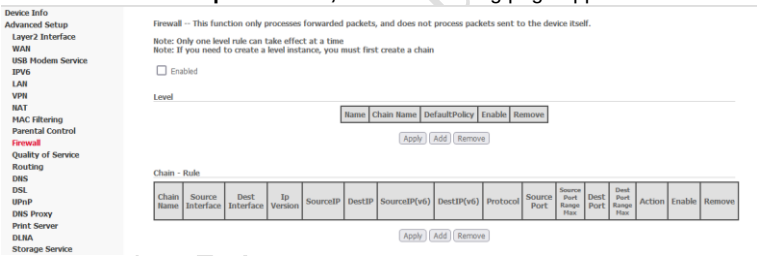
- **WAN Interface (Configured in bridge mode only)**: Select the proper WAN interface in the drop-down list.

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



5.2.8 Firewall

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



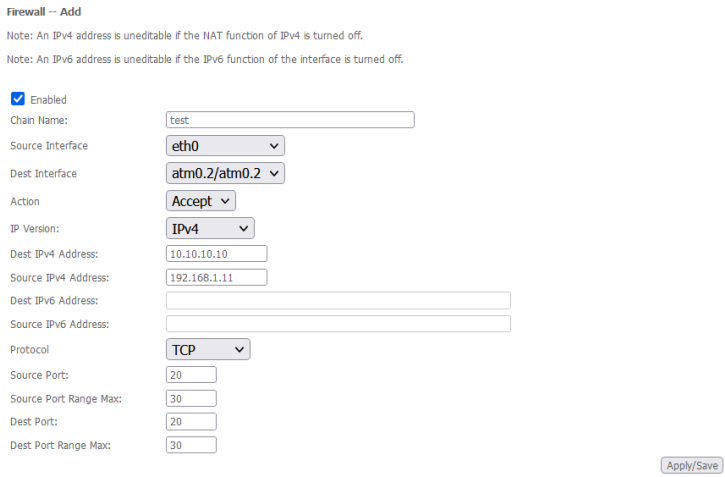
In this page, you are allowed to add, remove, or edit a level and Chain rule.

Note: If you need to create a level instance, you must first create a chain

5.2.8.1 Adding a Chain Rule

This section describes the steps for adding the chain rule.

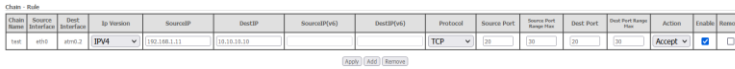
Step1 In the **Chain - Rule** page, click the **Add** button to display the following page.



Step2 In this page, you can modify follow parameters.

- **Chain Name:** The name of the chain.
- **Source Interface:**Select an interface which the packet receive.
- **Dest Interface:** Select the interface from which the packet is sent.
- **Action:** Set the processing action for the packets matching the rule..Accept or Drop.
- **IP Version:**. IP Version.
- **Dest IPv4 Address:**. Dest IPv4 Addresss of packet.
- **Source IPv4 Address :** Source IPv4 Address of packet.
- **Dest IPv6 Address:**. Dest IPv6 Addresss of packet.
- **Source IPv6 Address :** Source IPv6 Address of packet.
- **Protocol:** TCP or UDP
- **Source Port:** Source Port
- **Source Port Range Max:** Source Port Range Max
- **Dest Port:** Dest Port
- **Dest Port Range Max:** Dest Port Range Max
-

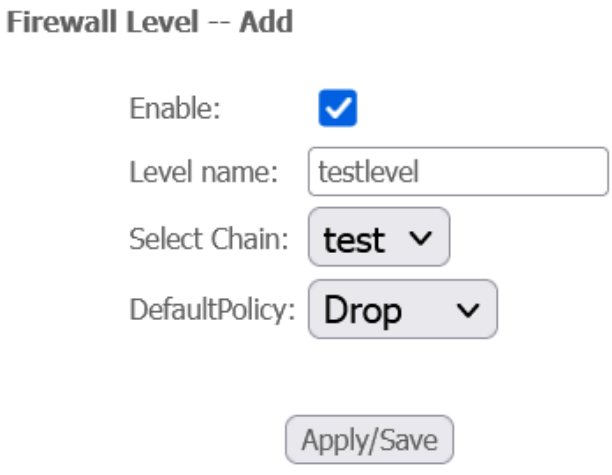
Step3 After setting the parameters, Click **Apply/Save** to save and apply the settings.



5.2.8.2 Adding a Level Rule

This section describes the steps for adding the Level rule.

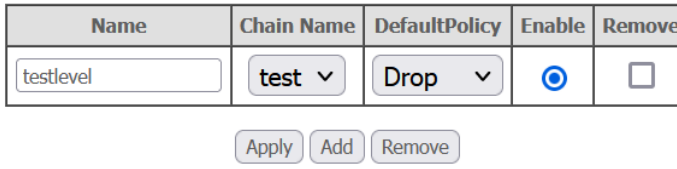
Step1 In the **Level** page, click the **Add** button to display the following page.



Step2 In this page, you can modify follow parameters.

- **Enable :** enable this level.
- **Level name:**The name the level.
- **Select Chain:** Select a chain to associate this level.
- **DefaultPolicy:** Default Policy.

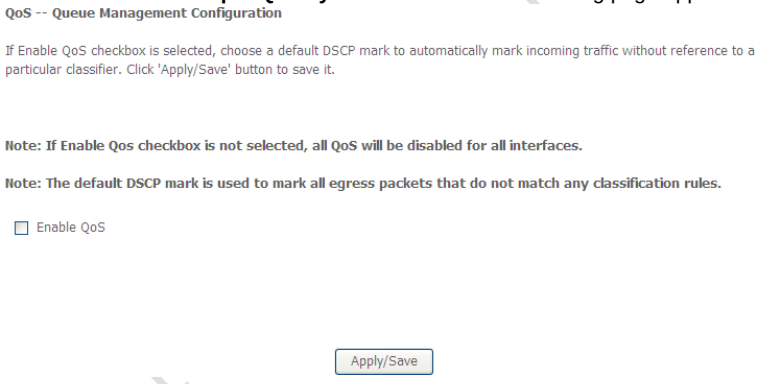
Step4 After setting the parameters, Click **Apply/Save** to save and apply the settings.



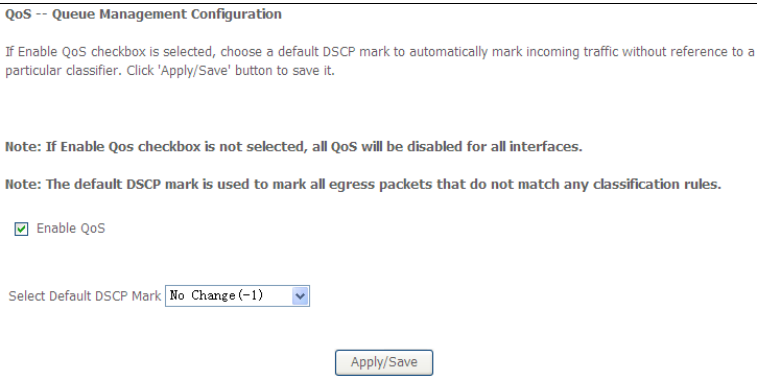
5.2.9 Quality of Service

Enabling QoS

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



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



In this page, enable the QoS function and select the default DSCP mark.
After finishing setting, click **Apply/Save** to save and apply the settings.

Note:

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

Queue Configuration

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

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 8 queues can be configured.
For each Ethernet WAN interface, maximum 8 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.

Note: Ethernet LAN queue configuration only takes effect when all the queues of the interface have been configured.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate (bps)	Min Bit Rate(bps)	Burst Size (bytes)	Enable	Remove
LAN Q8	1	eth1	8	1/SP						☑	☐
LAN Q7	2	eth1	7	2/SP						☑	☐
LAN Q6	3	eth1	6	3/SP						☑	☐
LAN Q5	4	eth1	5	4/SP						☑	☐
LAN Q4	5	eth1	4	5/SP						☑	☐
LAN Q3	6	eth1	3	6/SP						☑	☐
LAN Q2	7	eth1	2	7/SP						☑	☐
LAN Q1	8	eth1	1	8/SP						☑	☐
LAN Q8	9	eth2	8	1/SP						☑	☐

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

Note:

The lower integer value for precedence indicates the higher priority.

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

QoS Queue Configuration

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

Name:

Enable: Disable

Interface:

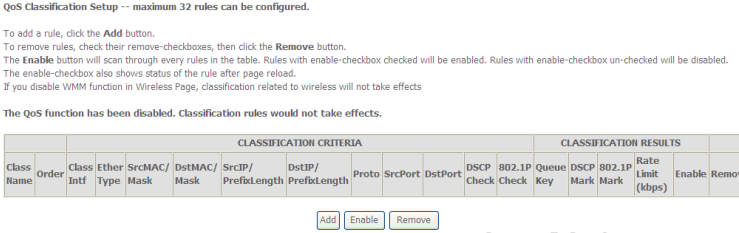
Apply/Save

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

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

QoS Classification

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


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

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

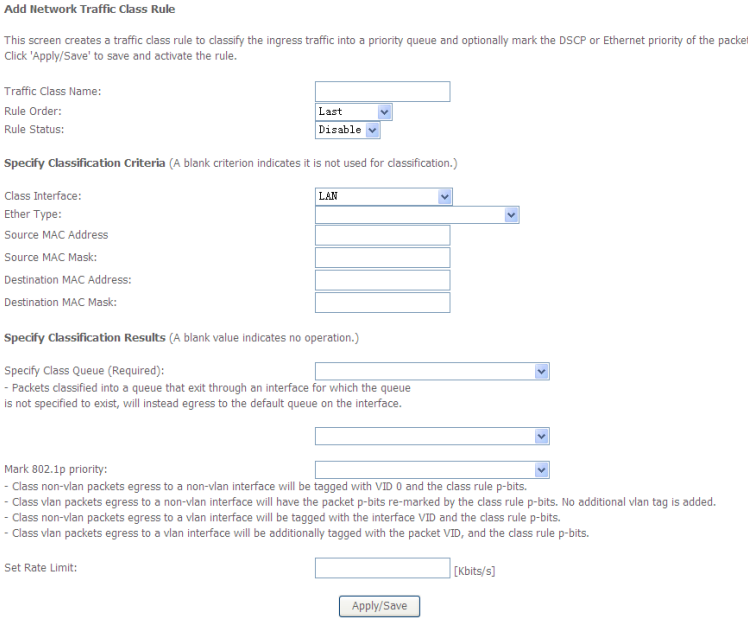
The QoS function has been disabled. Classification rules would not take effects.

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

Add Enable Remove

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

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


Add Network Traffic Class Rule

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

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

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

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

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

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

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

Set Rate Limit: [Kbits/s]

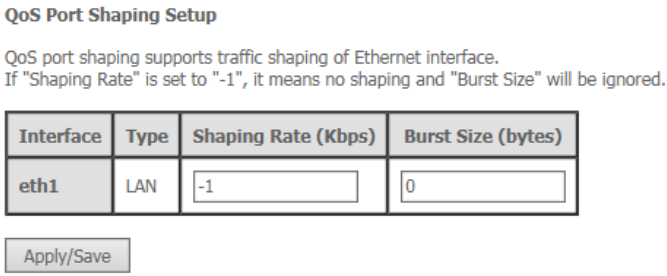
Apply/Save

Figure 5

QoS Port Shaping

Choose Advanced Setup **>** Quality of Service > QoS Port Shaping

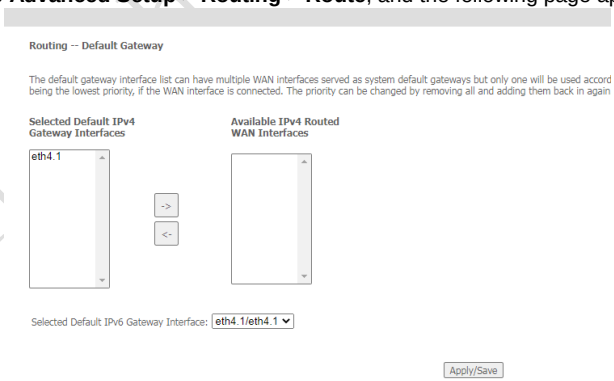
and the following page appears.



5.2.10 Routing

5.2.10.1 Adding a Route by GUI

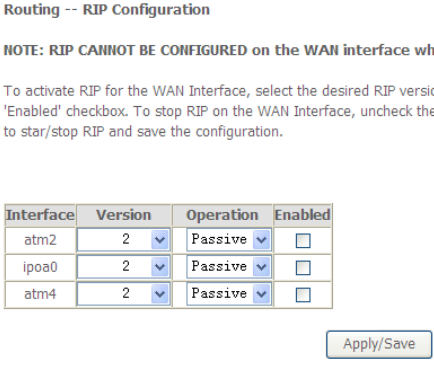
Choose **Advanced Setup** > **Routing** > **Route**, and the following page appears.



Step1 After setting the parameters, click **Apply/Save** to save and apply the settings.

RIP

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



In this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.11 DSL

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

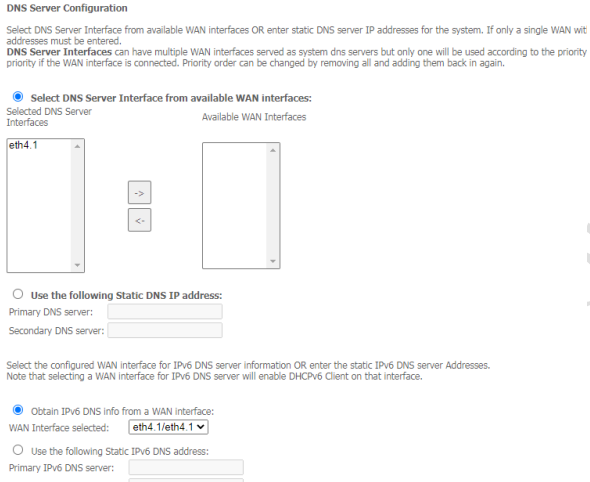
In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

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

5.2.12 DNS

5.2.12.1 Adding a DNS Server by GUI

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

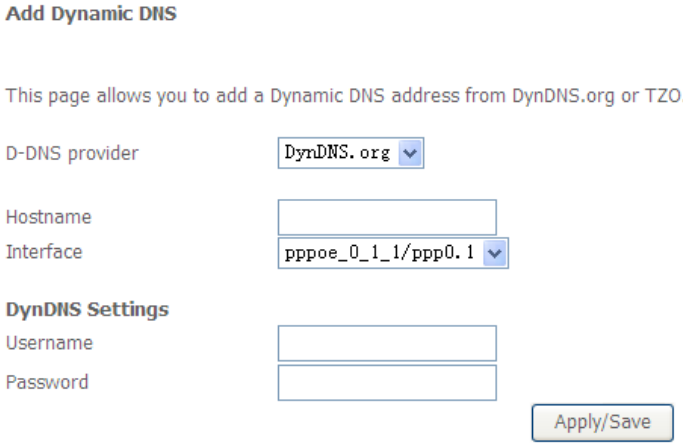


Step1 After setting the parameters, click **Apply/Save** to save and apply the settings.

Dynamic DNS

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

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

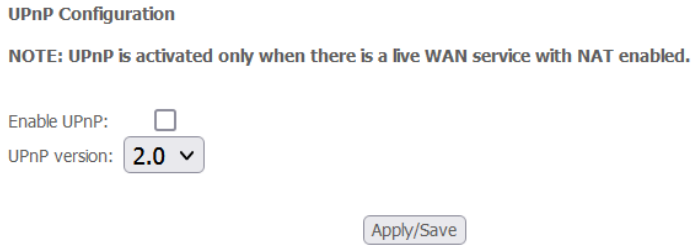


- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the Router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:**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

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

5.2.13 UPnP

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



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

Following is the cli command to enable or disable the upnp:

upnp
    enable
exit

5.2.14 Dnsmasq

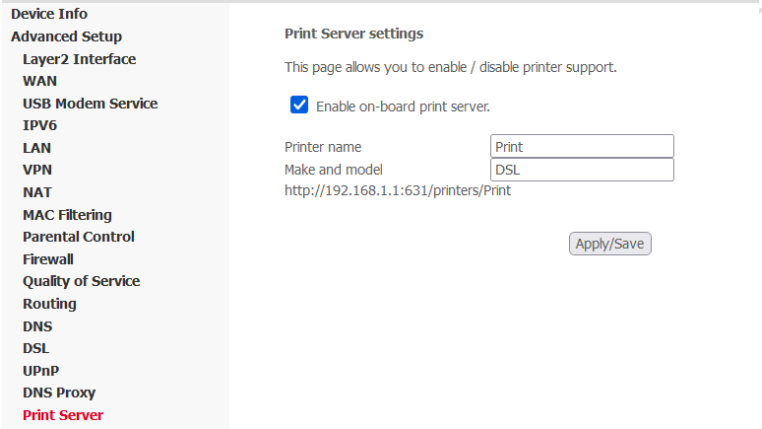
Choose **Advanced Setup > Dnsmasq** and the following page appears.

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

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

5.2.15 Print Server

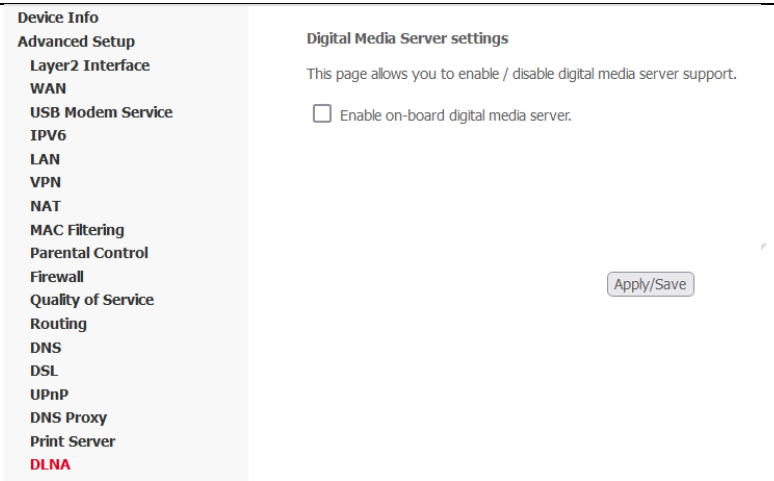
Choose **Advanced Setup > Print Server** and the following page appears.



In this page, you can enable or disable the **Print Server** function.
After enabling the **Print Server** function, enter the Printer name, Make and model, and then click **Apply/Save** to save and apply the settings.

5.2.16 DLNA

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

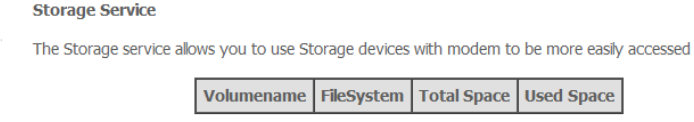


In this page, you can enable or disable the **DLNA** function.
After enabling the **DLNA** function, and then click **Apply/Save** to save and apply the settings.

5.2.17 Storage Service

5.2.17.1 Storage Device Info

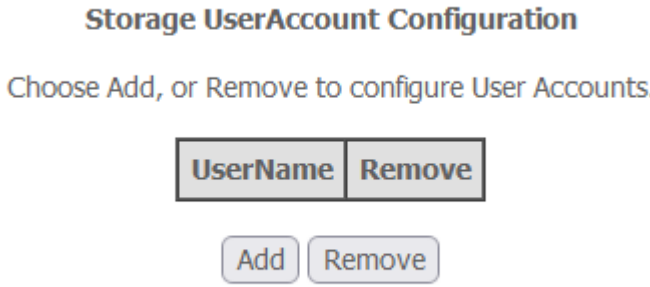
Choose **Advanced Setup > Storage Service > Storage Device Info** and the following page appears.



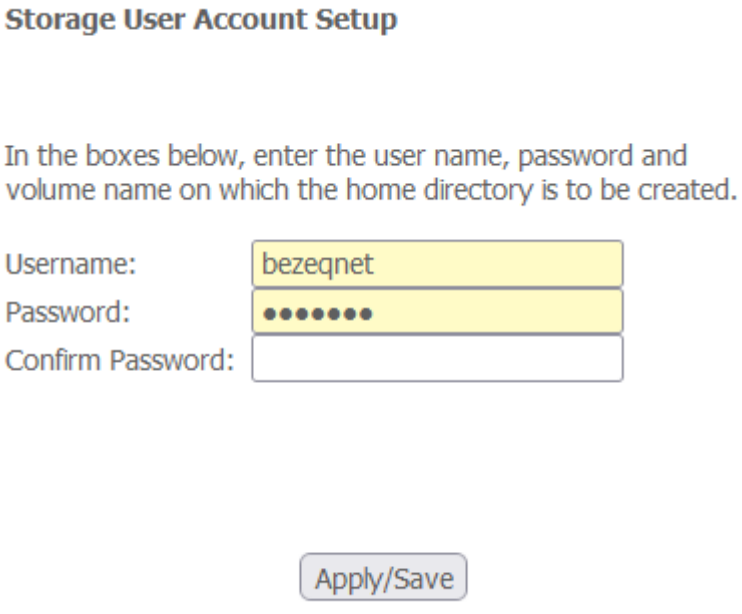
In this page, you can see the detail info about the USB device what plug to the Router.

5.2.17.2 Adding a User Account

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



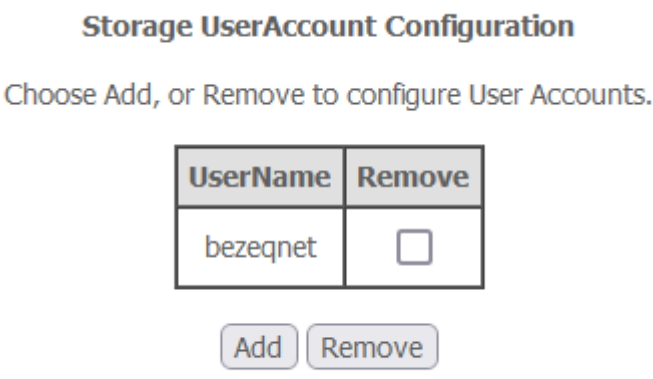
Step2 In the **Storage UserAccount Configuration** page, click the **Add** button to display the following page.



Step3 In this page, you can modify the Username, Password.

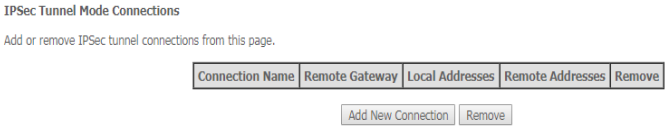
- **Username:** Set the Username to access the USB device.
- **Password:** Set the Password to access the USB device.

Step4 After setting the parameters, click **Apply/Save** to save and apply the settings.

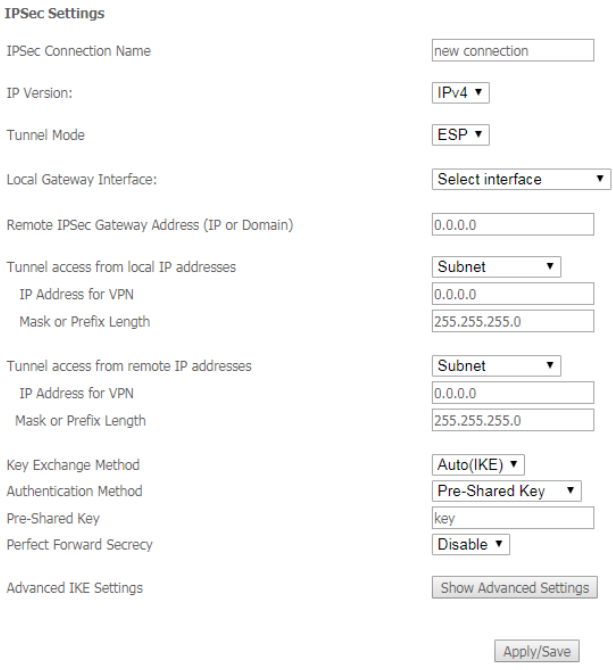


5.2.18 IPSec

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



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

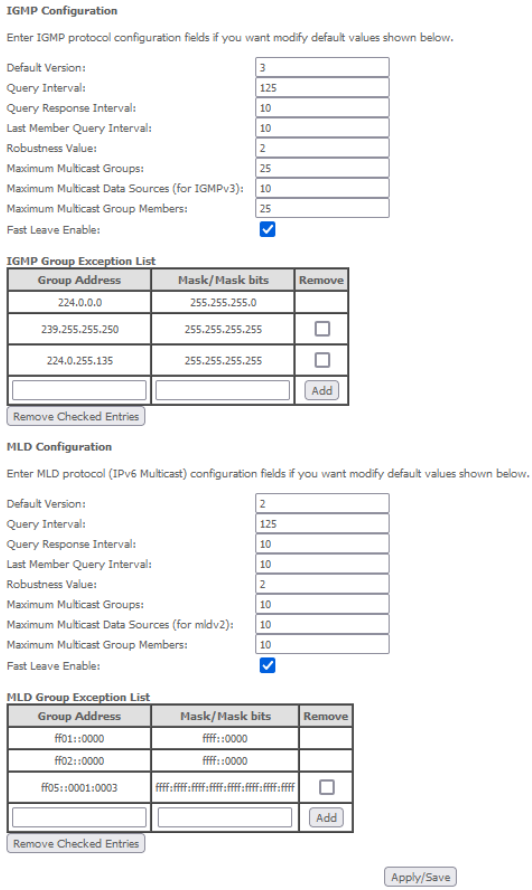


In this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

If you need to configure the advanced settings of this IPSec tunnel connection, please click the **Show Advanced Settings** button to display the other parameters. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.19 Multicast

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



IGMP Configuration

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

Default Version:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☑

IGMP Group Exception List

Group Address	Mask/Mask bits	Remove
224.0.0.0	255.255.255.0	
239.255.255.250	255.255.255.255	☐
224.0.255.135	255.255.255.255	☐
		Add

Remove Checked Entries

MLD Configuration

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

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv2):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	☑

MLD Group Exception List

Group Address	Mask/Mask bits	Remove
ff01::0000	ffff::0000	
ff02::0000	ffff::0000	
ff05::0001:0003	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	☐
		Add

Remove Checked Entries

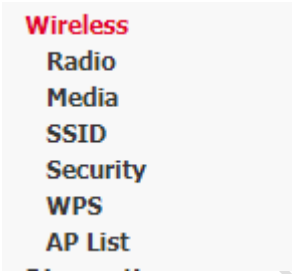
Apply/Save

In this page, you can configure the multicast parameters.

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

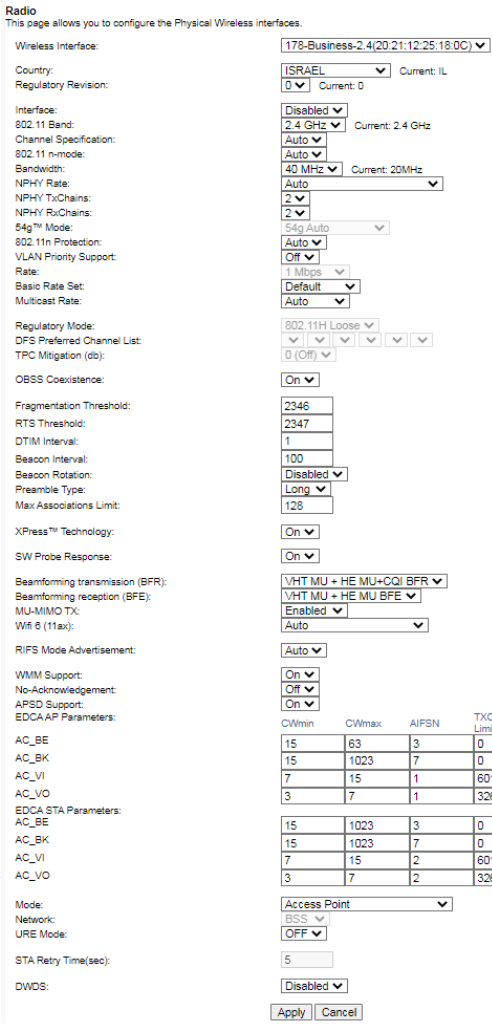
5.3 Wireless

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



5.3.1 Radio

Choose **Wireless** > **Radio** 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.



Radio
This page allows you to configure the Physical Wireless interfaces.

Wireless Interface: 178-Business-2.4(20:21:12:25:18:0C)

Country: ISRAEL Current: IL
Regulatory Revision: 0 Current: 0

Interface: Disabled
802.11 Band: 2.4 GHz Current: 2.4 GHz
Channel Specification: Auto
802.11 n-mode: Auto
Bandwidth: 40 MHz Current: 20MHz
NPHY Rate: Auto
NPHY TxChains: 2
NPHY RxChains: 2
54g™ Mode: 54g Auto
802.11n Protection: Auto
VLAN Priority Support: Off
Rate: 1 Mbps
Basic Rate Set: Default
Multicast Rate: Auto

Regulatory Mode: 802.11H Loose
DFS Preferred Channel List:
TPC Mitigation (db): 0 (Off)

OBSS Coexistence: On

Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Beacon Rotation: Disabled
Preamble Type: Long
Max Associations Limit: 128

XPress™ Technology: On

SW Probe Response: On

Beamforming transmission (BFR): VHT MU + HE MU+CQI BFR
Beamforming reception (BFE): VHT MU + HE MU BFE
MU-MIMO TX: Enabled
Wifi 6 (11ax): Auto

RIFS Mode Advertisement: Auto

WMM Support: On
No-Acknowledgement: Off
APSD Support: On
EDCA AP Parameters:

	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Admission Control	Discard Oldest First
AC_BE	15	63	3	0	0	Off	Off
AC_BK	15	1023	7	0	0	Off	Off
AC_VI	7	15	1	6016	3008	Off	Off
AC_VO	3	7	1	3264	1504	Off	Off

EDCA STA Parameters:

AC_BE	15	1023	3	0	0
AC_BK	15	1023	7	0	0
AC_VI	7	15	2	6016	3008
AC_VO	3	7	2	3264	1504

Mode: Access Point
Network: BSS
URE Mode: OFF

STA Retry Time(sec): 5

DWDS: Disabled

Apply Cancel

- Channel Specification: Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the

same channel in order to work correctly. This router supports auto channeling functionality.

- **802.11 n-mode::** Select **off** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network. You can select **20MHz in Both Bands**, **20MHz in 2.4G Band and 40MHz in 5G Band**, or **40MHz in Both Bands, 80MHz in 5G Band, 160MHz in 5G Band**
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.
- **Basic Rate Set:** Select the basic transmission rate ability for the AP.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.

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

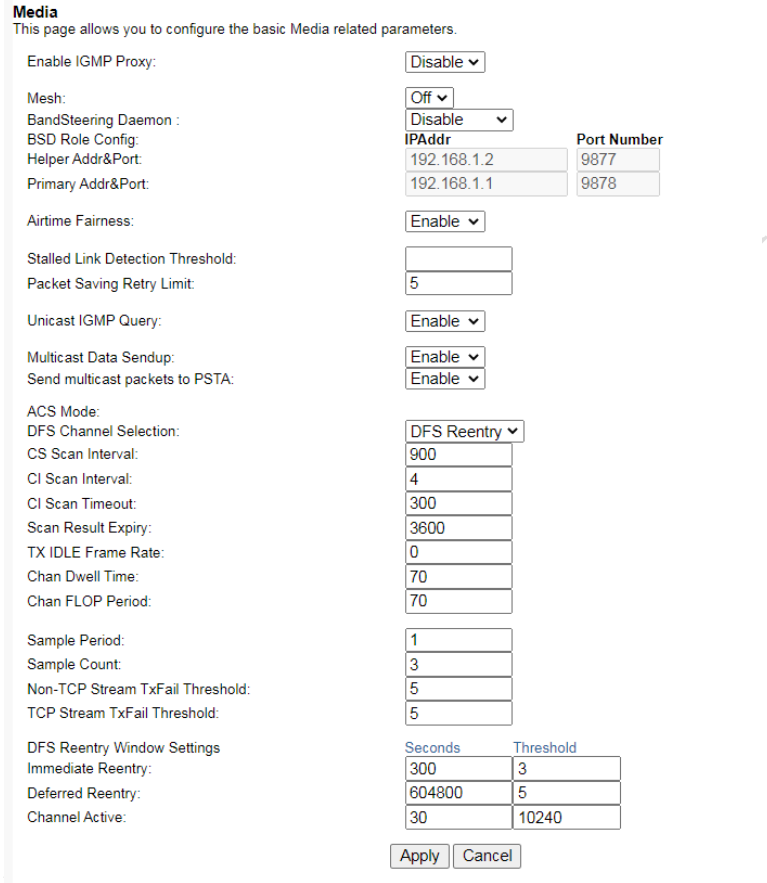
Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

Note:

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

5.3.2 Media

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



- **Enable IGMP Proxy:** Enable or disable IGMP Proxy.
- **Mesh:** Enable or disable mesh.
- **BandSteering Daemon**: select “standalone” to enable BandSteering.

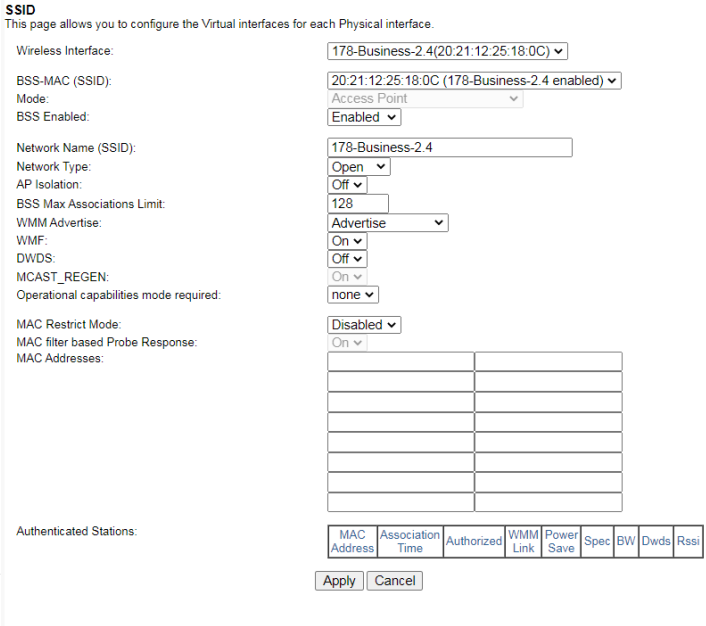
Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

Note:

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

5.3.3 SSID

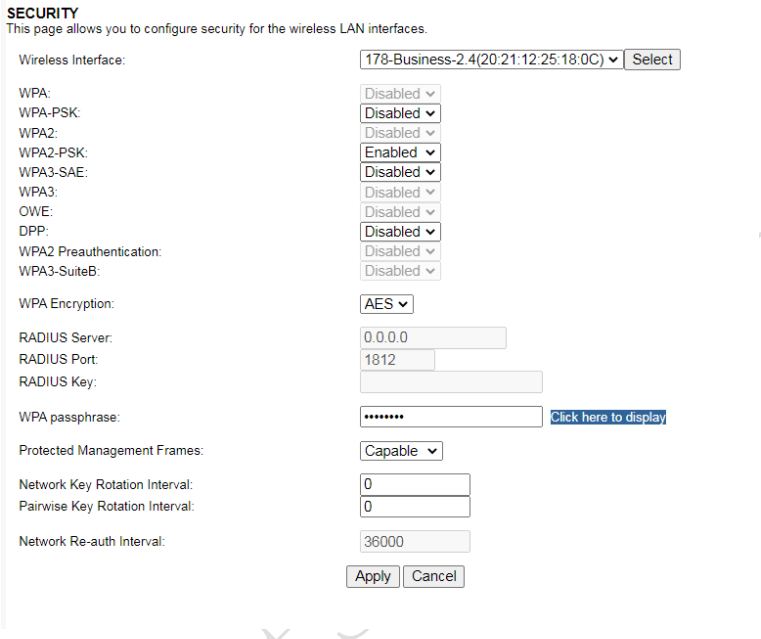
Choose **Wireless > SSID** to display the following page. In this page, It includes the wireless SSID.



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

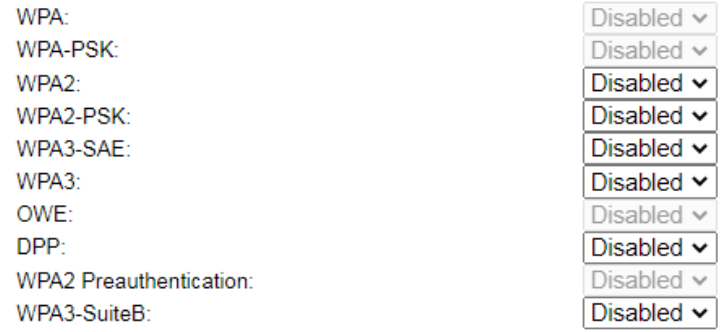
5.3.4 Security

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

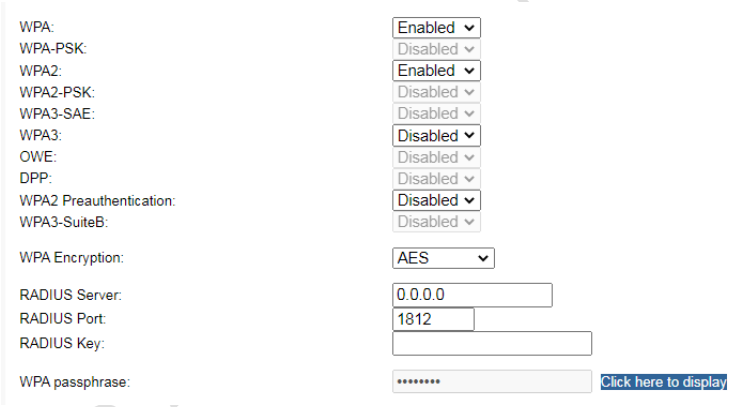


This page provides 7 types of network authentication modes, including open,WPA, WPA-PSK, WPA2, WPA2-PSK, WPA3-SAE, WPA3.

- **Open Mode**



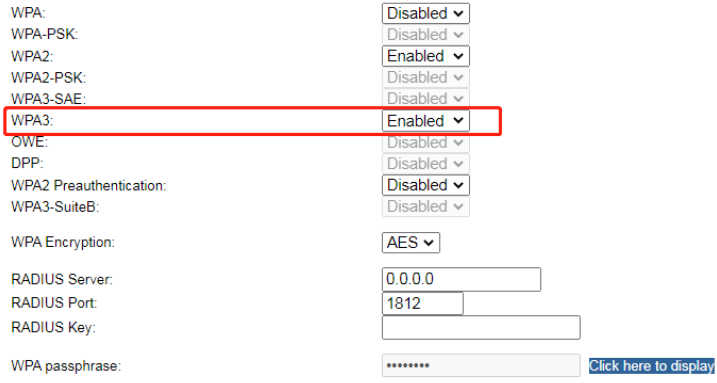
- **WPA and WPA2**



- **RADIUS Server:** 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.

Note: if you want to enable WPA, you need to enable WPA2 first

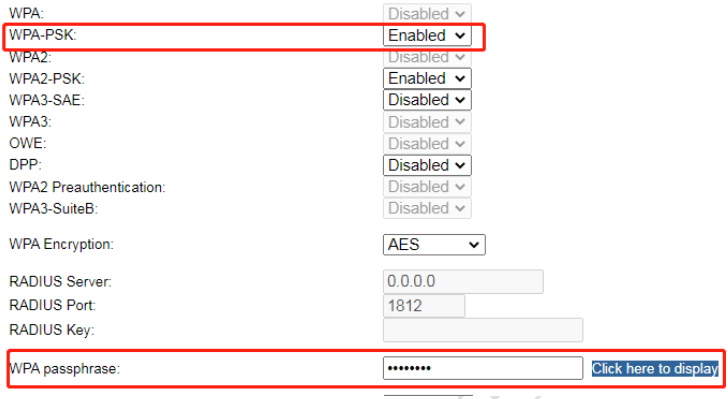
- **WPA2 and WPA3**



- **RADIUS Server:** 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.

Note: if you want to enable WPA3, you need to enable WPA2 first

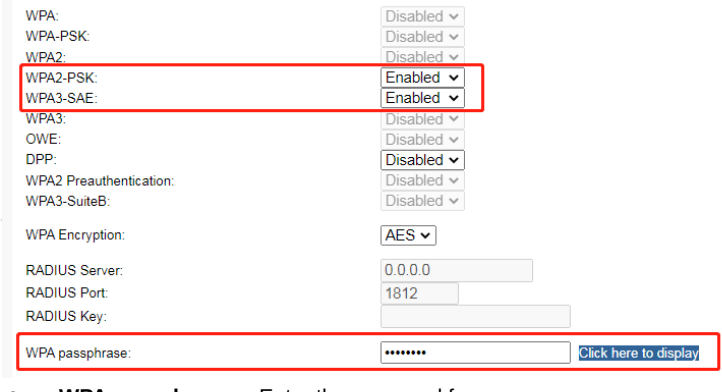
- **WPA-PSK and WPA2-PSK**



- **WPA passphrase:** Enter the password for access.

Note: if you want to enable WPA-PSK, you need to enable WPA2-PSK first

- **WPA2-PSK and WPA3-SAE**

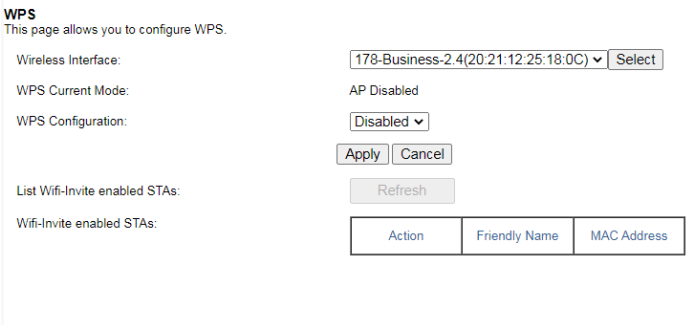


- **WPA passphrase:** Enter the password for access.

Note: if you want to enable WPA3-SAE, you need to enable WPA2-PSK first

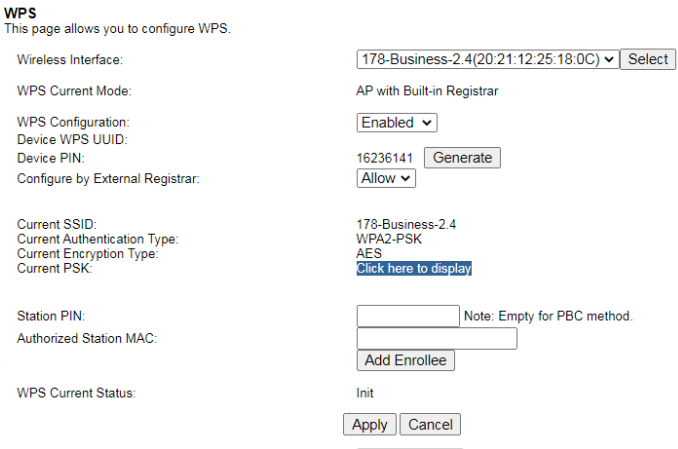
5.3.5 WPS

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



In this page, you can configure the network security settings by the Wi-Fi Protected Setup (WPS) method or setting the network authentication mode.

- **WPS Setup**



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

- PIN entry, a mandatory method of setup for all WPS certified devices.
  - **Station PIN:** If you select it, you need to enter the station PIN from client.

- **Device PIN**: The PIN is generated by AP.

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

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

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

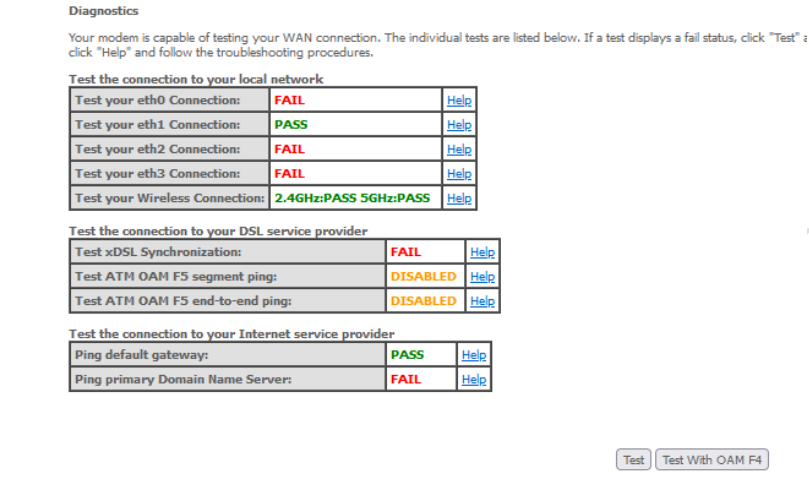
5.4 Diagnostics

5.4.1 Diagnostics

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

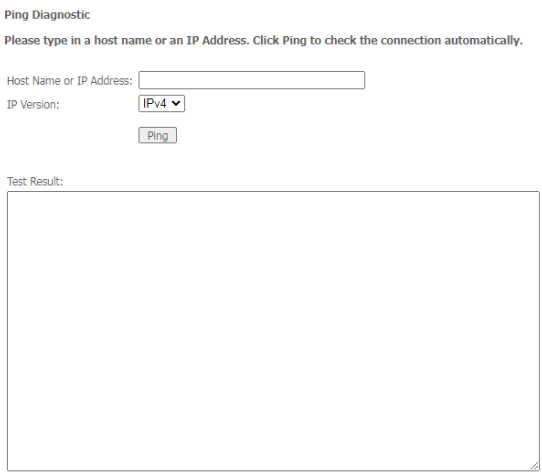
This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

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



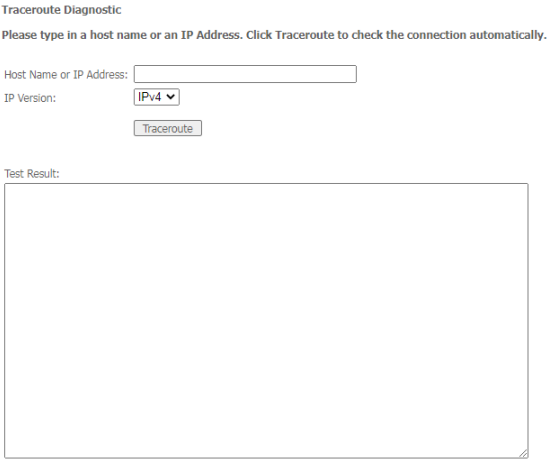
5.4.2 Ping

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



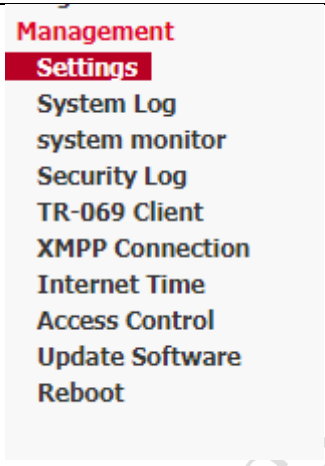
5.4.1 Traceroute

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



5.5 Management

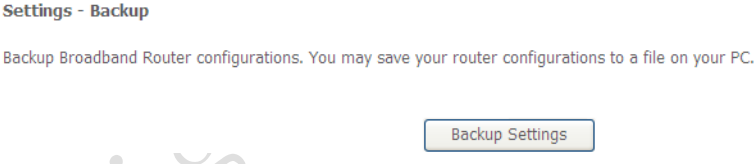
Choose **Management** and the submenus of **Management** are shown as below:



5.5.1 Settings

5.5.1.1 Backup

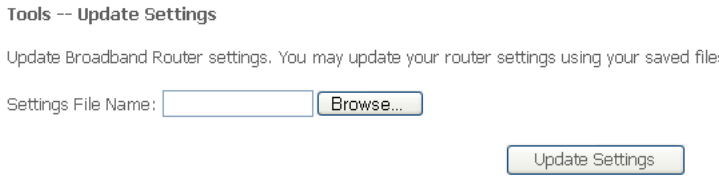
Choose **Management > Settings > Backup** to display the following page.



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

5.5.1.2 Update

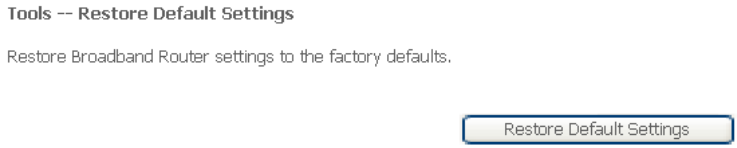
Choose **Management > Settings > Update**, and the following page appears.



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

5.5.1.3 Restore Default

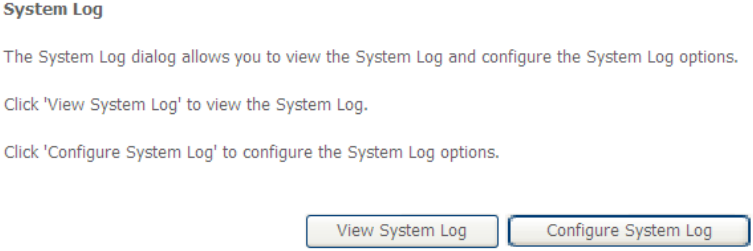
Choose **Management > Settings > Restore Default** to display the following page.



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

5.5.2 System Log

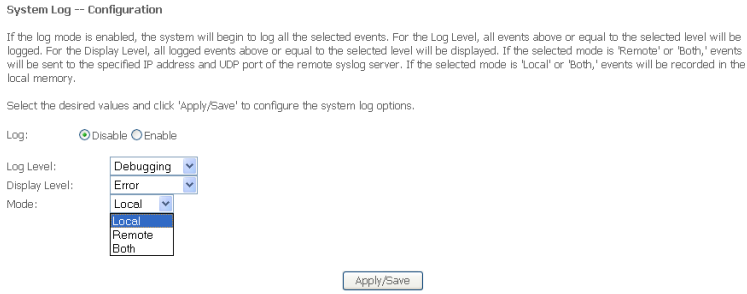
Choose **Management > System Log** to display the following page.



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

- **Configuring the System Log**

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



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

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

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

Note:

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

- **View System Log**

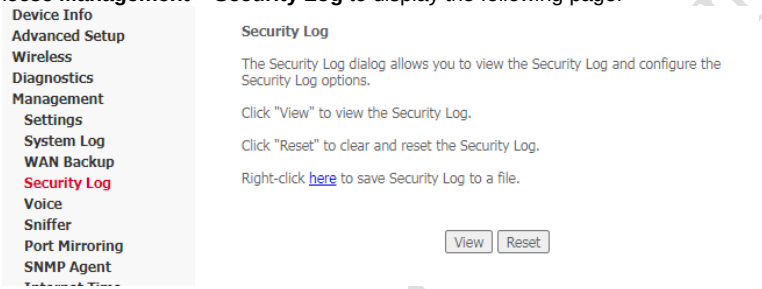
Click the **View System Log** button to display the following page.

In this page, you can view the system log.

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

5.5.3 Security Log

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



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

Click the **Reset** button to refresh the system log.

5.5.4 Voice

5.5.4.1 Overview

The VoIP solution of the Router allows you to connect two or more parties over a single broadband connection, providing the benefits and quality of digital voice and other advanced features. These parties include IP phone, analog phone attached to an Analog Telephone Adapter (ATA), and telephone in the PSTN network. With a Private Branch eXchange (PBX) or a signaling gateway, you can even connect to VoIP phones armed with other protocols than SIP. Router enables you to place and receive calls over the Internet using a standard telephone set connected to SIP Proxy or other devices which have/include the same functions as SIP Proxy.

With proper dial-plan setting, calls on the Router may be routed to PSTN network or VoIP network, depending on what digits you dial.

The Router provides 2 FXS interfaces and 1 FXO interface. FXO is connected to telephone line, through which you dial up to Internet. Normally the telephone line is multiplexed with both telephone signal and data signal. If not filtered out by a splitter before entering FXO interface, the incoming PSTN calls will be routed to FXS-connected analog phone or other VoIP user. You can use up to 2 analog phones, each connected to one FXS interface. The two are called endpoint, and serve as two independent IP phones.

5.5.4.1 SIP Entities

The VoIP solution of the Router uses Session Initiation Protocol (SIP) to create, modify, and terminate calls. SIP is an Internet application-layer protocol that runs in User Agent (UA) and Server Systems for controlling multimedia sessions between users, who may move from one location to another and use terminal devices with various media capabilities. For more details about SIP, refer to RFC3261.

The following describes the terminology of SIP.

Term	Description
POTS	The traditional telephones we use in home are plain old telephone services (POTSs).
UA	It includes UA Client (UAC), UA Server (UAS). UAC originates calls, and UAS listens for incoming calls. The Router can serve as

	UAS and UAC.
SIP Proxy	It routes call requests. If we create a call to invite our friends or relatives through SIP, our call is routed through SIP Proxy, for only it knows the position the corresponding POTS.
SIP Registrar	It maintains mappings from names (user ID) to addresses. An invite call identifies you from so many users who use SIP to communication by your user ID, which you have registered on the SIP Registrar. SIP Proxy uses user ID routes the coming call to your POTS.

Note**: SIP Server usually has functions of the SIP Proxy and of the SIP Registrar.**

The following figure shows the SIP application.

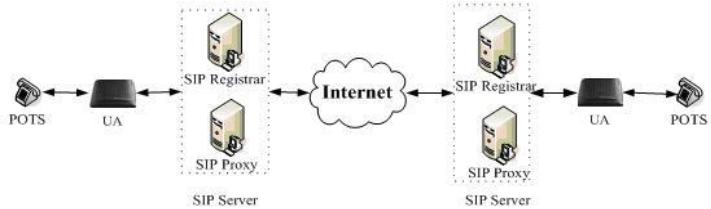
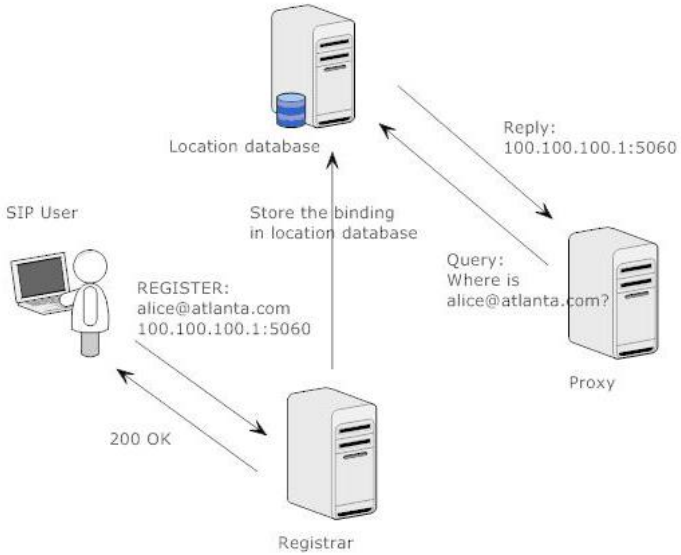


Figure 6 SIP application

5.5.4.2 SIP Call Flows

5.5.4.2.1 Registration

SIP user agent sends a REGISTER message to registrar server, containing its SIP URL and location. Registrar server stores the binding of the two in its database, named location database. When other request provides a SIP URL and queries this database for the corresponding location, location database server responds with the IP address.



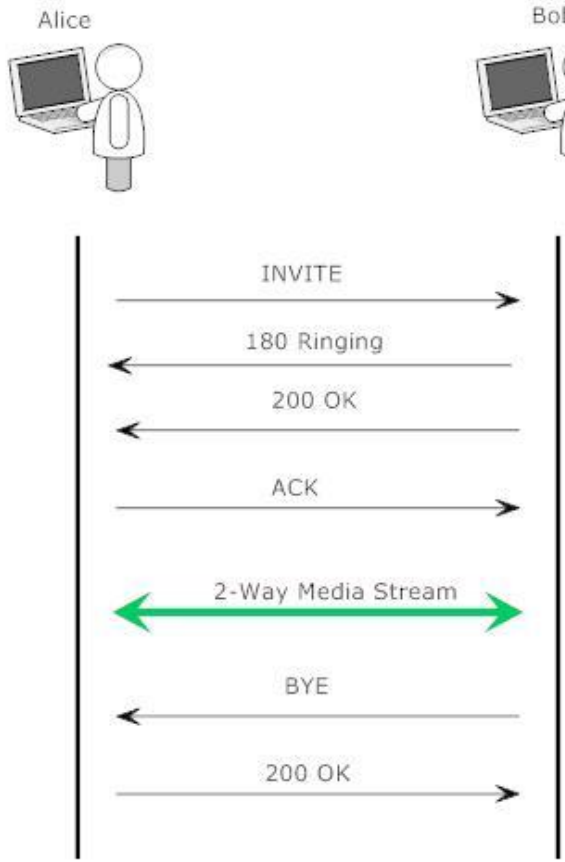
5.5.4.2.2 Simple Call Flow

Sometimes SIP user agents know the exact location of each other, and they are configured without proxy. In this case, both can talk directly.

Alice seizes phone, keys in the number of Bob, in SIP URL format. Assuming Bob is using a SIP-enabled IP phone with IP address 100.100.100.1, The SIP URL of Bob should be something like bob@100.100.100.1. After Alice presses the DIAL button on her phone, a SIP INVITE message is sent to the IP phone of Bob directly. Once the IP phone of Bob receives this message, it rings and replies with another SIP message to Alice. Then, Alice hears a ring-back tone.

Bob knows an incoming call is available, and off-hook his phone. At this time a 2-way voice connection is created, and both parties are able to hear and talk with each other.

In this example, Bob first on-hooks his phone, producing an ACK message sent back to Alice. The arrival of this message terminates the voice connection, making Alice hear a busy tone on her side.



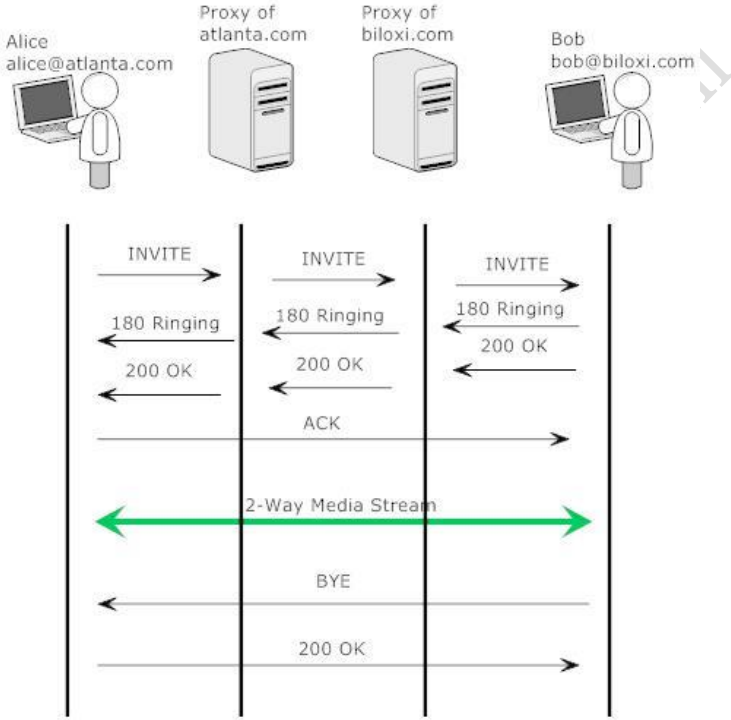
5.5.4.2.3 Call Flow in Proxy Mode

In proxy mode, every user agent takes use of proxy to relay its SIP message. Proxy may query a location database server about a SIP URL. Depending on the result, it may relay the request to a next-hop proxy, or send it to the destination peer.

In this flow, Alice is located in atlanta.com. She is going to place a call to Bob, whose SIP URL is bob@biloxi.com. Alice's user agent passes the INVITE message to its

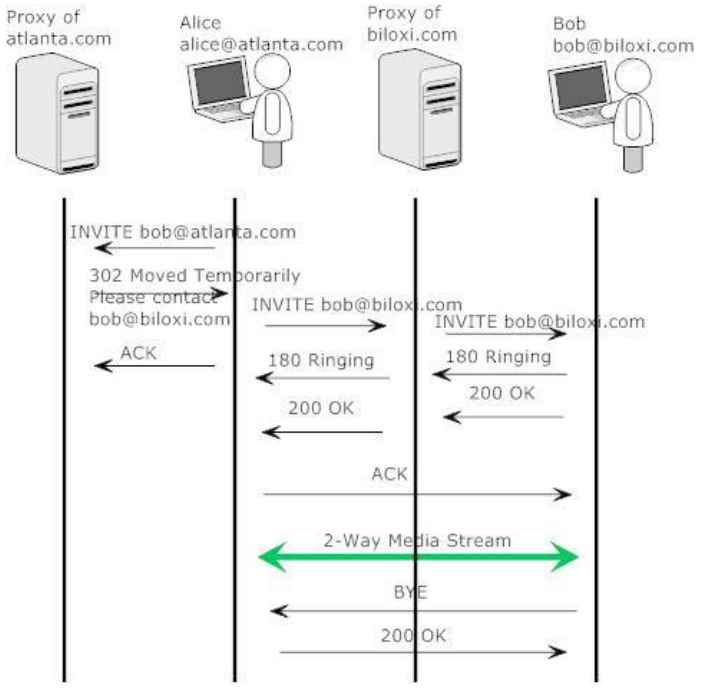
proxy, atlanta.com. From the request URL in SIP message, Alice's proxy determines the next hop is proxy biloxi.com, and passes this message to it.

Finally the phone of Bob rings, which triggers a message passed back to the UA of Alice, producing a ring-back tone in Alice's phone. Once Bob hooks up his phone, a 2-way voice stream is created.



5.5.4.2.4 Call Flow in Redirect Mode

In this flow Alice calls Bob at bob@atlanta.com. The UA of Alice sends the SIP message to its proxy, but gets a 302 message, indicating Bob now is resided in another location. This message also guides Alice how to reach its new location, bob@biloxi.com. At this time, Alice knows the correct location of Bob, and the call flow is like the ones in previous section.

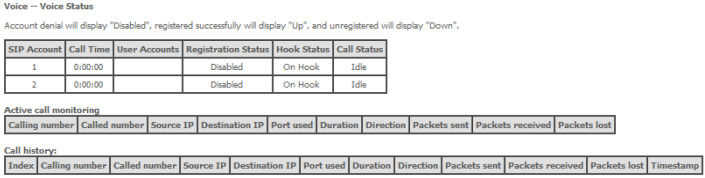

Proxy of
atlanta.com
Alice
alice@atlanta.com
Proxy of
biloxi.com
Bob
bob@biloxi.com
INVITE bob@atlanta.com
302 Moved Temporarily
Please contact
bob@biloxi.com
INVITE bob@biloxi.com
INVITE bob@biloxi.com
ACK
180 Ringing
180 Ringing
200 OK
200 OK
ACK
2-Way Media Stream
BYE
200 OK

5.5.4.3 Web Page Introduction

Once you have logged in web page, navigate to VoIP page from left menu tree. In this page, you can set some parameters you need to register SIP endpoints, place a call or some advanced feature. The VoIP page does not contains a Save or an Apply button, but you can save your settings permanently by clicking the Stop SIP client or Start SIP client.

5.5.4.3.1 VoIP Status

Choose **Management > Voice > VoIP Status** and the VoIP Status page appears.



Voice -- Voice Status

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

SIP Account	Call Time	User Accounts	Registration Status	Hook Status	Call Status
1	0:00:00		Disabled	On Hook	Idle
2	0:00:00		Disabled	On Hook	Idle

Active call monitoring

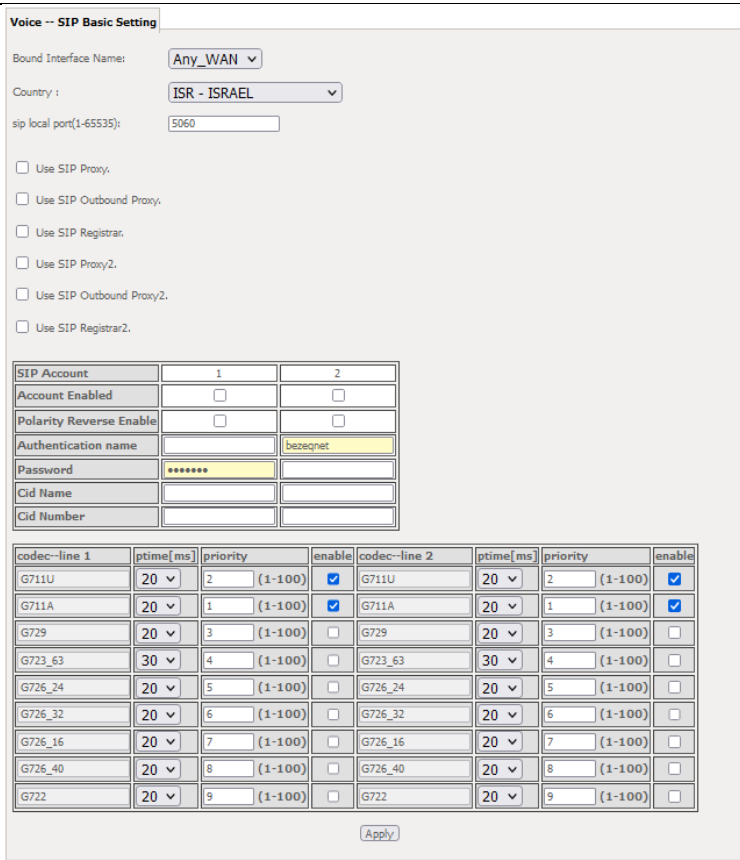
Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost

Call history:

Index	Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost	Timestamp

5.5.4.3.2 SIP Basic Setting

Choose **Management > Voice > SIP Basic Setting** and the SIP Basic Setting pageappears.



SIP Basic Setting page enables you to set some parameters, such as Preferred codec list, Preferred ptime, and SIP domain name. The following describes how to configure the SIP basic settings step by step.

- **Bound Interface Name:** In this field, you can select the way which VoIP of the Router connects to SIP Proxy: LAN or WAN. If you do not configure the 'Wan' tab under the Advanced Setup menu, you must select LAN, which is the default value. For details of selecting the VoIP connection type, consult your ISP.

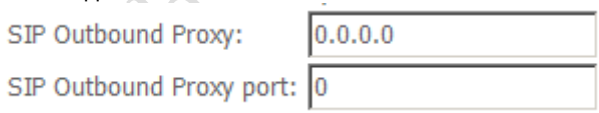
- **Country :**In this field, you can select country where your locale is. Different countries follow different standards used by the VoIP module of the Router, such as ring tone standard. The default value of the Locale selection is USA.
- **sip local port(1-65535):** sip local port

- **Use SIP Proxy:** Select the check box if your Router uses a SIP proxy. SIP Proxy allows other parties to call the Router through it. If you select the check box, the following fields appear:

SIP Proxy: Specify the IP address of the proxy.

SIP Proxy port: The port that this proxy is listening on. The default port value is 5060.

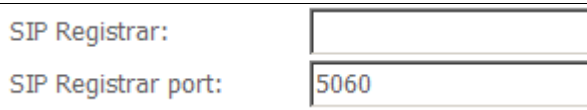
- **Use SIP Outbound Proxy:** Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. If you select the check box, the following fields appear:



SIP Outbound Proxy: The IP address of the Outbound Proxy. The default value is 0.0.0.0.

SIP Outbound Proxy port: The port that the Outbound Proxy is listening on. The default value is 0.

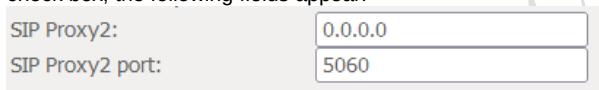
- **Use SIP Registrar:** Select this check box to register with the proxy. You can register your User ID on the SIP Registrar. SIP Registrar works with SIP Proxy, allowing other parties to call the Router through them. If you select the check box, the following fields appear:



SIP Registrar: The IP address of the SIP Registrar.

SIP Registrar port: The port that SIP Registrar is listening on. The default value is 5060.

- **Use SIP Proxy2:** Select the check box if your Router uses a SIP proxy. SIP Proxy allows other parties to call the Router through it. If you select the check box, the following fields appear:



SIP Proxy2: Specify the IP address of the proxy.

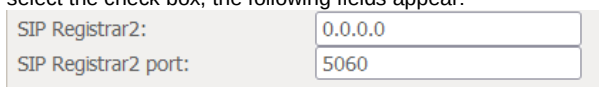
SIP Proxy2 port: The port that this proxy is listening on. The default port value is 5060.

- **Use SIP Outbound Proxy2:** Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. If you select the check box, the following fields appear:

SIP Outbound Proxy2: The IP address of the Outbound Proxy. The default value is 0.0.0.0.

SIP Outbound Proxy port2: The port that the Outbound Proxy is listening on. The default value is 0.

- **Use SIP Registrar2:** Select this check box to register with the proxy. You can register your User ID on the SIP Registrar. SIP Registrar works with SIP Proxy, allowing other parties to call the Router through them. If you select the check box, the following fields appear:



SIP Registrar2: The IP address of the SIP Registrar.

SIP Registrar2 port: The port that SIP Registrar is listening on. The default value is 5060.

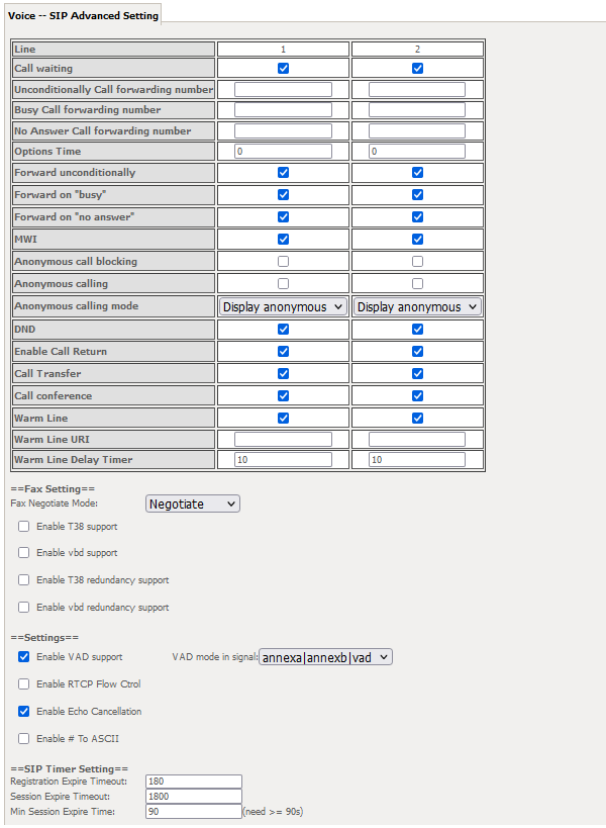
- **Account Enabled:** Line number is a telephone port in the Router to which you can connect a standard (POTS) telephone. If you select this check box, the corresponding line is disabled. You cannot use it to initiate or accept any call.
- **Polarity Reverse Enable:** The positive and negative poles of the line are reversed
- **Authentication Name:** The login name used for authentication with the SIP proxy.
- **Password:** The password used for authentication with the SIP proxy.
- **Cid Name:** Free text description which is displayed as your caller ID to remote parties.
- **Cid Number:** This is the VoIP user ID of the telephone, used for identification to initiate and accept calls.

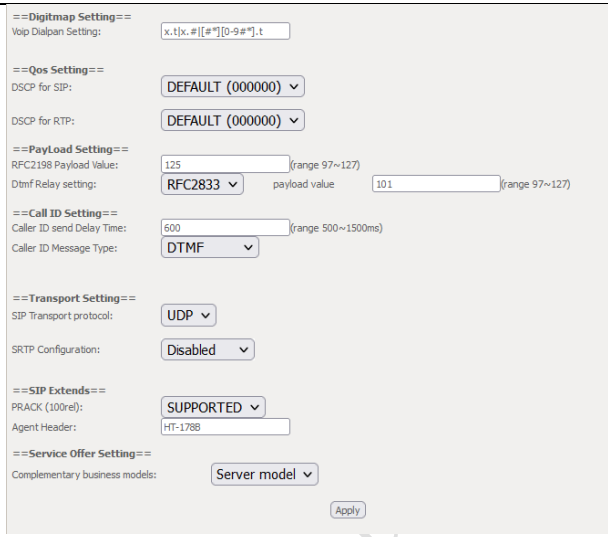
- **codec—line:** In this field, you can specify the priority of codec, and the priority of codec declined from left to right.Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G.723 is a codec that uses compression, so it is applicable in the environment where bandwidth is limited but its voice quality is not as good, compared to other codecs such as the G.711.If you specify none of the codecs, the system uses the default value and the Router selects the codec automatically.
- **Ptime:** In this field, you can set the Packetization Time (PT). PT is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

5.5.4.3.3 SIP Advanced Setting

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

The advanced setting page contains those parameters that are not usually used. In this page, you can configure advanced feature, such as FAX and MOH (Music on Hold).





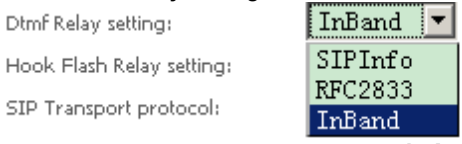
- **Line**: Stands for which line you want to configure.
- **Call waiting**: If call waiting is enabled on a line (see feature codes on the below), and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.
  - Check the feature “Call waiting” to enable this function
  - Dial ‘*61’ can also enable Call waiting and dial ‘*60’ can also disable Call waiting
  - Call forward feature settings (Busy or All) takes priority over the call waiting feature.
  - Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference
- **Unconditionally Call forwarding number**: Fill the “Unconditionally Call forwarding number” text box to set the Call forwarding number or dial *74 then the number, and then wait for 4 seconds or press ‘#’ key for finish the setting. Note that this does not actually enable forwarding; to do so, select the call forward action as described below.

Clear the “Call forwarding number” text box or dial *70 to disable all call forwarding features

- **Forward unconditionally:** A feature will forward all incoming calls to a appointed number (see Call forwarding number) unconditionally.
  - Check “Call forwarding all” to enable this feature.
  - Dial ‘*73’ can also enable this function and dial ‘*75’ can also disable this feature. Previous settings for Call Forward Busy or No Answer are not modified
- **Forward on busy**: A feature will forward all incoming calls to a appointed number (see Call forwarding number) when the line is busy
  - Check “Forward on busy” to enable this function
  - Dial ‘*72’ can also to enable this function, Incoming calls are immediately forwarded if the phone is off-hook
- **Forward no answer:** A feature will forward all incoming calls to a appointed number (see Call forwarding number) when the call is no answer.
  - Check “Forward no answer” to enable this function.
  - Dial ‘*71’ can also to enable this function. Incoming calls are forwarded if unanswered for 18 seconds.
- **MWI:** MWI stands for Message Waiting Indicator. When set this enabled, ROUTER will send a SIP SUBSCRIBE message to proxy, asking for a notification when its voicemail status changes. When its status do changes, proxy will send a NOTIFY message to gateway, causing a MWI tone streamed to user’s handset.
- **Anonymous Call Blocking**: A feature that can block the anonymous call.
  - Check the “Anonymous Call Blockin” to enable this function
  - Dial ‘*80’ can also to enable this function and DIal ‘*81’ can also to disable this function
- **Anonymous Calling:** A feature allow to Use anonymous name as call number when call out
  - Check the “Anonymous Calling” to enable this function
  - Dial ‘*83’ can also to enable this function and dial ‘*84’ can also to disable this function
- **DND**: A feature to reject all incoming call.

Check the ‘DND’ to enable this function. Dial ‘*86’ also can enable the function, and dial ‘*87’ can function it.

- **Enable T38 support:** Checking this box enables T38 support. When doing a fax transmission on ROUTER, after fax tone been detected, fax transmission will switch to T38 mode.
- **Registration Expire Timeout:** It is the interval ROUTER will initiate a new registration since last one. It is also known as 'registration assurance timer'. The gateway uses this mechanism to keep its binding record updated.
- **Voip Dial Plan Setting:** Set the VoIP dial plan. If user-dialed number matches it, the number is processed by ROUTER immediately.
- **DSCP for SIP:** Set the DSCP for SIP
- **DSCP for RTP:** Set the DSCP for RTP.
- **Dtmf Relay Setting**



Set DTMF transmit method, which can be following values:

SIP Info: Use SIP INFO message to transmit DTMF digits.

RFC2833: Use RTP packet to encapsulate DTMF events, as specified in RFC 2833.

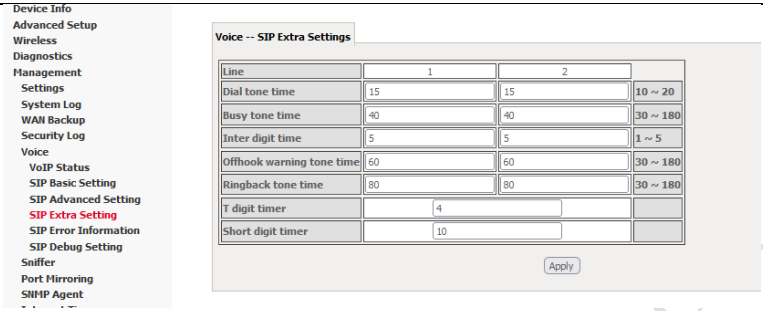
Voice Band: DTMF events will be mixed with user voice in RTP packet.

- **SIP Transport Protocol**

Select the transport protocol to use for SIP signaling. Note SIP proxy and registrar need to support the protocol you choose.

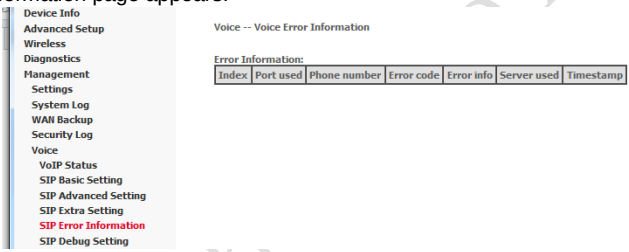
5.5.4.3.4 SIP Extra Setting

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



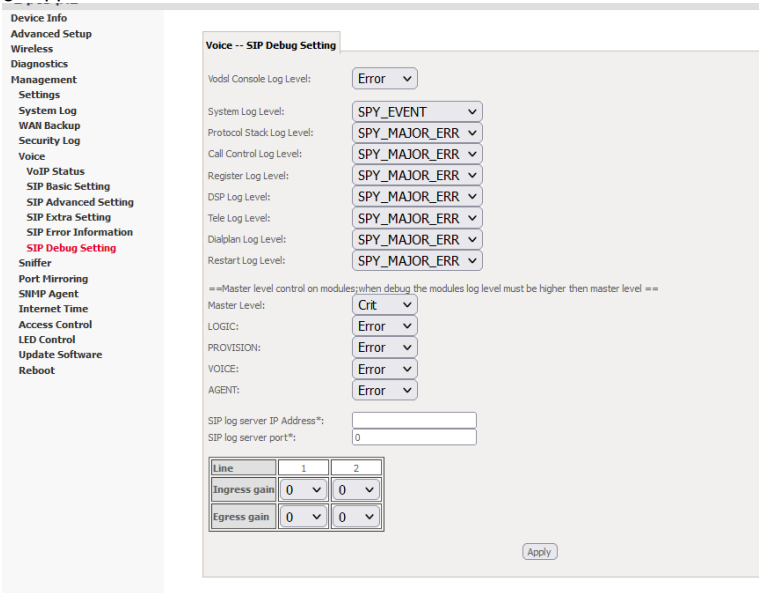
5.5.4.3.5 SIP Error Information

Choose **Management > Voice > SIP Error Information** and the SIP Error Information page appears.



5.5.4.3.6 SIP Debug Setting

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



5.5.4.4 VoIP Functionality

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

5.5.4.4.1 registering

Before using any VoIP functionality, Router has to register itself to a registrar. ROUTER also has to be configured with a proxy, which relays VoIP signaling to next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

Step 1 Select the right interface to use for registering, depending on where Proxy/Registrar resides. If use WAN link, make sure it's already up.

Step 2 Select the **Use SIP Proxy** check box, Fill **SIP domain name** with SIP proxy's IP address or domain name. Note if we use domain name, it must be resolvable to proxy's IP address.

Step 3 Select the **Use SIP Registrar** check box, and fill below IP/Port field with the right value.

Step 4 Fill the extension information: Authentication name, Password, Cid Name, Cid Number. **Authentication Name** and **Password** must be pre-configured in registrar database.

Step 5 VoIP LED should be on, indicating that SIP client is successfully registered.

5.5.4.4.2 Placing a call

This section depicts how to place a basic VoIP call.

(1) Pick up the handset on the phone.

(2) Now you hear the dial-tone. Dial the extension of remote party

(3) To end the dialing, wait for digit-timeout, or just press '#' immediately.

(4) After remote party answers the call, you're in voice connection.

5.5.4.4.3 Anonymous call

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

(5) Pick up the handset on the phone.
(6) Dial '*83' to enable anonymous call.
(7) Hook on the handset, and dial another extension as you like. Now your caller ID information is blocked.
(8) To enable caller ID transmission again, dial '*84' on the key pad.

5.5.4.4.4 Do Not Disturb (DND)

If DND enabled, all incoming calls will be rejected. DND is useful if you do not want others to bother you.

(9) Pick up the handset on the phone.
(10) Dial '*86' to enable DND function
(11) Hook on the phone. Now your phone will reject all incoming calls.
(12) To disable DND, press '*87' on the key pad.

5.5.4.4.5 Redial

For outgoing calls, Router remembers the number you dial. Next time when you want to dial that person, Router provides you the redial functionality.

(13) To re-dial the latest dialed person, press '*68' on the key pad.
(14) Now you have made the call, as if you just dialed the whole number.

5.5.4.4.6 Call Return

For incoming calls, ROUTER remembers the number of calling party.

(15) To return a call, press '*69'
(16) Now you have made the call as if you have dialed the whole number

5.5.4.4.7 Call Hold

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

(17) Assuming you are in a voice connection, you can press 'FLASH' to hold current call.

(18) Now you can call another party, or press 'FLASH' again to return to first call.

5.5.4.4.8 Call Waiting

Enabling call waiting allows third party to call in when you're in a voice connection.

(19) Pick up the phone attached to ROUTER.

(20) Press '*61' to enable call waiting function.

(21) Assuming you're in a voice connection, when another call comes in, ROUTER will stream a call waiting tone to your phone, indicating another call is available.

(22) Press 'FLASH' will switch to this call and the initial call will put to hold automatically.

(23) Press 'FLASH' multi-times will switch between these two calls back and forth.

(24) Pressing '*60' will disable call waiting function.

5.5.4.4.9 Blind Transfer

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

(25) Assume you have already been in a voice connection.

(26) Press 'FLASH' to hold the first party.

(27) Dial a third party.

(28) Before the third party answers the call, hook on your phone.

(29) Now the first party takes over the call and is in connection with the third party.

5.5.4.4.10 Consultative Transfer

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

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

(31) Press 'FLASH' to hold the first party.

(32) Dial a third party.

(33) After the third party answers the call, hook on your phone.

(34) Now the first party takes over the call and is in connection with the third party.

5.5.4.4.11 Call Forwarding No Answer

If this feature enabled, incoming calls will be forwarded to third party when you doesn't answer them. It involves two steps: setting the forwarding number and enable the feature.

(35) Dial '*74<NUM>#' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to.

(36) Dial '*71' to enable call forwarding no answer. That is, when our phone doesn't answer incoming call, this call will be forwarded.

(37) Press '*70' will disable call forwarding no answer.

5.5.4.4.12 Call Forwarding Busy

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

(38) Dial '*74<NUM>#' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.

(39) Press '*72' to enable call forwarding busy. That is, when our phone gets busy, this call will be forwarded.

(40) Press '*70' will disable call forwarding busy.

5.5.4.4.13 Call Forwarding All

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

(41) Dial '*74<NUM>#' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.

(42) Press '*73' to enable call forwarding all. That is, all incoming alls will be forwarded to the third party.

(43) Press '*75' will disable call forwarding all, but let call forwarding no answer and call forwarding busy unchanged.

(44) Press '*70' will disable all call forwarding function.

5.5.4.4.14 Three-Way Conference

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

(45) Assume you are in connection with a first party.

(46) Press 'FALSH' to put the first party on hold.

(47) Dial a third party.

(48) After the third party answers the call, press 'FLASH' again to invite the first party.

(49) Now all three parties are in a 3-way conference.

5.5.4.4.15 T38 Faxing

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

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

5.5.4.4.16 Pass-Through Faxing

If T38 support is not enabled, faxing will use normal voice codec as its coding approach. So this mode looks much like normal phone calls.

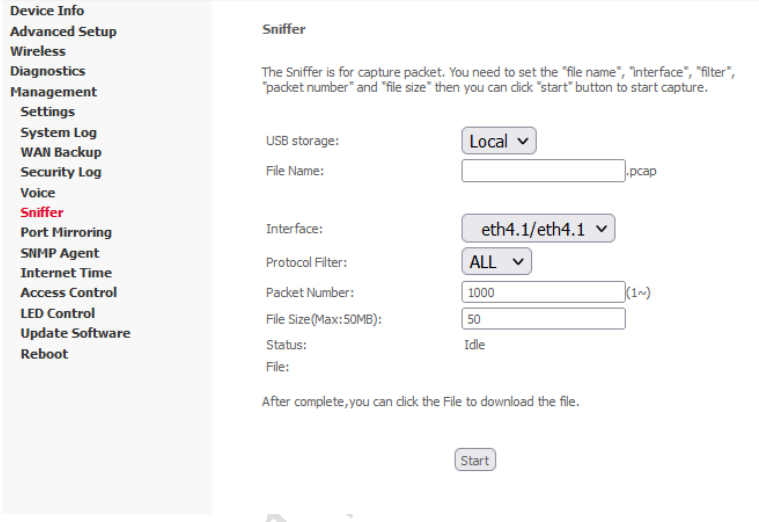
5.5.4.4.17 PSTN to VoIP Call

For incoming PSTN call, ROUTER can route it to local FXS-attached analog phones or other VoIP extension, depending on the setting. In 'Voice/SIP Advanced Setting', there are four schemes in 'Incoming PSTN call routing' drop list:

- Auto - PSTN Call switch to idle line: ROUTER automatically selects the idle line for incoming PSTN call.
- Line1 - PSTN Call switch to Line1: PSTN call is routed to line 1. If it is busy, PSTN call fails.
- Line2 - PSTN Call switch to Line2: PSTN call is routed to line 2.
- VoIP - PSTN Call switch to VoIP call: PSTN call is routed to VoIP extension, which is filled in 'PSTN Call Routing Data'.

5.5.5 Sniffer

Choose **Management > Sniffer**, and the following page appears.

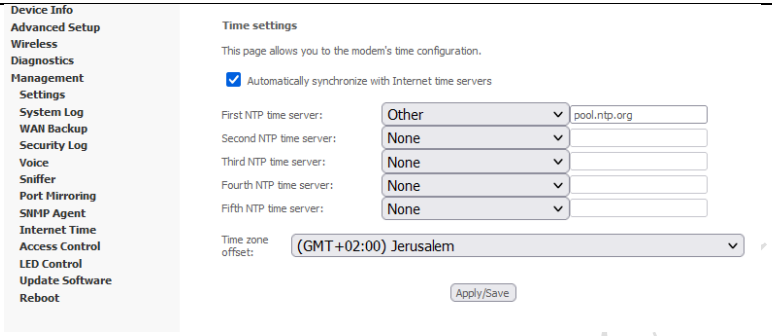


- **USB storage:** But after inserting the USB device, the captured packets will be automatically saved to the USB device.
- **File Name:** the name of the file
- **Interface:** Select the interface to capture packets
- **Protocol Filter:** Support to capture all protocols, or only capture TCP, or UDP
- **Packet Number:** Maximum number of capture packets
- **File Size(Max:50MB):** Maximum size of capture packets

After finishing setting, click the **Start** button to apply the settings.

5.5.6 Internet Time

Choose **Management > Internet Time**, and the following page appears.

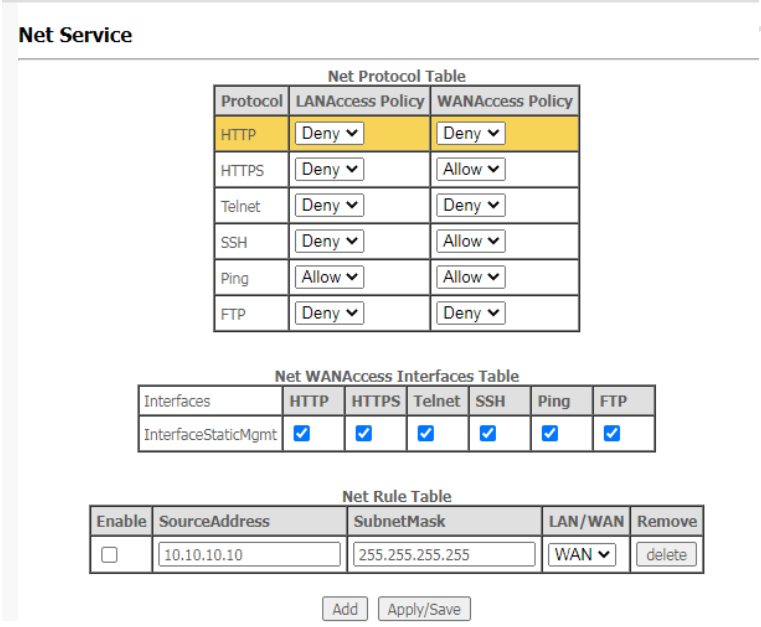


After finishing setting, click the **Save/Apply** button to save and apply the settings.

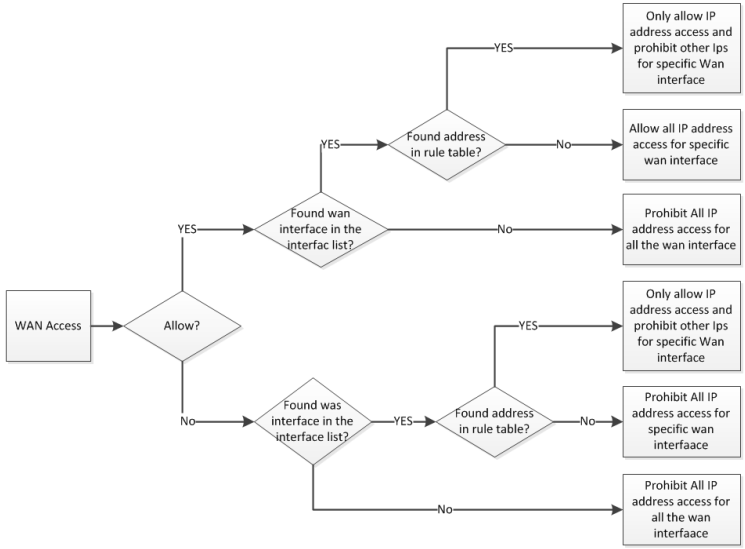
5.5.7 Access Control

5.5.7.1 Net Service

Choose **Management > Access Control > Net Service** to display the following page.

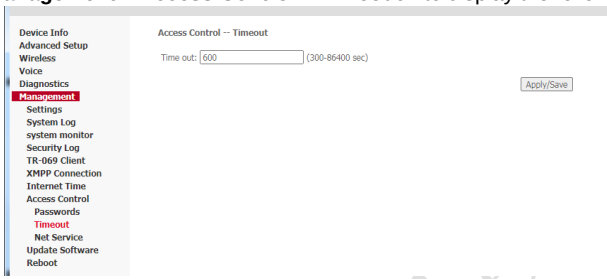


Net Service works together by three tables: Net Protocol Table, Net WANAccess Interfaces Table, Net Rule Table. The specific effective method is shown in the following figure:


WAN Access
Allow?
YES
Found wan interface in the interfac list?
YES
Found address in rule table?
YES
Only allow IP address access and prohibit other Ips for specific Wan interface
No
Allow all IP address access for specific wan interface
No
Prohibit All IP address access for all the wan interface
No
Found was interface in the interface list?
YES
Found address in rule table?
YES
Only allow IP address access and prohibit other Ips for specific Wan interface
No
Prohibit All IP address access for specific wan interfaace
No
Prohibit All IP address access for all the wan interfaace

5.5.7.2 Timeout

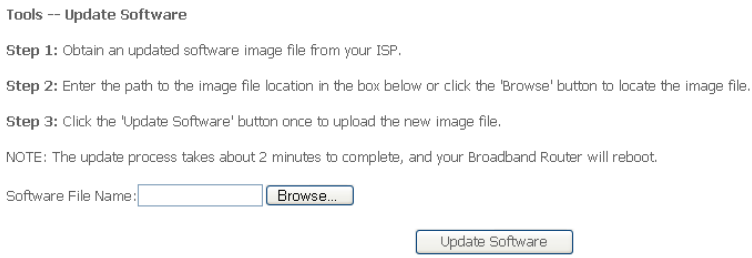
Choose **Management > Access Control > Timeout** to display the following page.



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

5.5.8 Update Software

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



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

Note:

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

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

Upgrade by cli:

upgrade img address

5.5.9 Reboot

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

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

6 Q&A

(50) **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.

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

A: Check the following:

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

(52) **Q**: Why I fail to access the web configuration page of the Router?

A: Choose **Start** > **Run** from the desktop, and ping ***10.10.0.138*** (IP address of the Router). If the Router is not reachable, check the type of the network cable, the connection between the Router and the PC, and the TCP/IP configuration of the PC.

(53) **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.

ANNEX

- FCC Regulations:
-
- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.
- However, there is no guarantee that interference will not occur in a particular installation If this equipment does cause harmful interference to radio or television
- reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the
- following measures:
- - Reorient or relocate the receiving antenna.
- - Increase the separation between the equipment and receiver.
- - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- - Consult the dealer or an experienced radio/TV technician for help.
-
- FCC Note:
- Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.
-
- RF Exposure Information
- This device meets the government’s requirements for exposure to radio waves.

- This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.
-
- This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm during normal operation.

- 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: HTTDL00AHT-178AX. If requested, this number must be provided to the telephone company.