- **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.

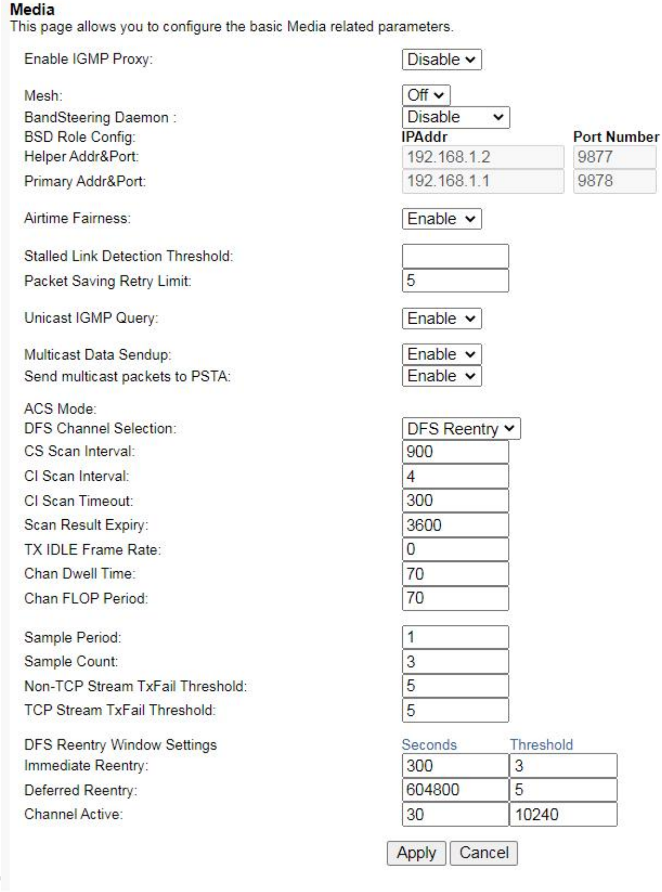
Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

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.



Media

This page allows you to configure the basic Media related parameters.

Enable IGMP Proxy:	Disable	
Mesh:	Off	
BandSteering Daemon :	Disable	
BSD Role Config:	**IPAddr**	**Port Number**
Helper Addr&Port:	192.168.1.2	9877
Primary Addr&Port:	192.168.1.1	9878
Airtime Fairness:	Enable	
Stalled Link Detection Threshold:		
Packet Saving Retry Limit:	5	
Unicast IGMP Query:	Enable	
Multicast Data Sendup:	Enable	
Send multicast packets to PSTA:	Enable	
ACS Mode:		
DFS Channel Selection:	DFS Reentry	
CS Scan Interval:	900	
CI Scan Interval:	4	
CI Scan Timeout:	300	
Scan Result Expiry:	3600	
TX IDLE Frame Rate:	0	
Chan Dwell Time:	70	
Chan FLOP Period:	70	
Sample Period:	1	
Sample Count:	3	
Non-TCP Stream TxFail Threshold:	5	
TCP Stream TxFail Threshold:	5	
DFS Reentry Window Settings	Seconds	Threshold
Immediate Reentry:	300	3
Deferred Reentry:	604800	5
Channel Active:	30	10240

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

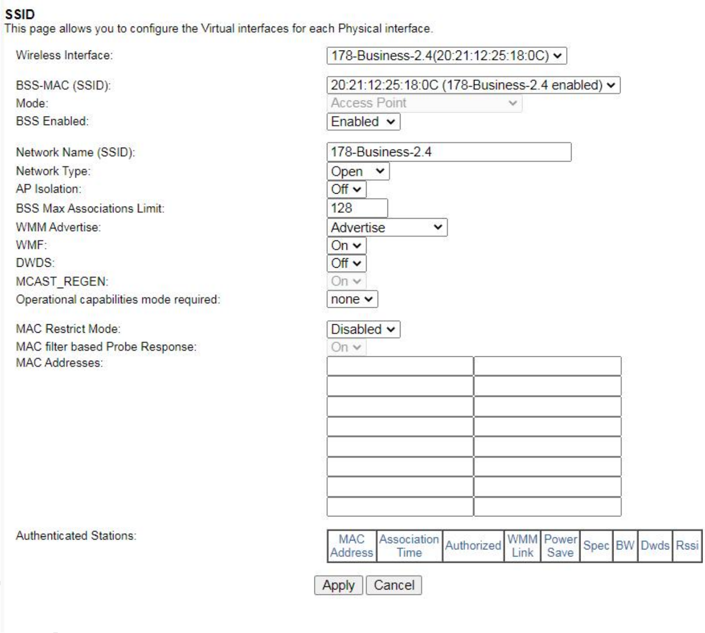
Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

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.



SSID

This page allows you to configure the Virtual interfaces for each Physical interface.

Wireless Interface:	178-Business-2.4(20:21:12:25:18:0C)
BSS-MAC (SSID):	20:21:12:25:18:0C (178-Business-2.4 enabled)
Mode:	Access Point
BSS Enabled:	Enabled
Network Name (SSID):	178-Business-2.4
Network Type:	Open
AP Isolation:	Off
BSS Max Associations Limit:	128
WMM Advertise:	Advertise
WMF:	On
DWDS:	Off
MCAST_REGEN:	On
Operational capabilities mode required:	none
MAC Restrict Mode:	Disabled
MAC filter based Probe Response:	On
MAC Addresses:	

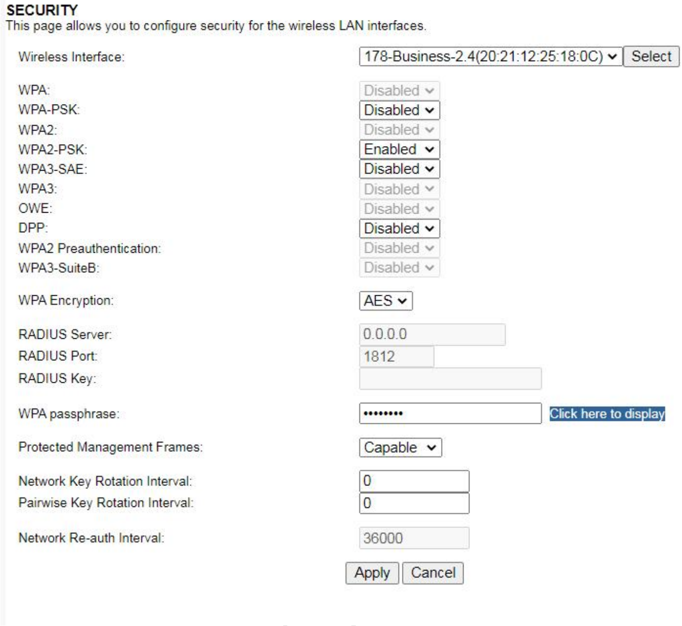
Authenticated Stations:

MAC Address	Association Time	Authorized	WMM Link	Power Save	Spec	BW	Dwds	Rssi

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.



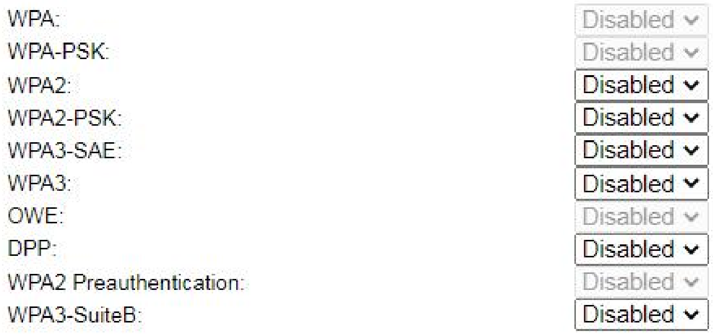
SECURITY

This page allows you to configure security for the wireless LAN interfaces.

Wireless Interface:	178-Business-2.4(20:21:12:25:18:0C) Select
WPA:	Disabled
WPA-PSK:	Disabled
WPA2:	Disabled
WPA2-PSK:	Enabled
WPA3-SAE:	Disabled
WPA3:	Disabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled
WPA Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA passphrase:	•••••••• Click here to display
Protected Management Frames:	Capable
Network Key Rotation Interval:	0
Pairwise Key Rotation Interval:	0
Network Re-auth Interval:	36000

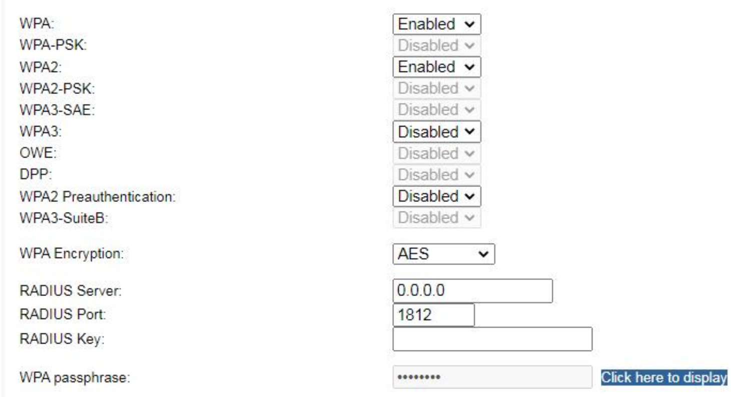
This page provides 7 types of network authentication modes, including open,WPA, WPA-PSK, WPA2, WPA2-PSK, WPA3-SAE, WPA3.

- **Open Mode**



WPA:	Disabled
WPA-PSK:	Disabled
WPA2:	Disabled
WPA2-PSK:	Disabled
WPA3-SAE:	Disabled
WPA3:	Disabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled

- **WPA and WPA2**

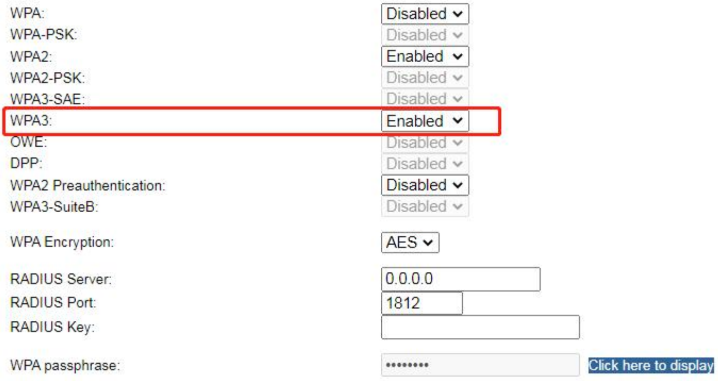


WPA:	Enabled
WPA-PSK:	Disabled
WPA2:	Enabled
WPA2-PSK:	Disabled
WPA3-SAE:	Disabled
WPA3:	Disabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled
WPA Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA passphrase:	•••••••• Click here to display

- **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**

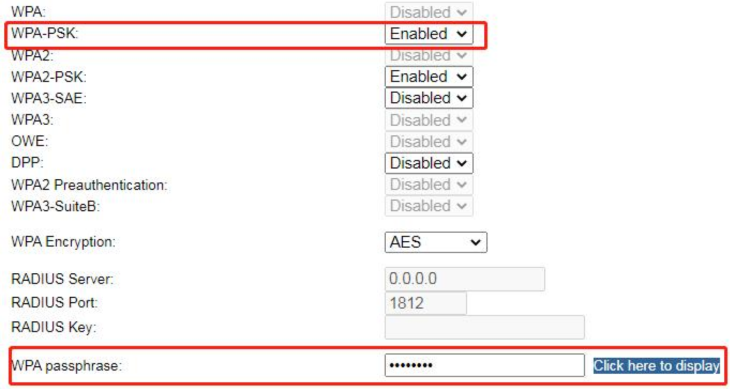


WPA:	Disabled
WPA-PSK:	Disabled
WPA2:	Enabled
WPA2-PSK:	Disabled
WPA3-SAE:	Disabled
WPA3:	Enabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled
WPA Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA passphrase:	•••••••• Click here to display

- **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**

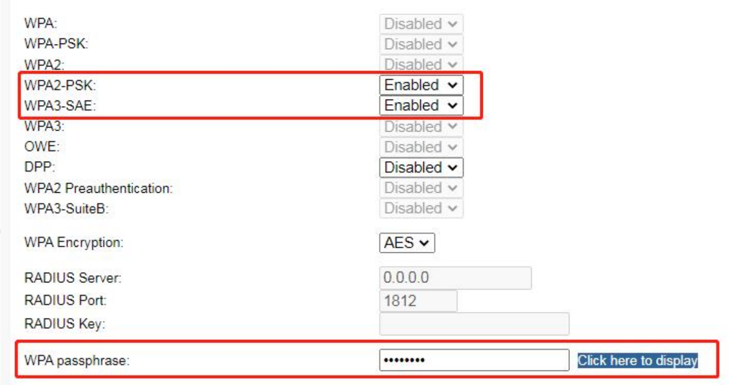


WPA:	Disabled
WPA-PSK:	Enabled
WPA2:	Disabled
WPA2-PSK:	Enabled
WPA3-SAE:	Disabled
WPA3:	Disabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled
WPA Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA passphrase:	••••••••

- **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**



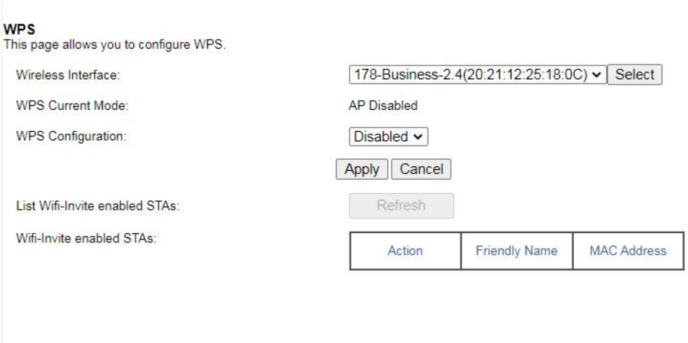
WPA:	Disabled
WPA-PSK:	Disabled
WPA2:	Disabled
WPA2-PSK:	Enabled
WPA3-SAE:	Enabled
WPA3:	Disabled
OWE:	Disabled
DPP:	Disabled
WPA2 Preauthentication:	Disabled
WPA3-SuiteB:	Disabled
WPA Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA passphrase:	••••••••

- **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.



WPS

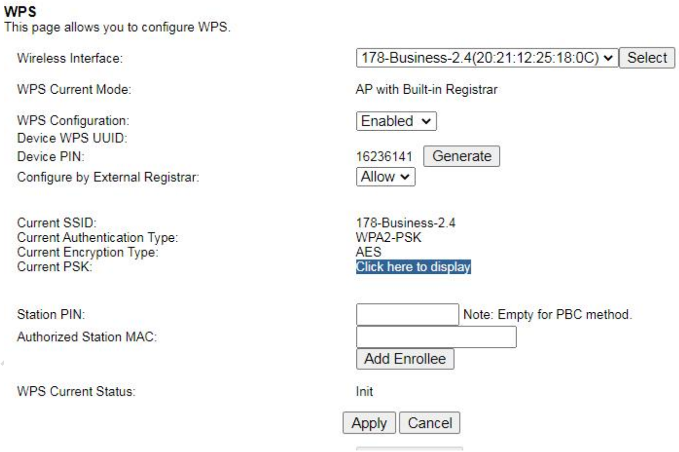
This page allows you to configure WPS.

Wireless Interface:	178-Business-2.4(20:21:12:25:18:0C) Select
WPS Current Mode:	AP Disabled
WPS Configuration:	Disabled
	Apply Cancel
List Wifi-Invite enabled STAs:	Refresh
Wifi-Invite enabled STAs:	

Action	Friendly Name	MAC Address

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**



WPS

This page allows you to configure WPS.

Wireless Interface:	178-Business-2.4(20:21:12:25:18:0C) Select
WPS Current Mode:	AP with Built-in Registrar
WPS Configuration:	Enabled
Device WPS UUID:	
Device PIN:	16236141 Generate
Configure by External Registrar:	Allow
Current SSID:	178-Business-2.4
Current Authentication Type:	WPA2-PSK
Current Encryption Type:	AES
Current PSK:	Click here to display
Station PIN:	Note: Empty for PBC method.
Authorized Station MAC:	
	Add Enrollee
WPS Current Status:	Init
	Apply Cancel

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.

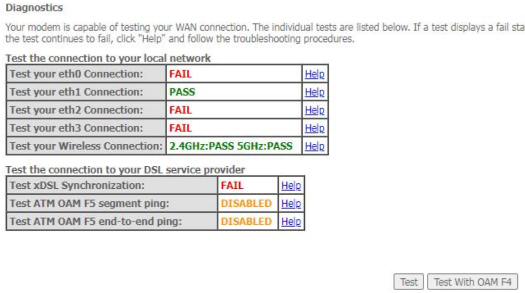
5.4 Diagnostics

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.



Diagnostics

Your modem is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Test'
the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

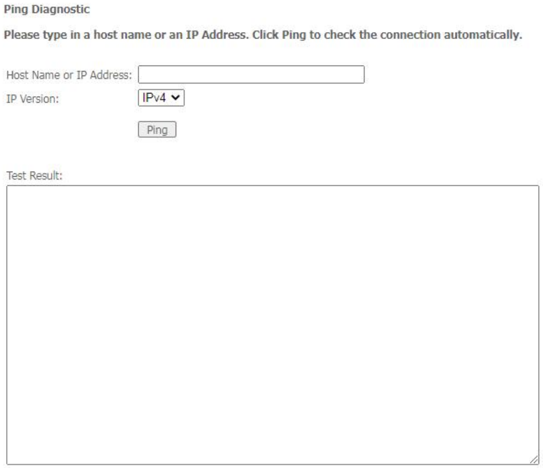
Test your eth0 Connection:	FAIL	Help
Test your eth1 Connection:	PASS	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	FAIL	Help
Test your Wireless Connection:	2.4GHz:PASS 5GHz:PASS	Help

Test the connection to your DSL service provider

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

5.4.2 Ping

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



Ping Diagnostic

Please type in a host name or an IP Address. Click Ping to check the connection automatically.

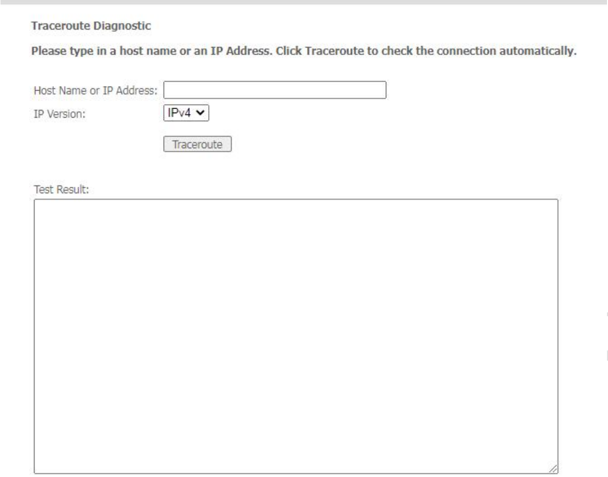
Host Name or IP Address:

IP Version: IPv4

Test Result:

5.4.1 Traceroute

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



Traceroute Diagnostic

Please type in a host name or an IP Address. Click Traceroute to check the connection automatically.

Host Name or IP Address:

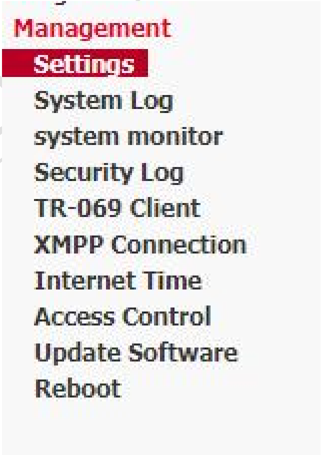
IP Version: IPv4

Traceroute

Test Result:

5.5 Management

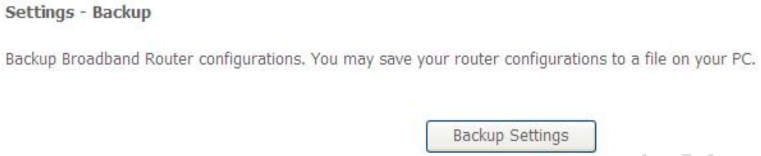
Choose **Management** and the submenus of **Management** are shown as below:



5.5.1 Settings

5.5.1.1 Backup

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



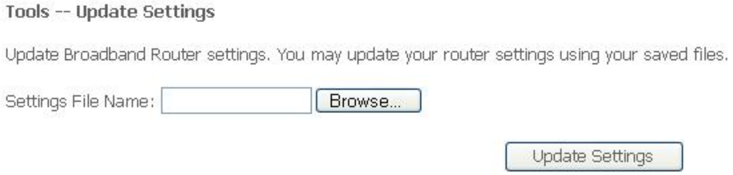
Settings - Backup

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

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.



Tools -- Update Settings

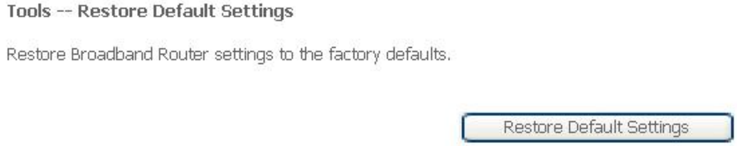
Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

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.



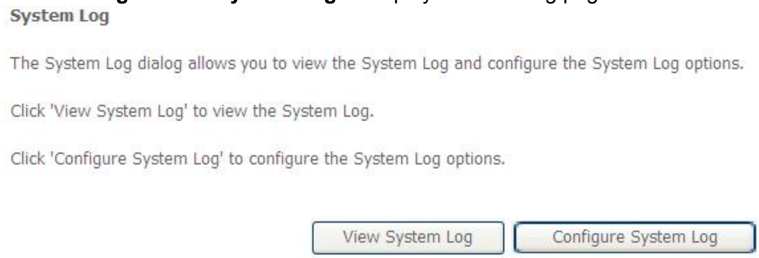
Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

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.



System Log

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

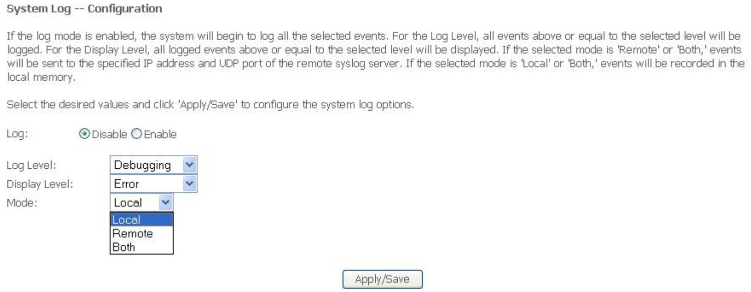
Click 'View System Log' to view the System Log.

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

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

- **Configuring the System Log**

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



System Log -- Configuration

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

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

Log: ● Disable ○ Enable

Log Level: Debugging

Display Level: Error

Mode: Local

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

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

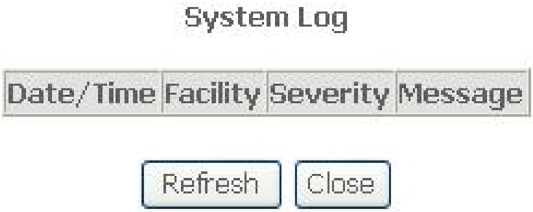
After finishing setting, click the **Apply/Save** button to save and apply the settings.

Note:

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

- **View System Log**

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



System Log

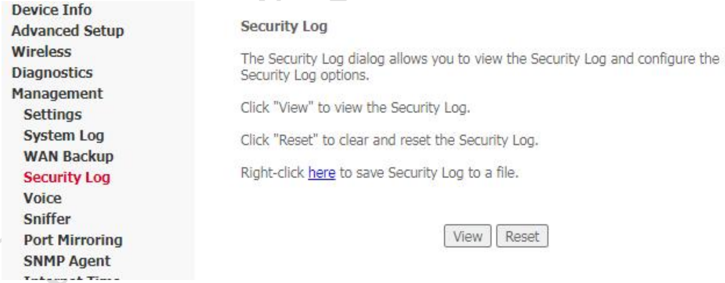
Date/Time	Facility	Severity	Message

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.



Security Log

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

Click "View" to view the Security Log.

Click "Reset" to clear and reset the Security Log.

Right-click here to save Security Log to a file.

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.

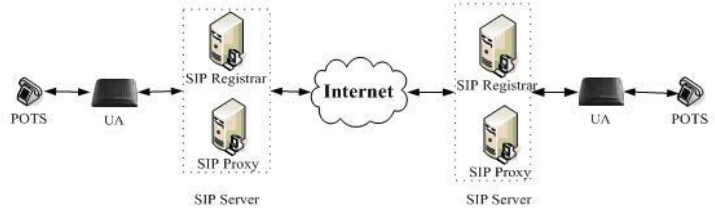
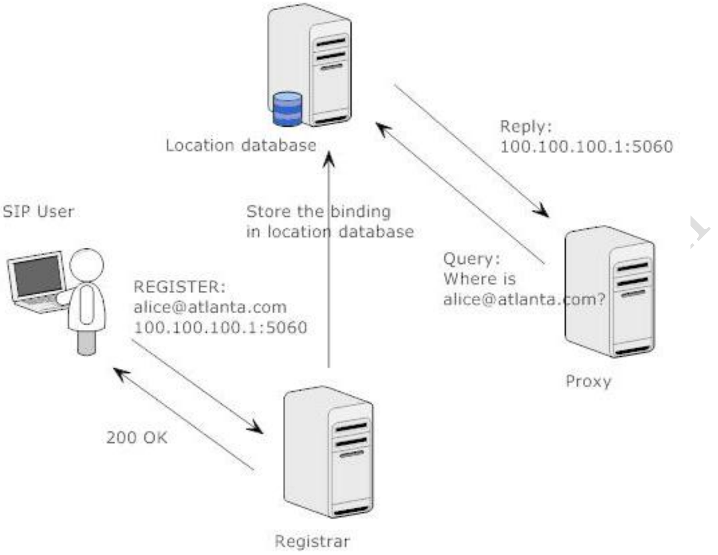


Figure 6 SIP application

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.



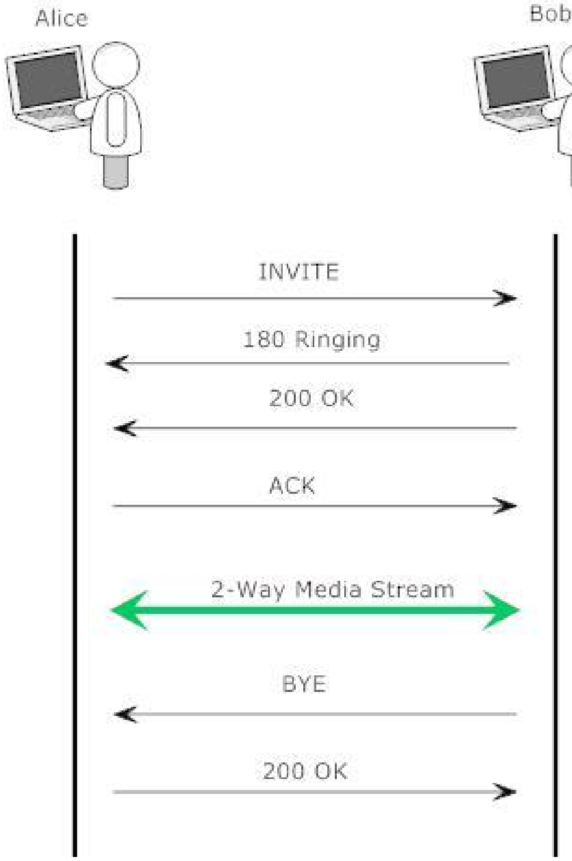
5.5.4.2.2 Simple Call Flow

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.

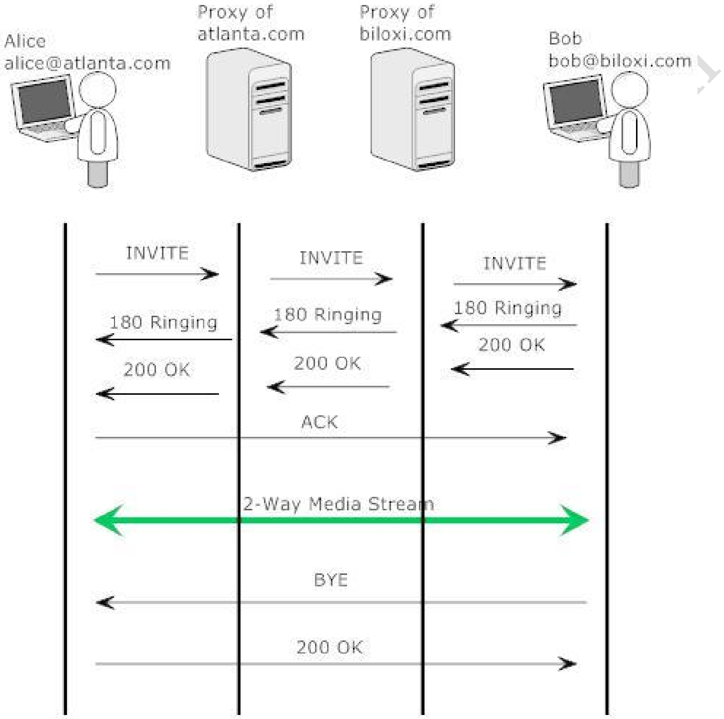


5.5.4.2.3 Call Flow in Proxy Mode

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.

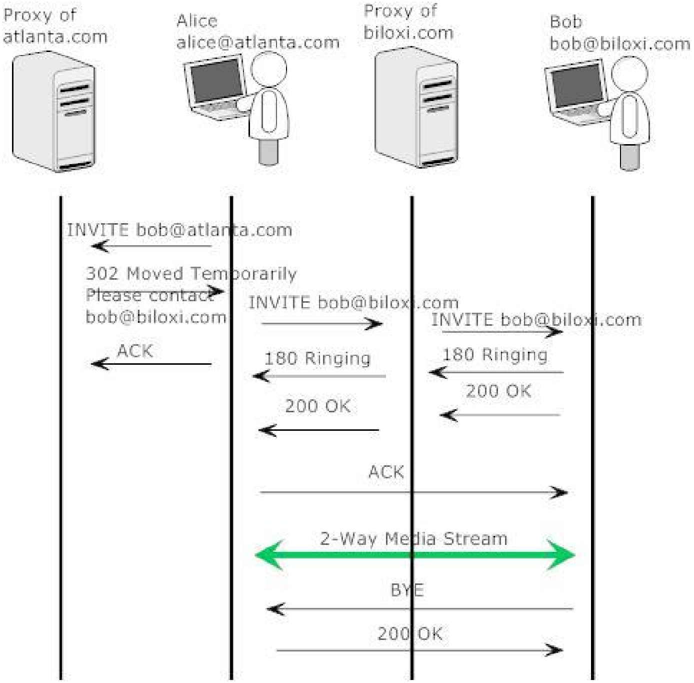
In this flow, Alice is located in atlanta.com. She is going to place a call to Bob, whose SIP URL is bob@biloxi.com. Alice's user agent passes the INVITE message to its proxy, atlanta.com. From the request URL in SIP message, Alice's proxy determines the next hop is proxy biloxi.com, and passes this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

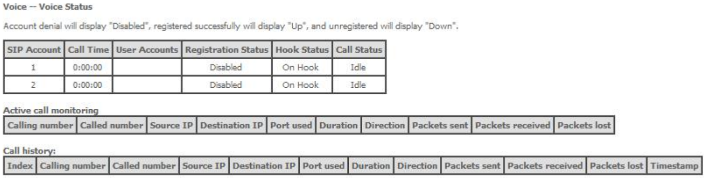

Proxy of
atlanta.com
Alice
alice@atlanta.com
Proxy of
biloxi.com
Bob
bob@biloxi.com
INVITE bob@atlanta.com
302 Moved Temporarily
Please contact
bob@biloxi.com
INVITE bob@biloxi.com
INVITE bob@biloxi.com
ACK
180 Ringing
180 Ringing
200 OK
200 OK
ACK
2-Way Media Stream
BYE
200 OK

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

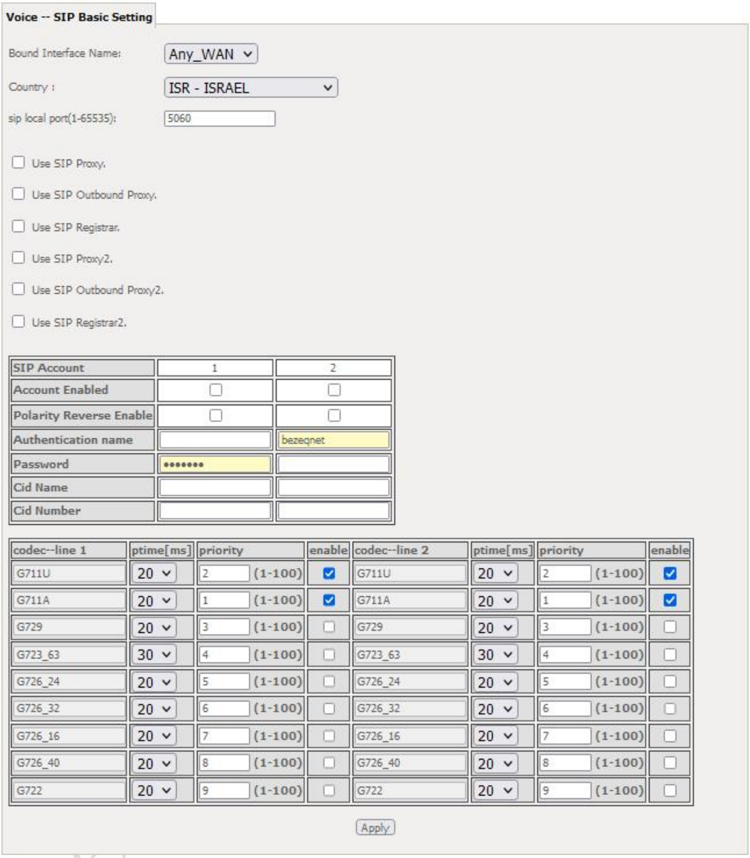
Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost

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.



Voice -- SIP Basic Setting

Bound Interface Name: Any_WAN

Country : ISR - ISRAEL

sip local port(1-65535): 5060

☐ Use SIP Proxy.

☐ Use SIP Outbound Proxy.

☐ Use SIP Registrar.

☐ Use SIP Proxy2.

☐ Use SIP Outbound Proxy2.

☐ Use SIP Registrar2.

SIP Account	1	2
Account Enabled	☐	☐
Polarity Reverse Enable	☐	☐
Authentication name		bezeqnet
Password	•••••••	
Cid Name		
Cid Number		

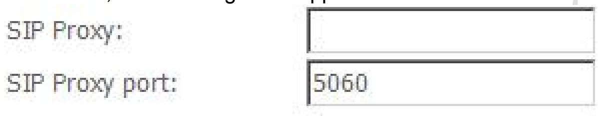
codec--line 1	ptime[ms]	priority	enable	codec--line 2	ptime[ms]	priority	enable
G711U	20	2 (1-100)	☑	G711U	20	2 (1-100)	☑
G711A	20	1 (1-100)	☑	G711A	20	1 (1-100)	☑
G729	20	3 (1-100)	☐	G729	20	3 (1-100)	☐
G723_63	30	4 (1-100)	☐	G723_63	30	4 (1-100)	☐
G726_24	20	5 (1-100)	☐	G726_24	20	5 (1-100)	☐
G726_32	20	6 (1-100)	☐	G726_32	20	6 (1-100)	☐
G726_16	20	7 (1-100)	☐	G726_16	20	7 (1-100)	☐
G726_40	20	8 (1-100)	☐	G726_40	20	8 (1-100)	☐
G722	20	9 (1-100)	☐	G722	20	9 (1-100)	☐

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:



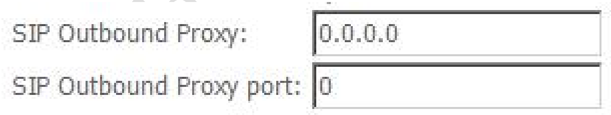
SIP Proxy:

SIP Proxy port: 5060

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:



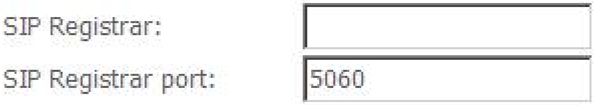
SIP Outbound Proxy: 0.0.0.0

SIP Outbound Proxy port: 0

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:

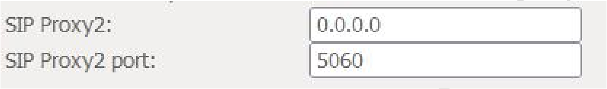


SIP Registrar:	
SIP Registrar port:	5060

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:

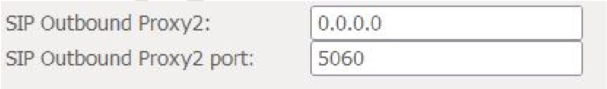


SIP Proxy2:	0.0.0.0
SIP Proxy2 port:	5060

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:

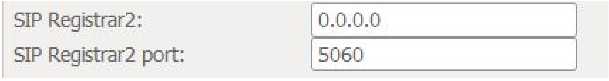


SIP Outbound Proxy2:	0.0.0.0
SIP Outbound Proxy2 port:	5060

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:	0.0.0.0
SIP Registrar2 port:	5060

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.

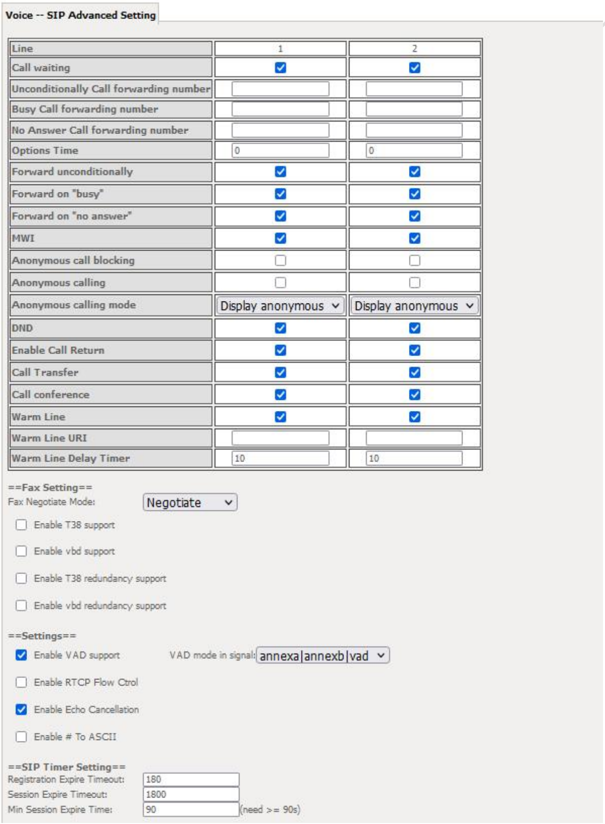
- **Account Enabled:** Line number is a telephone port in the Router to which you can connect a standard (POTS) telephone. If you select this check box, the corresponding line is disabled. You cannot use it to initiate or accept any call.
- **Polarity Reverse Enable:** The positive and negative poles 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).



Voice -- SIP Advanced Setting

Line	1	2
Call waiting	☑	☑
Unconditionally Call forwarding number		
Busy Call forwarding number		
No Answer Call forwarding number		
Options Time	0	0
Forward unconditionally	☑	☑
Forward on "busy"	☑	☑
Forward on "no answer"	☑	☑
MWI	☑	☑
Anonymous call blocking	☐	☐
Anonymous calling	☐	☐
Anonymous calling mode	Display anonymous	Display anonymous
DND	☑	☑
Enable Call Return	☑	☑
Call Transfer	☑	☑
Call conference	☑	☑
Warm Line	☑	☑
Warm Line URI		
Warm Line Delay Timer	10	10

==Fax Setting==

Fax Negotiate Mode: Negotiate

☐ Enable T38 support

☐ Enable vbd support

☐ Enable T38 redundancy support

☐ Enable vbd redundancy support

==Settings==

☑ Enable VAD support VAD mode in signal: annexa|annexb|vad

☐ Enable RTCP Flow Ctrol

☑ Enable Echo Cancellation

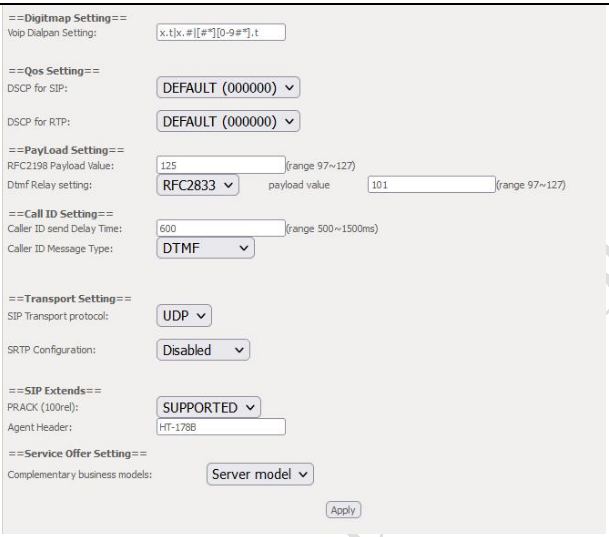
☐ Enable # To ASCII

==SIP Timer Setting==

Registration Expire Timeout: 180

Session Expire Timeout: 1800

Min Session Expire Time: 90 (need >= 90s)



==Digitmap Setting==

Voip Dialpan Setting: x.t|x.#|[#*][0-9#*].t

==Qos Setting==

DSCP for SIP: DEFAULT (000000)

DSCP for RTP: DEFAULT (000000)

==PayLoad Setting==

RFC2198 Payload Value: 125 (range 97~127)

Dtmf Relay setting: RFC2833 payload value 101 (range 97~127)

==Call ID Setting==

Caller ID send Delay Time: 600 (range 500~1500ms)

Caller ID Message Type: DTMF

==Transport Setting==

SIP Transport protocol: UDP

SRTP Configuration: Disabled

==SIP Extends==

PRACK (100rel): SUPPORTED

Agent Header: HT-178B

==Service Offer Setting==

Complementary business models: Server model

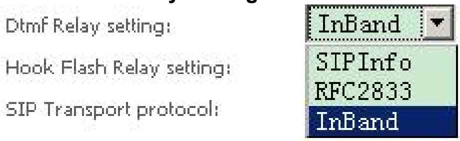
- **Line**: Stands for which line you want to configure.
- **Call waiting**: If call waiting is enabled on a line (see feature codes on the below), and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between 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**



Dtmf Relay setting: InBand

Hook Flash Relay setting:

SIP Transport protocol:

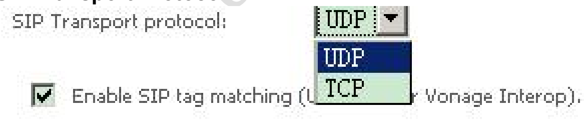
Set DTMF transmit method, which can be following values:

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**



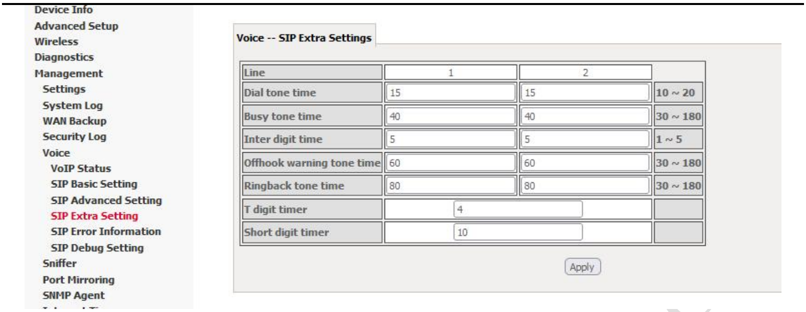
SIP Transport protocol: UDP

☑ Enable SIP tag matching (U r Vonage Interop).

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.

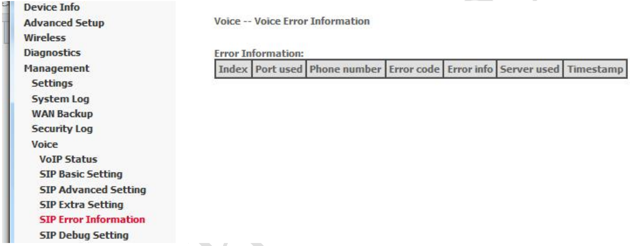


Voice -- SIP Extra Settings

Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 5
Offhook warning tone time	60	60	30 ~ 180
Ringback tone time	80	80	30 ~ 180
T digit timer	4		
Short digit timer	10		

5.5.4.3.5 SIP Error Information

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



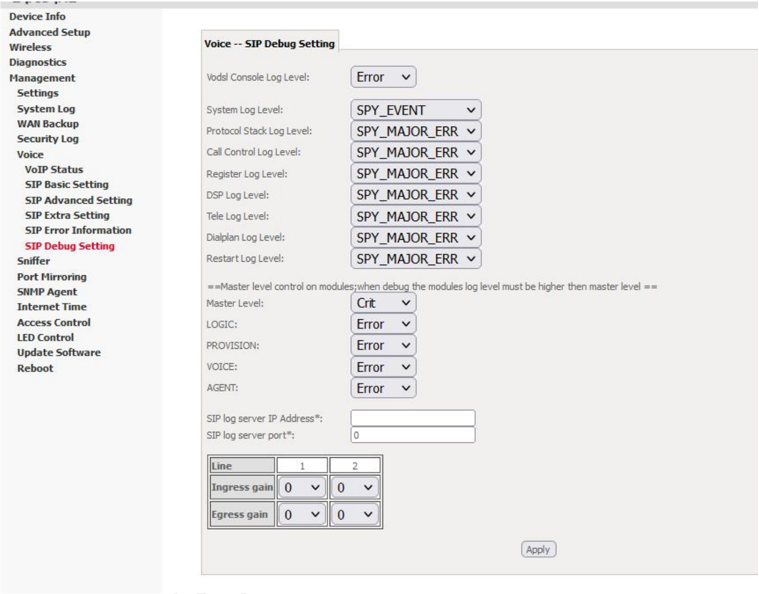
Voice -- Voice Error Information

Error Information:

Index	Port used	Phone number	Error code	Error info	Server used	Timestamp

5.5.4.3.6 SIP Debug Setting

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



Voice -- SIP Debug Setting

Vodsl Console Log Level: Error

System Log Level: SPY_EVENT
Protocol Stack Log Level: SPY_MAJOR_ERR
Call Control Log Level: SPY_MAJOR_ERR
Register Log Level: SPY_MAJOR_ERR
DSP Log Level: SPY_MAJOR_ERR
Tele Log Level: SPY_MAJOR_ERR
Dialplan Log Level: SPY_MAJOR_ERR
Restart Log Level: SPY_MAJOR_ERR

==Master level control on modules;when debug the modules log level must be higher then master level ==
Master Level: Crit
LOGIC: Error
PROVISION: Error
VOICE: Error
AGENT: Error

SIP log server IP Address*:
SIP log server port*: 0

Line	1	2
Ingress gain	0	0
Egress gain	0	0

Apply

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.

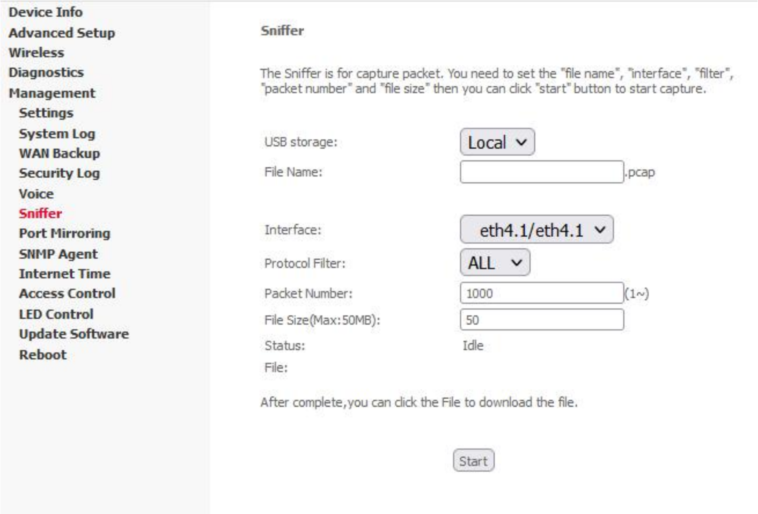
5.5.4.4.17 PSTN to VoIP Call

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.



Sniffer

The Sniffer is for capture packet. You need to set the "file name", "interface", "filter", "packet number" and "file size" then you can click "start" button to start capture.

USB storage: Local

File Name: .pcap

Interface: eth4.1/eth4.1

Protocol Filter: ALL

Packet Number: 1000 (1~)

File Size(Max:50MB): 50

Status: Idle

File:

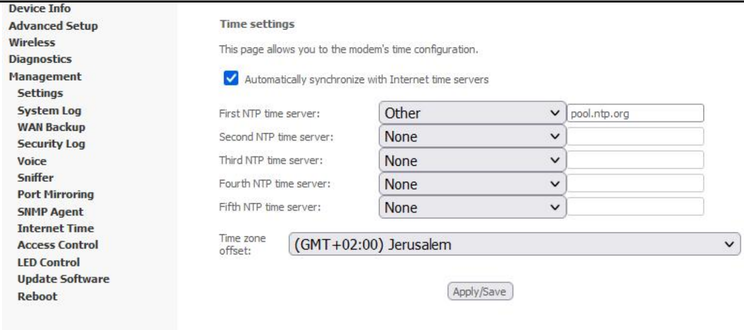
After complete,you can click the File to download the file.

- **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.



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server:	Other	pool.ntp.org
Second NTP time server:	None	
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

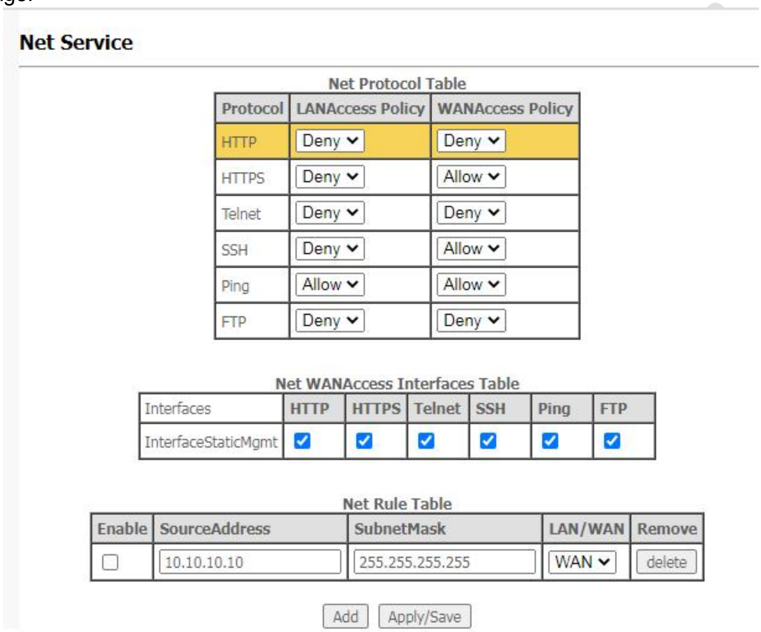
Time zone offset: (GMT+02:00) Jerusalem

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

Net Protocol Table

Protocol	LANAccess Policy	WANAccess Policy
HTTP	Deny	Deny
HTTPS	Deny	Allow
Telnet	Deny	Deny
SSH	Deny	Allow
Ping	Allow	Allow
FTP	Deny	Deny

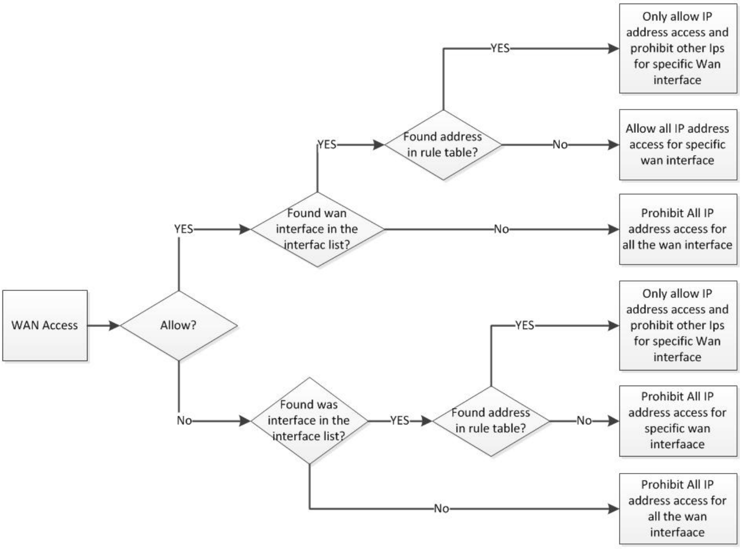
Net WANAccess Interfaces Table

Interfaces	HTTP	HTTPS	Telnet	SSH	Ping	FTP
InterfaceStaticMgmt	☑	☑	☑	☑	☑	☑

Net Rule Table

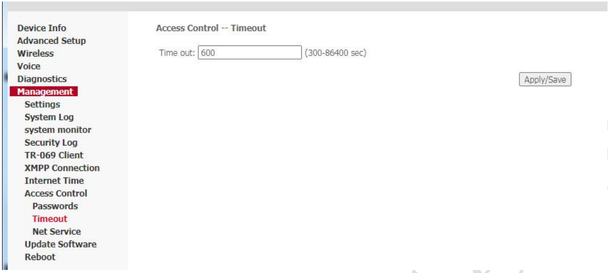
Enable	SourceAddress	SubnetMask	LAN/WAN	Remove
□	10.10.10.10	255.255.255.255	WAN	delete

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



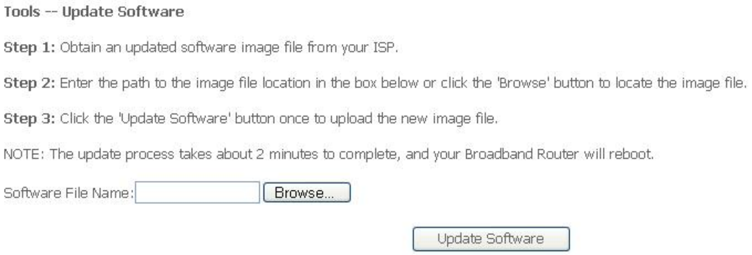
Access Control -- Timeout

Time out: 600 (300-86400 sec)

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.



Tools -- Update Software

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

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

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

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

Software File Name:

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.

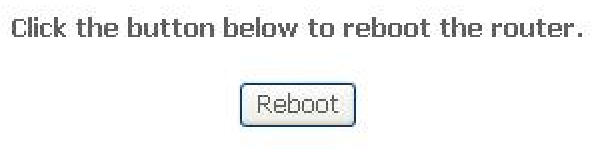
Please make sure that the new software for updating is correct, and do not use other software to update the router.

Upgrade by cli:

upgrade img address

5.5.9 Reboot

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



Click the button below to reboot the router.

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.