Installation and Configuration Manual of GW5051

Rev: 0.2

Table of Contents

Revision Information

Revision #	Description	Date	Author
V 0.1	First release.	April 16, 2010	Ken Leng Chris Han
V 0.2	Change the WAN configuration and WEB basic color	May 10, 2010	Ken Leng Chris Han

Regulatory statement (R&TTE)

European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835GHz; In France, the equipment must be restricted to the 2.4465-2.4835GHz frequency range and must be restricted to indoor use.

List of national codes

Country	*ISO 3166 2 letter code*	Country	*ISO 3166 2 letter code*
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CZ	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstei n	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
atvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

1. Introduction

GW5051 wireless VoIP gateway provides you the cost-effective and integrated voice and high-speed data access. Together with IEEE 802.11b/g, GW5051 provides wireless mobility. Power Sourcing Equipment (PSE) over WAN interface provides indoor For small enterprise and home
office, you are able to experience the quality voice over IP service and data connection with most convenient wireless broadband access solution.

The Users Manual shows you the installation and the configurations of the GW5051

Features

- PSE over WAN interface
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- VoIP which supports SIP protocol (RFC3261)
- Support IEEE 802.11b/g WLAN
- Network configuration through DHCP
- PPPoA / PPPoE
- NAT / NAPT
- Web-based configuration browser such as Microsoft IE, Netscape Navigator, Mozilla Firefox, etc.

System Requirements

Along with GW5051, you also need the following equipments or services before installation.

- Indoor unit which provides broadband connection and GW5051.
- Computers which equips at least an Ethernet 10Base-T/100Base-T network interface card (port) or 802.11b/g/n WLAN card / adapter.
- A web browser, such as Microsoft Internet Explorer (V5.0 or later version) or Netscape Navigator (V4.7 or later version), which is used to configure the GW5051.

2. Hardware Installation

2.1. Accessories

Upon opening the gift box of GW5051 wireless VoIP gateway, you will find following parts in the box.

- GW5051 x 1
- Power adapter x 1
- Power core x 1
- Ethernet cable x 1
- Telephone cable x 2
- Quick Installation Guide x 1

2.2. Connectorizations

All the connectors, reset button power switch and power jack are on the rear panel whose picture is shown below.

Picture / diagram are to be inserted here.

The functions of the connectors are described in following table.

Label	Color	Function
POWER	BLACK	Connect to power adaptor.
ON / OFF	BLACK	Turn on / off power.
RESET	BLACK	Shortly push RESET button to restart the device. Long press RESET button to reset the configuration to factory default and restart the device.
WAN	SILVER	Connect modem with 8P8C RJ45 cable. It also provide power to outdoor modem.
LAN1 ~ LAN4	YELLOW	RJ-45 connectors, connect the device to your PC's Ethernet port, or to the uplink port on your LAN's hub or home gateway, using the Ethernet cables.
VoIP1 ~ VoIP2	BLACK	RJ-11 connectors, connect the device to regular phones.

2.3. Indicators

All LED indicators are on front panel which is shown below. Their functions are listed in following table.

Picture / diagram are to be inserted here.

Label	Color	Function
POWER	Light-Green	Steadily off: Power is off. Solid on: Power on
WLAN	Light-Green	Steadily off: Wi-Fi is disabled. Blinking: Traffic is passing thru. Steadily on: Wi-Fi is activated.
VoIP1 ~ VoIP2	Light-Green	Steadily off: Regular phone is on hook. Solid on: Regular phone is off hook.
LAN1 ~ LAN4	Light-Green	Steadily off: Wired interface not established (Ethernet cable not detected or not connected properly). Blinking: Traffic is passing thru. Steadily on: Wired interface established (Ethernet cable detected).
WAN	Light-Green	Steadily off: Wired interface not established (Ethernet cable not detected or not connected properly). Blinking: Traffic is passing thru. Steadily on: Wired interface established (Ethernet cable detected).

2.4. Connecting the Hardware

You have to follow the steps to connect GW5051 to all the peripherals. The diagram, shown below, depicts the generic connections of all equipments. It might be different from the picture below which depends on your applications.

WARNING

Power off all the devices before connecting them. *They include the computer(s), LAN hub / switch (if applicable), and the GW5051.*

Picture / diagram are to be inserted here.

Step 1. Connect the indoor unit

Connect WAN interface of GW5051 and LAN port of indoor unit
using Ethernet cable. Please be well noted that the line must be xDSL subscribed.

Step 2. Connect the Telephone

Connect regular phone and VoIP interface of GW5051 using telephone line.

Step 3. Connect the PC

Connect the yellow cable to the ETH0 / ETH1 jack (yellow one) and plug the other end to WAN port of your PC or hub.

Step 4. Connect the Power Adaptor

Connect plug of the power adaptor to the power jack (black one) of GW5051 then connect the plug of power core to the outlet on the wall or power strip. Power on GW5051.

WARNING

In order for the safety, please don't use the power adaptor which is not we provide.

Step 5. Turn on your PC.

Power on your PC and hub if there is any.

Step 6. Configure GW5051

Configure GW5051 through the web browser on your PC. The detailed procedures shall be described in Chapter 3.

Step 7. Save the configurations and reboot

It is important to save all the configurations you set and reboot again to affect all the programming items.

3. Configuration

3.1. Before Configuration

Before configuration, you have to connect and power on GW5051 and PC according to the steps described in Chapter 2. The default IP address of GW5051 is “192.168.1.1” and the default port number is 80.

3.2. Establish the Connection

Enter the IP address and Port (default is 192.168.1.1:80) on your web browser. A dialogue box is popped up and request to ether the user name and password. (Figure 3-2-1)

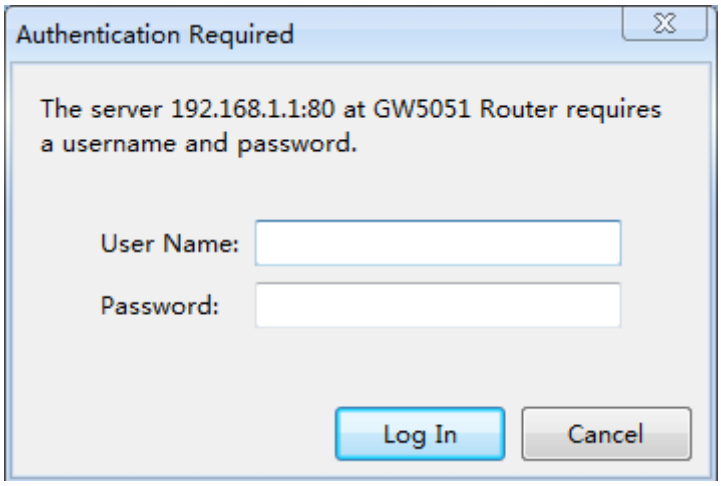


Figure 3-2-1. Authentication

Please use the default user name and password, “admin” and “admin”, and click OK button to login into the system.

Once authentication process is verified, the home page “Device Info” is shown on your browser. (Figure 3-2-2)

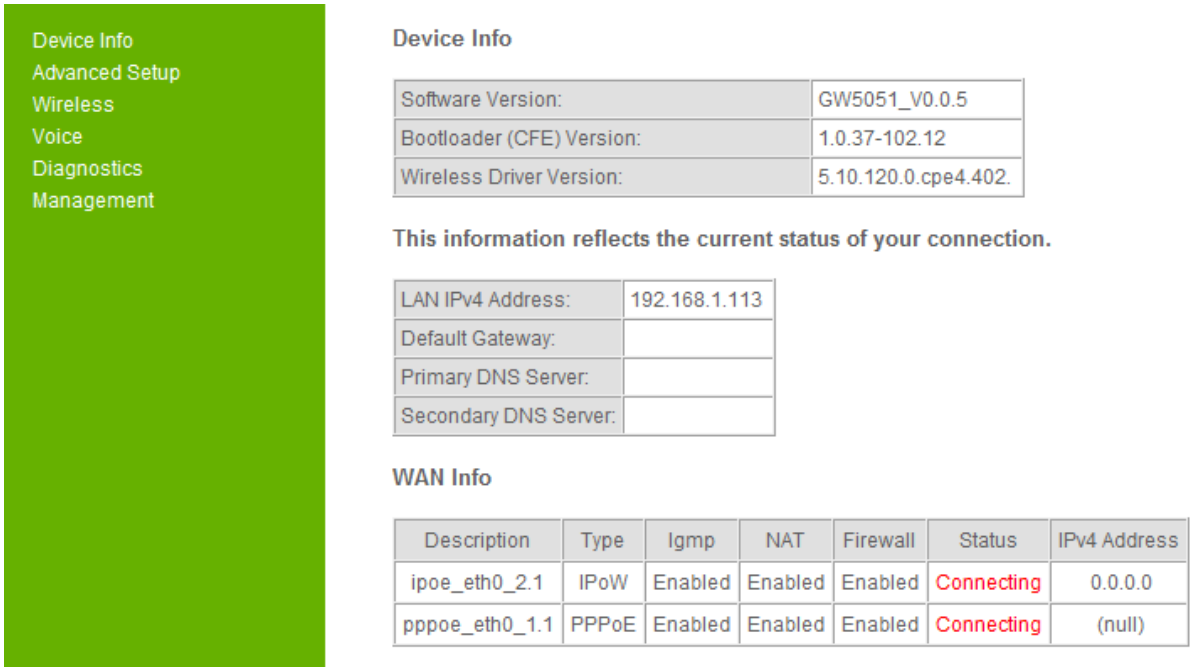


Figure 3-2-2. Device Info Page

In “Device Info” page, it shows you the basic information about the equipment, such as software version, MAC address, serial number, as well as runtime information like Memory usage ratio, time from last reboot. Also it will show information of the xDSL connection and WAN connection

3.3. LAN

Click the “Advanced Setup/LAN” button on the left hand side to enter into the configuration of LAN.

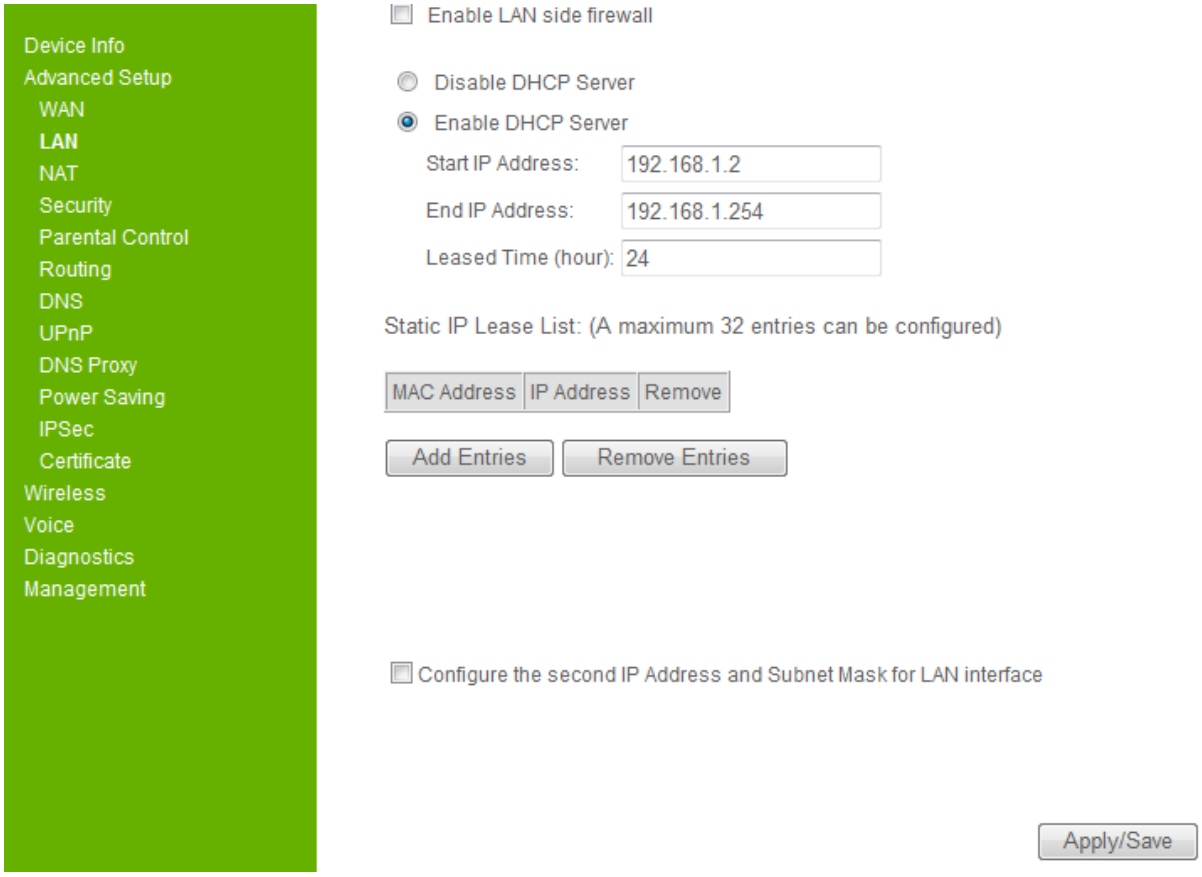


Figure 3-3. LAN

In this page, you may program the IP address of LAN, its Subnet Mask and the MTU (Maximum Transmission Unit). You may check or uncheck the “Enable IGMP Snooping”. There are two modes to be selected once you check this item.

Additionally, you may also disable or enable the DHCP server and related setting of DHCP server.

At the bottom of this page, you may check “Configure the second IP address and subnet mask for LAN interface” to setup additional LAN interface. Please be well noted that this IP address is used for management purpose only.

Before you leave, please click “Apply/ Save” button to save the changes you made.

3.4. WAN

Click the “Advanced Setup/ WAN” button on the left hand side of the web page to enter into the WAN configuration.

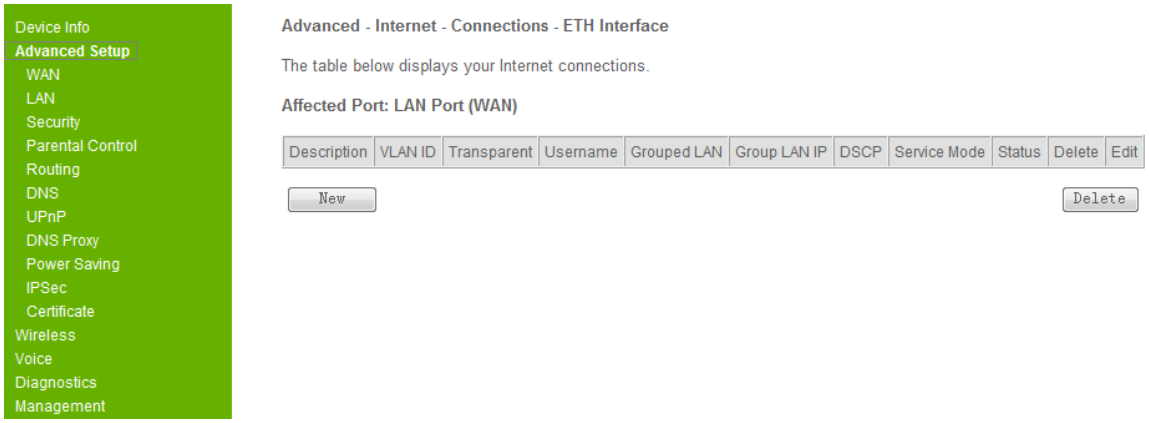


Figure 3-4. WAN Connection

Click the “New” button to create the WAN connection.

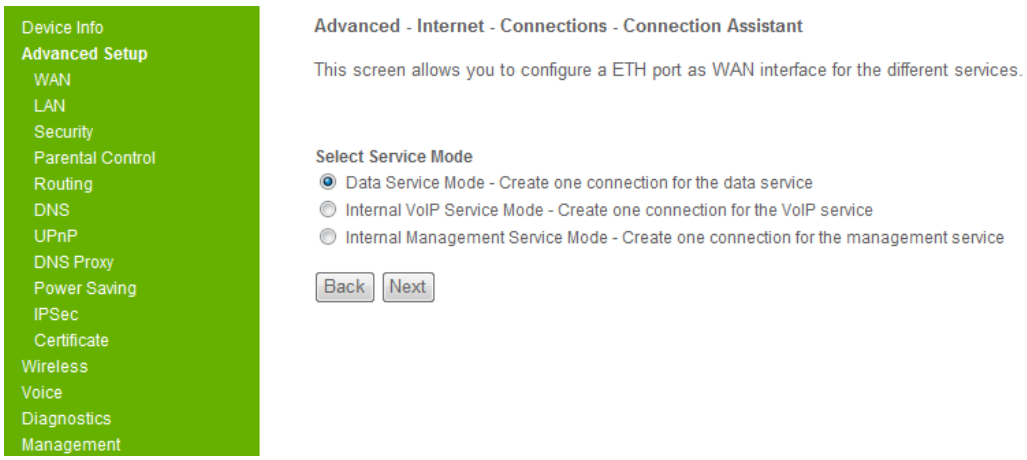
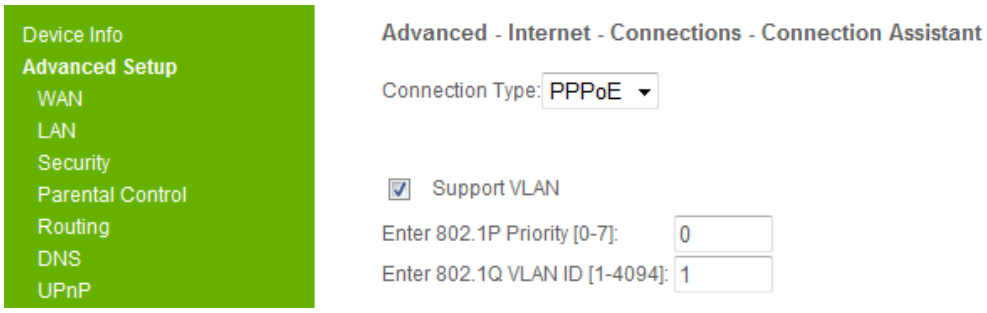


Figure 3-4. WAN Connection - 2

The detailed descriptions of each Service Mode are depicted forward.

3.4.1. DATA Service Mode

The DATA Service Mode allows you to create one connection for the data service. Select it and click the “Next” button, it will show



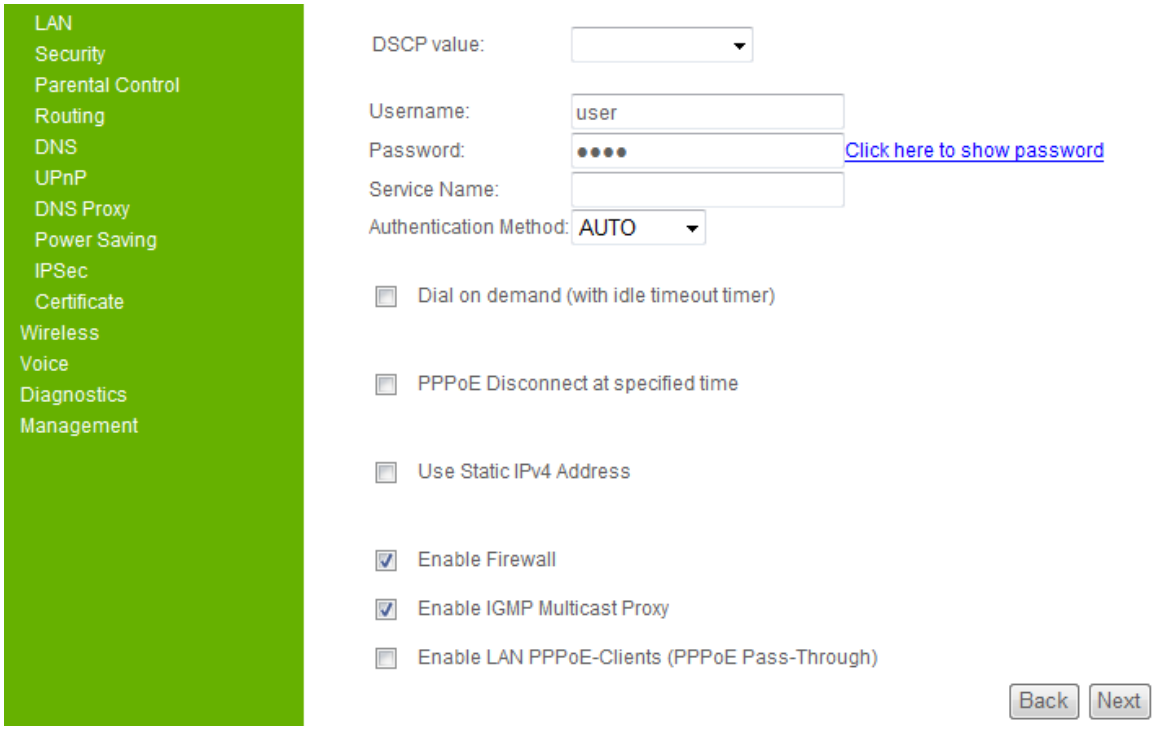


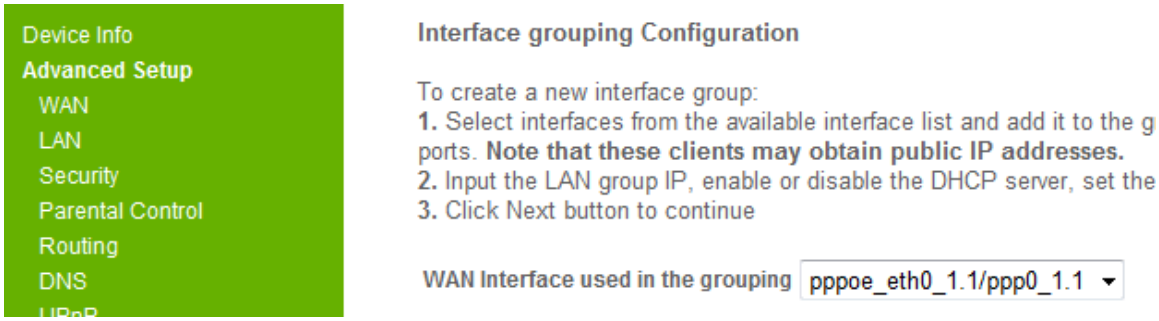
Figure 3-4-1. WAN – Data service Interface-PPPoE-1

Select your connection type, PPPoE and IPoE is for route mode, Bridge is for bridge mode.

If you select PPPoE connection type, please enter your username and password.

For advanced user, you can customize 802.1P priority, 802.1Q VLAN ID, DSCP value, dial on demand, disconnection time, static IP address, firewall, IGMP and LAN PPPoE service.

And then click the “Next” button.



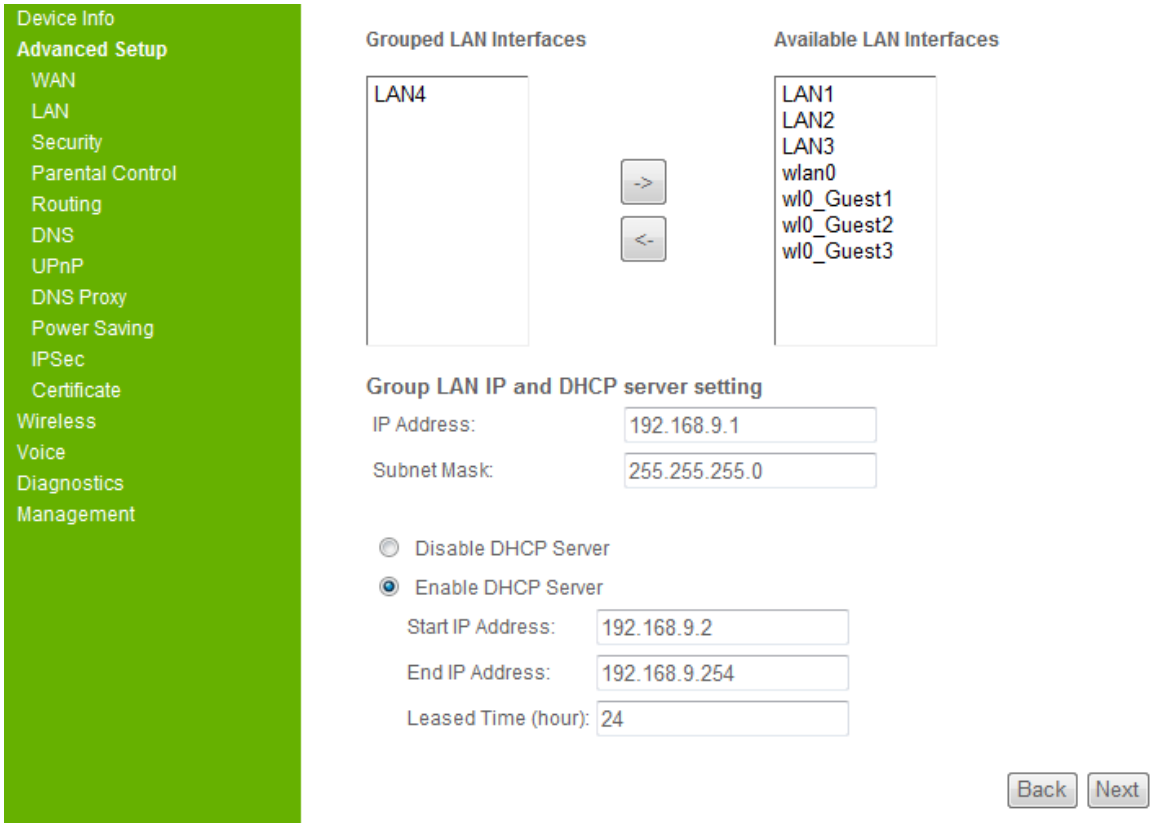


Figure 3-4-1. WAN – Data service Interface-PPPoE-2

The “WAN interface used in the grouping” shows the wan interface description name.

You can select the available Lan interfaces in the right list, and press “<-” button to move the select interface to the grouped Lan interfaces, you also can use “->” button to remove the select interface from the grouped Lan interfaces. Then you can set the group LAN IP address and the settings about DHCP server on this group LAN.

You must select one Lan interface at least to group with this wan interface and click the “Next” button.

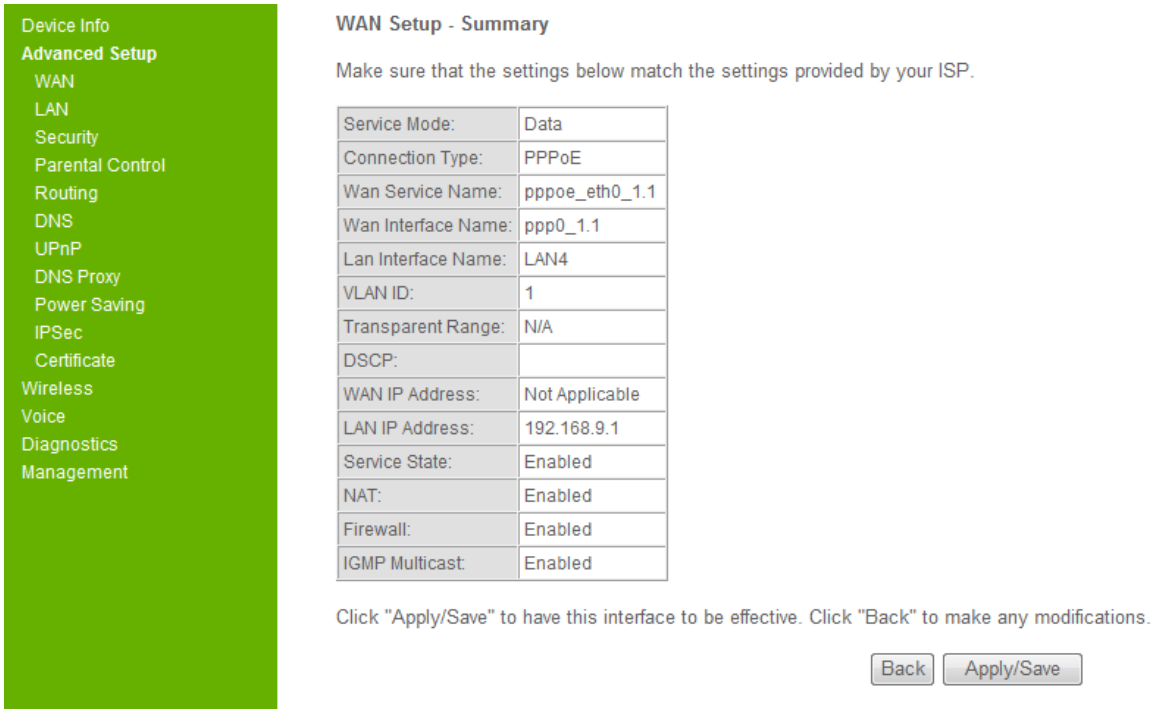


Figure 3-4-1. WAN – Data service Interface-PPPoE-3

Click the “Apply/Save” button to create the PPPoE wan data interface.

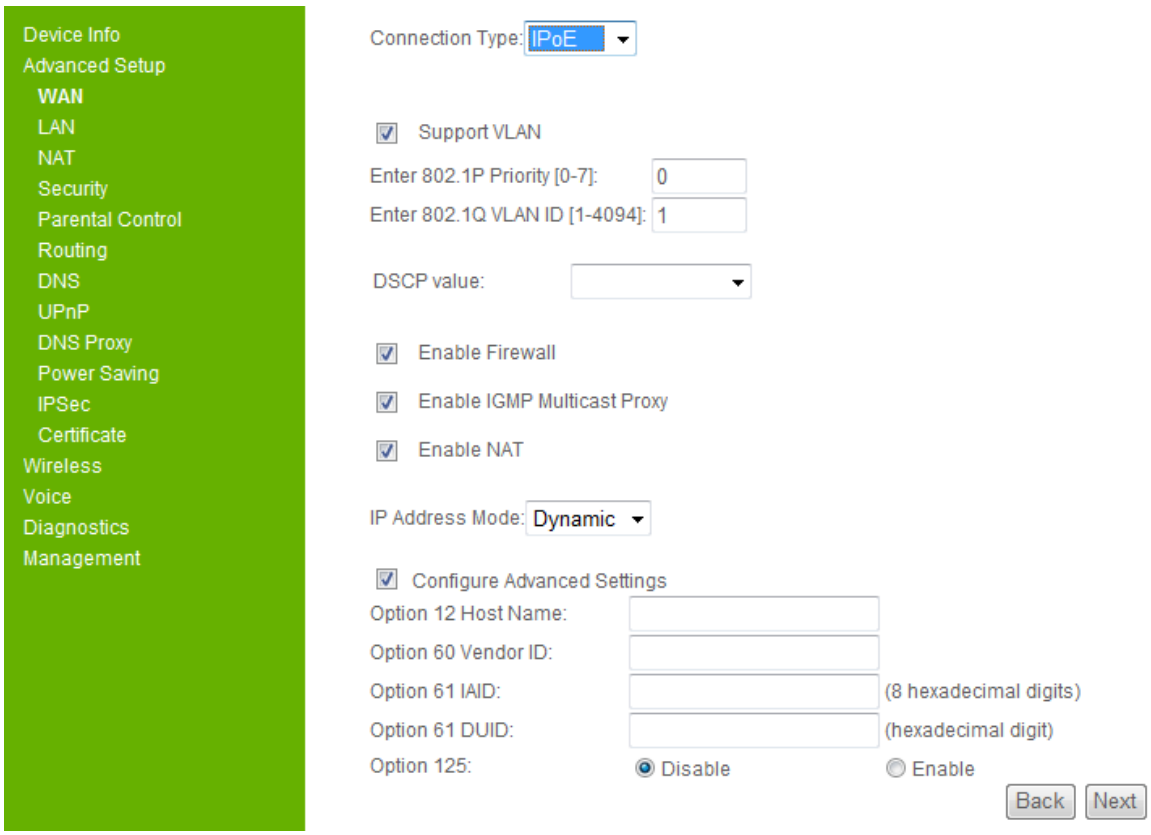


Figure 3-4-1. WAN – Data service Interface-IPoE-1

If you select IPoE connection type, set the VLAN and DSCP configuration.

For advanced user, you can customize firewall, IGMP, Nat and DHCP client.

And then click the “Next” button.

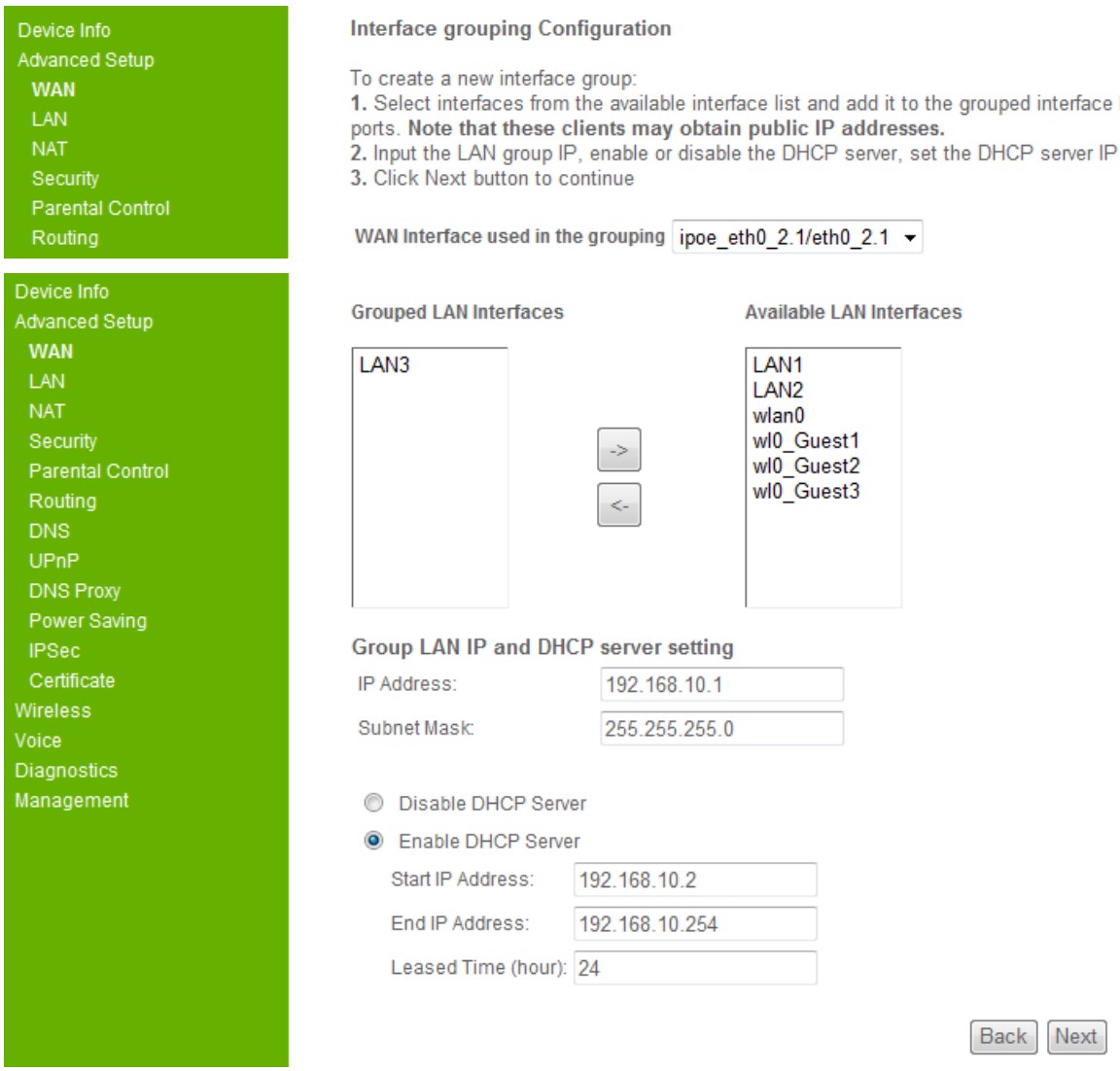


Figure 3-4-1. WAN – Data service Interface-IPoE-2

You must select one Lan interface at lease to group with this wan interface and click the “Next” button.

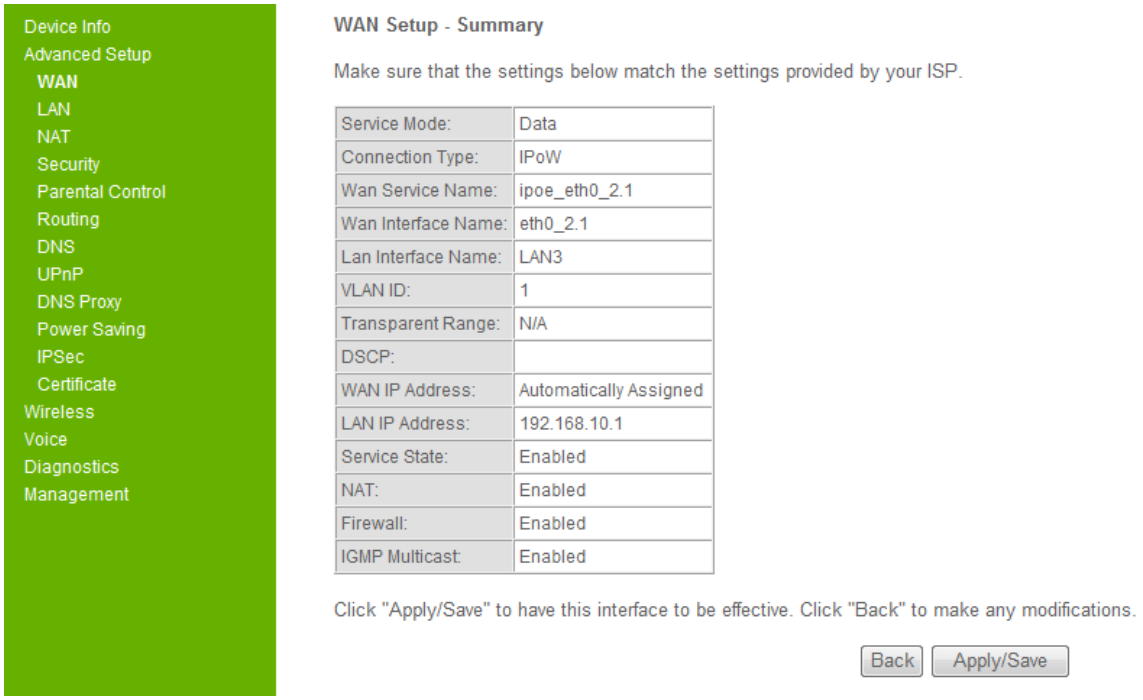


Figure 3-4-1. WAN – Data service Interface-IPoE-3

Click the “Apply/Save” button to create the IPoE wan data interface.

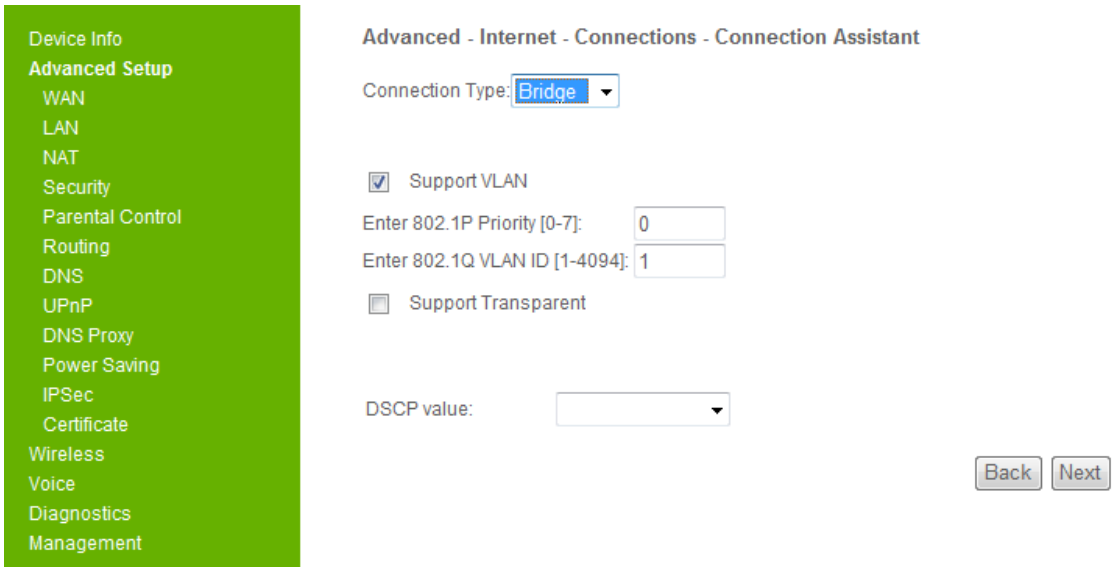


Figure 3-4-1. WAN – Data service Interface-Bridge-1

If you select Bridge connection type, you can set this bridge to support VLAN or support Transparent, but one interface can not support these two functions at the same time.

For advanced user, you can customize the supported VLAN ID or the transparent VLAN ID range, DSCP value.

And then click the “Next” button.

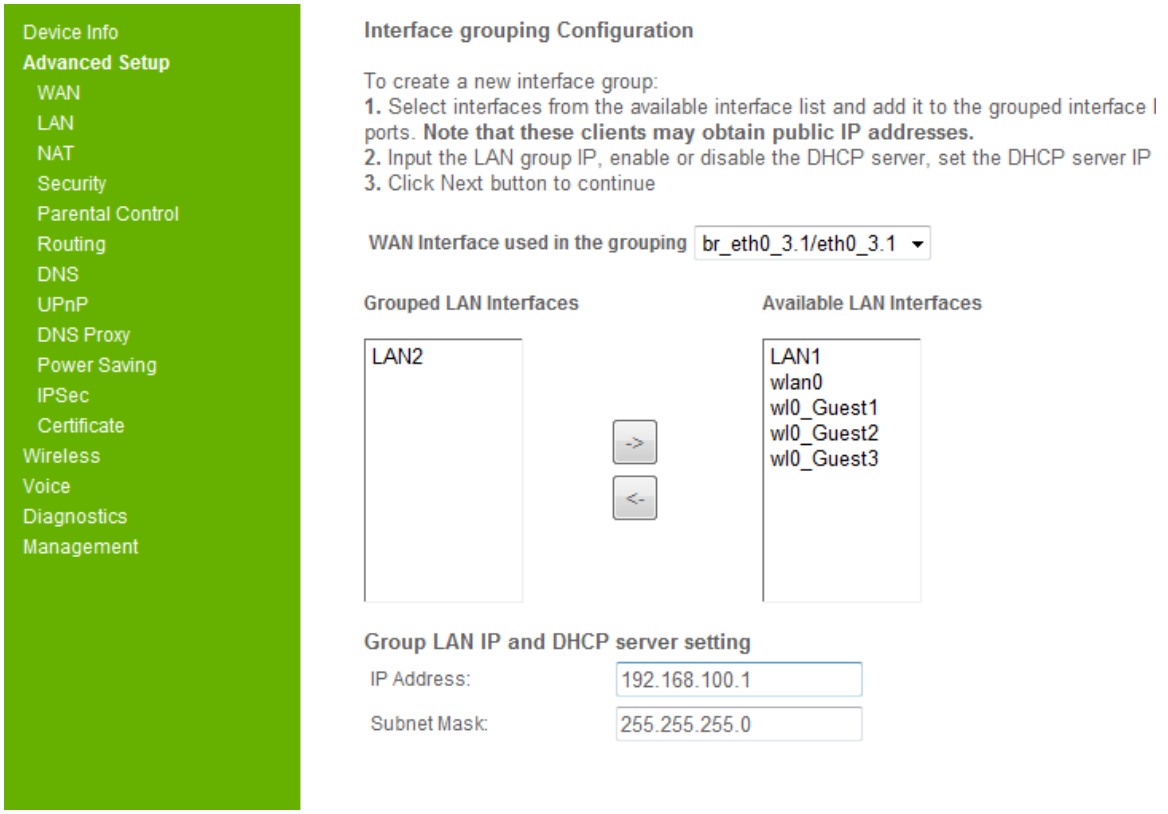


Figure 3-4-1. WAN – Data service Interface-Bridge-2

You must select one Lan interface at lease to group with this wan interface and click the “Next” button.

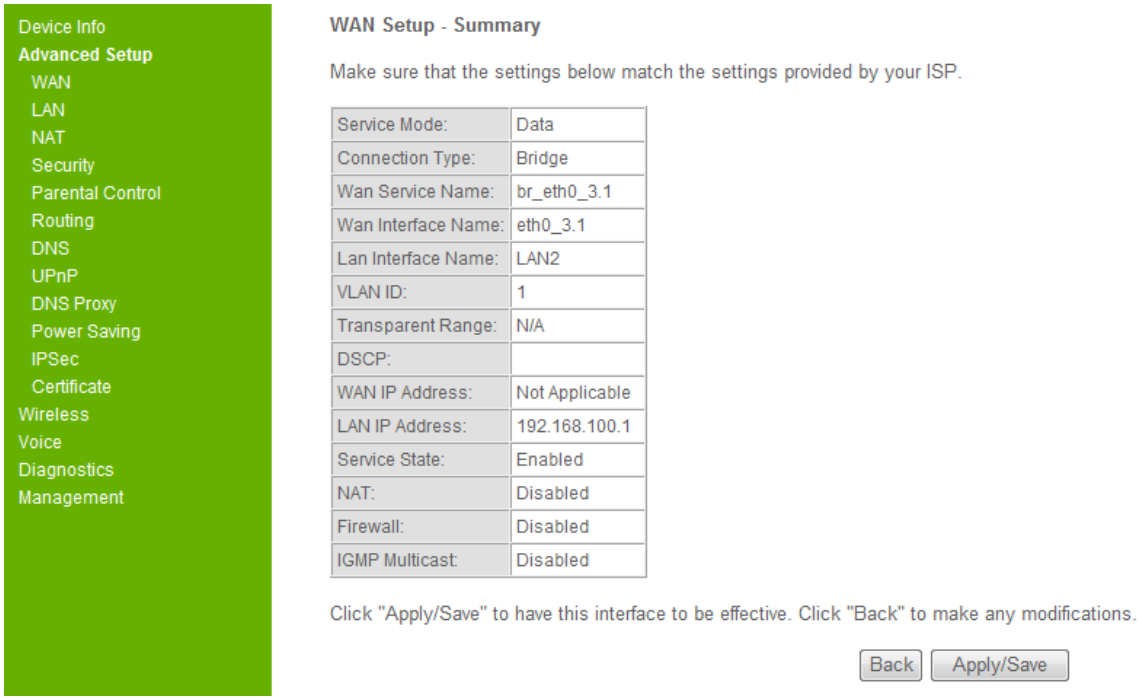


Figure 3-4-1. WAN – Data service Interface-Bridge-3

Click the “Apply/Save” button to create the Bridge wan data interface.

3.4.2. VoIP Service Mode

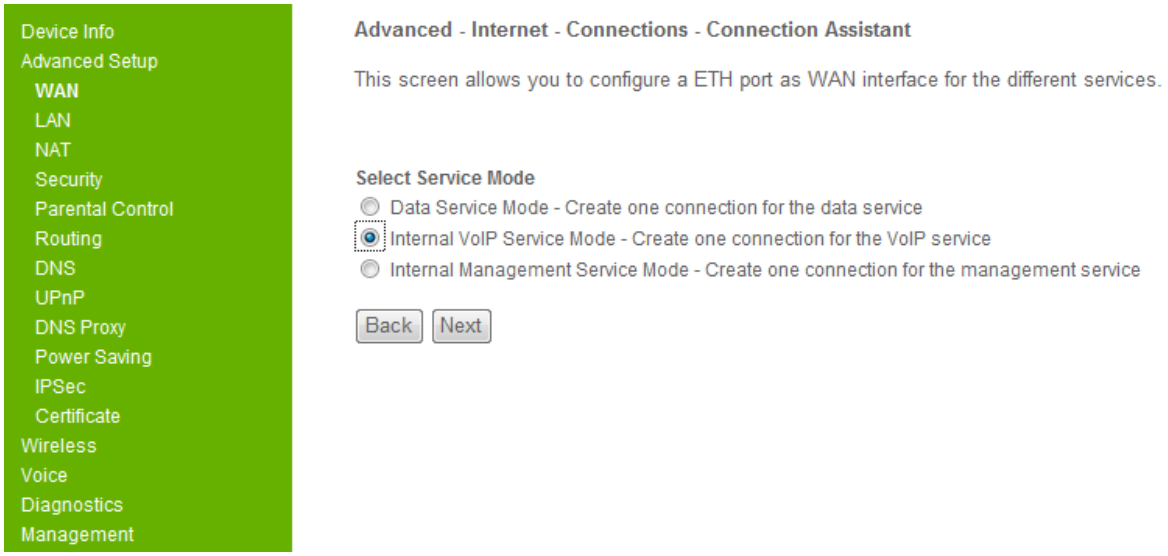


Figure 3-4-2. WAN – VoIP service Interface -1

The VoIP Service Mode allows you to create one connection for the VoIP service. Select it and click the “Next” button, it will show

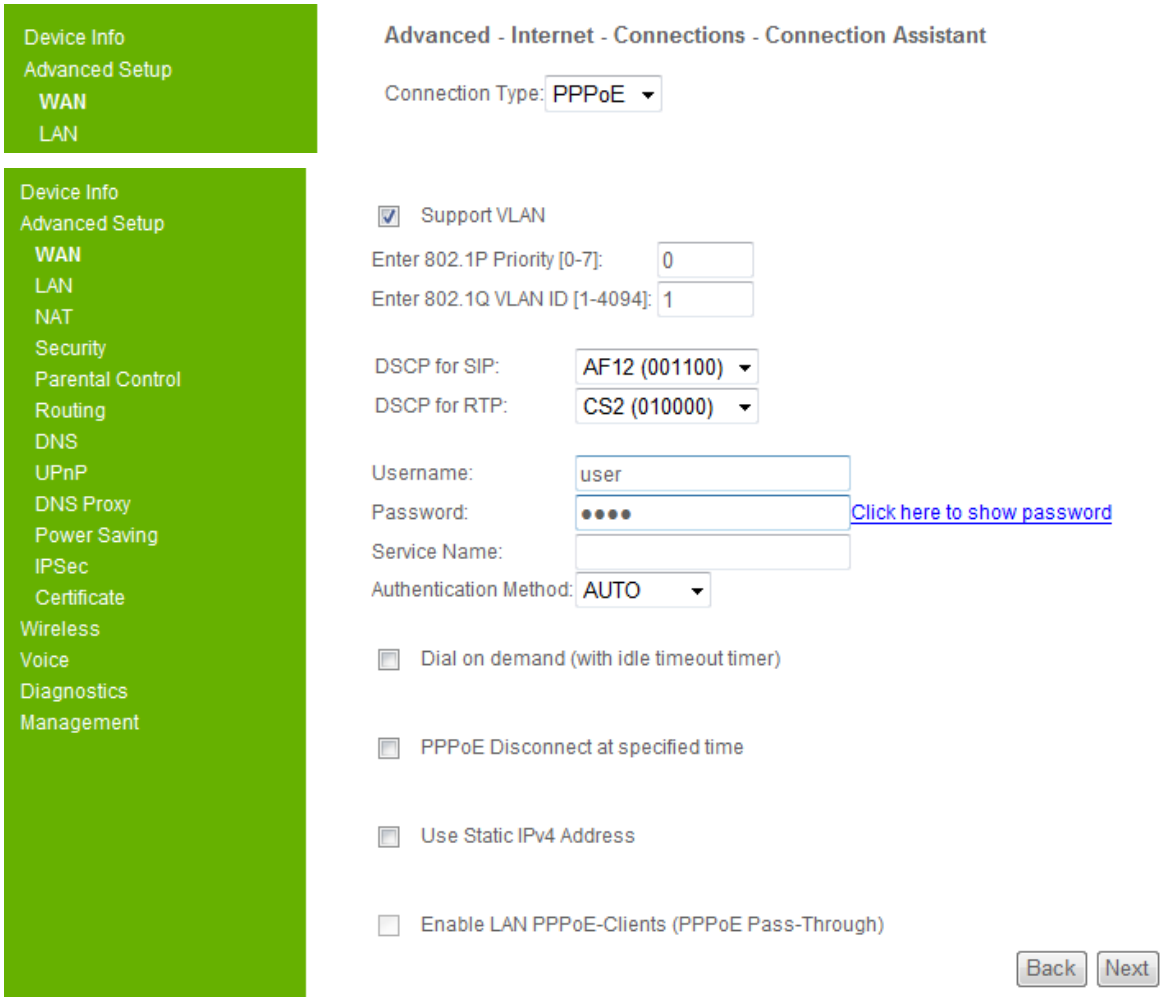


Figure 3-4-2. WAN – VoIP service Interface -2

For the VoIP service mode, the wan connect type is only available for PPPoE and IPoE.

For advanced user, you can customize the supported VLAN ID, DSCP for SIP, DSCP for RTP, the advanced PPPoE settings or the advanced IPoE settings.

And then click the “Next” button.

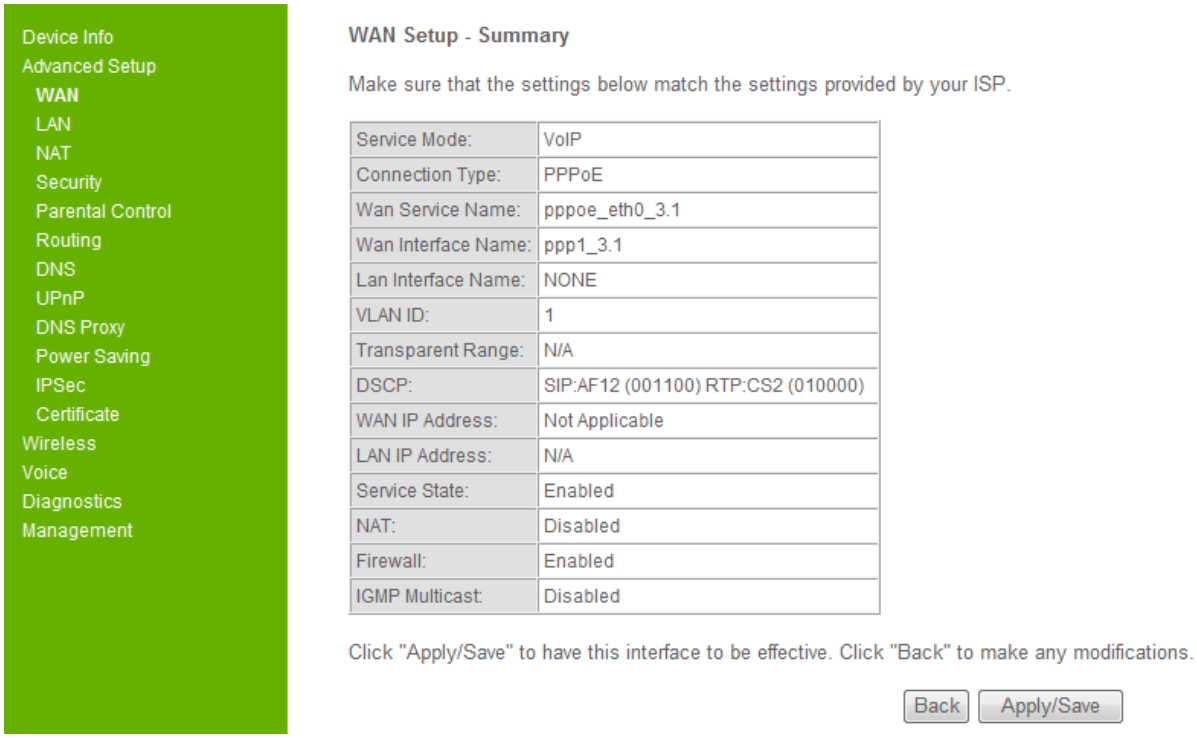


Figure 3-4-2. WAN – VoIP service Interface -3

Click the “Apply/Save” button to create the VoIP service interface.

3.4.3. Management Service Mode

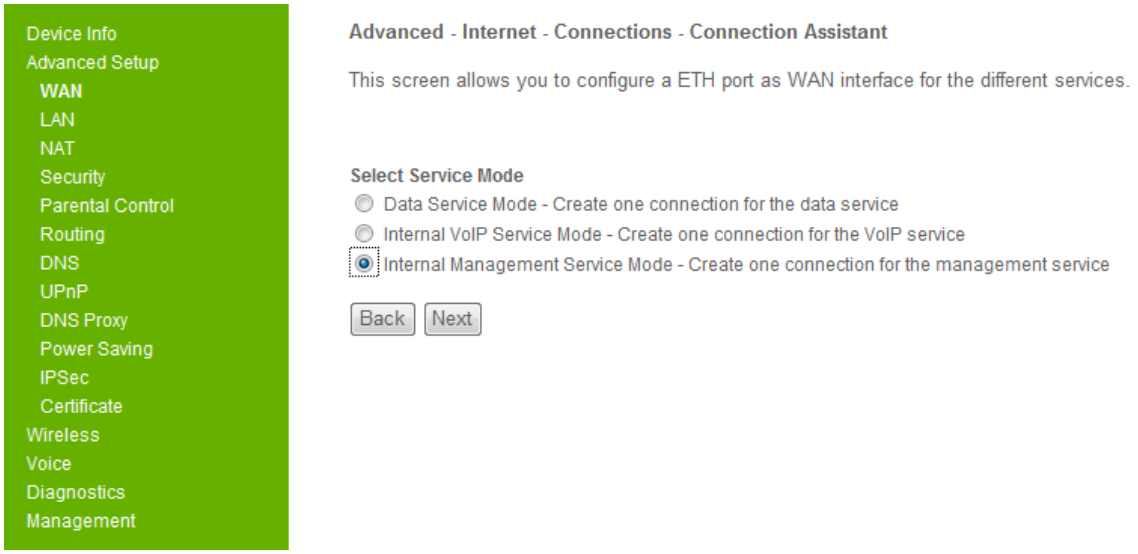


Figure 3-4-3. WAN – Management service Interface -1

The management Service Mode allows you to create one connection for the management service. Select it and click the “Next” button, it will show

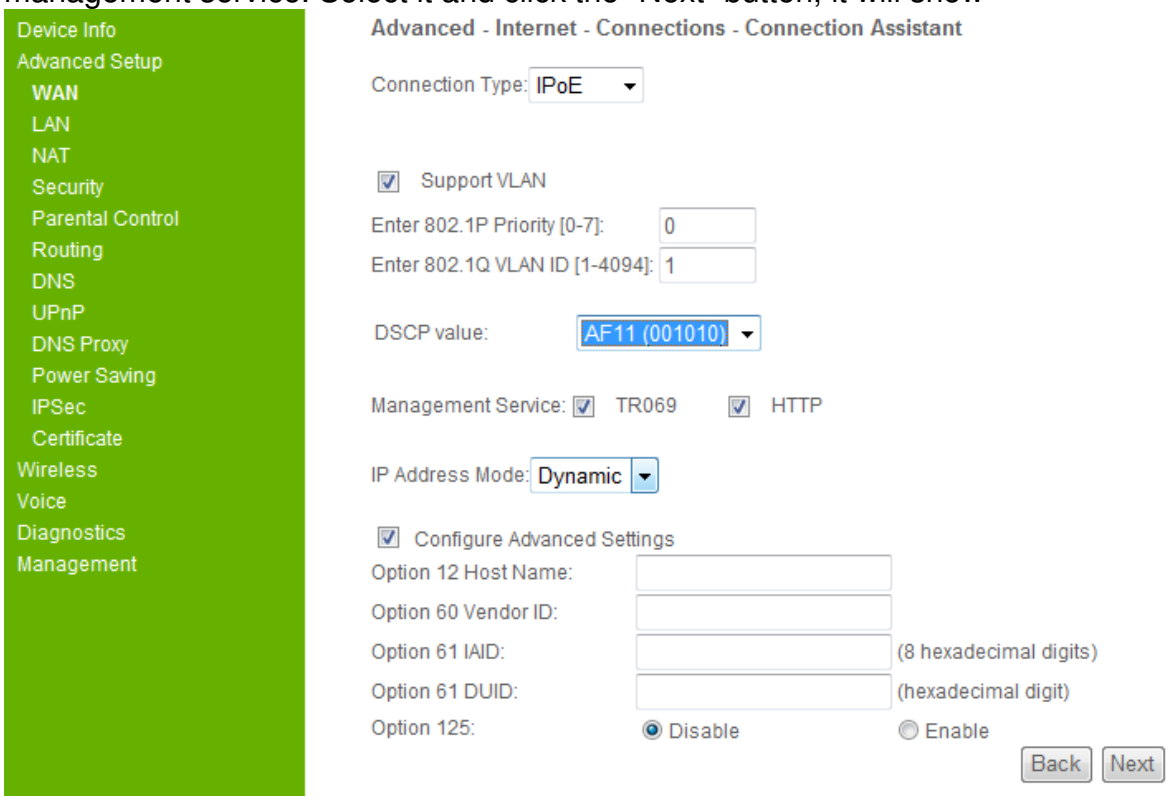


Figure 3-4-3. WAN – Management service Interface -2

For the management service mode, the wan connect type is only available for PPPoE and IPoE.

For advanced user, you can customize the supported VLAN ID, DSCP value, the management service, the advanced PPPoE settings or the advanced IPoE settings.

Here we only support the tr069 and http management service. You can select both of them or one of them.

And then click the “Next” button.

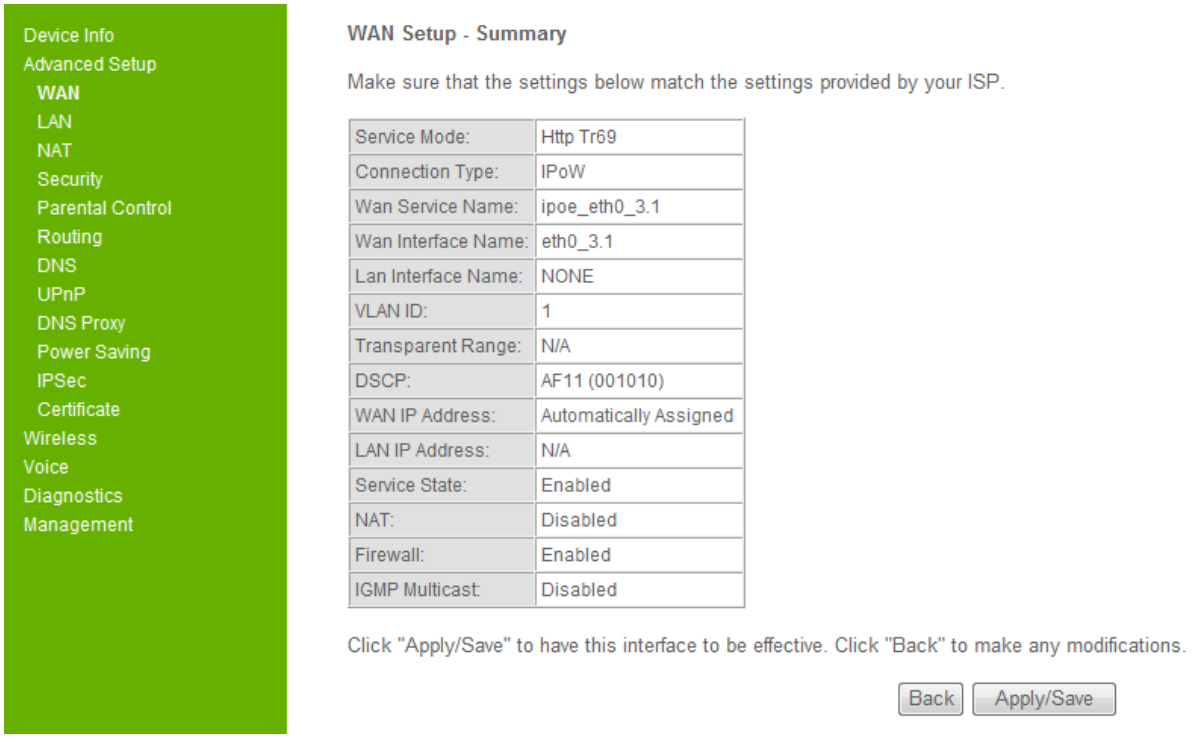


Figure 3-4-3. WAN – Management service Interface -3

Click the “Apply/Save” button to create the Management service interface.

3.5. Security

Click the “Advanced Setup/Security” on the left side of main web page, it allows users to configure IP filter, Figure 3-5-1 show the main page,

Figure 3-5-1 IP filtering

If you need add a new IP filter, click the “Add” button, then you can configure the IP filter parameters via Figure 3-5-2 web page,

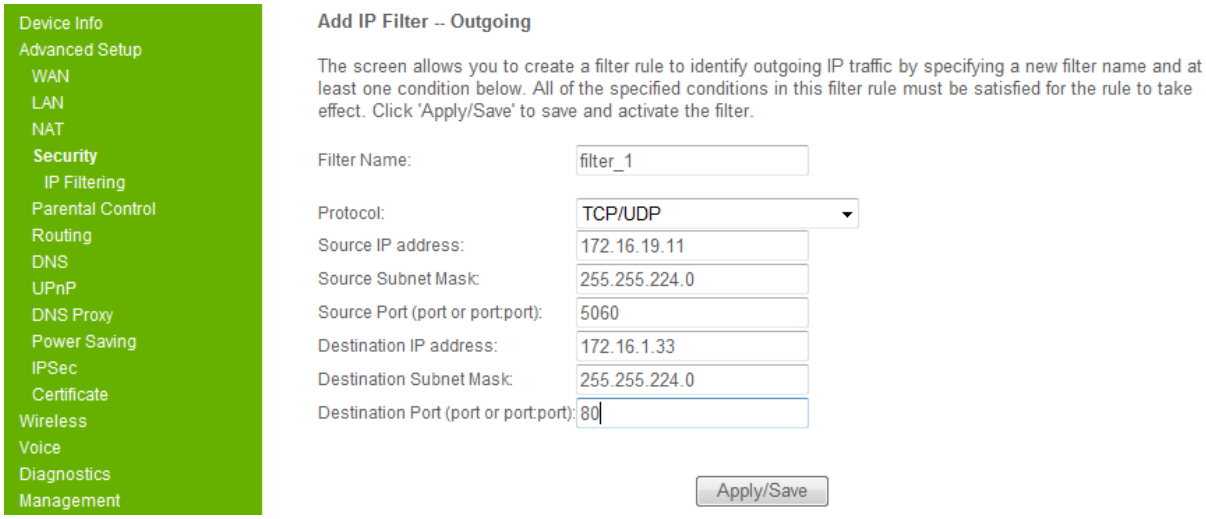


Figure 3-5-2 Add a new IP filter

After the configuration, click the “Apply/Save” button to make the change work.

If you need remove the corresponding IP filter, just choose the checkbox, and then click the “Remove” button, like Figure 3-5-3 shows.

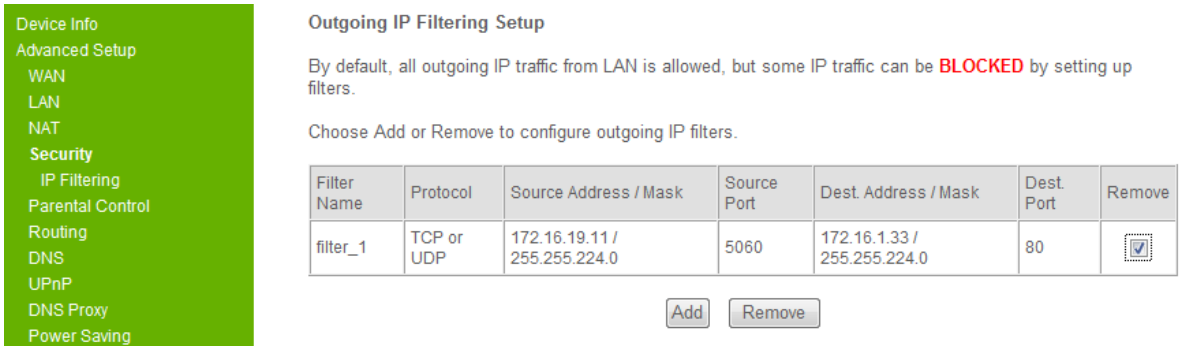


Figure 3-5-3 Remove a IP filter

3.6. Parental Control

The parental control support two features, they are time restriction and URL filter.

The timer restriction can be used to control a time period when a LAN device can access network or not. Figure 3-6-1 shows how to add a time restriction for a LAN device,

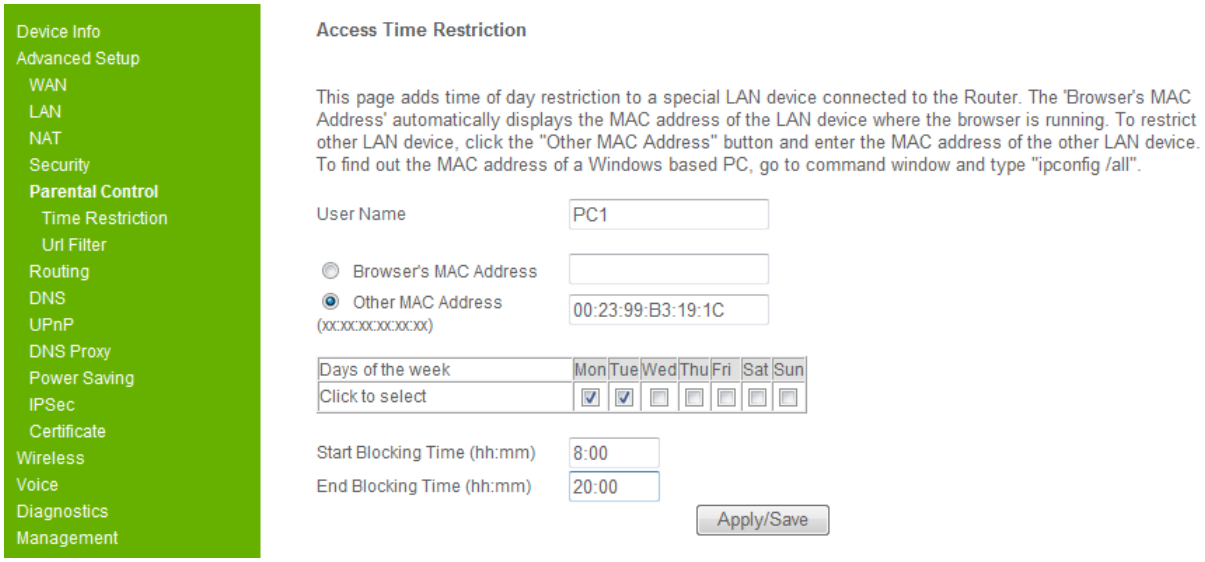


Figure 3-6-1 Add a time restriction

Please be noticed that the “Other MAC Address” is the MAC address of a LAN device, which you want to control. After the setting, click “Apply/Save” to make it work.
And more important, as the time restriction is supported based on acknowledge of the system time, make sure you have configured the NTP server.

The URL filter allows you to configure URLs, which are allowed or not allowed to access by LAN devices. Figure 3-6-2 shows the details, firstly you need to decide the URLS you entered are excluded or included. If the URL is permitted to access, choose the “exclude”, otherwise choose “include”.

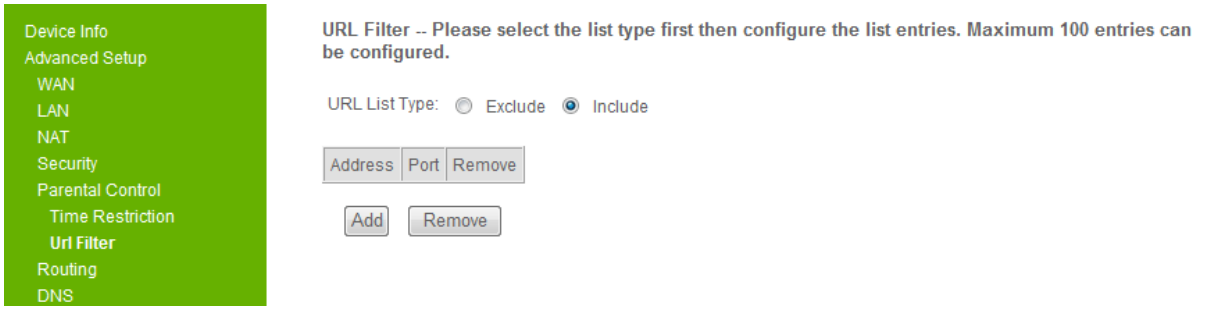


Figure 3-6-2 URL filter

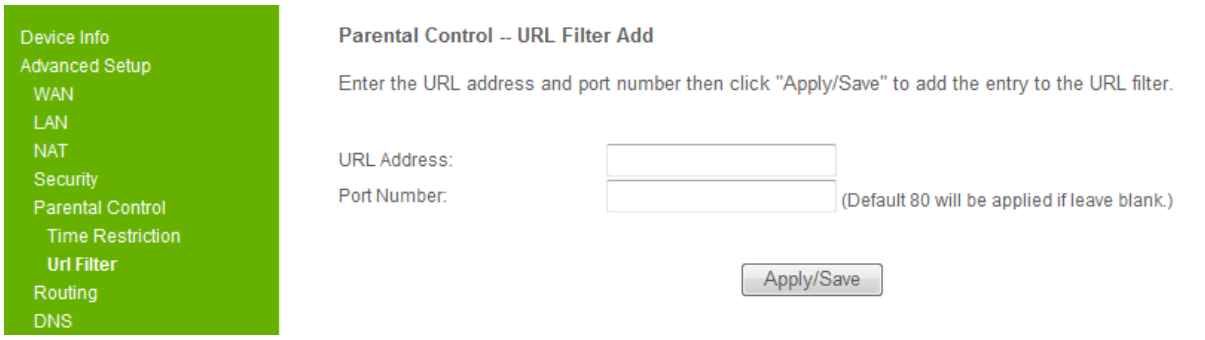


Figure 3-6-3 Add a new URL filter

Figure 3-6-3 shows how to add a new URL filter, about the "Port Number" parameter, you may enter nothing, GW5051 will apply the destination port with a default value (80, is the default http protocol port).

3.7. Routing

Routing application allows advanced users to configure route for GW5051 system. It allows users to control followings,

1) Select a wan interface as the default gateway.
2) Configure a static route
3) Configure policy route
4) RIP Configuration

Default gateway is configured when wan connection is successfully built. Figure 3-8-1 shows the view page, if you need a select another wan interface as a default way, select corresponding one then click "Apply/Save" button.

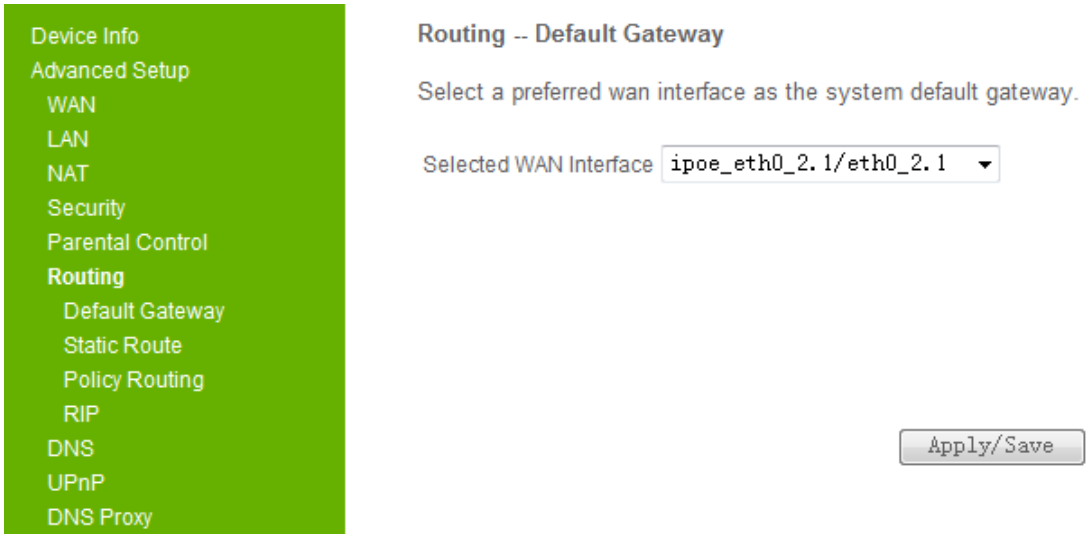


Figure 3-8-1 Routing-Default Gateway

To configure static route, you only click "Static Route" on left side of web page, you will see Figure 3-8-2,

Figure 3-8-2 Add/Remove static route

If you need add a static route, click the “Add” link, or you can remove existed static route settings.

Policy routing allows you add or remove a policy route setting, see Figure 3-8-3,

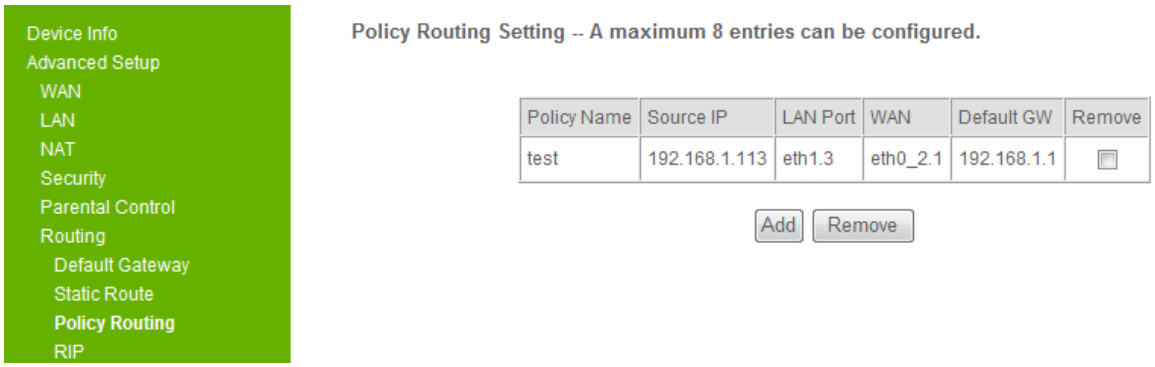


Figure 3-8-3 Policy Routing

If you need add a policy route, click the “Add” button, then you will be able to configure necessary parameters, see Figure 3-8-4 for details,

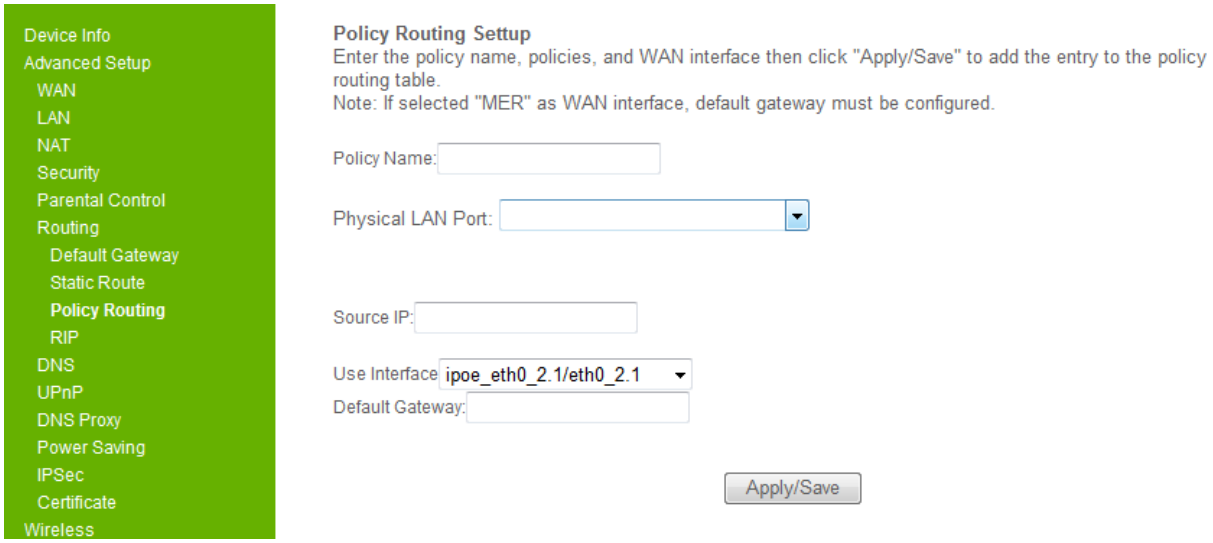


Figure 3-8-4 Add a Policy route

It should be noticed default gateway must be configured if the WAN interface is “MER” type, in other cases default gateway can be empty.

RIP option enable advanced users to control RIP settings, as Figure 3-8-5 shows, the RIP is not available when WAN has NAT enabled.

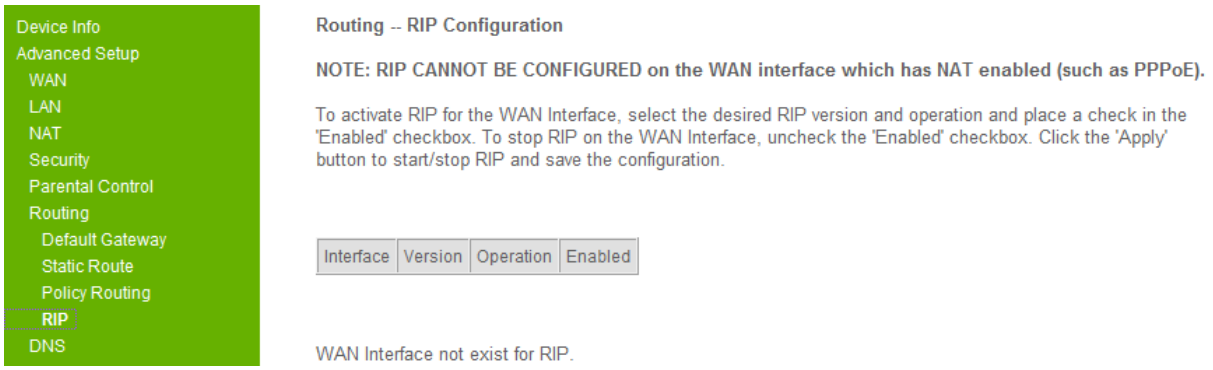


Figure 3-8-5 RIP Configuration page

3.8. DNS

DNS support two type of settings, one is DNS server, the other is Dynamic DNS setting.

Figure 3-9-1 shows the DNS server configuration page,

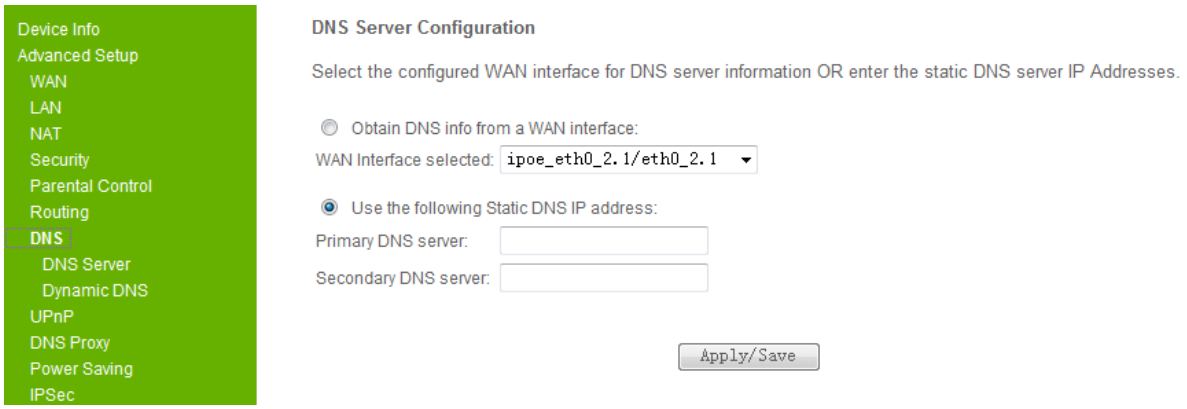


Figure 3-9-1 DNS server Configuration

The DNS server information can be obtained from the wan interface list, or configured by users. You can configure the dynamic DNS priority is high or static DNS is high.

When select the dynamic DNS priority is high, DNS server information will be obtained from the wan interface list. Selected DNS Interfaces list can have multiple WAN interfaces served as system DNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.
If you are sure about local DNS server address, you can configure it self and select the priority of the static DNS is high.
However at most cases, DNS information should be configured via wan interface. Click “Apply/Save” to make your change work.

Figure 3-9-2 shows how the dynamic DNS setting page,

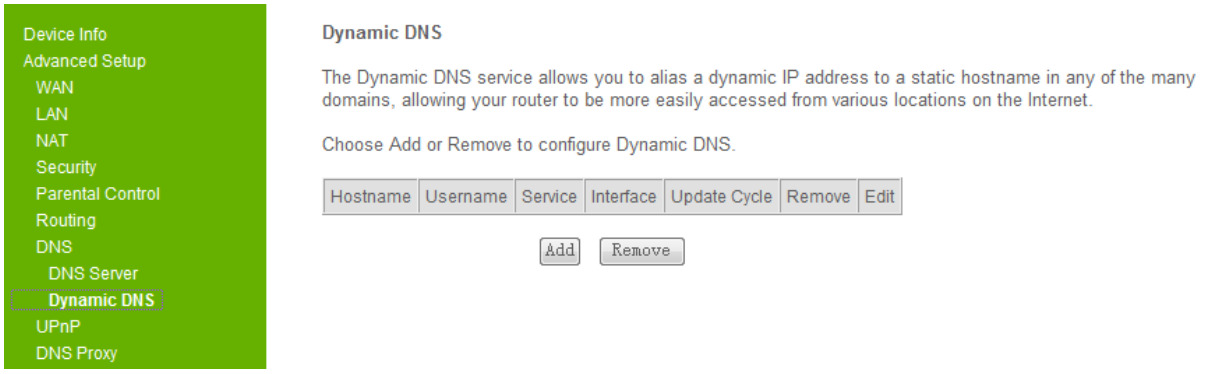


Figure 3-9-2 Dynamic DNS

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

3.9. Power Saving

This Power Saving Features provide the ability to turn off specific interfaces at specific times. Following page is provided as an example,

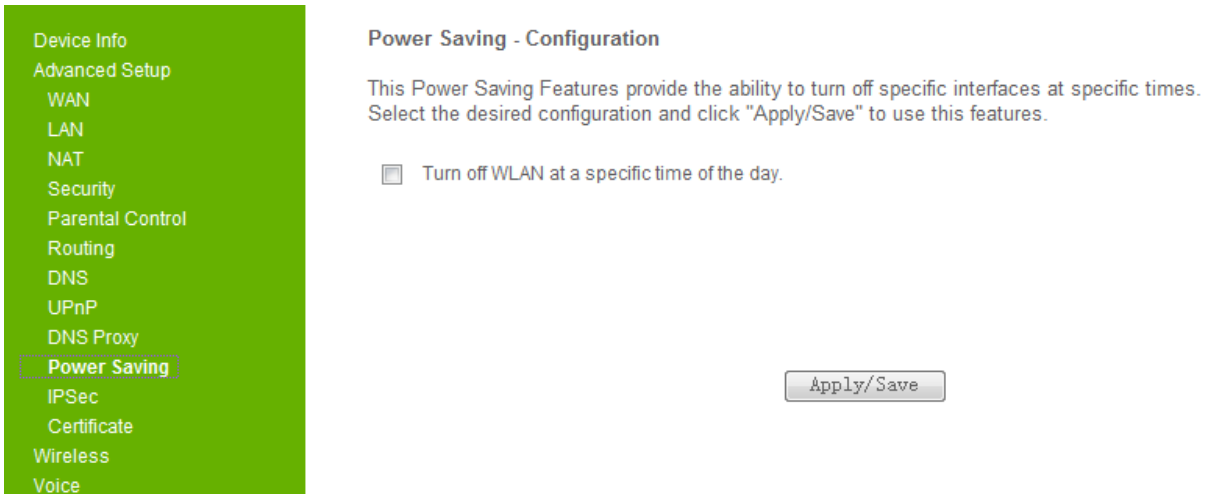


Figure 3-12-1 Example of Power Saving Configuration

3.10. Certificate

“Certificate” application enable users to import the certificate of trusted CA. Click “Certificate/Trusted CA”, as Figure 3-16-1 shows,

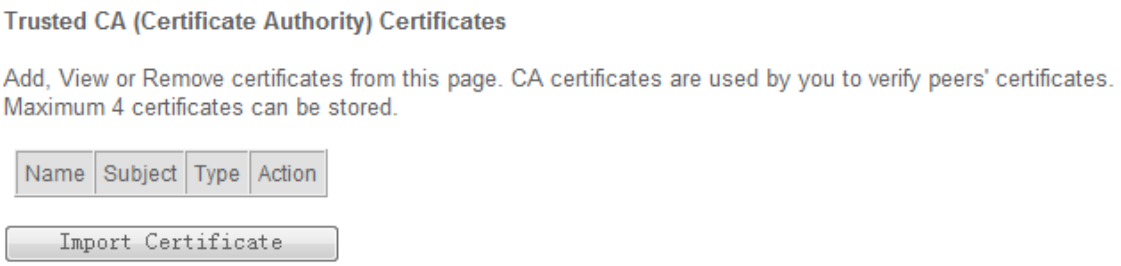


Figure 3-16-1 Trusted CA-Edit Page

3.11. Wireless

Click the “Wireless” button on the left hand side of this web page to enter into the configuration with respect to the wireless connection. There are totally 6 sub-manuals in wireless connection.

1. Network
2. Security
3. MAC Filter
4. Wireless Bridge
5. Advanced
6. Station Info

The detailed descriptions of each category are depicted forward.

3.11.1. Network

The “Network” is the first one in wireless configuration. In this page, it allows you to setup the generic features of wireless connection. The basic features consist of enable / disable the wireless connection, hide / reveal the existence of AP, setting Service Set ID (SSID) of wireless network, selection of countries and its maximum number of clients. The Basic Service Set ID (BSSID), MAC address of AP, is also shown on this page. You may enable guest to use the service of this wireless connection. In the end, click “Apply/Save” to effect the configuration.

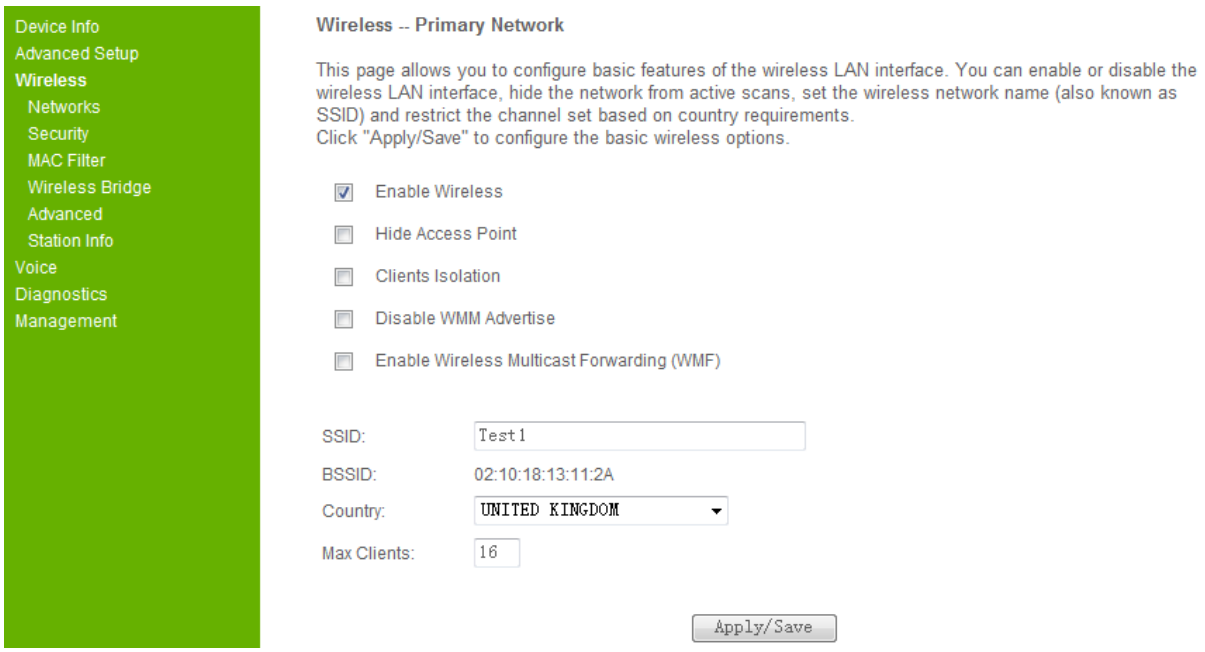
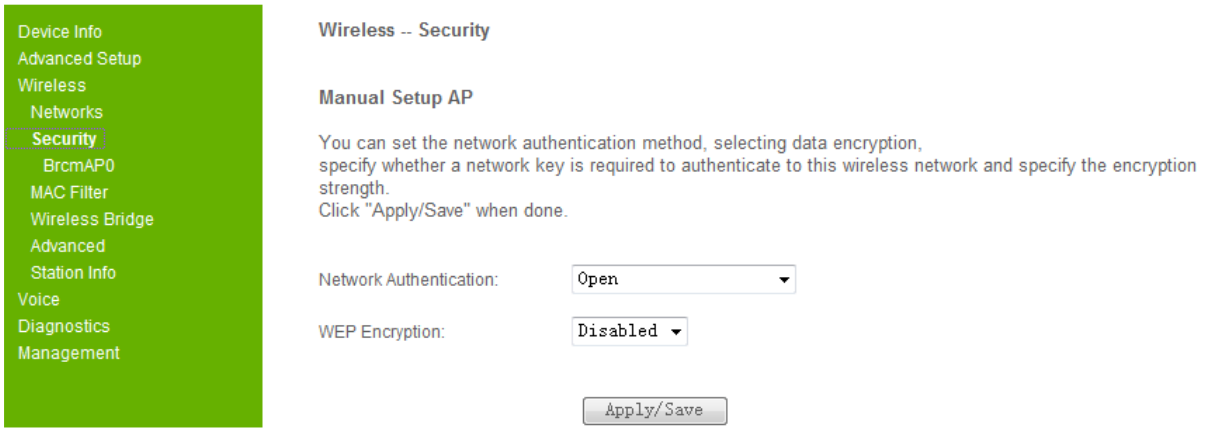


Figure 3-5-1. Wireless – Network

3.11.2. Security

Click the second category “Security” to enter into the configurations with respect to the security. All items in this category are described in detail below.



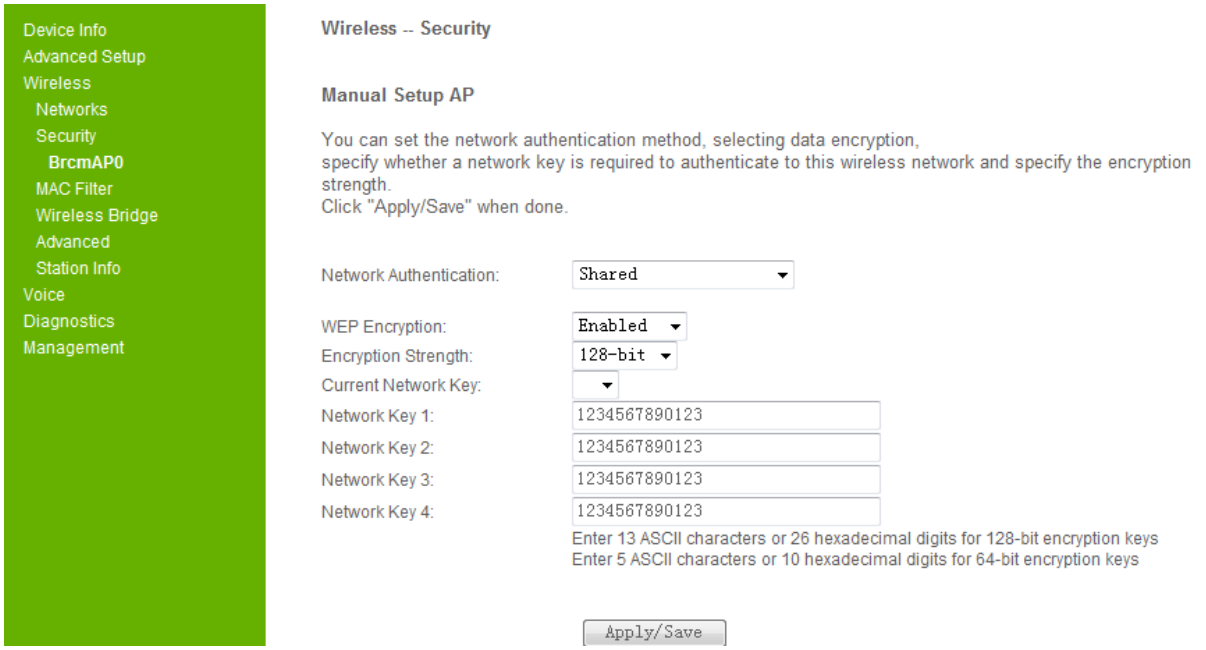


Figure 3-5-2. Wireless – Security

Network Authentication: Select the network Authentication method. 802.1X and WPA require to set valid RADIUS parameters. WPA-PSK requires a valid WPA Pre-Shared Key to be set.

802.1X: As the IEEE standard for access control for wireless and wired LANs, 802.1x provides a means of authentication and authorizing devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network.

WPA / **WPA2:** The Wi-Fi Alliance put together WPA / WPA2 as a data encryption method for 802.11 wireless LANs. WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys.

WPA / **WPA2 Pre-Shared Key:** Set the WPA / WPA2 Pre-Shared Key (PSK).

WPA / **WPA2 Group Rekey Interval:** Set the WPA / WPA2 Group Rekey Interval in seconds. Leave blank or set to zero to disable periodic re-keying.

Radius Server: Set the IP address of the RADIUS server to use for authentication and dynamic key derivation.

RADIUS Server: It is responsible for receiving user connection requests, authenticating the user, and then returning all of the configuration information necessary for the client to deliver the server to the user.

Radius Port: Sets the UDP port number of the RADIUS server. The port number is usually 1812 or 1645 and depends on the server.

Radius Key: Set the shared secret for the RADIUS connection.

Data Encryption (WEP): Selecting Off disables WEP data encryption. Selecting WEP enables WEP data encryption and requires that a valid network key be set and selected unless 802.1X is enabled.

WEP: It stands for Wired Equivalent Privacy, is a protocol for wireless LANs or local area networks. This WEP is defined in the 802.11 Standard. WEP is designed so security levels are maintained at the same level as the wired LAN. WEP's aim is to provide security by encrypting data over radio waves. WEP protects data as it's transmitted from one end point to another. WEP is used at two lowest layers, the data link and physical layer. WEP is designed to make up for the inherent security in wireless transmission as compared to wired transmission.

Shared Key Authentication: Set whether shared key authentication is required to associate. A valid network key must be set and selected if required.

In the end, click "Apply/Save" to effect the configuration.

3.11.3. MAC Filter

Click the third category “MAC Filter” to enter into the related configuration of the MAC address.

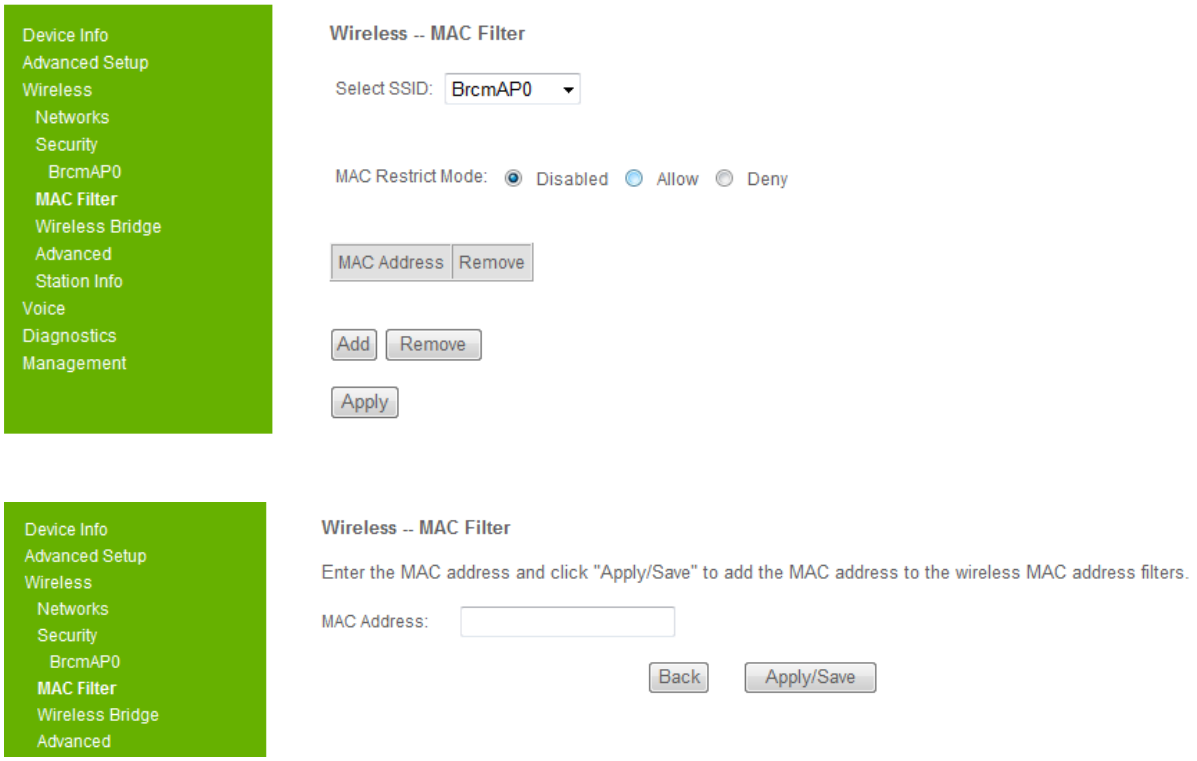


Figure 3-5-3. Wireless – MAC Filter

In this page, it allows you to **Add** / **Remove** hosts with the specified MAC addresses that are able or unable to access the wireless network. When you select to **Allow** the access of wireless network, only the PC with specified MAC addresses in the user defined list can access the wireless network. When you select **Deny** the access of wireless network, the PC with specified MAC addresses are unable to access to wireless network.

Note: The MAC addresses in the list would immediately take effect when **Allow** or **Deny** is checked.

3.11.4. Wireless Bridge

Click the fourth category “Wireless Bridge to enter into the configuration of the bridge.

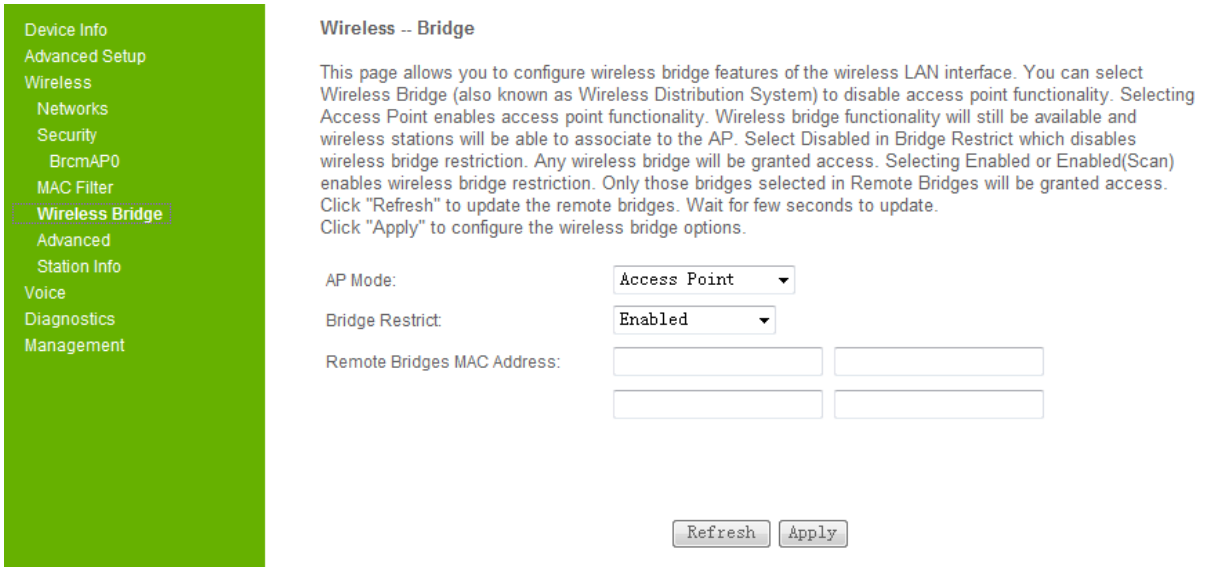
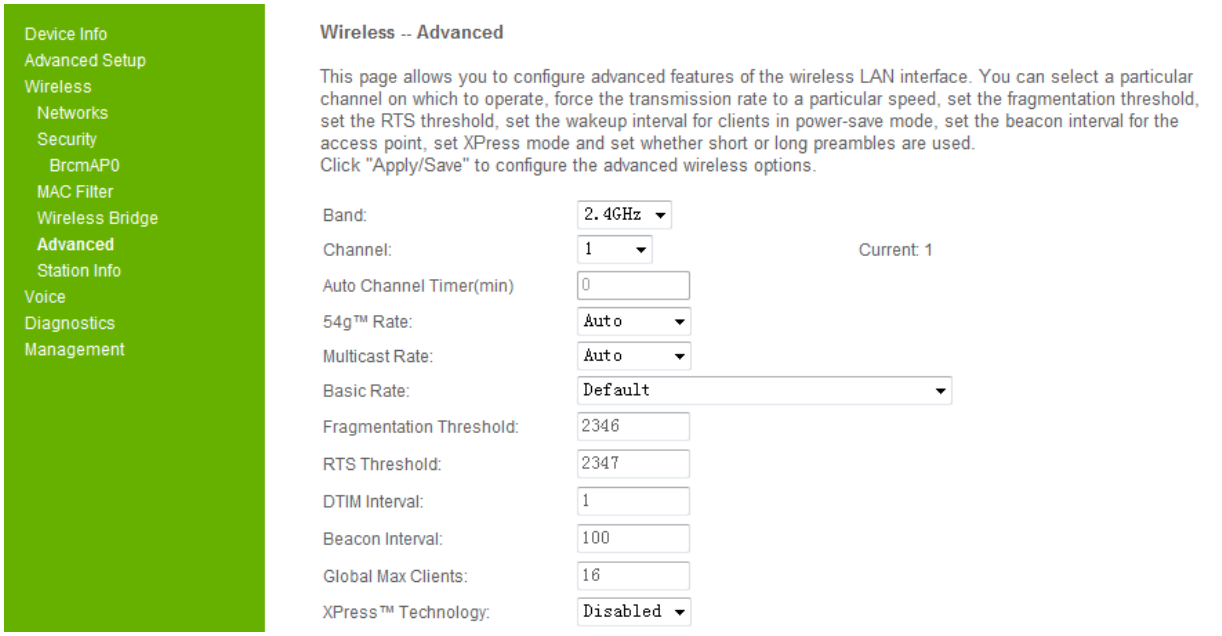


Figure 3-5-4. Wireless – Wireless Bridge

It allows the users to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

3.11.5. Advanced

Click the fifth category “Advanced” to configure the advanced feature of the wireless network.



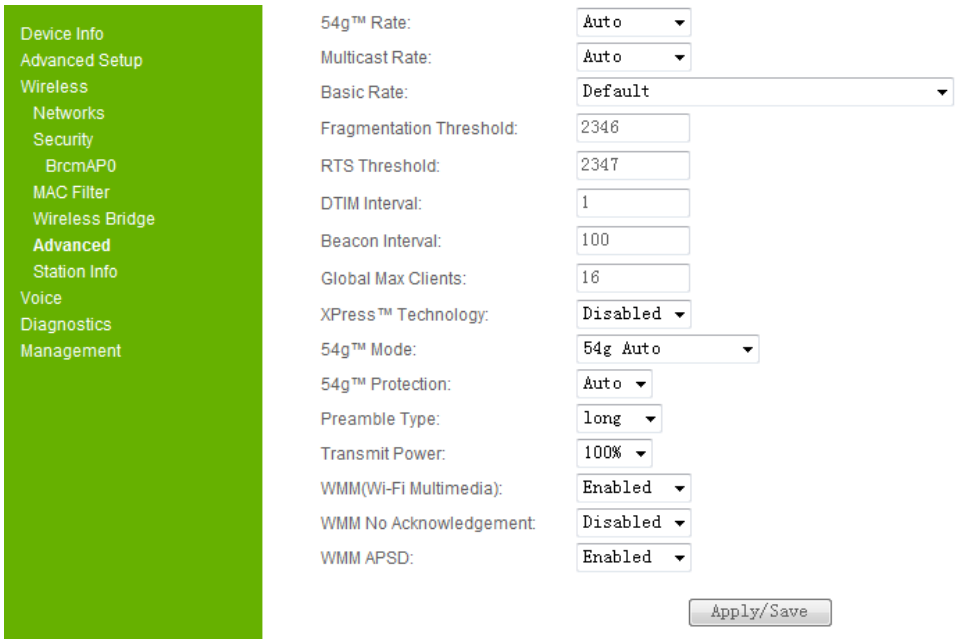


Figure 3-5-5. Wireless – Advanced

Channel: Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly.

Rate: The default setting is “Auto”. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from one transmission speed, or keep the default setting, “Auto”, to have the IAD automatically use the fastest possible data rate.

Multicast Rate: The default setting is 54Mbps. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from one transmission speed, or keep the default setting, to have the IAD automatically use the fastest data rate for multicast packets.

Basic Rate: Select the basic rate that wireless clients must support.

Fragmentation Threshold: This value should remain at its default setting of 2346. The range is 256~2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS Threshold: This value should remain at its default setting of 2347. The range is 0~2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the packet RTS threshold size, the RTS / CTS mechanism will not be enabled. The IAD 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.

DTIM Interval: The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast message.

Beacon Interval: The default value is 100. Its range is between 1 and 65535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network.

XPress™ Technology: Select to enable / disable this proprietary mode.

54g™ Mode: Select the mode to **54g Auto** for the widest compatibility. Select the mode to **54g Performance** for the fastest performance among 54g certified equipment. Set the mode to **54g LRS** if you are experiencing difficulty with legacy 802.11b equipment.

54g protection: In **Auto** mode, the IAD will use RTS / CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection **off** to maximize 802.11g throughput under most conditions.

WMM (Wi-Fi Multimedia): Select to enable / disable the support.

3.11.6. Station Info

Click the last category “Station Info” to display the status of authenticated wireless stations.

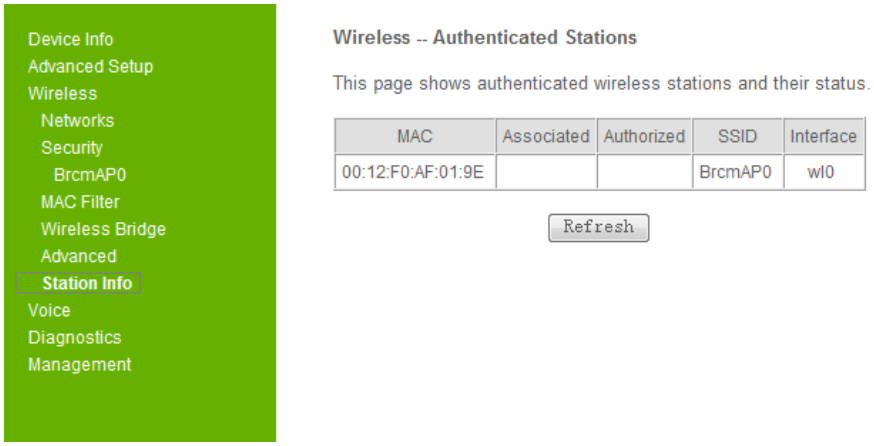


Figure 3-5-6. Wireless – Station Info

3.12. Voice

Click the “Voice” button on the left side of the main web page, there are seven sub options for voice function,

Re-injection
Basic settings
Call features
Dial Plan
Audio Codec
Advanced settings
Debug settings

Details of configurations are given in the following descriptions.

3.12.1. Basic Settings

This sub option is used to configure basic items of voice service, including the Interface, SIP Service provider information, and SIP accounts. Figure 3-8-2 shows the details as an example,

Voice -- Basic Settings

Phone 1 - Registration Status: Registered
Phone 2 - Registration Status: Registered

SIP Registrar Address: 192.168.1.251 Port: 5060
SIP Proxy Server Address: 192.168.1.251 Port: 5060
SIP Outbound Proxy: Port: 5060

Phone setting information:

Phone	Phone Number	Display Name	Username	Password
1	7701	7701	7701	••••
2	7702	7702	7702	••••

Cancel Apply/Save

Figure 3-8-2 Basic settings of voice function

Generally, there are three steps to configure basic settings,
Step 1, Configure the “Interface”, the “Interface” option, on which the voice function runs, can be configured with “Any_WAN” or “LAN”. When wan connection is built successfully, it is mostly configure with “Any_WAN”.

Step2, configure the SIP service provider information, including the SIP registrar address, and proxy server address, and also users need configure SIP outbound proxy and SIP domain name if the service provider asked.

Step3, configure the SIP accounts. As you can see from the page, there are two lines available.

3.12.2. Call Features

Call features are used to configure SIP call features for each line. Figure 3-8-3 shows all the call features supported by GW5051,

Phone 1 - Call Feature Status: **Registration successful**
Phone 2 - Call Feature Status: **Registration successful**

Line	1	2
Call waiting	☑	☑
Call forwarding number		
Forward unconditionally	☐	☐
Forward on "busy"	☐	☐
Forward on "no answer"	☐	☐
MWI	☐	☐
Anonymous call blocking	☐	☐
Do not send my phone number	☐	☐
Do not disturb	☐	☐

☐ Enable T38 support

Cancel Apply/Save

Figure 3-8-3 Call features of voice function

As you can see, “Call waiting” function is enabled as default, if you need other call features enabled, choose the corresponding item, and then click “Apply/Save” button. Moreover, the GW5051 support T38 fax transport, if you need that support, enables the option, and don’t forget to click “Apply/Save” after that.

3.12.3. Dial Plan

Figure 3-8-4 shows the dial plan configuration when you click the “Dial plan” item of the left side on the main page.

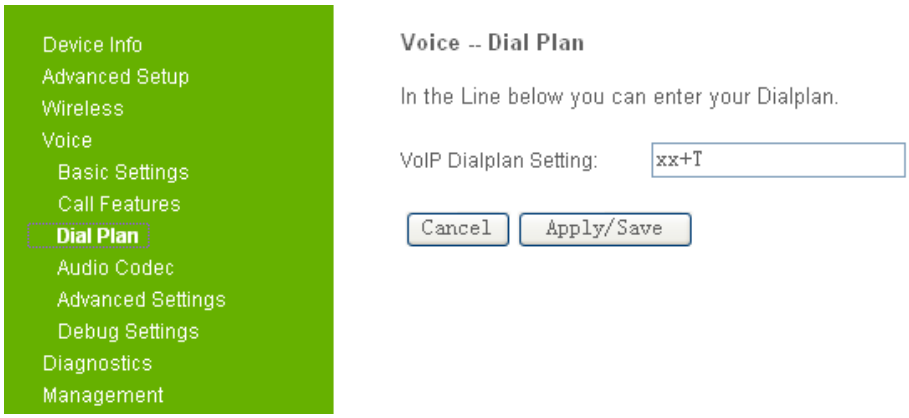


Figure 3-8-4 Dial plan Configuration of voice function

Generally supported dial plan string is like the following,
[1-9]xxx|xx+*|xx+#|00x.T|011x.T|x+T
However, if you are not sure about settings, keep the dial plan unchanged with default value.

3.12.4. Audio Codec

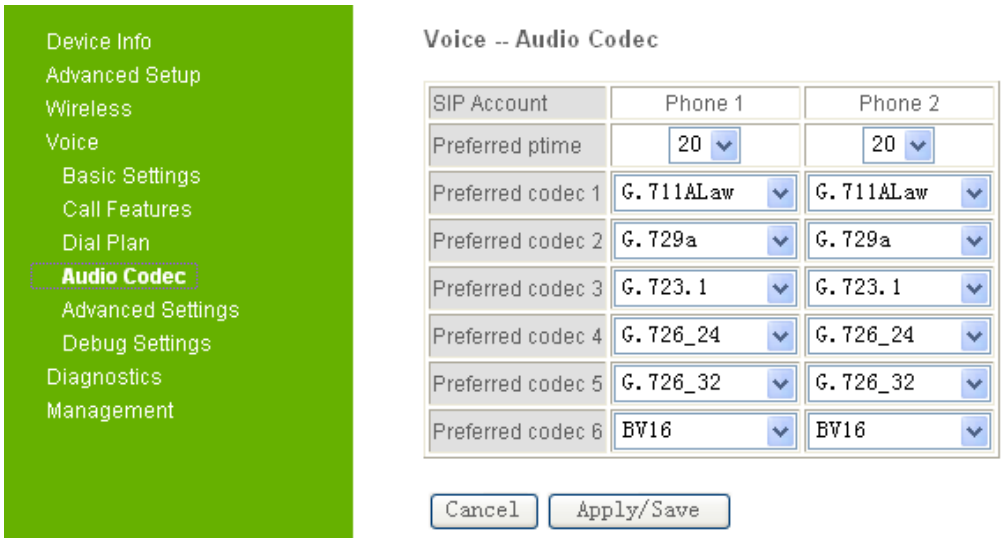


Figure 3-8-5 Audio Codec configuration of voice function

Figure 3-8-5 shows the audio codec setting for each line. You can choose six different codec for each line, and also you can choose a “ptime” value, which may have obvious influence on voice quality. Do click the “Apply/Save” button to make the settings work.

3.12.5. Advanced Settings

You can configure the advanced settings for voice application, if you are familiar with the voice service. Figure 3-8-6 shows the details,

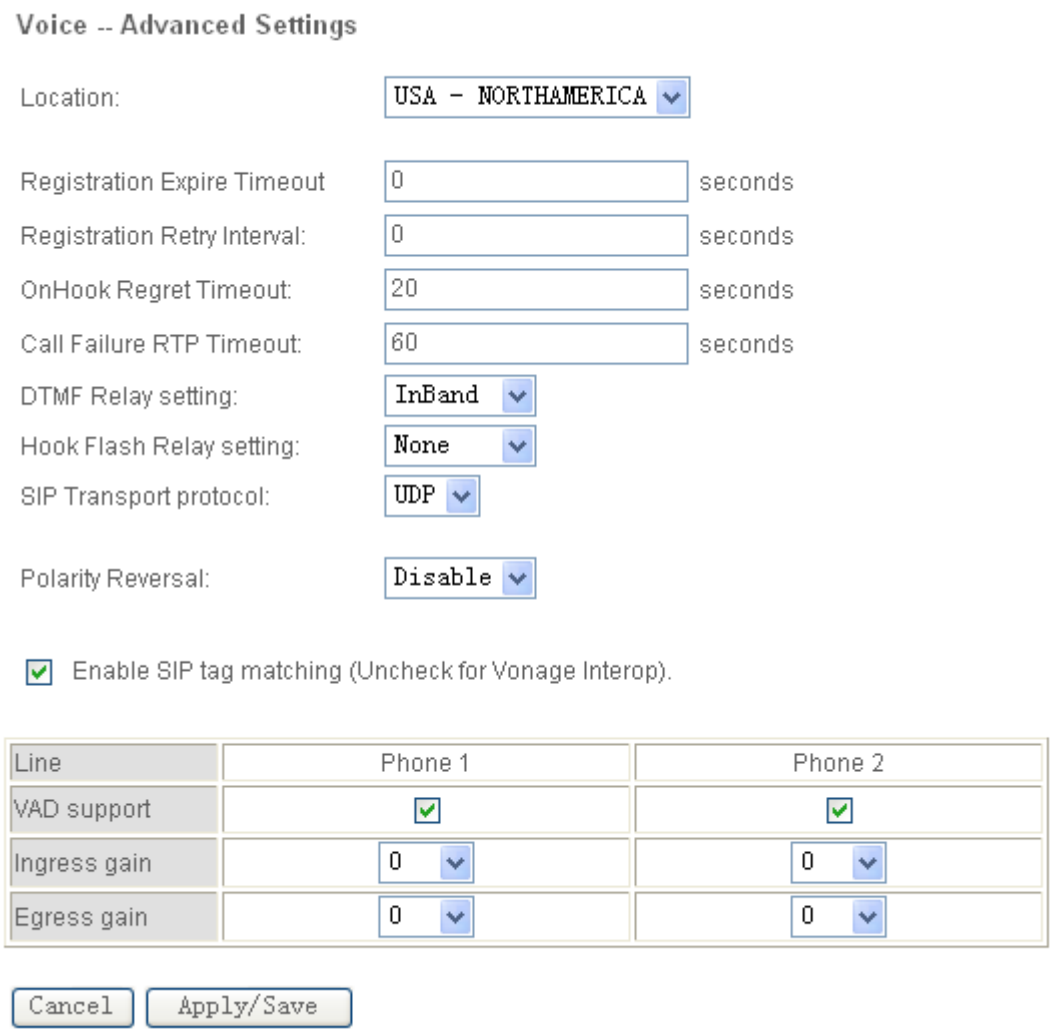


Figure 3-8-6 Advanced settings of voice function

Location option indicates the country mode used by the voice application.

Registration Expire Timeout option, if service provider asked, you can configure this option.

Registration Retry Interval, if GW5051 SIP accounts register to SIP server fail, you can configure this option, to make GW5051 retry the registration after a while.

OnHook Regret Timeout, On hook regret function allows you continue your call after you hang up the phone. You have a regret timeout to pick up the phone again and continue your call. This works only in case of incoming call.

Call failure RTP Timeout, active call failure treatment by RTP timeout and call resources disconnection.

DSCP for SIP and DSCP for RTP, options, these two parameters are used for QoS setting,
Configure difference DSCP value for SIP or RTP transport if you are familiar with the service, otherwise voice quality may be affected abnormally.

DTMF relay, it allows you to set the way how the DTMF is transmitted during voice call. Generally, DTMF digit can be passed via in-band or RFC2833 (out of band). SIP-INFO option is not suggested unless the service provider permitted.

HOOK Flash Relay Setting, which is used to configure the way how the hook flash is transmitted. Generally it is not need, so the default value is None.

SIP Transport Protocol, GW5051 both support UDP and TCP to transport SIP signal.

Polarity Reversal, payphone supporting. If you use GW5051 with a payphone, please enable this option.

Ingress gain and Egress gain support, it allows you to configure different level for each line.

3.12.6. Debug Settings

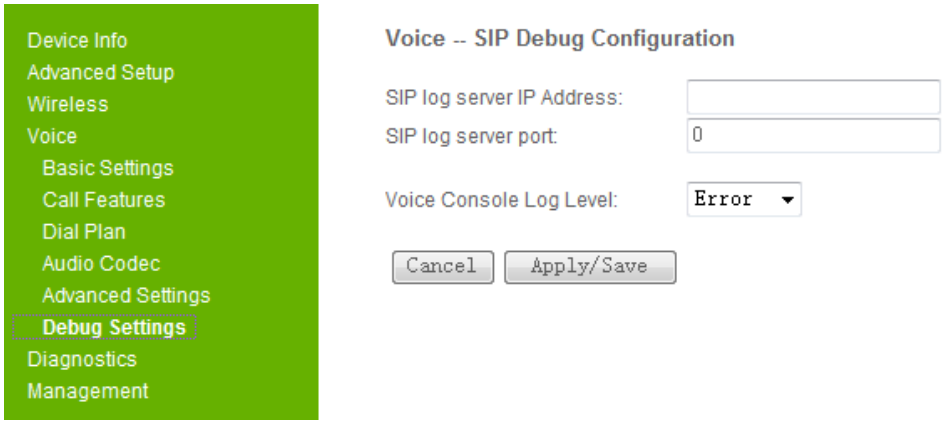


Figure 3-8-7 Debug Settings of voice function

Debug settings allows you to record the voice log, you only need to configure the log server information, which includes IP address and port.

The voice console log level support three log levels, which are
Error, Notice, Debug.

Under Error level setting, error logs will be recorded in log server if errors take place,

Under Notice level setting, more information will be recorded, and the Debug level will record the most information, which is used mostly for debug purpose only.

3.13. Management

3.13.1. Backup Settings and Restore Default Settings

Click “Management/Setting/Backup” on the left side of main page, it enables users to save current configuration to a file,

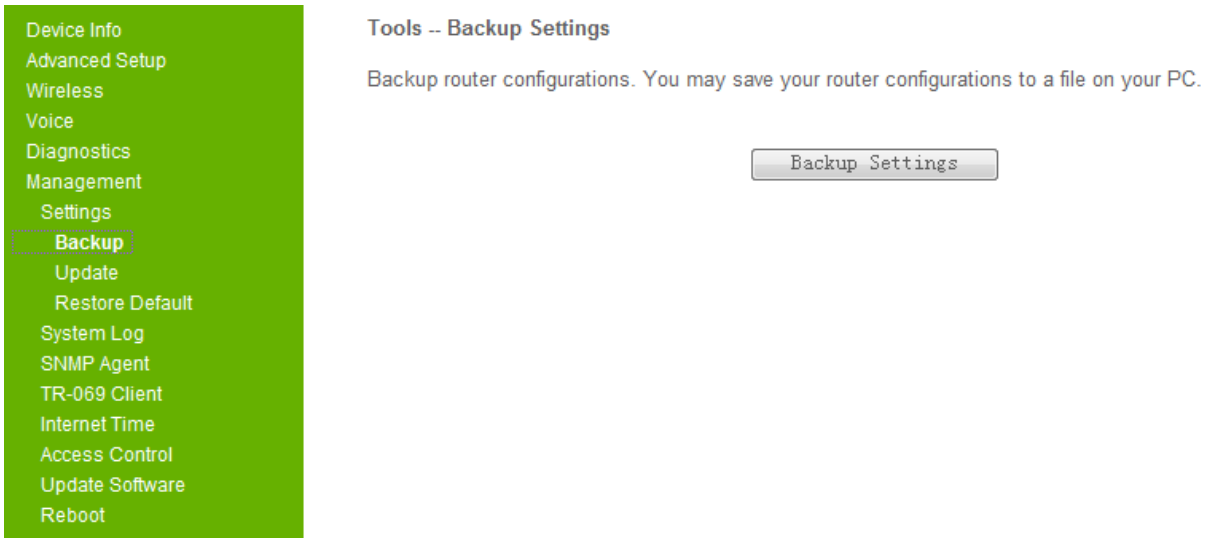


Figure 3-19-1 Backup Settings

Click “Management/Setting/Restore Default” on the left side of main page, it will allows users to reset all default settings for GW5051, in Figure 3-19-1,

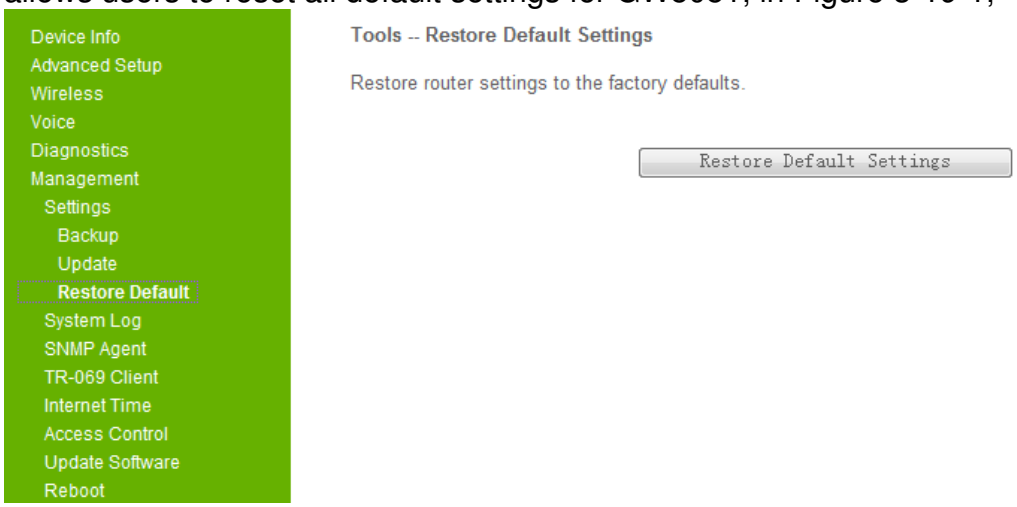


Figure 3-19-2 Restore default settings

Click the “Restore Default Settings” button, then system will reboot for a while.

3.13.2. TR-069 Client

Click the “Management/TR-069 Client”, you will access the Figure 3-19-3 to edit TR-069 client,

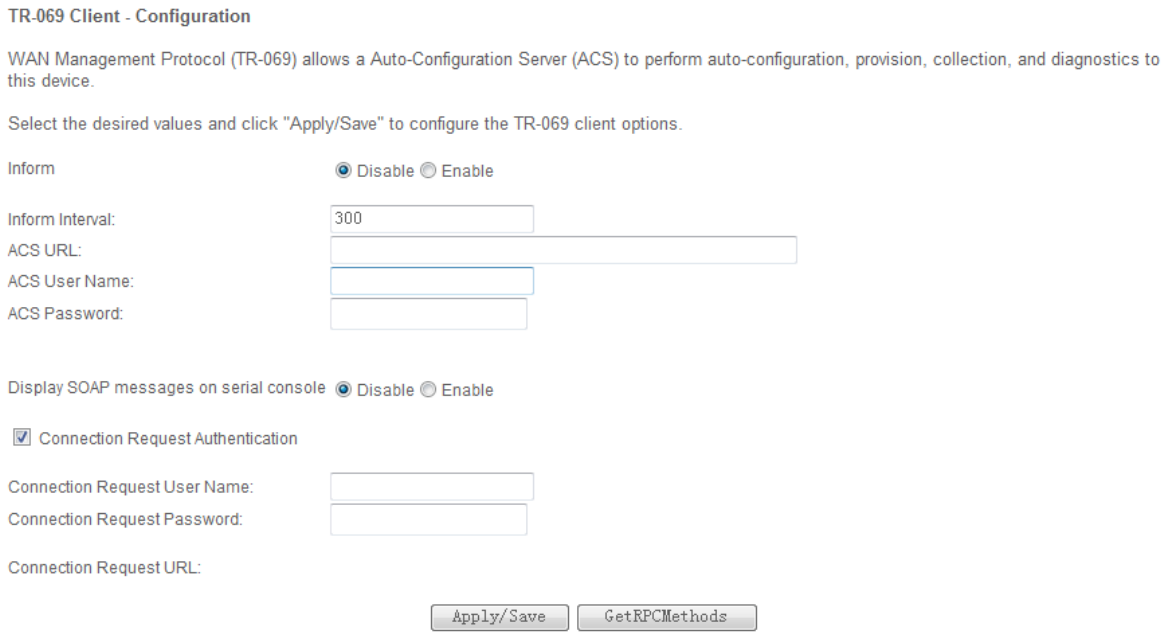


Figure 3-19-3 TR-069 Configuration

Fill in the information, which should be provided by service provider. And then Click “Apply/Save” button to make it work.

3.13.3. Internet Time

If you need GW5051 to get time from NTP server, you need to access this page to configure your local NTP information, see Figure 3-19-4, you need to choose corresponding NTP server.

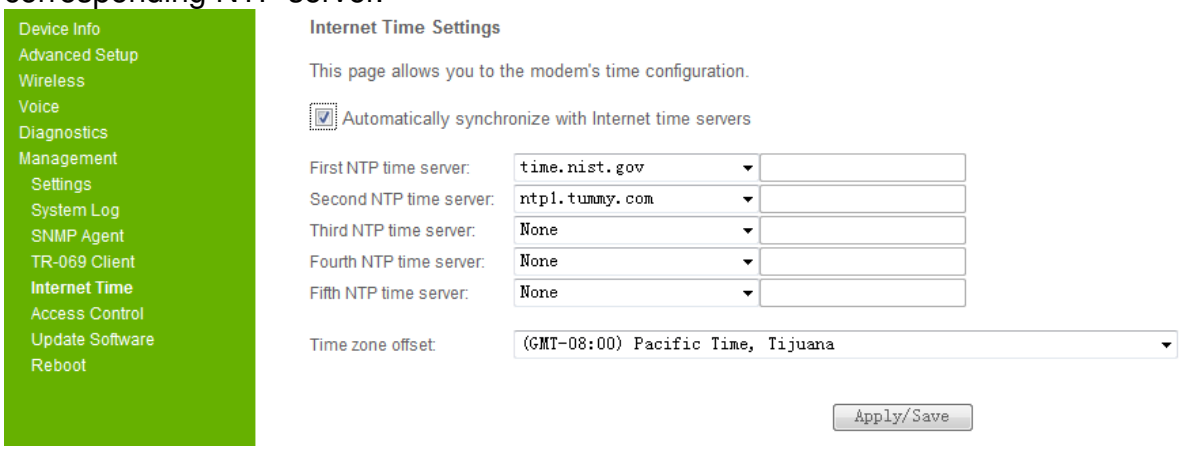


Figure 3-19-4 Internet Time Settings

3.13.4. Access Control

Access control enables to configure access accounts, and also to control remove access.

Passwords, see Figure 3-19-5,

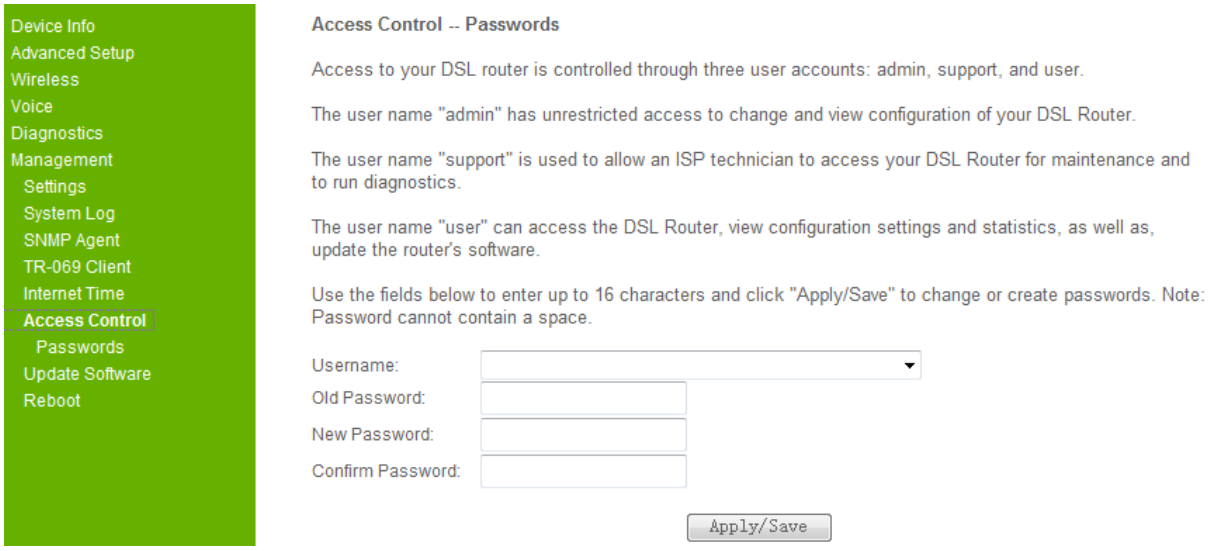


Figure 3-19-5 Access Control—Passwords

It allows you to set password for existed users.

3.13.5. Update Software

Figure 3-19-7 show the web page, which is used by updating software,

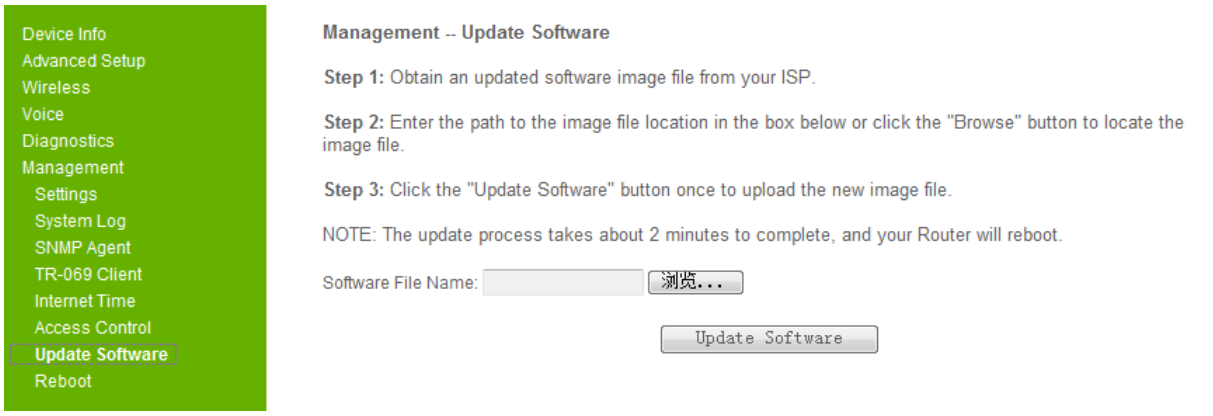


Figure 3-19-7 Update Software

It should be noticed that the update will take about more than 3 minutes; users should wait for a while, and the DSL will reboot by itself.

Conclusion:

E=12.14V/m is the maximum E-Field strength when safety distance between the EUT and human body is maintained at least 20cm, which is below 61V/m as required in Annex III table 2 of EC Council Recommendation (1999/519/EC). This proves that the unit complies with the EN 62311 for RF exposure requirement.

TECOM CO., LTD.
23, R&D ROAD 2, SBIP
HSIN-CHU, TAIWAN, ROC
PHONE: +886-3-577-5141
FAX: +886-3-579-7196

EU Declaration of Conformity

for

R&TTE Directive 99/5/EC

We,

TECOM CO., LTD.

---

hereby, declare that the essential requirements set out in the **R&TTE Directive 99/5/EC** have been fully fulfilled on our product with indication below:

Product Name: **VOIP GATEWAY**

Model / Brand Name: **GW5051 / Alvarion**

The following standards have been applied for the investigation of compliance:

EN 300 328 V 1.7.1:2006

EN 301489-1 V1.8.1 2008-04

EN 301489-17 V2.1.1 2009-05

EN 62311:2008

EN 60950-1:2006 + A11:2009

And apply notified body assessment:

Notified Body number 0700

PHOENIX TESTLAB GmbH

Königswinkel 10

D-32825 Blomberg

Germany

Furthermore, the ISO requirement for the in-process quality control procedure as well as the manufacturing process has been reached. The technical document as well as the test reports will be kept for a period at least 10 years after the last product has been manufactured at the disposal of the relevant national authorities of any Member State for inspection.

Detail contact information for this declaration has been listed below as the window of any issues relevant for this declaration.

FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) Statement

This Equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

1.The 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.

2.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.