DVG-G5402SP
Wireless VoIP Gateway

User's Manual

Version 1.0

(31 May 2007)

FCC Warning

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 communication. 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.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse B. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase B. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe B. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe B. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

Contents

1. Introduction

1-1 Product Overview

The DVG-G5402SP Wireless VoIP Gateway is designed to carry both voice and facsimile over the IP network and wirelessly share Internet access. It uses the industry standard SIP call control protocol so as to be compatible with free registration services or VoIP service providers' systems. As a standard user agent, it is compatible with all common Soft Switches and SIP proxy servers. While running optional server software, the gateway can be configured to establish a private VoIP network over the Internet without a third-party SIP Proxy Server.

The gateway can be seamlessly integrated into an existing network by connecting to a phone set and fax machine. With only a broadband connection such as an ADSL bridge/router, a Cable Modem or a leased-line router, the gateway allows you to use voice and fax services over IP in order to reduce the cost of all long distance calls.

The DVG-G5402SP is also an 802.11b/g wireless access point. Allow wireless clients to connect to it and share your broadband Internet connection. A built-in 4-port switch makes it possible to connect up to 4 Ethernet-enabled computers or devices to also share your Internet connection.

The wireless voip gateway can be configured a fixed IP address or it can have one dynamically assigned by DHCP over PPPoE. It adopts either the G.711, G.726, G.729A or G.723.1 voice compression format to save network bandwidth while providing real-time, toll quality voice transmission and reception.

1-2 Hardware Description

Front Panel

Power: Power LED. A steady light indicates a proper connection to a power source.

Prov./Alm.: A blinking light indicates the gateway is attempting to connect with the Provisioning server. Once the service connects, the LED will turn off. The LED will light solid if the self-test or boot-up fails.

Register: The Register LED will turn on when the gateway is connected to a VoIP service provider. The LED will turn off if not connected to a service provider.

WAN: When a connection is established the 10 or 100 LED will light up solid. The LED will blink to indicate

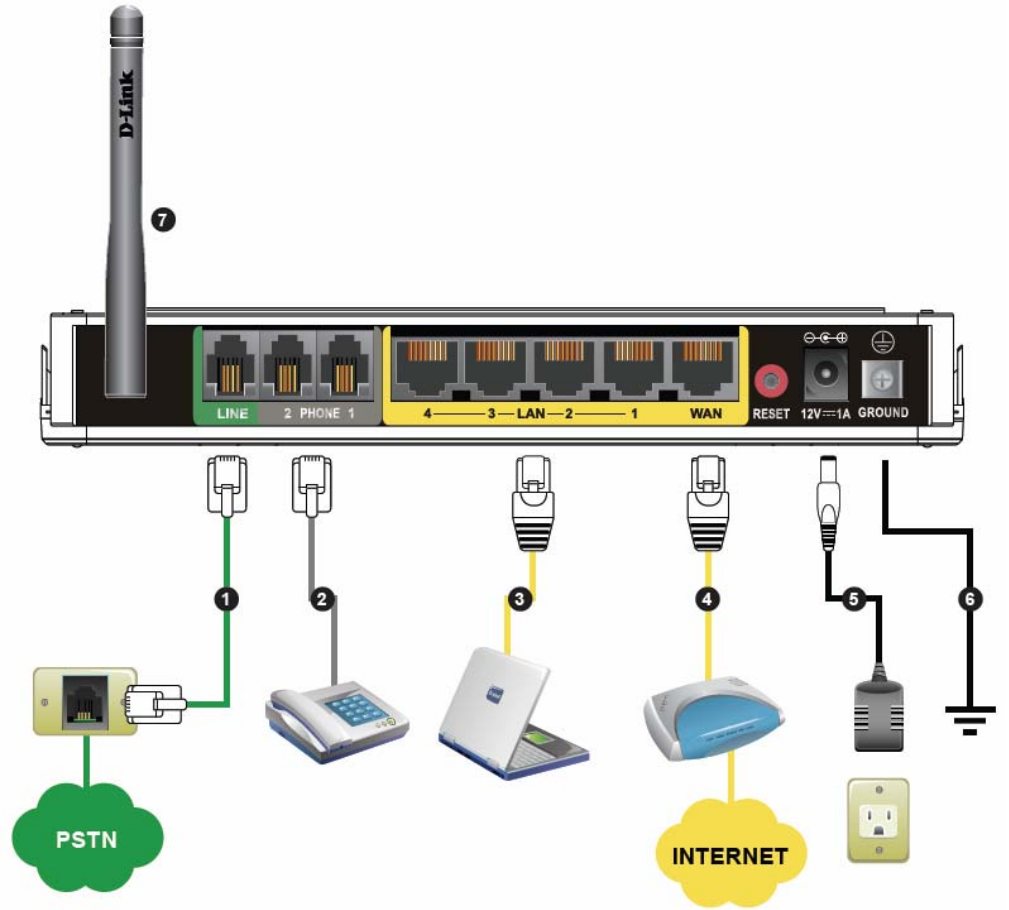
WLAN: A steady light indicates a wireless connection. A blinking light indicates that the DVG-G5402SP is receiving/transmitting from/to the wireless network.

LAN: When a connection is established the 10 or 100 LED (bottom) will light up solid on the appropriate port. The LEDs will blink to indicate activity. If the 10 or 100 LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.

Phone: This LED displays the VoIP status and Hook/Ringing activity on the phone port that is used to connect your normal telephone(s). If a phone connected to a phone port is off the hook or in use, this LED will light solid. When a phone is ringing, the indicator will blink.

Line: Light on means the line is in use (off-hook), and vice versa.

Rear Panel



1. **Line:** Connect to your original telephone line on the wall jack with RJ-11 cable.
2. **Phone Port (1-2):** Connect to your phones using standard phone cabling (RJ-11).
3. **LAN:** Connect to your Ethernet enabled computers using Ethernet cabling.
4. **WAN:** Connect to your broadband modem using an Ethernet cable.
5. **Power Receptor:** Receptor for the provided power adapter.
6. **Ground:** A conducting connection with the earth Connect with the ground so as to make the earth a part of an electrical circuit using metal wire.
7. **Antenna:** Connect to a wireless network.

WARNING: DO NOT (1) connect the phone ports to each other (FXS to FXS) or (2) connect any phone port directly to a PSTN line (FXS to PSTN) or to an internal PBX line (FXS to PBX extension). Doing so may damage your VoIP gateway.

Use Reset Button to restore factory default settings (IP address, Login ID and Password):

1. **Disconnect the power plug.**
2. **Press and hold the reset button for 6 seconds.**
3. **Reconnect the power plug while pressing down on the reset button.**
4. **Release the reset button after 6 seconds. Factory settings will be restored.**

2. Gateway Configuration – Use Web Browser

The VoIP gateway allows users to configure its settings using a web interface (Web UI). You can access the Configuration Menu by opening a web-browser (e.g., Internet Explorer or Netscape Navigator) and entering the factory default LAN IP address: 192.168.8.254. The IP address of the Web UI is same as the default LAN IP noted elsewhere in this user's manual.

You can also use an ordinary telephone, connect it to the gateway, and dial "101" to inquire about the current WAN Port IP address and then use the WAN port to log-in.

Instructions

1. Open a Web-Browser (e.g., Explorer, Navigator, Opera, Firefox).
2. Enter the LAN port IP address. The default LAN port IP address is: 192.168.8.254.
3. The log-in screen below will appear after you connect. (The factory default settings for **Login ID** and **Password** are blank (i.e., no login ID, no password).)

The gateway does not allow multiple people to configure the gateway simultaneously. Please remember to logout or restart the system if you are not using the web configuration function.

2-1 SETUP

2-1-1 WAN Settings

WAN (Wide Area Network) Settings are settings that are used to connect to your ISP (Internet Service Provider). The WAN settings are provided to you by your ISP and often times referred to as "public settings". Please select the appropriate option for your specific ISP.

IP Configuration (Setting WAN Port)

There are five methods of obtaining a WAN port IP address:
1. Static IP
2. DHCP, which means a Dynamic IP (Cable Modem)
3. PPPoE (dial-up ADSL)
4. PPTP
5. BigPond (for Australia only)

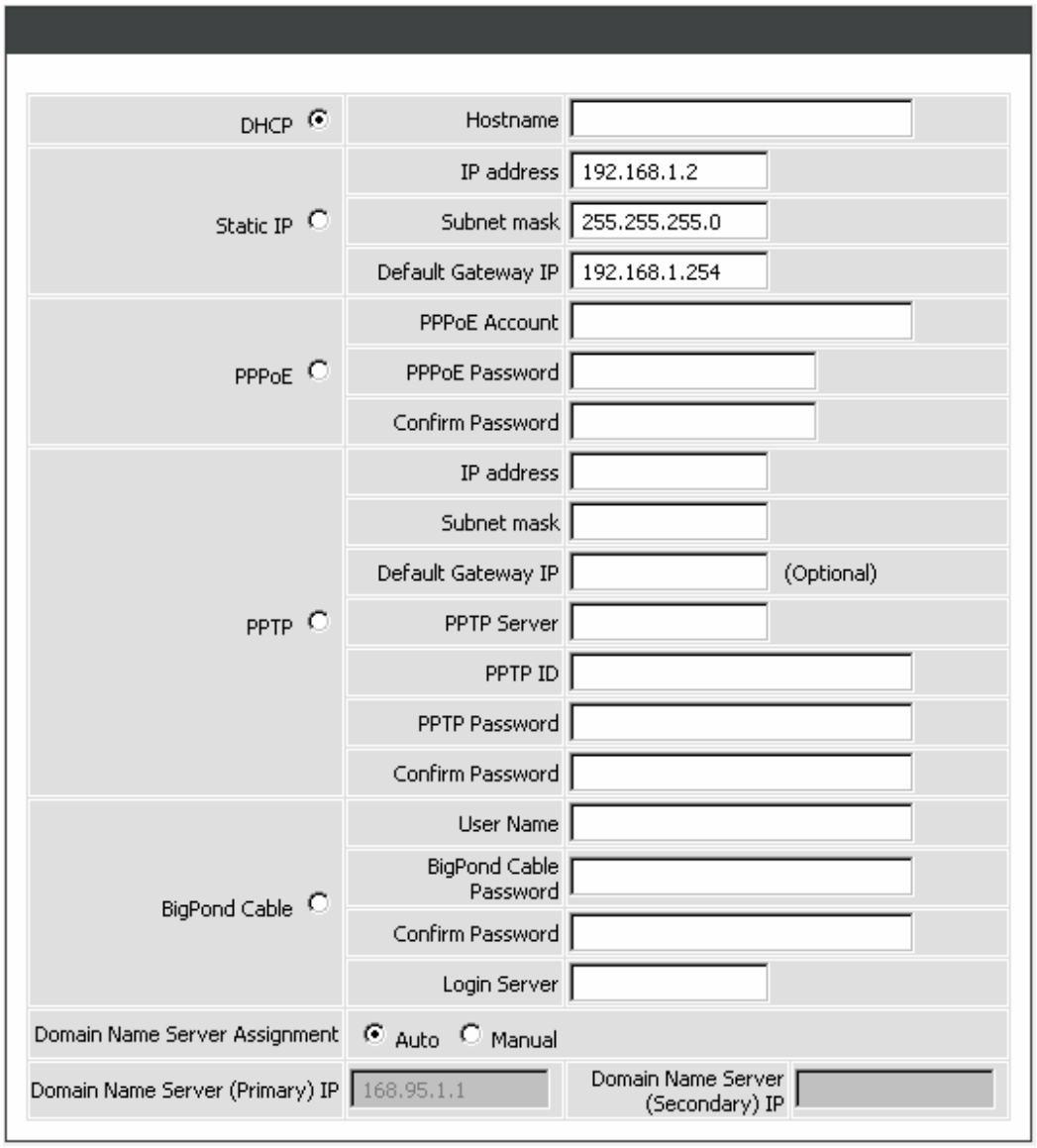
Methods for using DHCP and PPPoE for obtaining an IP address may vary. If you are not familiar with creating a network connection, please contact your local ISP.

After selecting the suitable option, click **Accept** at the bottom of the screen to save the settings.

You need to save the changes and restart the gateway to make the changes active. Saving the settings: Click **MAINTENANCE** and select **Save/Restart** in System from the left menu. Tick **Save Settings** and **Restart**, then click **Accept**. Wait for about 40 seconds before the gateway obtaining an IP address by the method you selected.

Note: When the system has obtained a new IP address, and you are using a WAN port to enter the Web Configuration Screen, the new IP address has to be used before you can get connected to the gateway. The same principle applies to the next two settings.

SETUP → WAN SETTINGS



DHCP: Select this option if your ISP (Internet Service Provider) provides you an IP address automatically. Cable modem providers typically use dynamic assignment of IP Address. The Host Name field is optional but may be required by some Internet Service Providers.

Static IP: Select this option if your ISP (Internet Service Provider) provides you a Static IP address. Enter the **IP address**, **Subnet Mask** and **Default Gateway IP**.

PPPoE: Select this option if your ISP requires you to use a PPPoE (Point-to-Point Protocol over Ethernet) connection. Enter the **PPPoE Account**, **PPPoE Password** and re-enter Password to confirm.

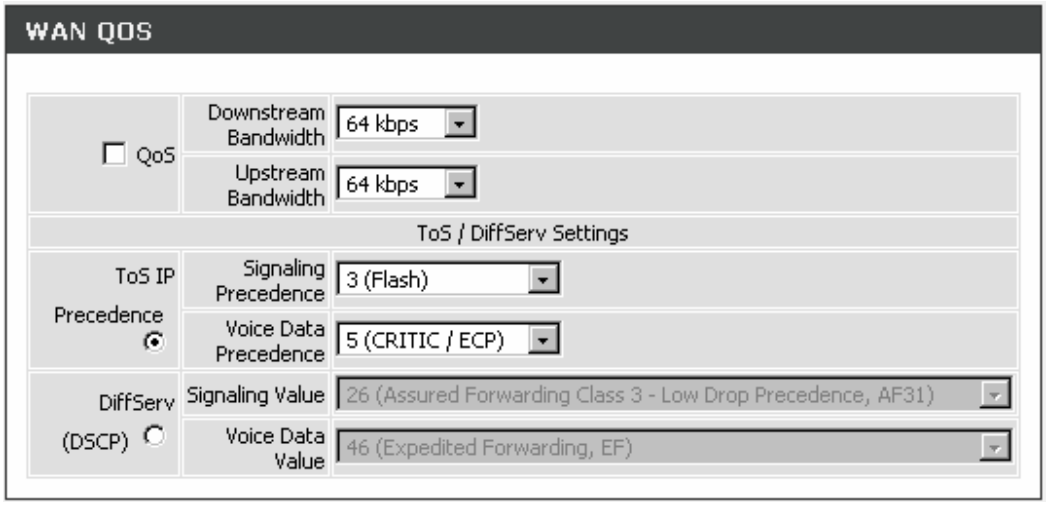
PPTP: Point-to-Point Tunneling Protocol (PPTP) is a WAN connection. Enter the **IP Address**, **Subnet mask**, **PPTP Server**, **PPTP ID** and **Password**.

BigPond: Dynamic IP Address for BigPond is a WAN connection used in Australia. Enter the username and password for the BigPond account and the login server if required.

Domain Name Server Assignment: Select **Auto** or **Manual** to get the IP address of Domain Name Server assigned by ISP or manually.

Domain Name Server IP: Enter the primary and secondary IP address of Domain Name Server if Domain Name Server Assignment is **Manual**. Otherwise, the gateway will not be able to access hosts using hostnames instead of IPs.

SETUP → WAN SETTINGS



QoS: Check the box to guaranty the voice quality. Voice packets have the highest priority in IP networks, and the data transmission is distributed to less bandwidth.

Downstream Bandwidth - Select the downstream bandwidth that is the same as the actual bandwidth subscribed from the drop-down menu.

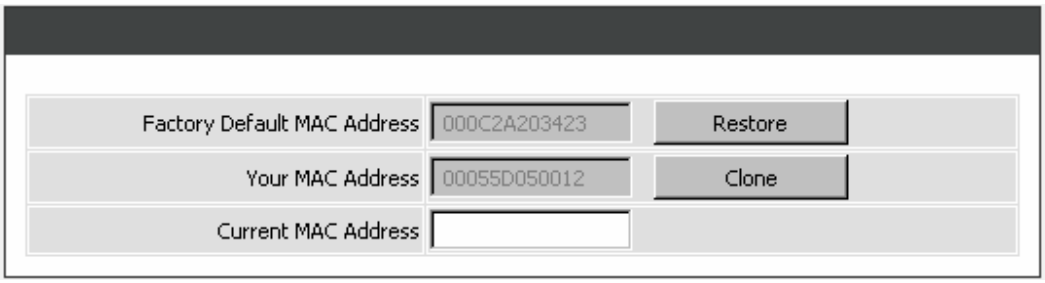
Upstream Bandwidth - Select the upstream bandwidth that is the same as the actual bandwidth subscribed from the drop-down menu.

ToS IP Precedence: Select the precedence for signaling (data) and voice (voice data) from the drop-down menu.

DiffServ (DSCP): Select the number of signaling (data) and voice (voice data) values for priority marking from the drop-down menu.

Note: For the gateway, ToS IP Precedence and DiffServ are the same function. You only select one for priority marking.

SETUP → WAN SETTINGS



Factory Default MAC Address: The original MAC address of the gateway.

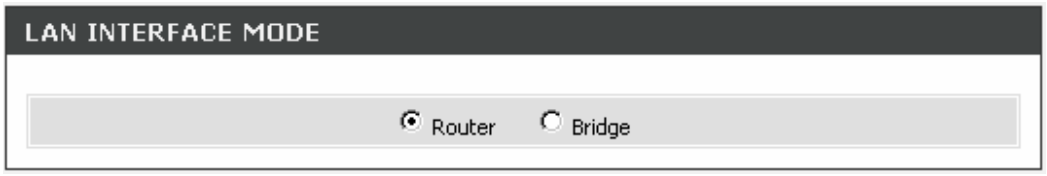
Your MAC Address: It is left blank as you log-in via the WAN port.

Current MAC Address: It shows the current MAC Address if you ever used the difference MAC address from Factory Default MAC Address. You can click **Clone** to automatically copy the MAC address of the Ethernet Card installed in the computer used to configure the device.

Note: This is only necessary to fill the field if required by your ISP.

2-1-2 LAN Settings

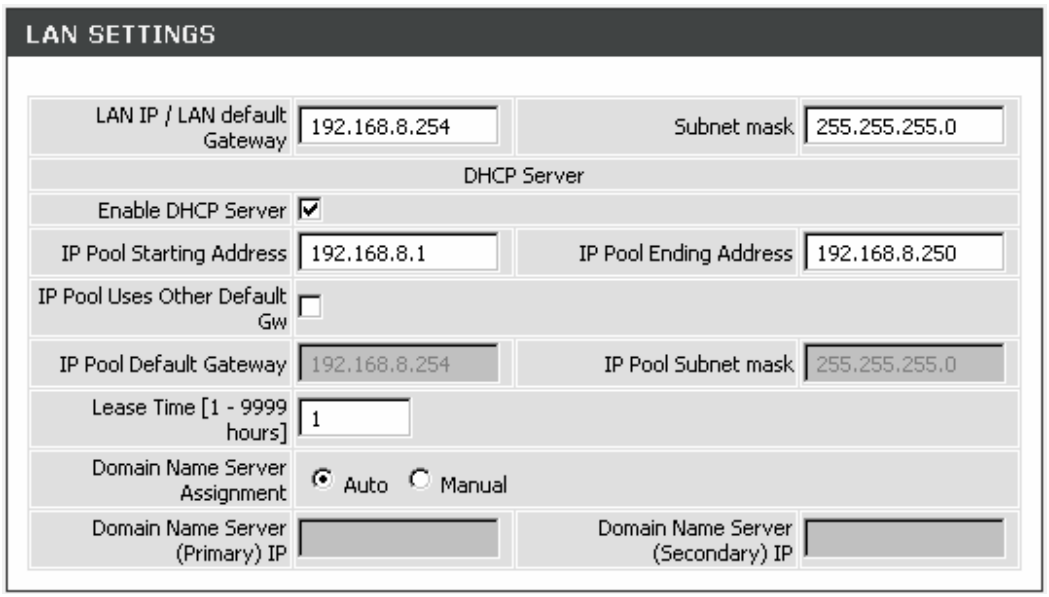
SETUP → LAN SETTINGS



LAN Interface Mode: Select the gateway serving as a **Router** with NAT or **Bridge** between WAN port and LAN port without NAT.

Note: It is still accessible if LAN Interface Mode is Bridge.

SETUP → LAN SETTINGS



LAN IP / LAN default gateway: Enter the LAN IP address of the gateway. It is also the default gateway for DHCP clients.

Subnet make: Enter the subnet mask for DHCP clients.

Enable DHCP Server: This variable is to assign the IP address for the devices connected to LAN port of the gateway.

IP Pool Starting Address: Enter the starting IP address for the DHCP server's IP assignment.

IP Pool Ending Address: Enter the ending IP address for the DHCP server's IP assignment.

IP Pool Uses Other Default Gw: Check the box to assign different default gateway for DHCP clients.

IP Pool Default Gateway: Enter the new default gateway that is different from LAN IP of the gateway.

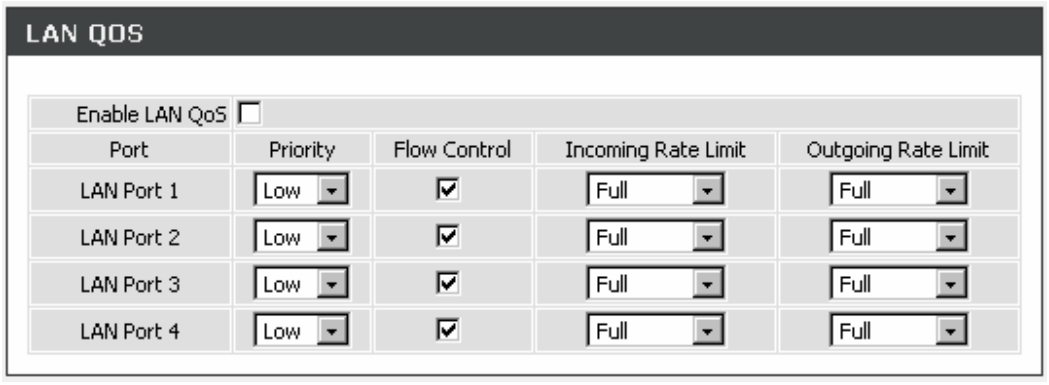
IP Pool Subnet mask: Enter the new subnet mask.

Lease Time: Enter the length of time for the IP lease.

Domain Name Server Assignment: Select **Auto** or **Manual** to get the IP address of Domain Name Server assigned by ISP or manually.

Domain Name Server IP: Enter the primary and secondary IP address of Domain Name Server if Domain Name Server Assignment is **Manual**. Otherwise, the gateway will not be able to access hosts using hostnames instead of IPs.

SETUP → LAN SETTINGS



Enable LAN QoS: Check the box to enable LAN QoS by Hardware.

Priority: Use the drop-down menu to select **Low** or **High** for the gateway to deliver the packets from LAN interface when the packets arrive at the same time.

Flow Control: Check the box to limit incoming and outgoing rate if ticked.

Incoming Rate Limit: Use the drop-down menu to select the proper rate limit for the specific LAN port. The flow is from LAN to WAN, and the rate limit can not exceed the real upstream bandwidth.

Outgoing Rate Limit: Use the drop-down menu to select the proper rate limit for the specific LAN port. The flow is from WAN to LAN, and the rate limit can not exceed the real downstream bandwidth.

2-1-3 Wireless Settings

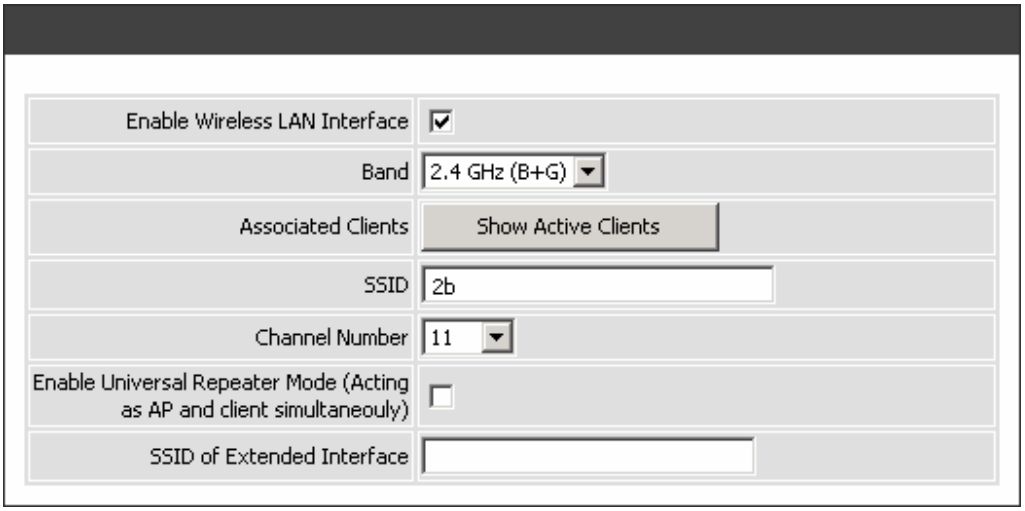
This section instructs you how to setup your wireless network on the Gateway device.

Setup Hint:

1. Every device in the same wireless network must use the same SSID.
2. To avoid wireless network overlap, a specific and different channel is needed.
3. Make sure security used by every device in the same wireless network is compatible with the wireless AP.

2-1-3-1 Basic Settings

Wireless Settings → Basic Settings



Enable Wireless LAN Interface: Enable wireless basic settings on LAN interface.

Band: The Gateway can operate in 2.4GHz ISM band with different speed of wireless connection, Select the wireless band of your network.

2.4GHz (B) - Allow all 802.11B compliant wireless devices to associate with the wireless AP.

2.4HGz (G) - Allow all 802.11G compliant wireless devices to associate with the wireless AP.

2.4GHz (B+G) - Allow a mix of both IEEE802.11b and IEEE802.11g compliant wireless devices to associate with the wireless AP.

Associated Clients: Click on **Show Active Clients** button, you can see all clients associated to the AP.

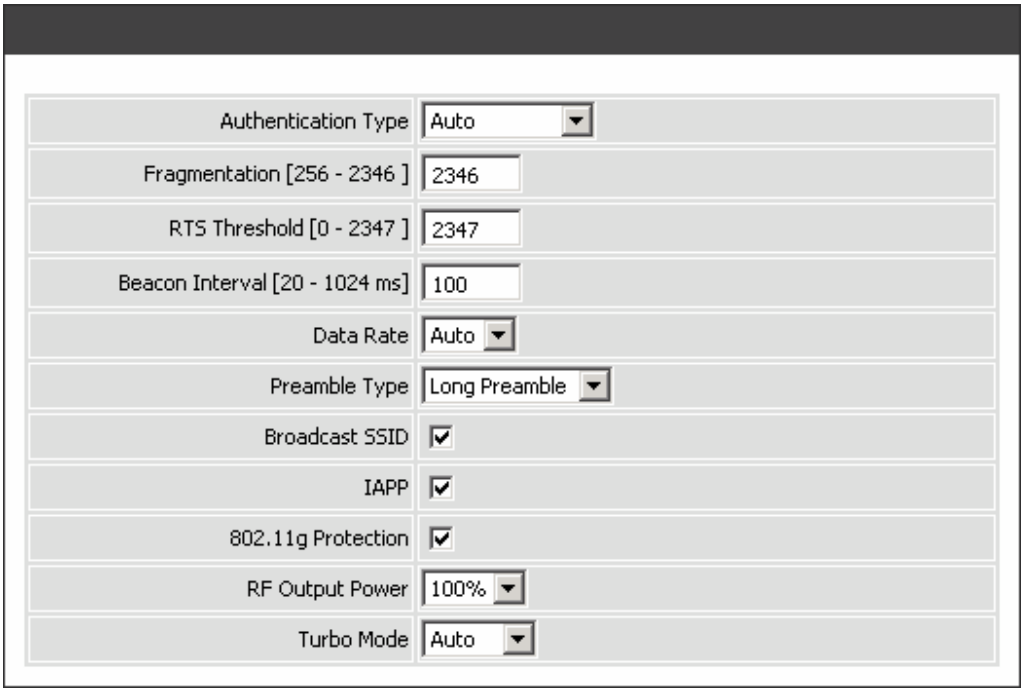
SSID: SSID is the name of your wireless network. All wireless-equipped devices share the same SSID to communicate with each other. It must be unique to identify separated wireless network. For security, you should change the default SSID to a special ID.

Channel Number: Select a clear and appropriate channel for your wireless network. A device on your wireless network must use a specific channel to transmit and receive data. If wireless network has overlap, change a different channel number.

2-1-3-2 Advanced

This section introduces advanced configuration for the wireless access point. If you are not familiar with the following functions, keep the default parameters. In some cases, incorrect settings may reduce wireless performance.

Wireless Settings → Advanced



Authentication Type: Select the type of authentication.

Open System - Any wireless client can associate with the wireless access point but the client must have the same WEP key to exchange data.

Shared Key - Wireless clients must have the same WEP key to associate with wireless access point and exchange data.

Auto – Auto-detect the authentication type.

Fragmentation: A packet can be fragmented into small units to pass over a network medium that can not support the original packet size. If you encounter a busy network, a lower value of Fragment Threshold could improve performance. If the traffic flows are not very busy, a higher Fragment Threshold provides good network performance. In most case, keeping the default value=2346 is recommended.

RTS Threshold: RTS Threshold is a mechanism to implement in collision avoidance. In a large wireless network, two stations do not hear each other but can hear wireless access point. When the two send data to Access Point at the same time, it may result in data collision and a loss of messages for both wireless stations. In most case, keeping the default value=2347 is recommended.

Beacon Interval: The default value is **100**. The Beacon Interval indicates the frequency interval of target beacon transmission time which can be found in a packet body. The Gateway transmits the beacon packet to help a wireless client to identify the existence of nearby access point. If the beacon intervals are too long, it would be hard to access the network. If the beacon intervals are too short, the resources would be wasted.

Data Rate: IEEE802.11b supports Auto, 1, 2, 5.5, 11 Mbps signaling rate. EEE802.11g supports Auto, 6, 9, 12, 18, 24, 36, 48, 54 Mbps signaling rate. The data rate will change automatically to get better throughput depending on range and environment of the wireless network.

Preamble Type: Preamble Type defines the length of the preamble which sends out with a packet format. Specify an appropriate preamble type for your network, if you do not know which one to select, keeping the default setting **Long Preamble** is recommended.

Broadcast SSID: Disable the SSID broadcast. This is to prevent users from seeing your wireless network.

IAPP: IAPP (Inter Access Point Protocol) provides the communication among access points in order to support mobile station roaming mechanism from one access point to another.

802.11g Protection: In 802.11b/g Mixed mode, it can be used for protection mechanism. The 802.11g OFDM traffic can keep the connection stable and avoid 802.11b interference. But that might cause the poor throughput.

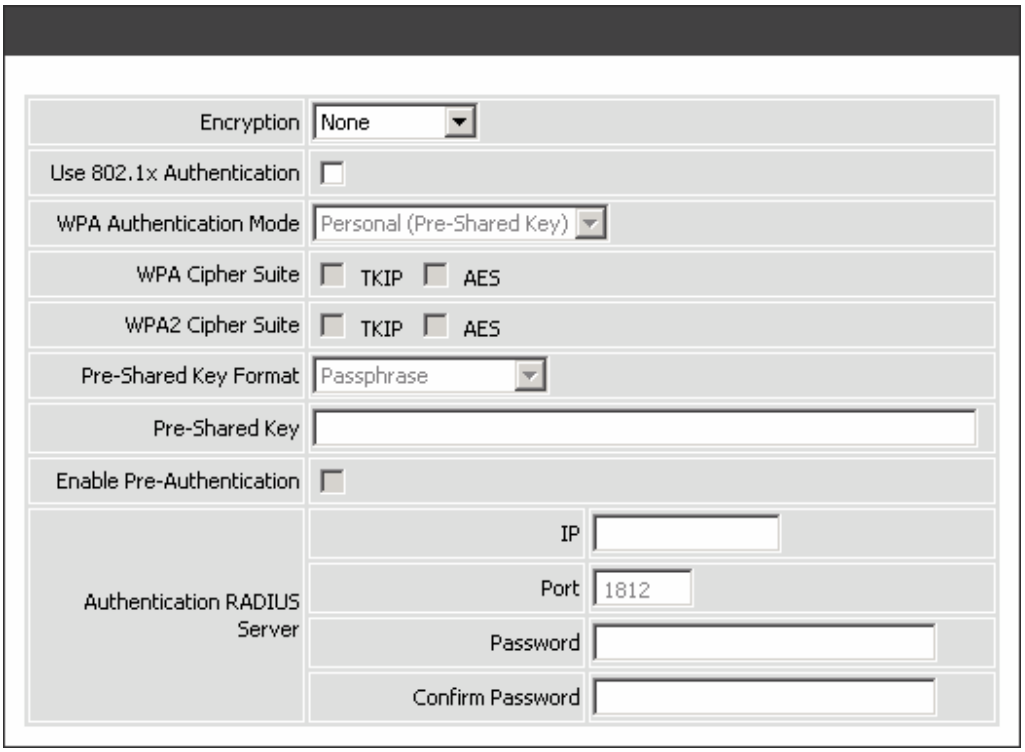
RF Output Power: You can adjust the percentage of power 100, 50, 25, 10, 5 of your Gateway to change the coverage of wireless network. Keep the default value, 100% to reach full range.

Turbo Mode: The AP would identify the wireless station's chipset to improve the performance.

2-1-3-3 Security Settings

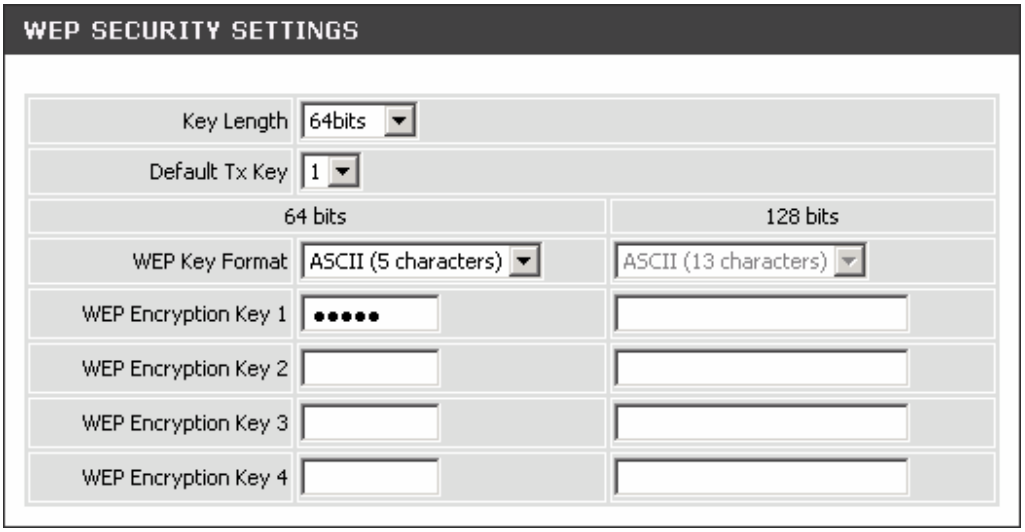
This section introduces you different ways of wireless security you can setup. It is important to enable secure algorithm to protect your data from eavesdropping by unauthorized wireless users.

Wireless Settings → Security Settings



Encryption: Select the encryption/authentication type: None, WEP, WPA, WPA2 and WPA2 Mixed.

Wireless Settings → Security Settings (WEP)



Key Length: Select 64-bit or 128-bit data encryption.

Default Tx Key: You can select one of the keys as active key at a time.

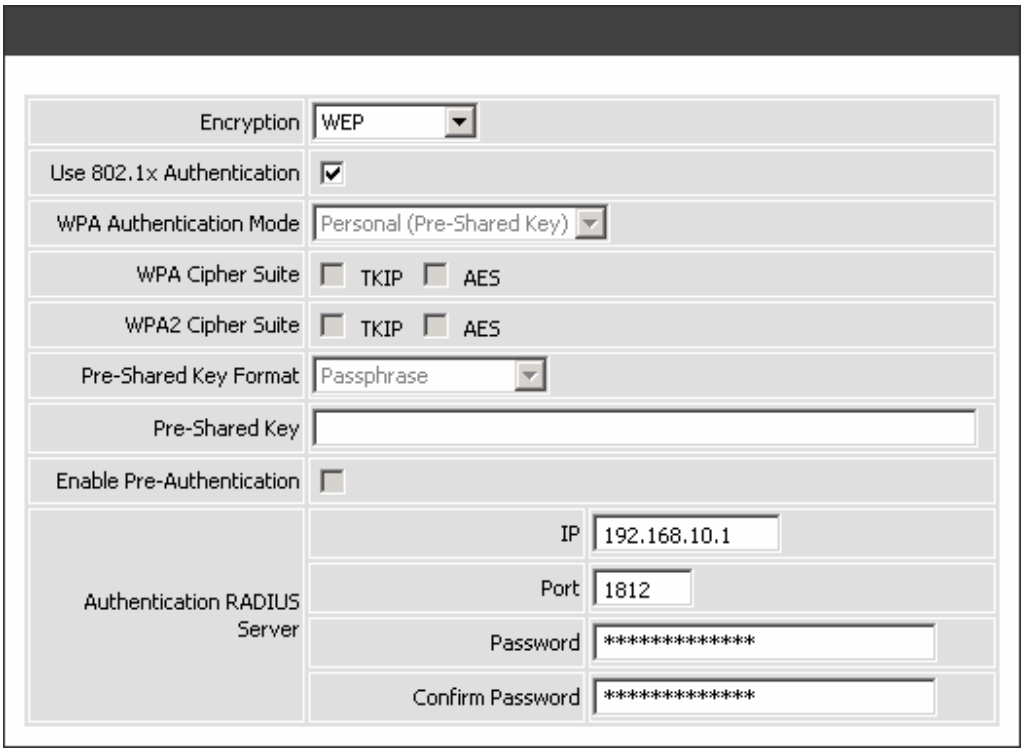
WEP Key Format: Select the preferred WEP Key Format according to which WEP encryption you choose. When WEP 64bits is enabled, you can select ASCII (5 characters) and Hex (10 characters). When WEP 128bits is enabled, you can select ASCII (13 characters) and Hex (26 characters).

WEP Encryption Key 1 – 4: You can manually input key value from Key1 to Key4. Type a character sting and apply changes.

For a 64-bit WEP key-- Enter 5 characters (ASCII sting) or 10 hexadecimal characters ("0-9", "A-F").

For a 128-bit WEP key-- Enter 13 characters (ASCII sting) or 26 hexadecimal characters ("0-9", "A-F").

Wireless Settings → Security Settings (WEP)



Use 802.1x Authentication: Enable or disable using 802.1x Authentication.

Authentication RADIUS Server:

Port - Enter the port number of the authentication RADIUS server. Keep the default value: 1812 unless the server required change to another number.

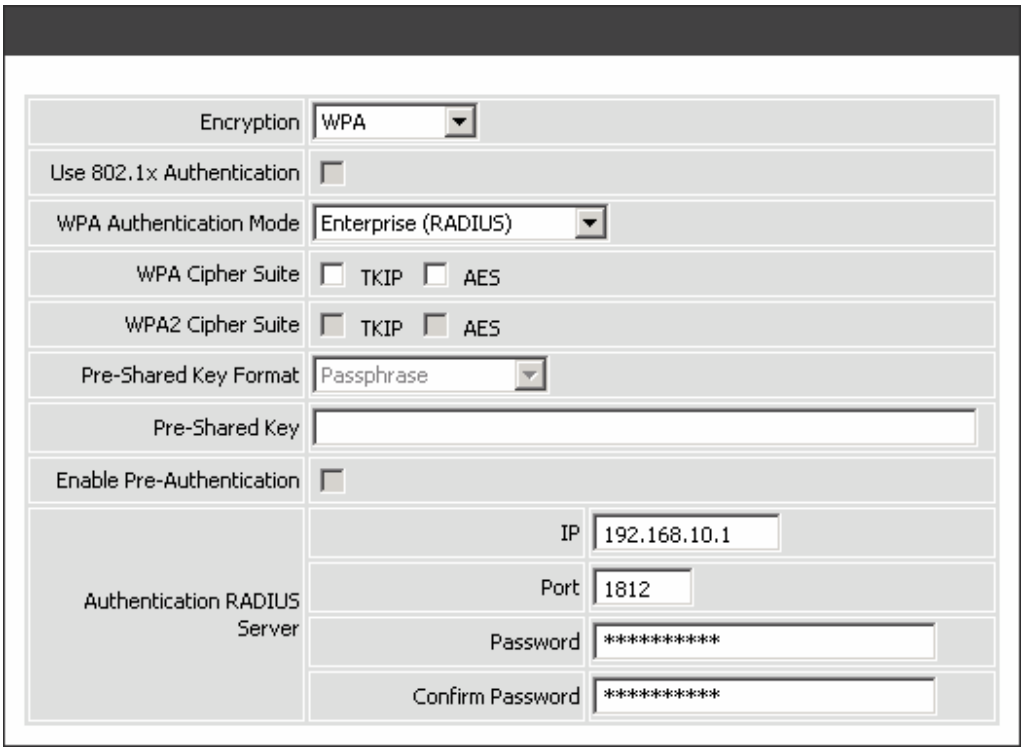
IP address - Enter the IP address of the authentication RADIUS server.

Password - Enter a password as the key of the communication between the authentication server and the access point. The password of the access point must be the same with that of the authentication sever.

WPA Authentication Mode

The wireless network can use WPA Authentication to verify whether a wireless device is allowed to access your Access Point or not. You can choose to use Enterprise (RADIUS) method or Personal (Pre-Shared Key). The encryption mechanism used for RADIUS and WPA-PSK is the same. The difference between the two is that WPA-PSK uses a specific characters sting like password instead of a user-authentication.

Wireless Settings → Security Settings (WPA)



Select the type of WPA (WPA, WPA2, WPA2 Mixed), choose the proper security mode according to your wireless network.

WPA Cipher Suite: WPA Cipher Suite is used for the configuration of WPA or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

WPA2 Cipher Suite: WPA2 Cipher Suite is used for the configuration of WPA2 or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

Enable Pre-Authentication: To use pre-authentication before actually associating with a new AP.

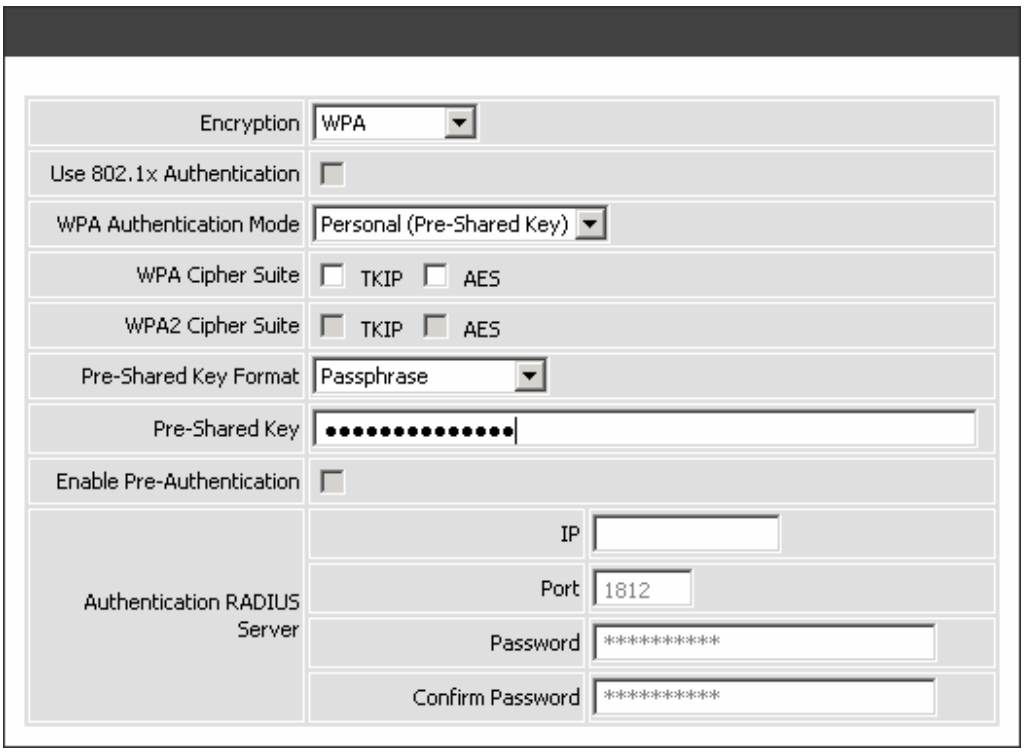
Authentication RADIUS Server:

Port - Enter the port number of the authentication RADIUS server. Keep the default value: 1812 unless the server required change to another number.

IP address - Enter the IP address of the authentication RADIUS server.

Password - Enter the password such as a security Key.

Wireless Settings → Security Settings (WPA-PSK)



Select the type of WPA-PSK (WPA-PSK, WPA2-PSK, WPA2 Mixed-PSK), choose the proper security mode according to your wireless network.

WPA Cipher Suite: WPA Cipher Suite is used for the configuration of WPA or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

WPA2 Cipher Suite: WPA2 Cipher Suite is used for the configuration of WPA2 or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

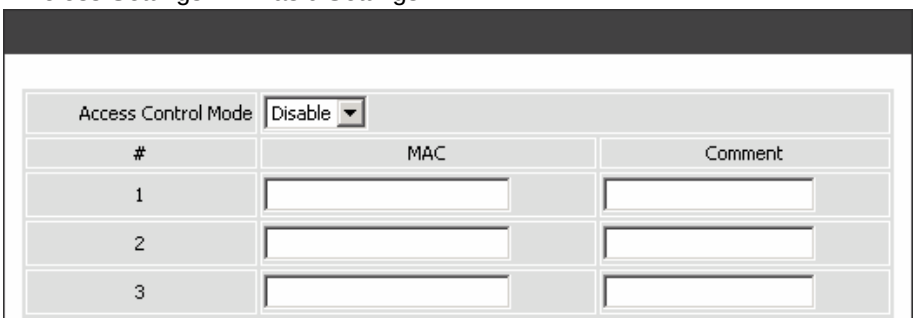
Pre-Shared Key Format: Select the Format of Pre-Shared Key. You can select Passphrase or Hex (64 characters) by entering a character string. You may input 8-64 characters ranging from "A-Z" and "0-9".

Pre-Shared Key: Enter a key of 8-64 characters long in the Pre-Shared Key filed. Make sure this key is exactly the same on all other wireless stations.

2-1-3-4 Access Control

The Access Control setting provides a service that you can control different access rights for different wireless clients connected to your Gateway. The local and remote stations are limited to access Internet through your Access Points using MAC address of wireless client. Choose the appropriate Access Control Services from Wireless Access Control Mode option.

Wireless Settings → Basic Settings



Disable: The Gateway does not response to any access rules. You are not allowed to make configuration changes on this page.

Allow Listed: When **Allow Listed** is enabled, only those wireless clients whose MAC addresses are in the Access Control List have rights to connect to your Access Point.

Deny Listed: When **Deny Listed** is enabled, only those wireless clients whose MAC addresses are in the Access Control List will be blocked and restricted access to your Access Point.

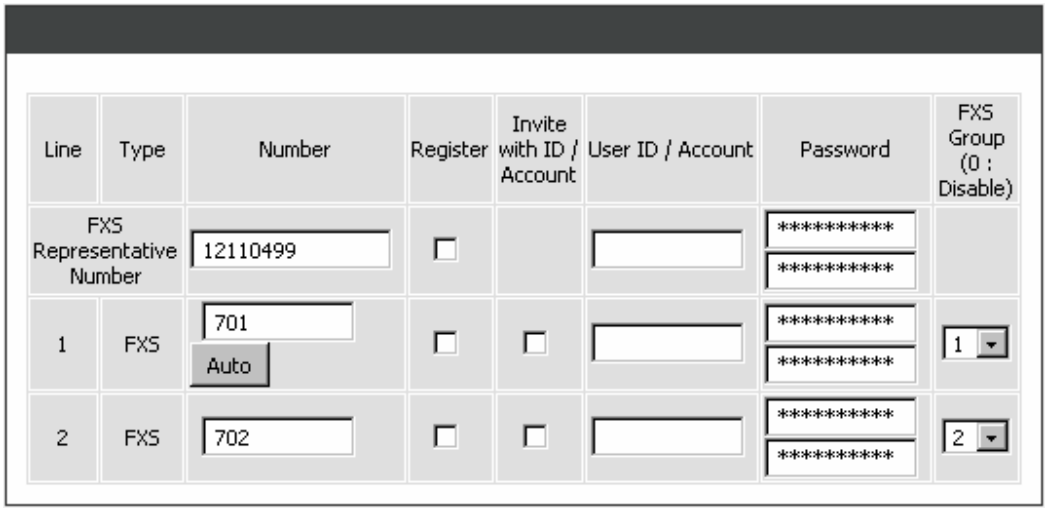
MAC Address: Specify the MAC address which you want to allow/deny access your Access Point.

Comment: The space is reserved for comment or notation.

2-1-4 VoIP Settings (SIP Basically setting)

As there are various VoIP Service Providers, the gateway has been designed to be compatible with them according to RFC standards. If any registration problem occurs, please consult your VoIP Service Provider.

SETUP → VOIP SETTINGS



Number: Enter the number, text or number and text in this field. It is the Caller ID for the called party when you make a VoIP call. If you register the gateway to a SIP proxy server, then it will be the number provided by SIP proxy server. Number and User ID/Account are usually the same from most SIP proxy severs. Each line has a number. And the number of each line is not reiteration.

FXS Representative Number: Enter the representative number for Line 1 and Line 2. If the gateway is configured to register with SIP proxy server, Line 1 and Line 2 are using this number to call through SIP proxy server.

Note: Please ensure if your VoIP Service Provider allows one account for multi-port using.

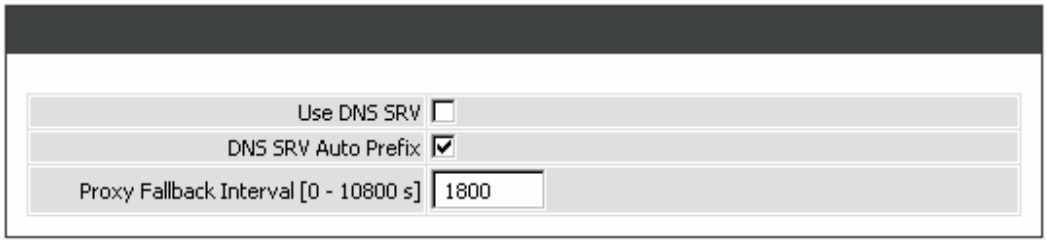
Register: Check the box to register with SIP proxy server if ticked.

Invite with ID / Account: Check the box to call through SIP proxy server without registration. It is always ticked when Register is also ticked. Most VoIP Service Providers will interdict the connection without registration.

Password: Enter password and re-enter to confirm.

FXS Group: Select group hunting priority for each line from the drop-down menu. It is to assign an unassigned call according to the Hunting Priority by the gateway when there is an incoming call. A setting of "0" zero is to disable the hunting function.

SETUP → VOIP SETTINGS

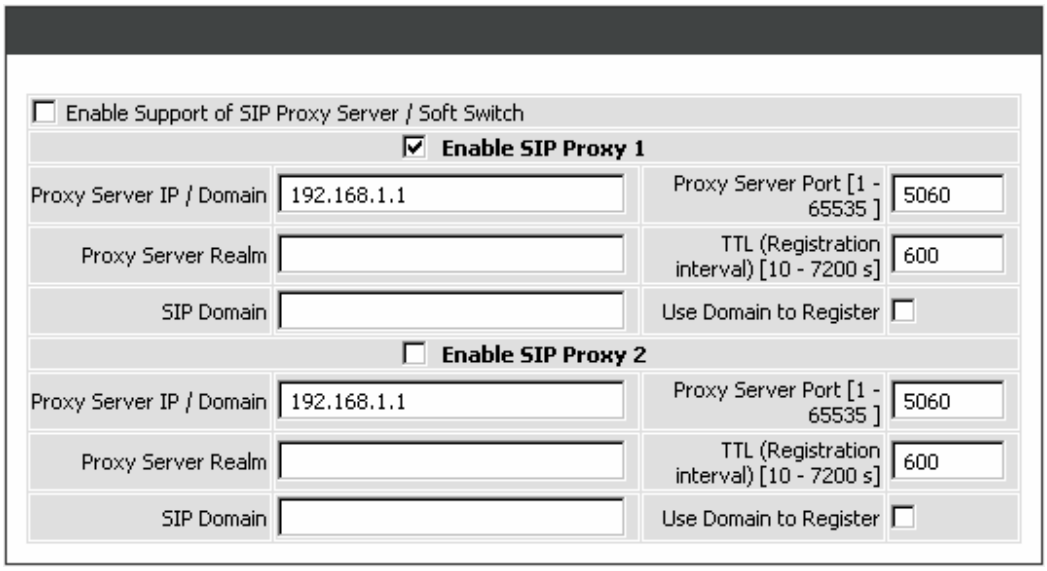


Use DNS SRV: Check the box to use DNS SRV to connect to the SIP proxy server. Domain Name Server (DNS) SRV helps clients connecting to the SIP proxy server with a specific domain and get back the IP address of any available server.

DNS SRV Auto Prefix: Check the box to use ***_sip._udp.domain.com*** to query IP by default. The gateway will use ***domain.com*** to query IP if un-ticked.

Proxy Fallback Interval: Enter the interval for the gateway querying the IP address of the main server if the gateway has registered to the secondary server.

SETUP → VOIP SETTINGS



Enable Support of SIP Proxy Server / Soft Switch: Check the box to register the gateway with SIP proxy server or soft switch. The gateway is registered with SIP Proxy 2 if all lines have failed to register with SIP Proxy 1. SIP Proxy 2 will be a backup proxy if both SIP Proxy 1 and 2 are enabled.

Proxy Server IP/Domain: Enter the IP address or URL (Uniform Resource Locator) of SIP proxy server or soft switch.

Proxy Server Port: Enter the SIP proxy server's listening port for the SIP in this field. Leave this field to the default if your VoIP Service Provider did not give you a server port number for SIP.

Proxy Server Realm: Enter the realm for SIP proxy server. It is used for authentication in a SIP server. In most cases, the gateway can automatically detect your SIP server realm. So you can leave this option blank. However, if your SIP server requires you to use a specific realm you can manually enter it here.

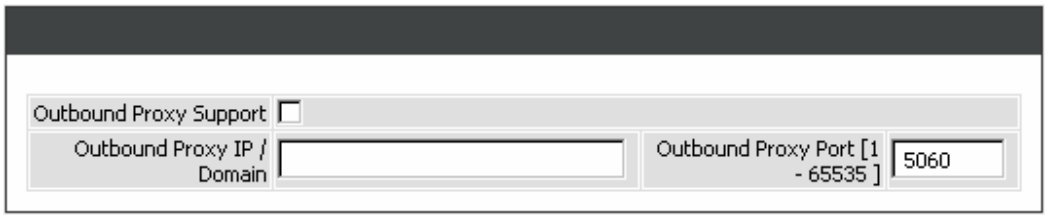
TTL (Registration interval) [10-7200 s]: Enter the desired time interval at which the gateway will report to your SIP proxy server.

SIP Domain: Enter the SIP domain provided by your VoIP Service Provider. (Note that some SIP proxy servers might not require this.) If you enable "Uses Domain to Register", the gateway will register to the SIP proxy server with the domain name you filled in. Otherwise, the gateway will register to a SIP proxy server with the IP it resolves.

Use Domain to Register: Check the box to use Domain to register with SIP proxy server. The gateway is registered to the SIP proxy server with IP address if un-ticked.

Note: Proxy Server Realm, **SIP Domain** and **Use Domain to Register** are the parameters provided by VoIP Service Provider. If you fail to make a call, please contact your VoIP Service Provider.

SETUP → VOIP SETTINGS

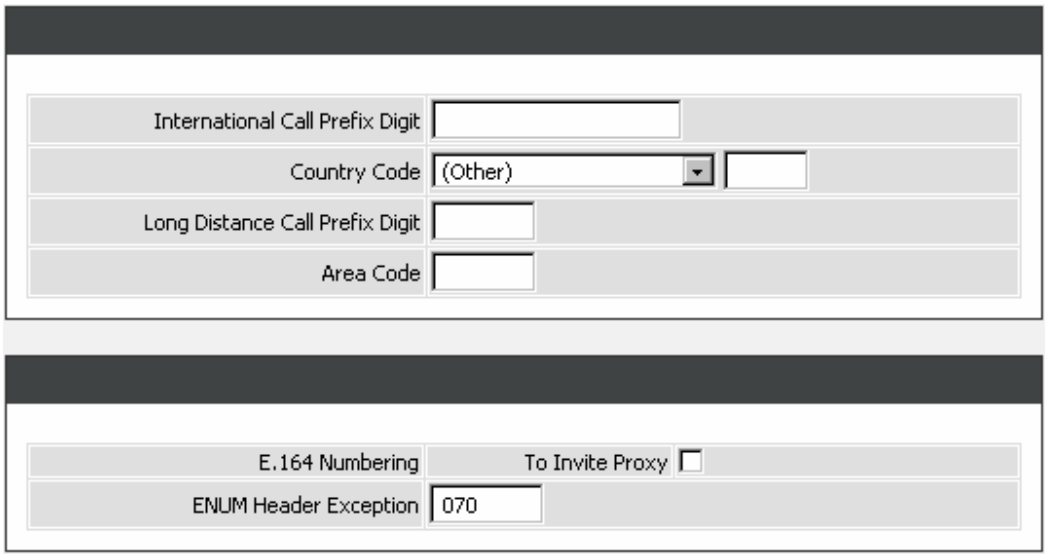


Outbound Proxy Support: Check the box to send all SIP packets to the destined outbound proxy server. An outbound proxy server handles SIP call signaling as a standard SIP proxy server would do. Further, it receives and transmits phone conversation traffic (media) between two communication parties. This option tells the gateway to send and receive all SIP packets to the destined outbound proxy server rather than the remote gateway. This helps VoIP calls to pass through any NAT protected network without additional settings or techniques. Please make sure your VoIP Service Provider supports outbound proxy services before you enable it.

Outbound Proxy IP/Domain: Enter the outbound proxy's IP address or URL.

Outbound Proxy Port: Enter the outbound proxy's listening port.

SETUP → VOIP SETTINGS



International Call Prefix Digit: Enter the International call prefix.

Country Code: Select the desired country code from the drop-down menu or enter the country code if **Other** is selected.

Long Distance Call Prefix Digit: Enter the long-distance prefix digit for making a long-distance call.

Area Code: Enter the area code.

E.164 Numbering: This variable is followed the E.164 rule, but it depends on the SIP proxy server.

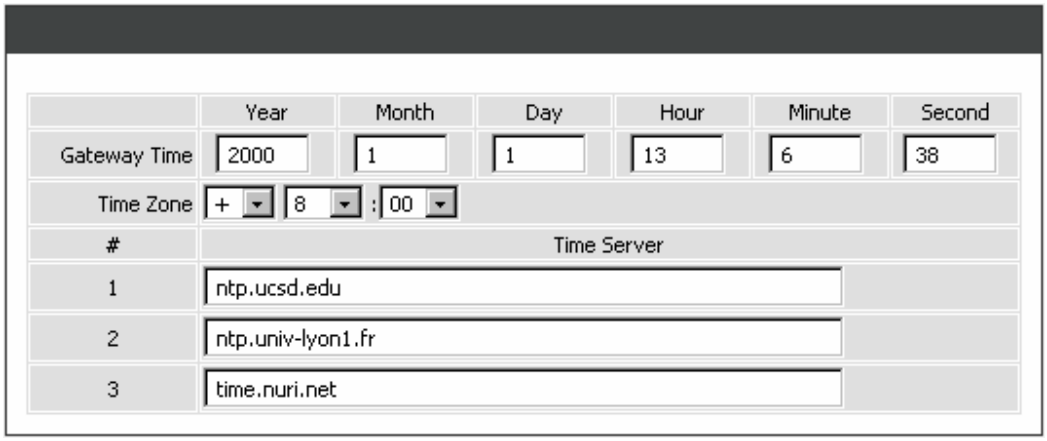
To Invite Proxy: Click the check box to send the number following the E.164 rule by the gateway.

ENUM Header Exception: Enter the prefix number that the gateway sends the number without followed the E.164 rule.

Note: E.164 Numbering depends on the proxy. If you fail to make a call, please contact your VoIP Service Providers.

2-1-5 Time and Date (NTP)

SETUP → TIME AND DATE



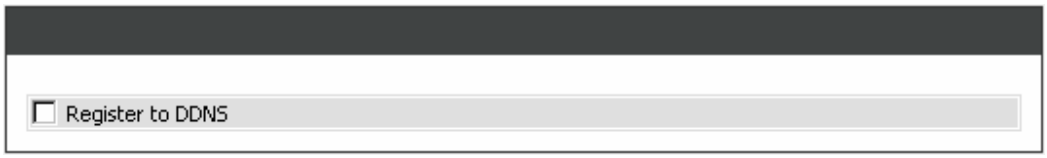
Gateway Time: It shows the current time of the gateway.

Time Zone: Select your time zone from the drop-down menu.

Time Server #1~#3: Enter the domain name or IP address of a NTP server. The gateway should sync up during start up.

2-2 ADVANCED

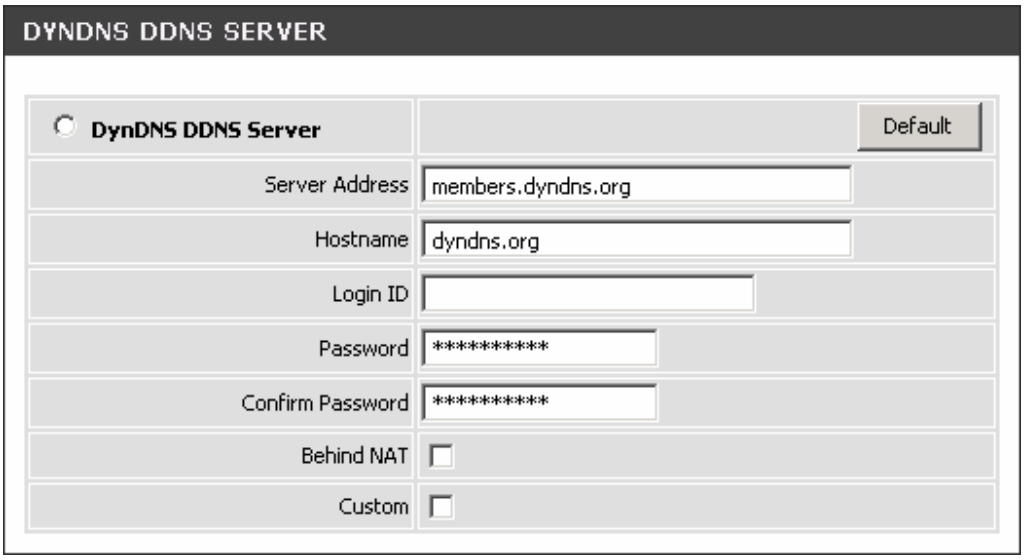
ADVANCED → DDNS

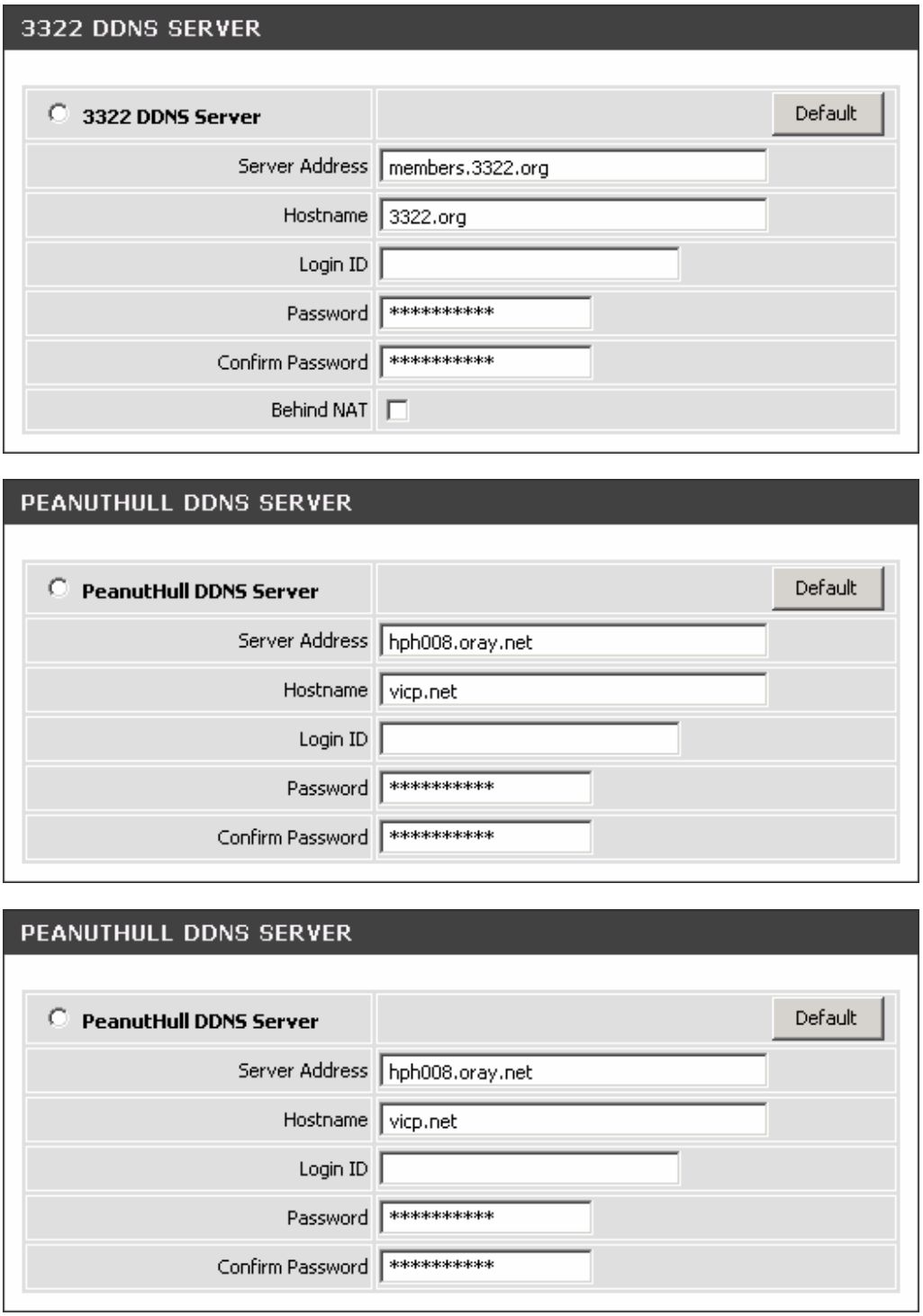


Register to DDNS: Check the box to enable DDNS function. It is only necessary when the gateway is set up behind an Internet sharing device that uses a dynamic IP address and does not support DDNS.

The gateway supports the DNS service of DynDNS、TZO、3322.org、PeanutHull or a private server. You will need to choose one of these DNS service and apply for an account with DynDNS 、TZO 、3322.org 、PeanutHull or a private server before you type in the following information.

ADVANCED → DDNS





Server address: Enter the IP address or URL (Uniform Resource Locator) of the DDNS Server.

Hostname: Enter the URL of the system (or NAT) – applied from domain name registration providers (e.g. www.dyndns.org).

Login ID and Password: Enter the Login ID and password used to log-in to the DDNS server.

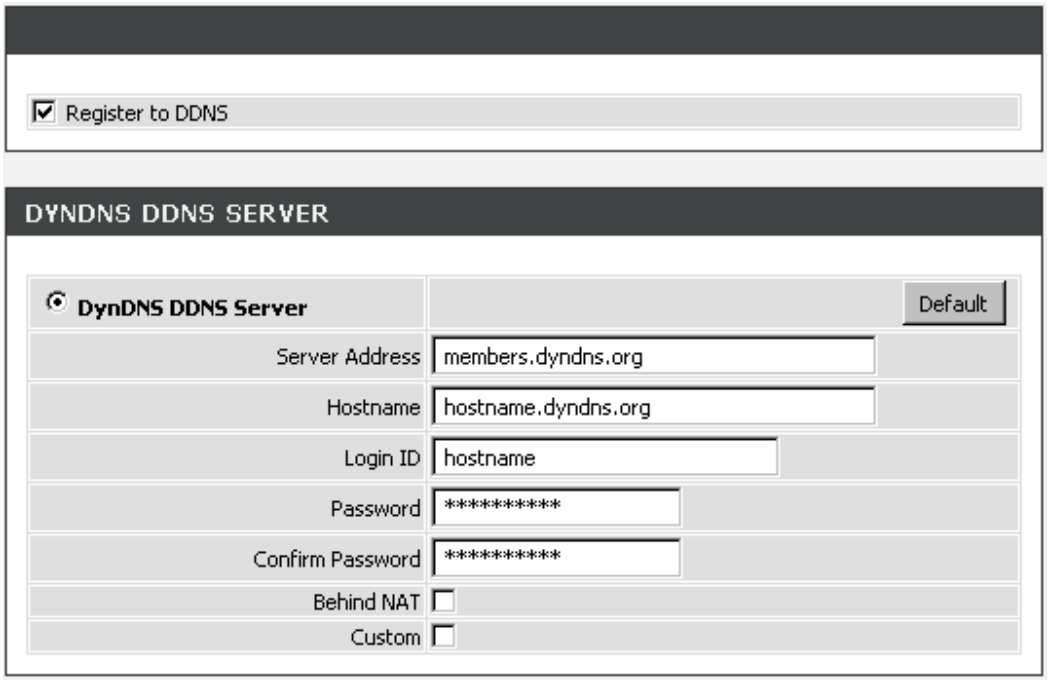
Behind NAT: Check the box if the gateway is set up behind a NAT device.

Custom: Only for DynDNS. Check the box if you have a custom hostname in DynDNS.

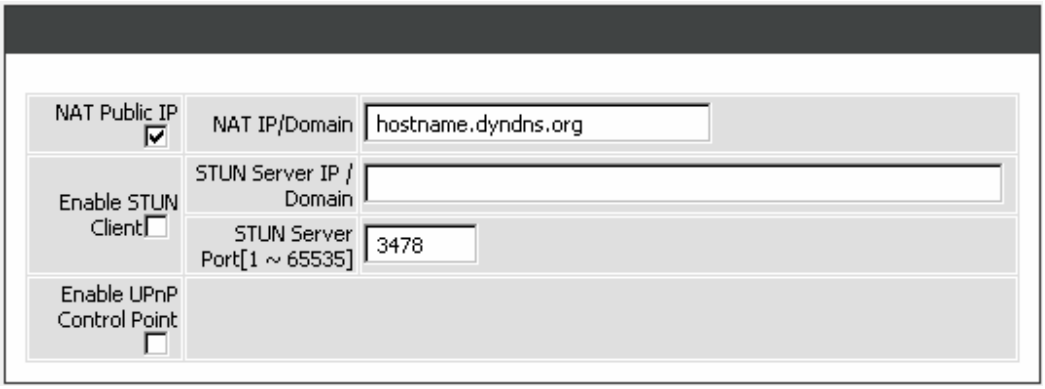
Note: If the gateway is set up under NAT, then enter the hostname in the NAT IP/Domain that is the same as the Hostname of the DDNS.

Example:

ADVANCED → DDNS



ADVANCED → NAT TRAVERSAL

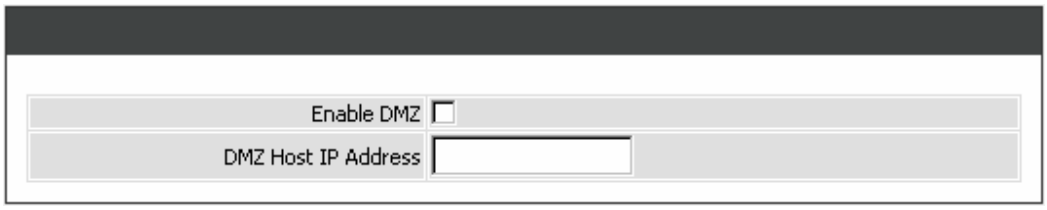


2-2-1 Firewall Settings

2-2-1-1 DMZ

DMZ (Demilitarized Zone) allows the server on the LAN site to be directly exposed to the Internet for accessing data and to forward all incoming ports to the DMZ Host. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

ADVANCED → Firewall Settings → DMZ



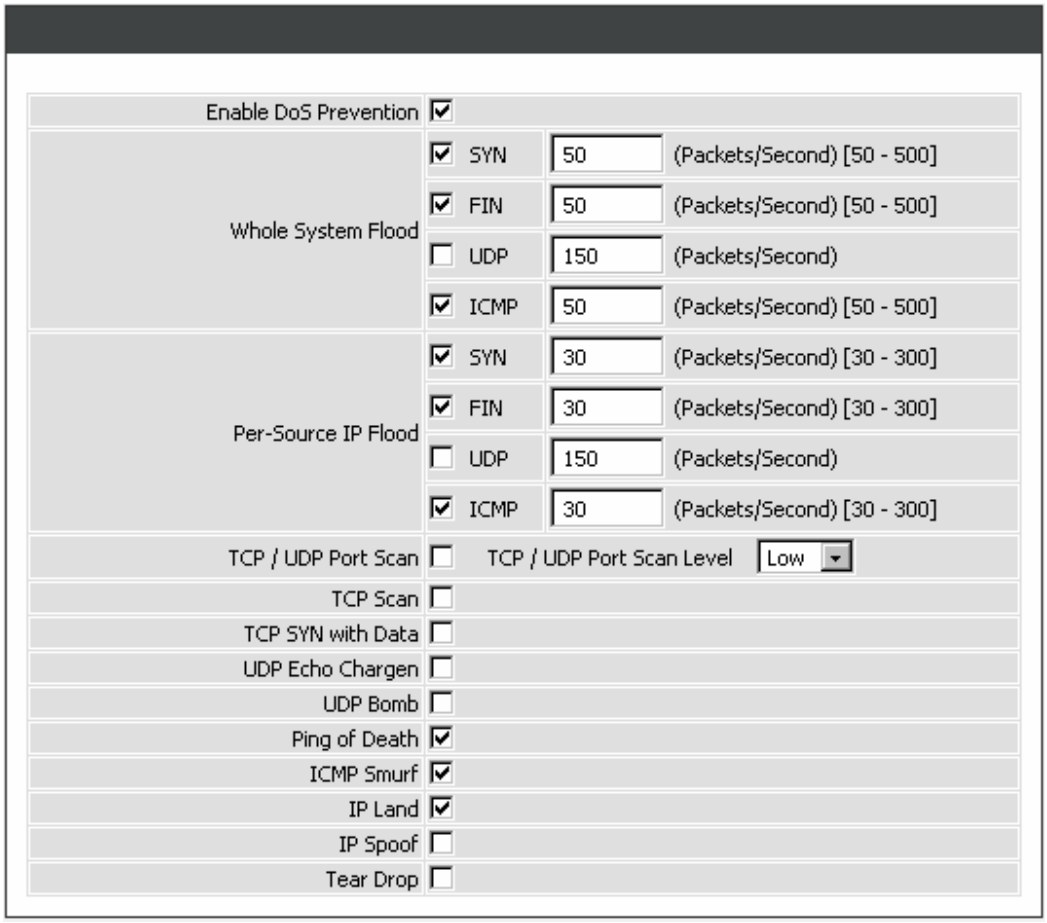
Enable DMZ: Check the box to enable DMZ feature.

DMZ Host IP Address: Enter the IP address of that computer as a DMZ Host with unrestricted Internet access.

Note: Either this function or virtual server can be selected for use in accessing external services.

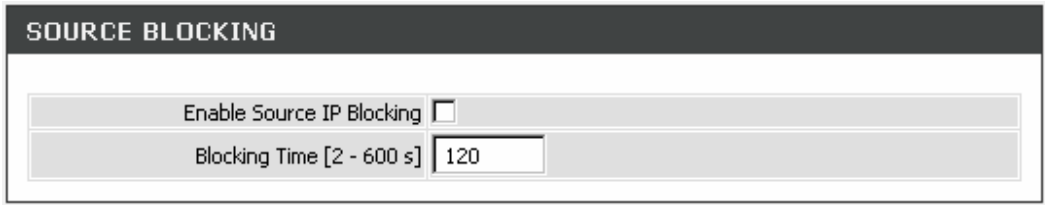
2-2-1-2 DoS Prevention Settings

ADVANCED → Firewall Settings → DOS PREVENTION SETTINGS



Enable DoS Prevention: Check the box to prevent DoS attacks from WAN or LAN. There are various types of DoS attacking. Leave settings in this field to the default if you are not familiar with it.

ADVANCED → Firewall Settings → DOS PREVENTION SETTINGS



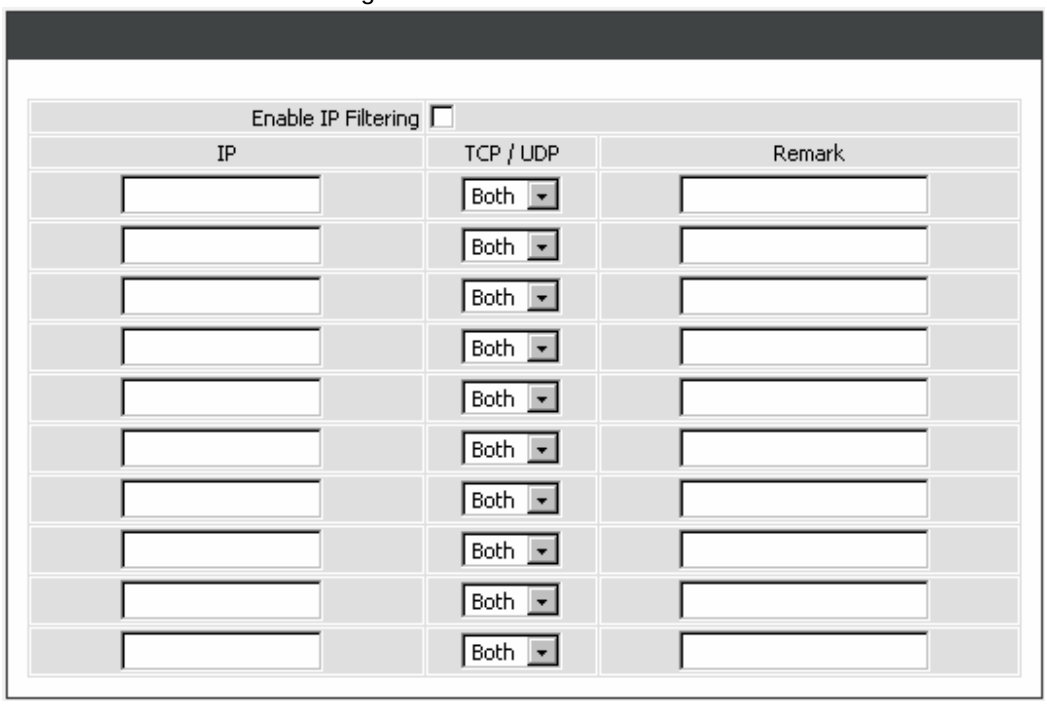
Enable Source IP Blocking: Check the box to block a particular IP address that detects the connection confirmed with the type of DoS attacking by the gateway.

Blocking Time: Enter the blocking time to block the particular IP.

2-2-1-3 IP Filtering

Use IP Filters to deny particular LAN IP addresses from accessing the Internet. You can deny specific port numbers or all ports for a specific IP address. The screen will display well-known ports that are defined. To use them, click on the edit icon. You will only need to input the LAN IP address(es) of the computer(s) that will be denied Internet access.

ADVANCED → Firewall Settings → IP FILTERING



Enable IP Filtering: Check the box to deny particular LAN IP addresses from accessing the Internet.

IP: Enter the IP address that you want to deny in this filed.

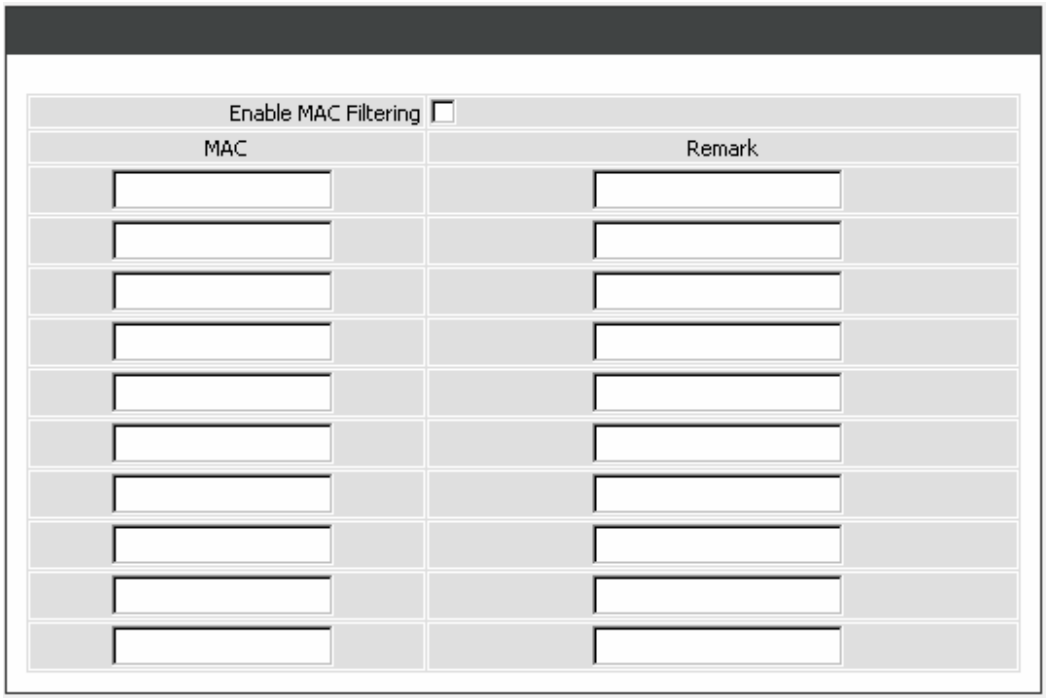
TCP/UDP: Select **TCP**, **UDP** or **Both** that will be used with the IP address that will be blocked.

Remark: Enter comments.

2-2-1-4 MAC Filtering

Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address that are connected to the gateway.

ADVANCED → Firewall Settings → MAC FILTERING



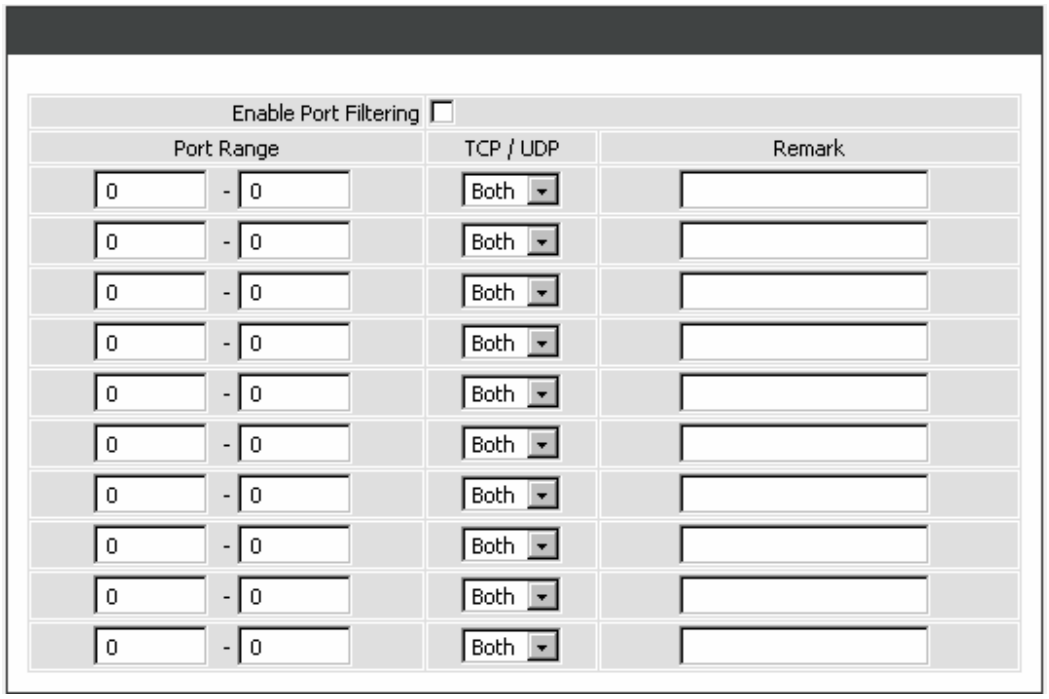
Enable MAC Filtering: Check the box to deny from accessing Internet.

MAC: Enter the MAC of the computer in the LAN (Local Area Network) to be used in the MAC filter table.

2-2-1-5 Port Filtering

Port filtering enables you to control all data that can be transmitted over routers. When the port used at the source end is within the defined scope, it will be filtered without transmission.

ADVANCED → Firewall Settings → PORT FILTERING



Enable Port Filtering: This variable is to restrict certain types of data packets by port.

Port Range: Enter the port range that will be denied access to the Internet.

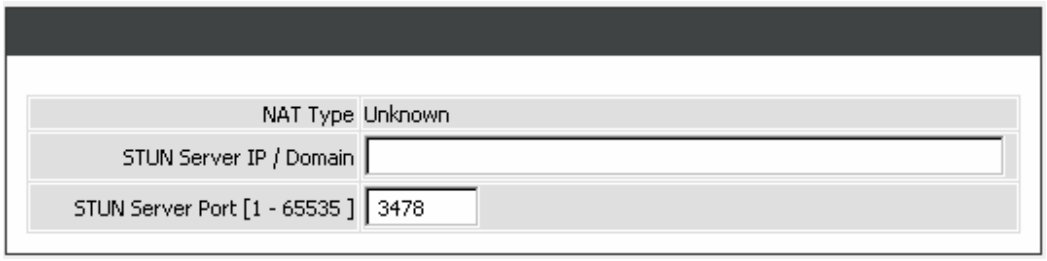
TCP/UDP: Select **TCP**, **UDP** or **Both** that will be used with the port that will be blocked.

Remark: Enter comments.

2-2-1-6 STUN Inquiry

Use "STUN Inquiry" to detect your IP sharing device's NAT type and communication between a STUN server and client.

ADVANCED → Firewall Settings → STUN INQUIRY



NAT Type: It shows the NAT type of your router.

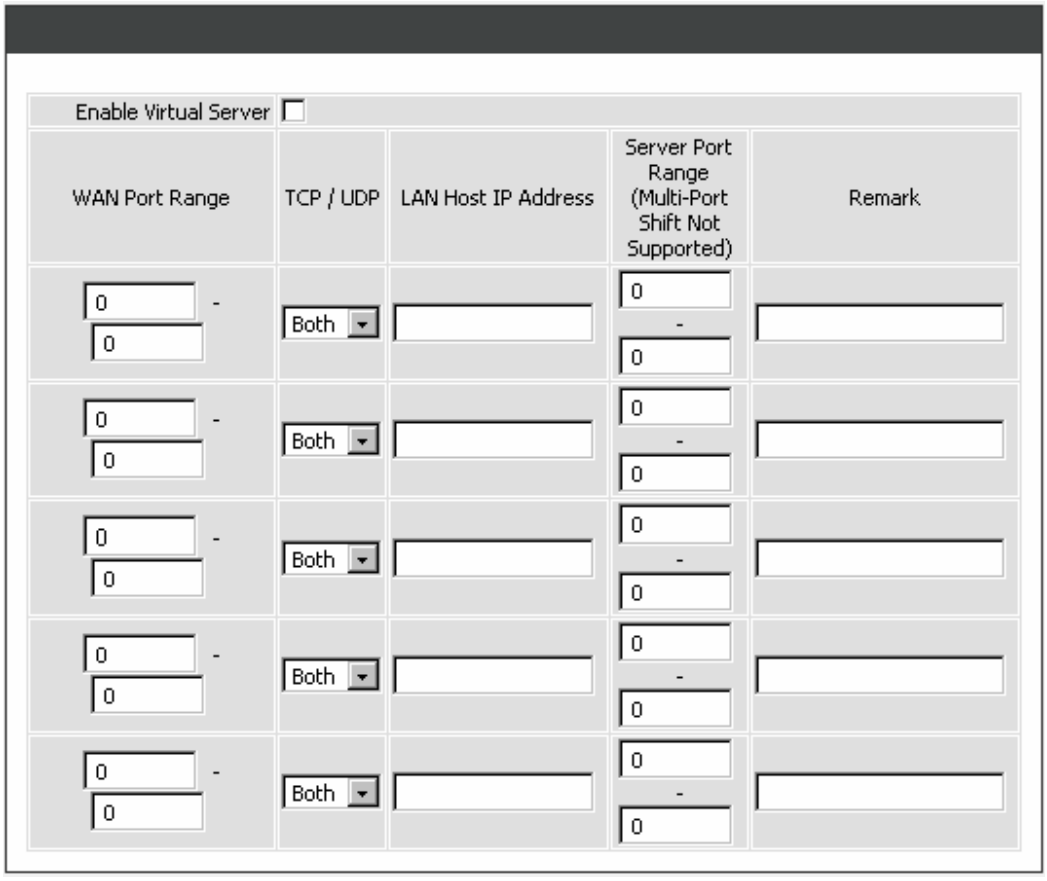
STUN Server IP/Domain: Enter the IP address or URL of the STUN server for query.

STUN Server Port: Enter the STUN Server's listening port.

2-2-1-7 Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

ADVANCED → Firewall Settings → VIRTUAL SERVER



Enable Virtual Server: Check the box to enable port forwarding.

WAN Port Range: Enter the port range for the WAN side.

TCP/UDP: Select the communication protocols used by the server, **TCP**, **UDP** or **Both**.

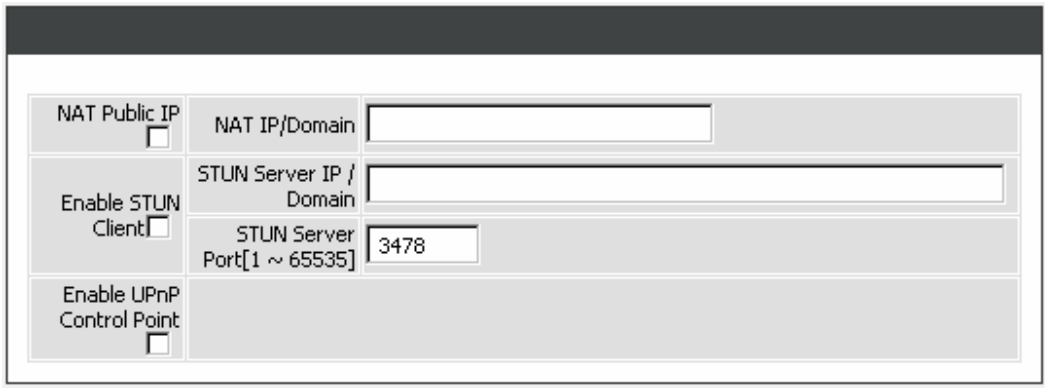
LAN Host IP Address: Enter the IP address of the device that provides various services.

Server Port Range: Enter the port range used by the LAN host.

2-2-2 NAT Traversal

If your gateway is set up behind an Internet sharing device, you can select either the NAT or STUN protocol.

ADVANCED → NAT TRAVERSAL



NAT Public IP: Check the box to use the IP address of the Internet sharing device if the gateway is set up behind an Internet sharing device. Also the gateway will use the IP address of the Internet sharing device as the public IP when it connects to Internet. Furthermore, some of the Internet sharing device's type is symmetric NAT. You need to set Virtual Server or Port Mapping (Forwarding) from the Internet sharing device for the listen port and communication ports (RTP ports) of the gateway.

NAT IP/Domain: Enter the real public IP address of the IP sharing device or the router; or enter a true URL (Uniform Resource Locator) when DDNS is used. Please refer to the DDNS settings.

Note: If you are setting a public IP in this field, it has to be a static public IP, otherwise VoIP communication may not be established properly. Please contact your ISP to check if your Internet connection has static public IP addresses.

Enable STUN Client: Check the box to use the STUN protocol prevents problems from setting the IP sharing function. (Some NATs do not support this protocol.)

Note: You can use the "Status → STUN Inquiry" page to detect the NAT type of your Internet sharing device. If the NAT type is "Symmetric NAT," then the gateway is not able to traverse the NAT. It is not a flaw of the gateway design, but rather a limitation of the STUN protocol.

STUN Server IP/Domain and Port: Enter the IP address and listen port of the STUN server. You can set two STUN server IPs separated by a semicolon.

Enable UPnP Control Point: Check the box to enable the gateway's IP traffic to pass through an Internet sharing device. This function only works when the Internet sharing device supports UPnP and has it enabled.

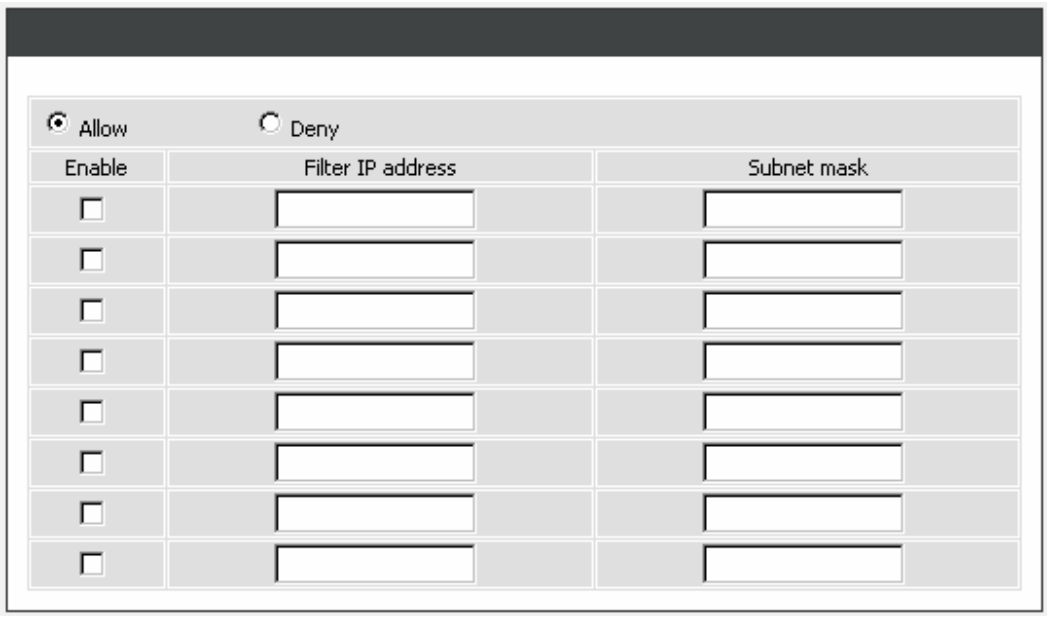
Note: The "Status → Current Status" page will show the status of UPnP.

2-2-3 VOIP

2-2-3-1 Caller Filter

This function allows you to accept or reject any incoming call from the IP address listed in the filter rule. The call from the IP address of SIP proxy server is always accepted, despite Deny is selected or the IP address of SIP proxy server is not in the filter rule of Allow.

ADVANCED → VoIP → CALLER FILTER



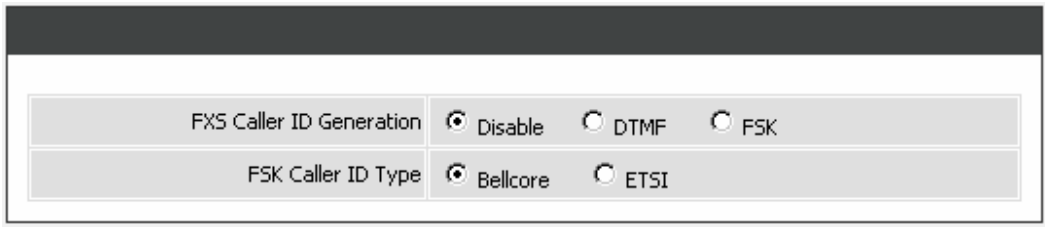
Enable: This variable is to activate the filter rule.

Filter IP Address: Enter the start IP address which you would like to Allow or Deny.

Subnet mask: Enter the subnet mask you would like to Allow or Deny.

2-2-3-2 Caller ID

ADVANCED → VoIP → CALLER ID

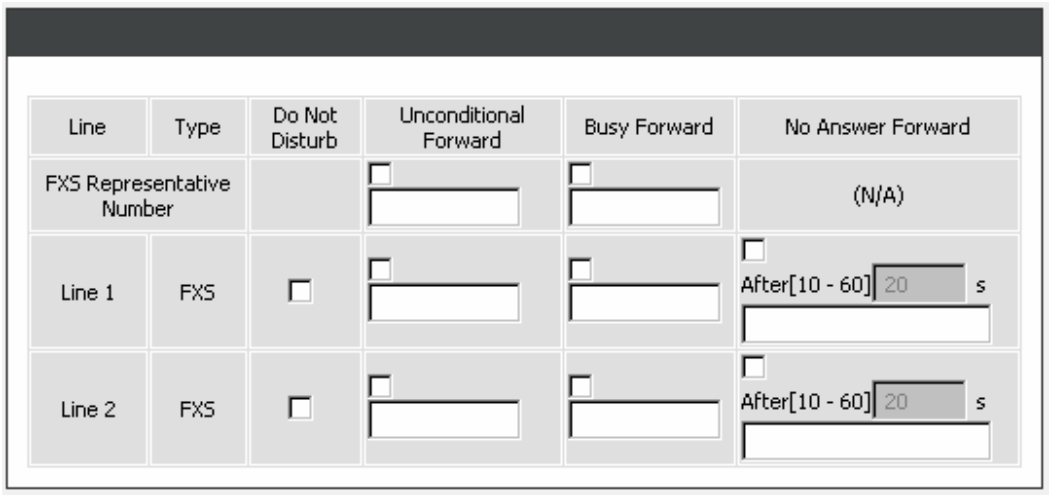


FXS Caller ID Generation: Select **DTMF** or **FSK** to enable the caller ID display function on FXS ports. When enabled, the caller's phone number will be displayed on your phone set when the call comes through.

FSK Caller ID Type: Either Bellcore or ETSI can be selected.

2-2-3-3 Calling Features

ADVANCED → VoIP → CALLING FEATURES



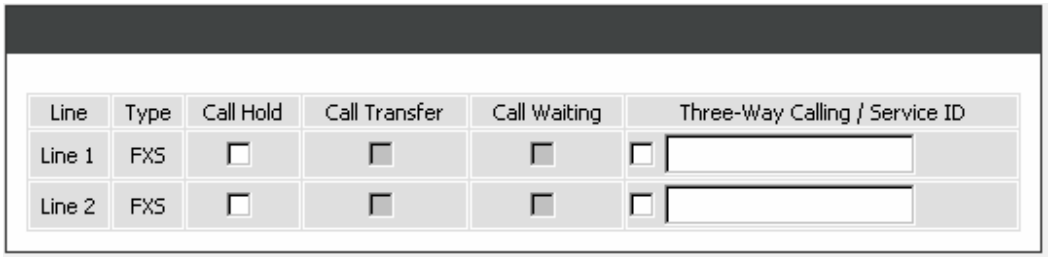
Do Not Disturb: Check the box to reject (busy tone played) incoming calls.

Unconditional Forward: Check the box to forward incoming calls to the assigned "Forwarding Number" automatically. If configured forwarding to FXO it only makes FXO hook off, but not making FXO dial out.

Busy Forward: Check the box to forward incoming calls to the "Forward incoming Number" when the line is busy.

No Answer Forward: Check the box to forward incoming calls to the "Forward incoming Number" after ringing timeout (configurable from 10 to 60 seconds) expires.

ADVANCED → VoIP → CALLING FEATURES



Line	Type	Call Hold	Call Transfer	Call Waiting	Three-Way Calling / Service ID
Line 1	FXS	☐	☐	☐	☐
Line 2	FXS	☐	☐	☐	☐

Call Hold: Check the box to hold the call on the specific FXS port.

Note: Call Transfer or Call Waiting can only be activated when Call Hold is checked..

Call Transfer: Check the box to transfer the call to another destination (FXS port only).

Call Waiting: Check the box to accept incoming call while talking (FXS port only).

Calling Feature Instructions:

Call Hold: The call will be held after the FLASH button is pressed on the phone set. The gateway will play a hold music (provided by your ITSP or VSP) to the remote end.

Call Transfer: The call will be held after FLASH button is pressed on local phone set (the gateway plays on-hold music to the remote end). Meanwhile, the local user can dial out another number after the dial tone is heard. After the handset is on-hooked, the call originally on hold will then be transferred to the new number regardless the status of the new call. If wrong number is dialed for the new call, press the FLASH button will switch back to the call on hold. Also, if the local user doesn't hang up the phone after the new call is set up, press the FLASH button will switch between the original call and the new call. Please note that the PBX between phone sets and the gateway must support FLASH features in order to use this function. If a phone set is connecting directly to the FXS port of the gateway and the FLASH button does not function, please adjust the settings in "Flash Detect Time" from "Advanced Options" section.

Note: The availability of the above features also depends on your VoIP network. Please also check with your service provider for these services.

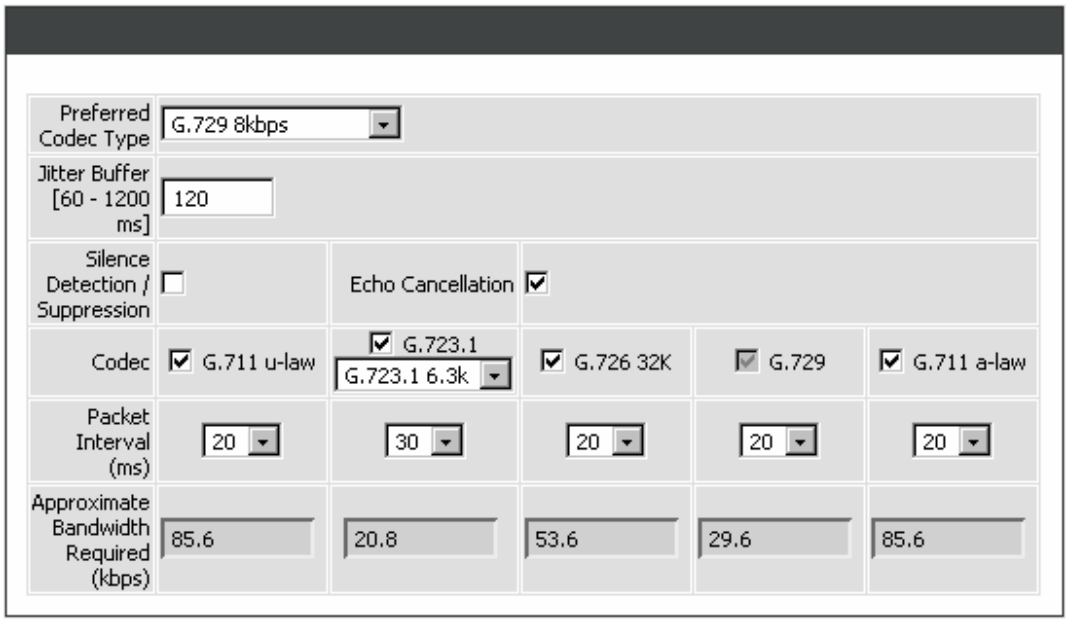
Examples of establishing a Three-Way call:

1. Phone1 dials to Phone2, Phone2 answers the call.
2. Phone1 presses Flash then calls Phone3 (Phone2 is on hold) and Phone3 answers the call.
3. Phone1 dials *61 and then presses Flash to start the conference call.
   Or
4. Phone1 dials to Phone2, Phone2 answers the call.
5. Phone3 dials to Phone1 (Call Waiting), Phone1 presses Flash to pick up the second call and talk to Phone3.
6. Phone1 dials *61 and then presses Flash to start the conference call.

Note: The availability of a Three-Way call also depends on your VoIP network. Please also check with your service provider for these services.

2-2-3-4 Codec Settings

ADVANCED → VoIP → CALLING FEATURES



Preferred Codec Type: Select a preferred codec type for all calls. Since different voice codecs have different compression ratios, the sound quality and occupied bandwidths are also different. The factual codec may determine by the called party. It is recommended that you use the default provided (G.723.1) codec because it occupies less bandwidth and provides better sound quality.

Jitter Buffer: Enter the jitter of receiving packets.

Silence Suppression: Check the box to enable the silence packets and send less voice data (package) during the silent period while talking.

Echo Canceling: Check the box to remove echo and improve voice quality during conversation.

Codec: Check the box to codec for the gateway to support. All codecs are selected and supported by default. You can un-check the box that is not used.

Packet Interval: Select the frame size of voice package from different codec. It defines the time interval for the gateway to send a RTP packet or voice packet to the receiving side. The smaller the value, the greater the bandwidth takes, and larger values might cause voice delay.

Approximate Bandwidth Required: It shows the bandwidth required from different codec and packet interval.

2-2-3-5 CPT/Cadence Settings

The CPT has 2 sets of parameter tables. Please adjust the CPT based on the local PSTN or PBX settings and requirements.

ADVANCED → VoIP → CPT / CADENCE SETTINGS

CPT # 1 Enable Setting 1 Default

Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2
Dial Tone	350	440	3000	0	0	0
Congestion Tone	480	620	250	250	0	0
Busy Tone	480	620	500	500	0	0
Ring-Back Tone	440	480	1000	2000	0	0

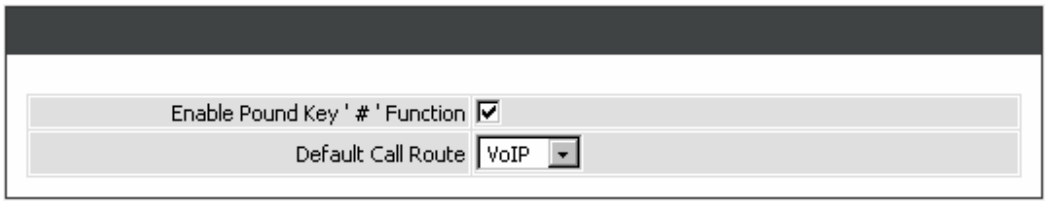
CPT # 2 Enable Setting 2

Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2
Dial Tone	400	0	300	100	3500	100
Congestion Tone	400	0	250	250	0	0
Busy Tone	400	0	500	500	0	0
Ring-Back Tone	400	0	500	100	500	2000

2-2-3-6 Digit Map

Digit Map combines the original feature of Digit Map and Speed Dial. You can use "?" or "%" in the column of Scan Code, VoIP Dial-out and PSTN Dial-out. "?" represents a single digit, and "%" represents a wildcard. The function of the signs is to mapping the numbers between the number received from user and the replaced or modified number for actual dial out. With this function, user can easily add certain leading digits to replace a full set of numbers. There are 50 sets of leading digit entries to choose voice routing interface.

ADVANCED → VoIP → DIGIT MAP



Enable Pound Key ' # ' Function: Check the box to treat ' # ' as a digit and send out with other numbers when dialing. If you un-check the box and ' # ' is pressed after dialing, it will speed up the phone number detection of the gateway.

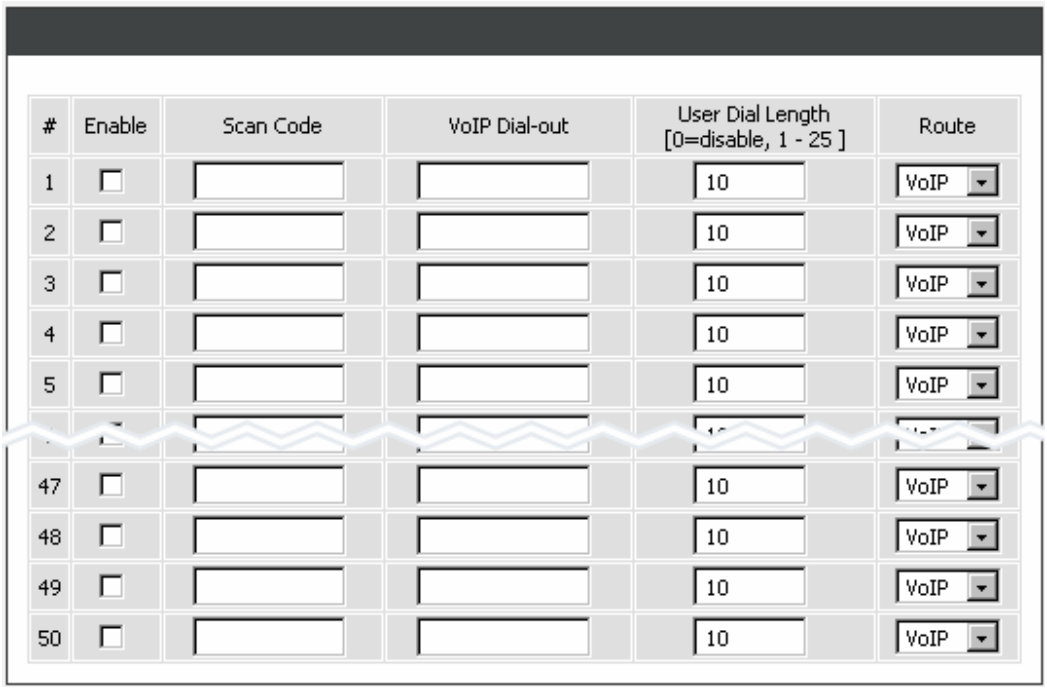
Default Call Route: Select **VoIP** or **Deny** as the default call route for the calls.

ADVANCED → VoIP → DIGIT MAP

Test Dial No.: You need to set a rule in the Digit Map Rule section first before entering the numbers for test and display.

Result: It will show the numbers for VoIP Dial-out according to the Digit Map Rule as below.

ADVANCED → VoIP → DIGIT MAP



#	Enable	Scan Code	VoIP Dial-out	User Dial Length [0=disable, 1 - 25]	Route
1	☐			10	VoIP
2	☐			10	VoIP
3	☐			10	VoIP
4	☐			10	VoIP
5	☐			10	VoIP
47	☐			10	VoIP
48	☐			10	VoIP
49	☐			10	VoIP
50	☐			10	VoIP

Enable: Check the box to enable the detection of Digit Map Rule entry.

Scan Code: Enter the digits for the gateway to scan while user is dialing.

VoIP Dial-out: Enter the actual dialing number rule for the gateway to call through the Internet.

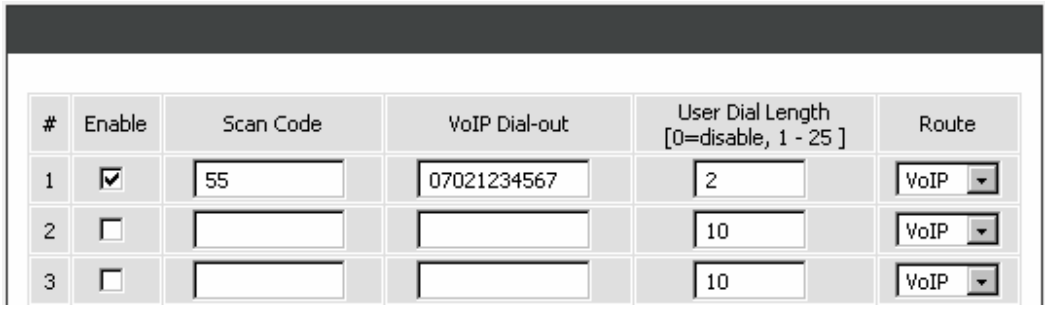
User Dial Length: Enter the total number of digits that user dialed.

Route: Select **VoIP** or **Deny** for this entry.

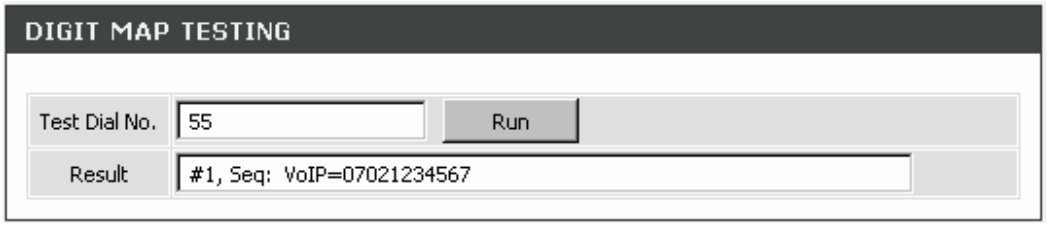
Methods of Digit Map:

Method 1- Single mapping: Fill a short code into the Scan Code column, and enter the desired phone number into the VoIP Dial-out column.

For example,
Scan Code: 55
VoIP Dial-out: 07021234567
User Dial Length: 2
Route: VoIP

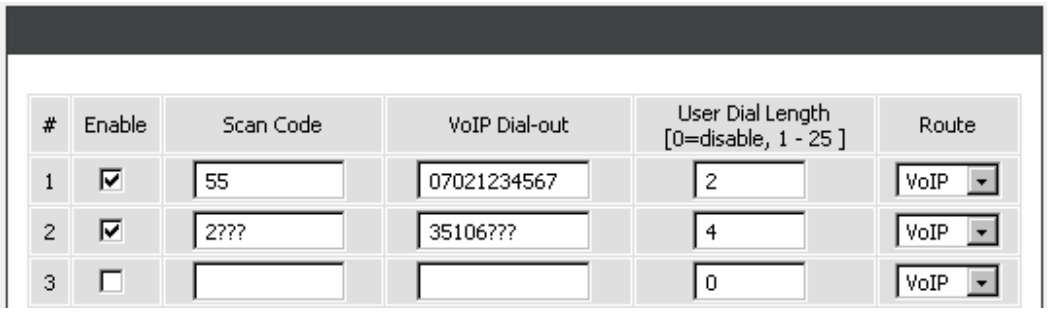


Pick up the handset and dial 55, the gateway will dial 07021234567. You also can use Digit Map Testing to see the result of what gateway will dial.



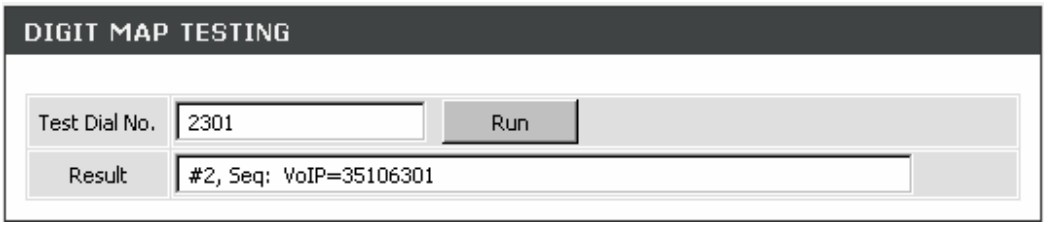
Method 2- Multi mapping: Fill the prefix code into the Scan Code column and the format to transfer into the VoIP Dial-out column.

For example,
Scan Code: 2???
VoIP Dial-out: 35106???
User Dial Length: 4
Route: VoIP



#	Enable	Scan Code	VoIP Dial-out	User Dial Length [0=disable, 1 - 25]	Route
1	☑	55	07021234567	2	VoIP
2	☑	2???	35106???	4	VoIP
3	☐			0	VoIP

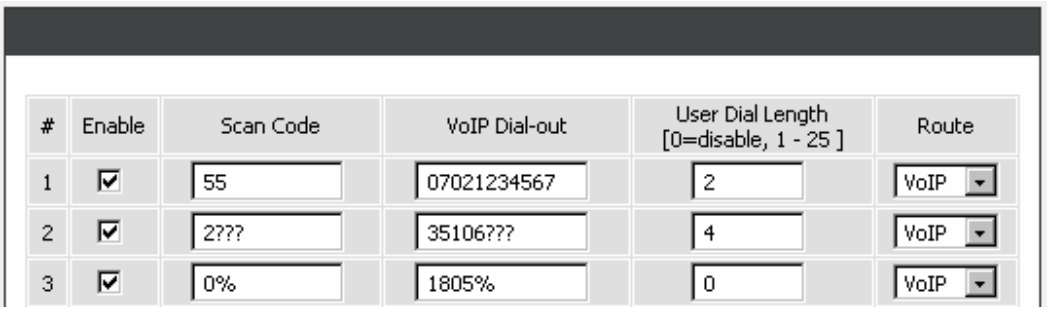
Pick up the handset and dial 2301. The gateway will dial 351006301 and go through PSTN/FXO. You also can use Digit Map Testing to see the result of what gateway will dial.



DIGIT MAP TESTING

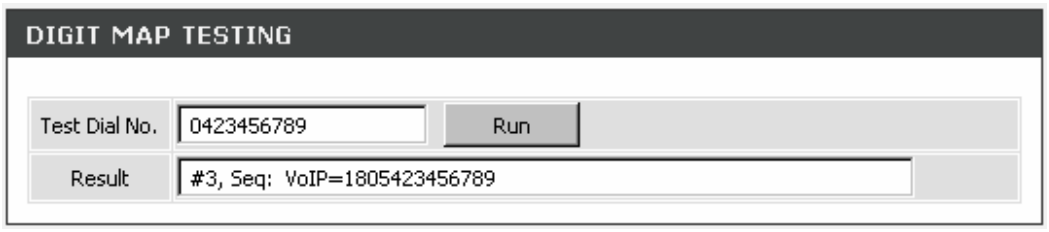
Test Dial No.	2301	Run
Result	#2, Seq: VoIP=35106301	

For example,
Scan Code: 0%
VoIP Dial-out: 1805%
User Dial Length: 0
Route: VoIP



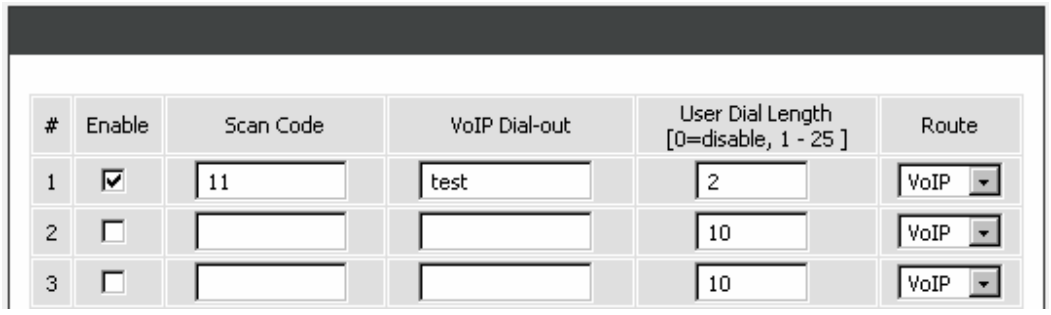
#	Enable	Scan Code	VoIP Dial-out	User Dial Length [0=disable, 1 - 25]	Route
1	☑	55	07021234567	2	VoIP
2	☑	2???	35106???	4	VoIP
3	☑	0%	1805%	0	VoIP

Pick up the handset and dial 0423456789. The gateway will dial 0423456789 and go through Internet first. If the call is fail to Internet, the gateway will dial 1805423456789 and go through PSTN/FXO. You also can use Digit Map Testing to see the result of what gateway will dial.



Method 3- Substitution: It helps you dial to destination that you can not dial by phone. Destination like: test@1.1.1.1. Fill in the number into the **Scan Code** column and enter the desired name into the **VoIP Dial-out** column.

For example,
Scan Code: 11
VoIP Dial-out: test
User Dial Length: 2
Route: VoIP



Pick up the handset and dial 11. The gateway will dial "test" and go through Internet. You also can use Digit Map Testing to see the result of what gateway will dial.

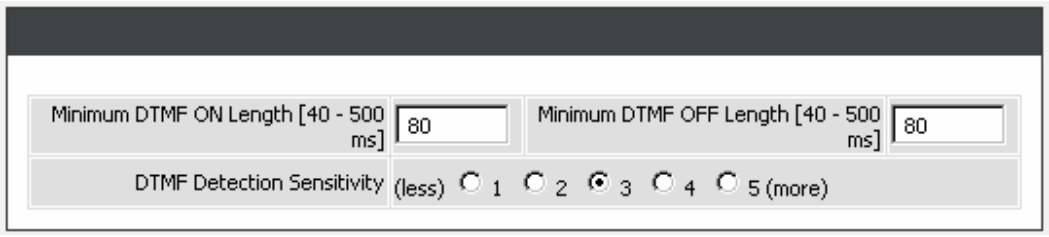
2-2-3-7 DTMF & PULSE

ADVANCED → VoIP → DTMF & PULSE

Dial Wait Timeout: Enter the timeout duration after the user picks up the phone set.

Inter Digits Timeout: Enter the timeout duration between the intervals of each key pressed. When exceeding the set timeout duration without entering further digits, the numbers entered will be dialed out.

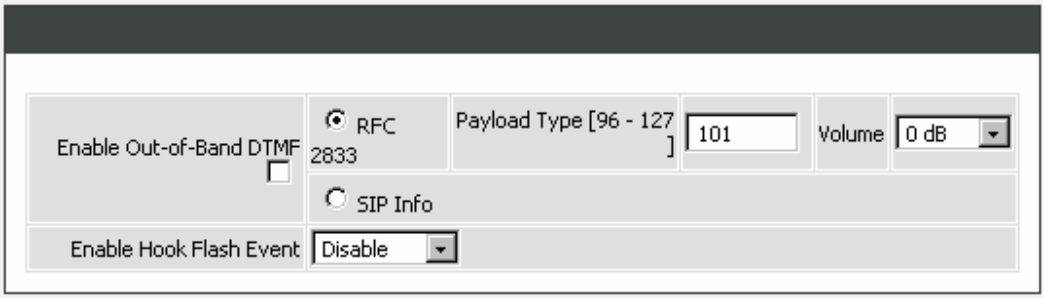
ADVANCED → VoIP → DTMF & PULSE



Minimum DTMF ON Length (Dial on)/ Minimum DTMF OFF Length (Dial off - between tones): This variable is to set the length of DTMF playback.

DTMF Detection Sensitivity: This variable is to set the sensitivity of the telephone keys for the gateway to detect the DTMF.

ADVANCED → VoIP → DTMF & PULSE



Enable Out-of-Band DTMF: This variable is to set the method of DTMF transmission. RFC2833 or SIP Info.

Note: Out-of-Band DTMF transport method varies from VoIP networks, please contact your VoIP provider for the preferred method.

Payload Type: payload type of RFC2833.

Volume: Select the volume of RFC 2833 from the drop-down menu.

Enable Hook Flash Event: Select **Auto**, **RFC2833**, or **SIP info** for the signaling method of Hook Flash Event.

2-2-3-8 Fax Settings

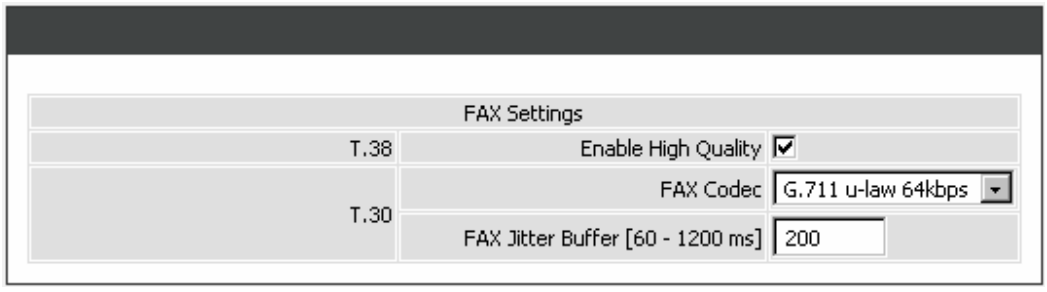
ADVANCED → VoIP → FAX SETTINGS

Fax / Modem: Select the appropriate type for fax detection by the gateway.

Disable - Select it if you are not sending fax, but it is still accepted fax by the gateway.
T.38 Fax - Select it if you are using T.38 as the protocol for fax transmission. T.38 is used for reliable and efficient facsimile transmission over network. It transmits and receives FAX waveform (relaying) over the codec negotiated during call setup this bandwidth consumed is lowered. T.38 protocol also supports redundancy to get better FAX quality.
T.30 Fax - Select it if you are using T.30 as the protocol for fax transmission. It transmit FAX signal as voice thus uncompressed G.711 would be the choice. (G.726 also works but not recommended). Due to this nature, T.30 always requires a SDP change (change of codec within a session, SIP Re-Invite required) after FAX tone detected by the callee. It will consume more network resources and will affect transmission quality. The gateway is still able to change the protocol from T.38 to T.30 if the called party uses T.38 for fax transmission.
T.30 Fax/Modem - Select it if you use it as the protocol for transmission of fax/modem over IP network.
T.30 Only - Select it if you are using G.711 a-law or G.711 u-law for fax transmission. The gateway won't accept T.38 for fax transmission.
T.38 Native - Select it if you are only using T.38 for fax transmission.

Note: When a fax tone is detected from the call, the gateway will automatically switch from voice mode to fax mode. Hence, the fax settings will be temporarily applied to a specific port which detects the fax tones, instead of its default voice settings.

ADVANCED → VoIP → FAX SETTINGS



Enable High Quality: Check the box to increase approximately two times the bandwidth in order to compensate possible loss of packet during transmission and offers a better and reliable fax quality.

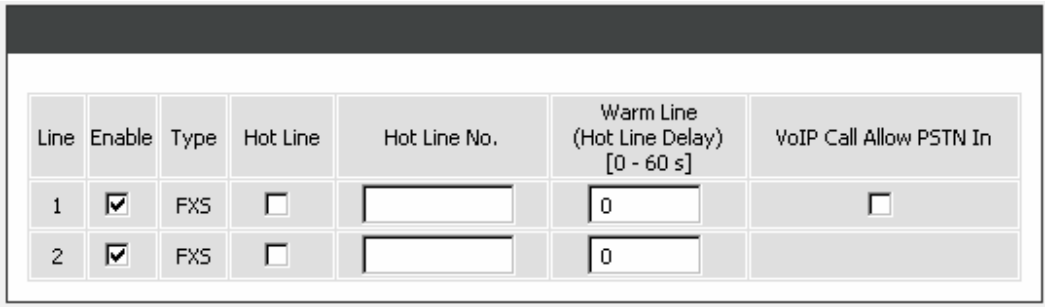
FAX Codec: Select **G.711 a-law**, **G.711 u-law**, or **G.726** for T.30 from the drop-down menu.

FAX Jitter Buffer: Enter the buffer or jitter when receiving packets.

Note: When you send a fax over an IP network, the IP network needs to support fax over IP functionality (either T.38 or T.30). Please consult your VoIP service provider for this setting.

2-2-3-9 Hot Line

ADVANCED → VoIP → HOT LINE



Enable: Check the box to enable the Hot Line function for a dedicated line; if the line is not being used, disable them (Pause Function) will avoid unnecessary waiting when an incoming call diverts to this line.

Hot Line: Check to direct the call automatically to a pre-configured destination without any action when the FXS is off-hook. (ie. as the user picks up the phone). When the FXS is under Hot Line mode, no other phone numbers can be dialed.

Hot Line No.: Enter the number for pre-defined destination.

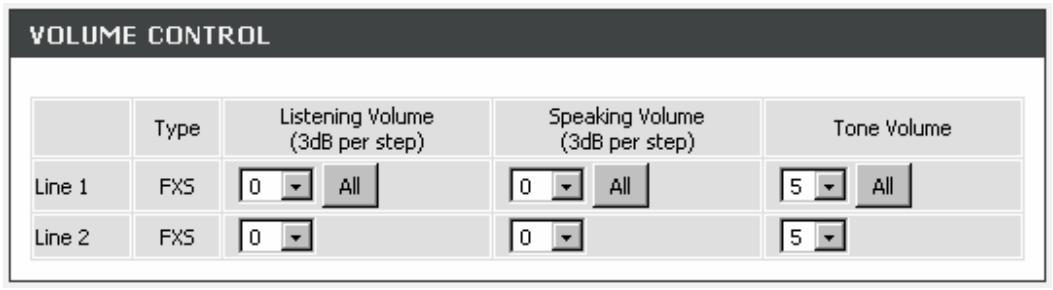
Warm Line: Enter the time for the call to start with a pause, so the user can dial another number. The call will be automatically directed to the pre-configured destination within timeout period.

VoIP Call Allow PSTN In: Check the box to allow an incoming waiting call from PSTN while VoIP call is in use. To enable this feature, following settings need to be done first:

1. Tick **VoIP Call Allow PSTN In** to allow a waiting call from PSTN.
2. Tick **Call Hold** to hold the VoIP call when pressing the FLASH button on the phone set. (Calling Feature → Call Hold).

2-2-3-10 Line Settings

ADVANCED → VoIP → LINE SETTINGS

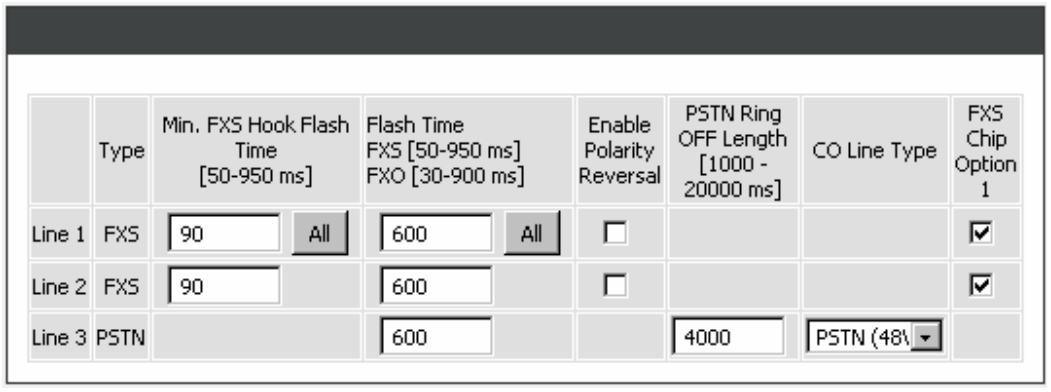


Listening Volume: Use the drop-down menu to adjust the hearing (listening) volume.

Speaking Volume: Use the drop-down menu to adjust the speaking volume.

Tone Volume: Use the drop-down menu to adjust the tone volume. It will apply to all tones generated by the gateway including Dial Tone, Ring Back Tone and Busy Tone.

ADVANCED → VoIP → LINE SETTINGS



Min. FXS Hook Flash Time: Enter the minimum flash time for FXS detecting. When the flash signal generated by the phone set is shorter than Min. FXS Hook Flash Time, FXS port will be on-hook.

Flash Time:

FXS - Enter the maximum flash time for FXS detecting. When the flash signal generated by the phone set is longer than the Flash Time, FXS port will be on-hook.

PSTN - Enter the time for PSTN to detect if the voltage keeps the on-hook status.

Enable Polarity Reversal:

FXS - Check the box to activate the generation of polarity reversal from FXS.

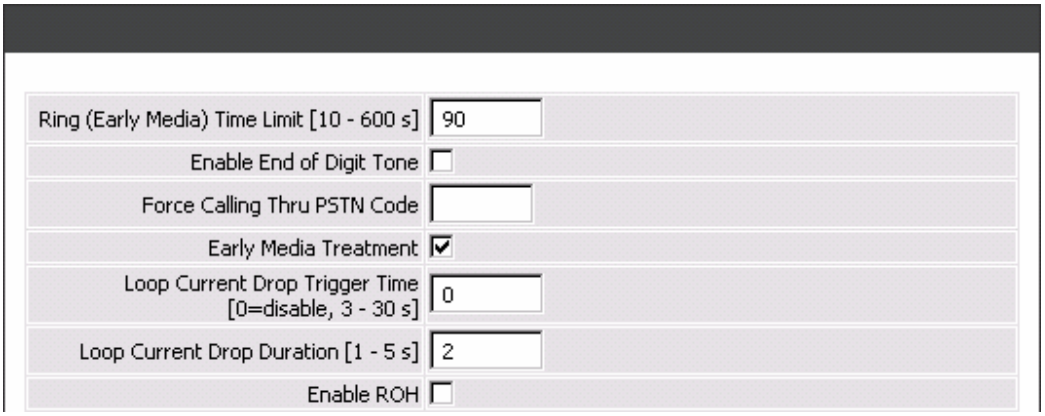
FXO - Check the box to activate the detection of polarity reversal from FXO. Some telephone switches or PBX require this feature to reverse the line polarity to inform the remote end to drop an ongoing call. Please consult with the telephone service provider for availability of this feature.

PSTN Ring OFF Length: Enter the ring length detected if the remote party is on-hook from PSTN by PSTN port. If the ring length form PSTN is longer than this setting, the PSTN/FXO will be on-hook, and it will stop the ringing from FXS.

CO Line Type: Select **PSTN (48V)** or **PABX (24V)** for the CO line type connected to PSTN port.

FXS Chip Option 1: Check the box to avoid mis-detecting the loop state of a subscriber line or PBX user loop from FXS interface. In some cases, the off-hook voltage might cause the FXS interface mis-detect the idle and the active state, in order to avoid this situation, un-check this feature.

ADVANCED → VoIP → LINE SETTINGS



Ring (Early Media) Time Limit[10 - 600secs]: Enter the timeout to cancel a call if no one answers the phone.

Enable End of Digit Tone: Check the box to activate the function of playing a "Beep-Beep" tone to notify the user that the call is in progress.

Force Calling Thru PSTN code: Enter the code to get a PSTN line before dialing out. For example: If you specify code "33" in this option and would like dial "23456789" via a PSTN line: Dial "33" and you will hear dial tone from the PSTN line, now you're able to dial "23456789" via PSTN line.

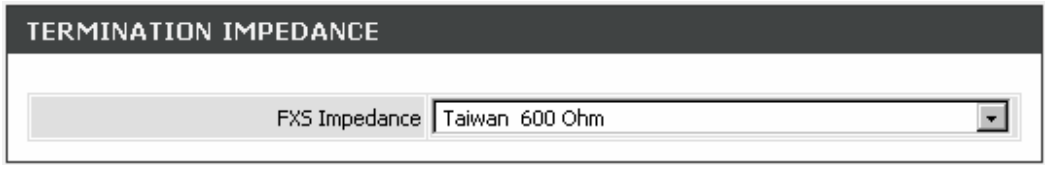
Early Media Treatment: Check the box to send the one-way RTP immediately when a connection with a VoIP service provider has been set up.

Loop Current Drop Trigger Time: Enter the time to avoid the line being engaged when FXS port is connected to PBX. It stops the loop current from FXS port when FXS port is playing busy tone. The setting "0" zero is to disable this function.

Loop Current Drop Duration: Enter the drop duration for loop current.

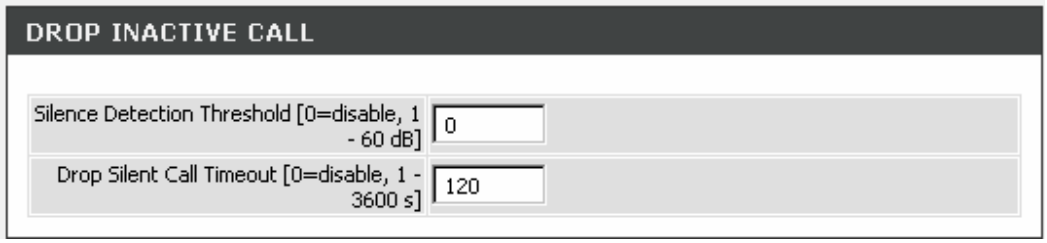
Enable ROH: Check the box to play Receiver Off-Hook tone in order to notify user to hang up the phone set if FXS is off-hook for more than 20 seconds.

ADVANCED → VoIP → LINE SETTINGS



FXS Impedance: Select different impedance from the drop-down menu.

ADVANCED → VoIP → LINE SETTINGS



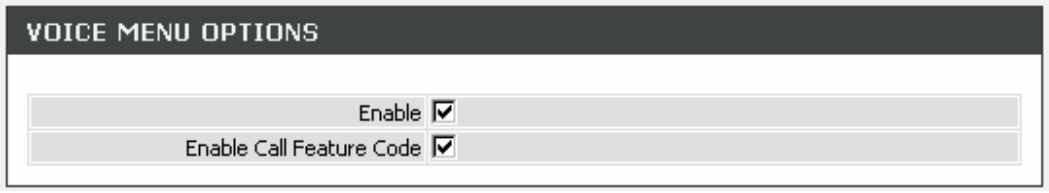
This feature is a call drop standard for a gateway to determine whether or not to hang up the phone. The gateway will disconnect the call automatically to avoid keeping the line engaged if the detected volume is below the **Silence Detection Threshold** or the time exceeds the **Drop Silent Call Timeout**.

Silence Detection Threshold: Enter the threshold (dB) to detect if there is voice coming from RJ-11 interface.

Drop Silent Call Timeout: Enter the duration (second) for detecting if there are RTP packets receiving from RJ-45 interface.

Note: Improper values for above settings might cause unexpected automatic disconnection of a call. Default values are recommended.

ADVANCED → VoIP → LINE SETTINGS



Voice Menu Options: Check the box to enable IVR function.

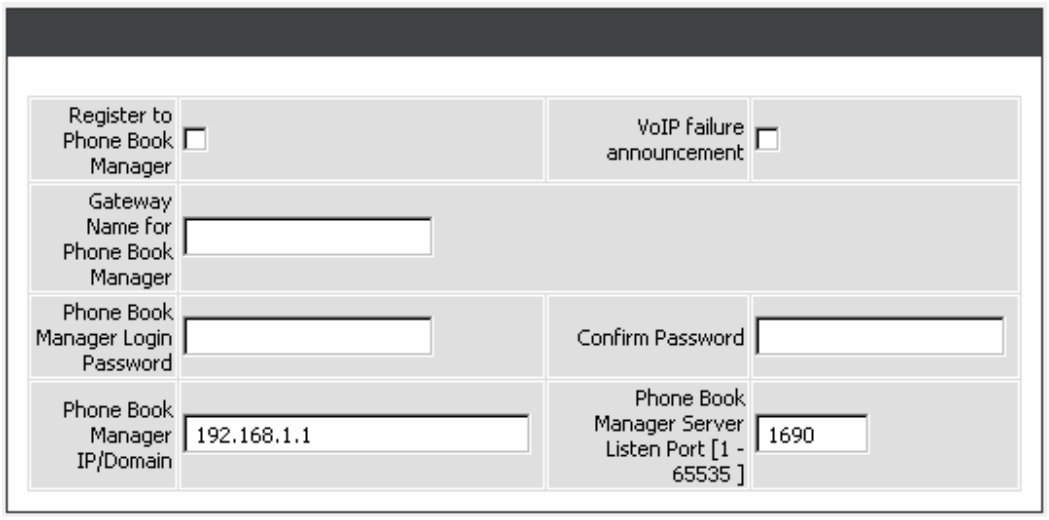
Enable Call Feature Code: Check the box to enable the advanced function for Call Features, such as Call Pickup, Automatic Redial and Unattended transfer..

2-2-3-11 Phone Book

Some peer information needs to be added to this section before the gateway makes peer-to-peer calls.

Phone Book Manager: You can register the gateway to a Phone Book Manager server to make peer-to-peer communication without entering the phone number and the IP address of the remote peer.
Phone Book: It is used for peer-to-peer communication. Some peer information needs to be added to this section prior to making peer-to-peer calls. You need to enter the phone number and the IP address of the remote peer.

ADVANCED → VoIP → PHONE BOOK



Register to Phone Book Manager: Check the box to register to a Phone Book Manager Server.

VoIP failure announcement: Check the box to activate the gateway to play a voice announcement if the gateway fails to register to the Phone Book Manager while FXS is off-hook.

Gateway Name for Phone Book Manager: Enter the alias registered with the Phone Book Manager.

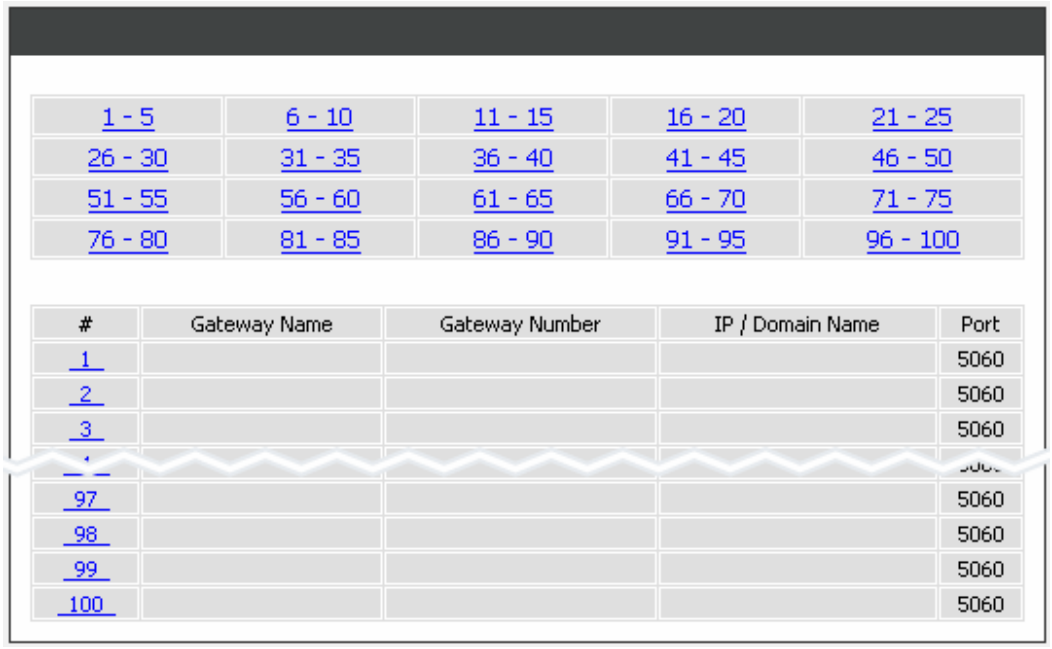
Phone Book Manager Login Password: Enter the registered password that is the same as Phone Book Manger.

Phone Book Manager IP / Domain: Enter the IP address of the Phone Book Manager. It supports URL (Uniform Resource Locator).

Phone Book Manager Listen Port: Enter the listen port of the Phone Book Manager Server for transmitting signals between the Phone Book Manager Server and client.

Note: Make sure that Phone Book Manager Login Password and Phone Book Manager Listen Port are the same as those set in Phone Book Manager.

ADVANCED → VoIP → PHONE BOOK



The gateway can be configured and stored 100 phone numbers to a phone book and can provide an IP address query when calling to other VoIP devices. If no Phone Book manager is dedicated within a gateway group, then each gateway system have to set up phone data to allow gateways to communicate with others.

Gateway Name: Enter the alias of the remote peer.

Gateway Number: Enter the phone number of the remote peer.

IP / Domain Name: Enter the IP address or URL (Uniform Resource Locator) of the remote peer.

Port: Enter the listen port of the remote peer.

2-2-3-12 SIP Advanced

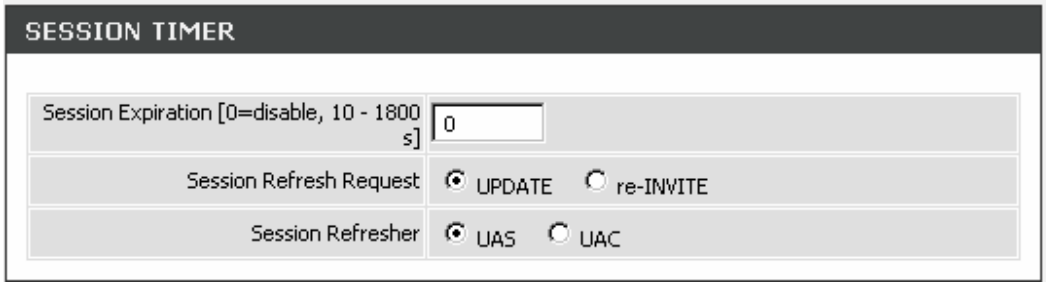
ADVANCED → VoIP → SIP ADVANCED

Listen Port UDP: Enter the gateway's listening port in this field. Leave it as default settings, unless it conflicts with ports used by other device in your network.

RTP Starting Port UDP: Enter the starting port number or transmitting voice data among VoIP devices. Each line requires 2 ports.

For example, if the starting port is 9000, then Line 1 will take up ports 9000 and 9001, and Line 2 will take up ports 9002 and 9003, and so forth.

ADVANCED → VoIP → SIP ADVANCED

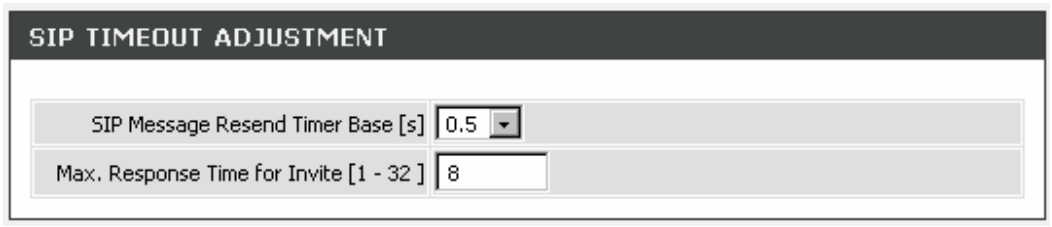


Session Expiration: This field will set the time that the gateway will allow a SIP session to remain die (without traffic) before dropping it.

Session Refresh Request: Select **UPDATE** or **re-INVITE** to send refresh requests to the Server.

Session Refresher: This determines which side of an expired call session will initiate the session refresh. uac – specifies that the Caller side will initiate the session refresh. uas – specifies that the Call receiver (the "Callee") will initiate the session refresh.

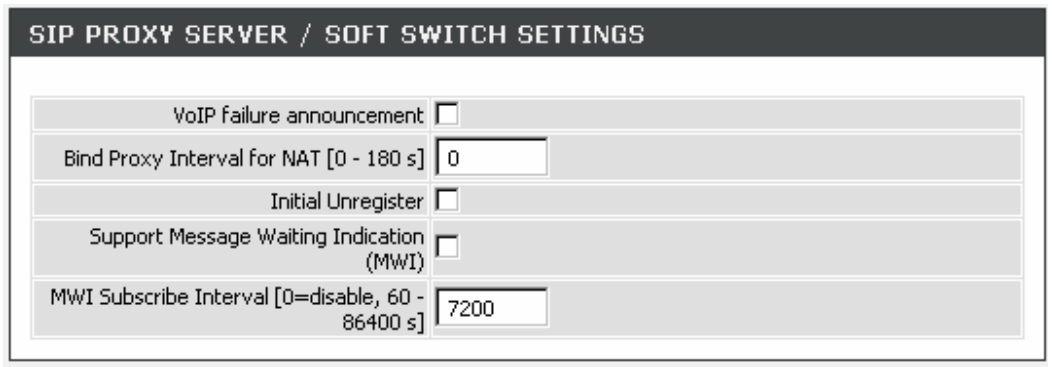
ADVANCED → VoIP → SIP ADVANCED



SIP Message Resend Timer Base: Select the resend timer base from the drop-down menu if response is not received within the base time. The sequence of sending is like "base time" * 2, and send again at "base time" *2 *2. The maximum resend time is four seconds. Resend action will stop when the total resend time has reached 20 seconds.

Max. Response Time for Invite: Enter the maximum response time for INVITE packet. When the destination does not reply within the set time, the call is failed.

ADVANCED → VoIP → SIP ADVANCED



VoIP failure announcement: Check the box to play a voice announcement if the gateway fails to register to the SIP proxy server while FXS is off-hook.

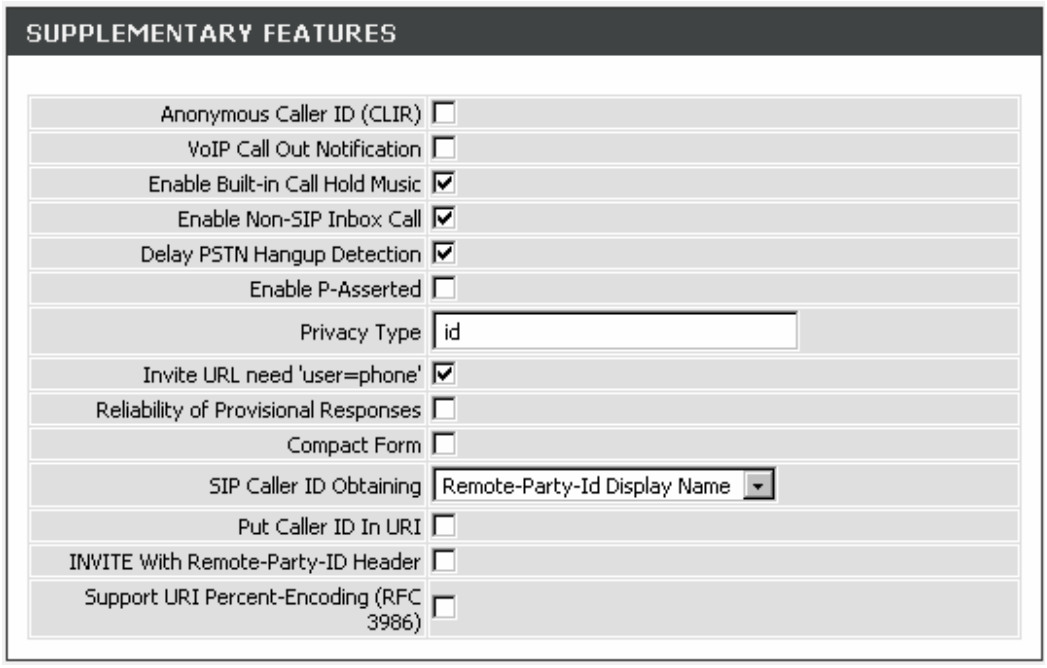
Bind Proxy Interval for NAT: Check the box to keep the binding exist by sending packets when the gateway is behind a NAT and SIP proxy server is not able to keep the binding.

Initial Unregister: Check the box to send an unregistered message initially by the gateway and then it will perform a general register process.

Support Message Waiting Indication: Check to box to enable Message Waiting Indication. It is available only when Voice Mail Service is available from the SIP proxy server.

MWI Subscribe Interval: Enter the subscribe time for gateway to check the voice mail.

ADVANCED → VoIP → SIP ADVANCED



Anonymous Caller ID (CLIR): Check the box to lock the delivery of the Caller ID to the called party.

VoIP Call Out Notification: Check the box to enable the function of playing a tone to notify user that the call is through VoIP.

Enable Built-in Call Hold Music: Check the box to enable the function of playing music when receiving Call Hold request.

Enable Non-SIP Inbox Call: Check the box to make local calls. Local Call here means the call does not go through the Internet and if the dialed number is the extension of other line. You can un-check it to configure as all calls go through the Internet.

Delay PSTN Hangup Detection: Check the box to delay the detection of dully PSTN line on-hook status from PSTN port. You can un-check it to change the sensitivity of detection from PSTN port to detect the PSTN line on-hook status.

Enable P-Assert: Check the box to enable the caller ID protection.

Privacy Type: It is used to disguise the caller ID when queried via an ITSP/Third-Party Assertion. The Privacy Type includes 'user', 'header', 'session', 'none', 'critical', 'id' and 'history'.

Invite URL need 'user=phone': Check the box to add 'user=phone' as a hint that the part left to the '@' sign is actually a phone number.

Reliability of Provisional Responses: Check the box to send a PRACK request during the progress of the request processing. Reliability of Provisional Responses is to ACK at every SIP packet. With this method, SIP packet will act like TCP, ie. every packet sent will receive an ACK to make sure that packet sent has been received by other peer.

Compact Form: Check the box to represent common header field names in an abbreviated form. This may be useful when SIP message is too large to be carried on and recognized by the user agent.

SIP CallerId Obtaining: Select the part of the SIP packet from the gateway to obtain Caller ID. There are several places where the Caller ID is located.

Remote-Party-Id Display Name - It is located at SIP → Remote-Party-ID → Before [<sip:]
Remote-Party-Id User Name - It is located at SIP → Remote-Party-ID → After [<sip:], Before [@]
From-Header Display Name - The standard is in SIP → Message Header → From → SIP Display info.

Put Caller ID In URI: This feature is to put Caller ID in URL. The Caller ID is located in SIP → Message Header → After [From:], Before [<sip:] by default settings. It will be located in SIP → Message Header → After [<sip:], Before [@]if ticked.

INVITE With Remote-Party-ID Header: Check the box to comprise the information of Remote-Party-ID in the message header of INVITE. Different format of INVITE header might cause the call not to be connected. Please consult with your VoIP Service Provider before enabling it.

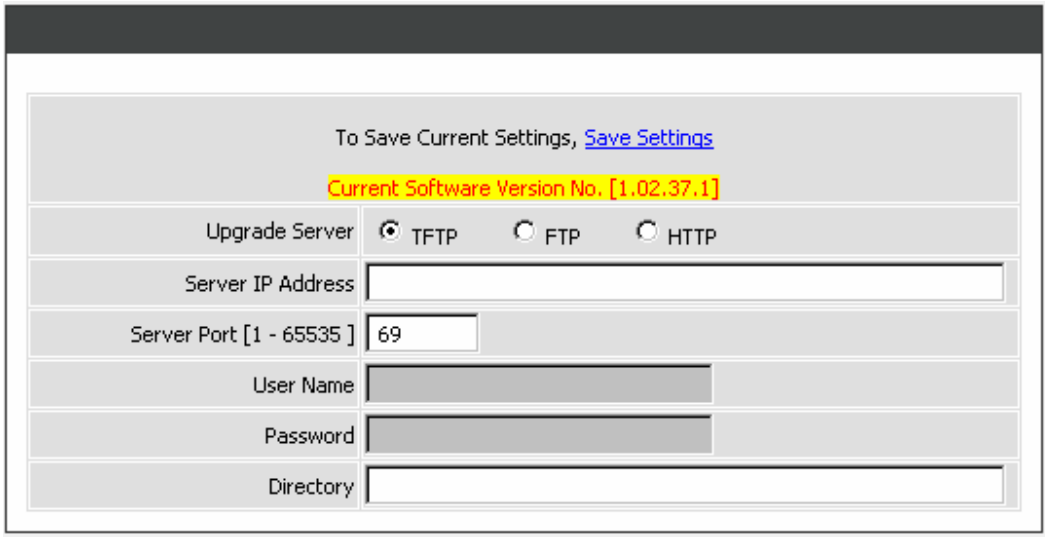
Support URI Percent-Encoding(RFC 3986): Check the box to encode/decode the letters of the basic Latin alphabet, digits, and a few special characters which follow RFC 3986.

2-3 MAINTENANCE

2-3-1 Firmware Upgrade

The gateway supports a software upgrade function from a remote server. Please consult your VoIP Service Provider for information about the following details.

MAINTENANCE → FIRMWARE UPGRADE



Upgrade Server: Select the upgrade type: **TFTP**, **FTP**, or **HTTP**.

Software Upgrade Server IP: Enter the server's IP address.

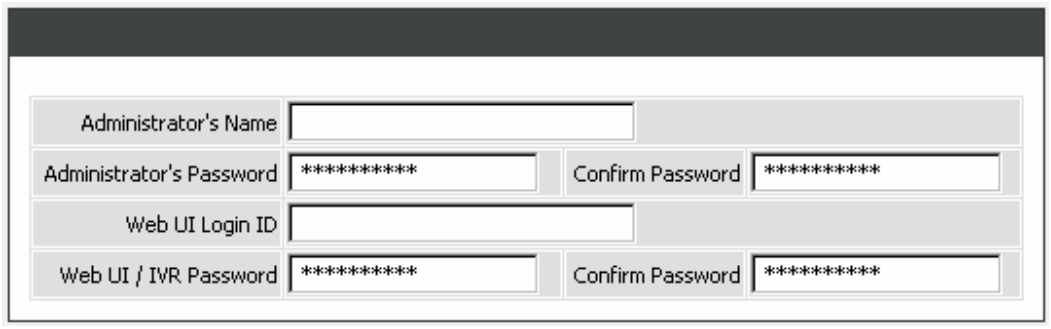
Software Upgrade Server Port: Enter the server's port.

User Name/ Password: Enter the account information for accessing the server if needed.

Directory: Enter the location of the firmware file.

2-3-2 Login Account

MAINTENANCE → LOGIN ACCOUNT

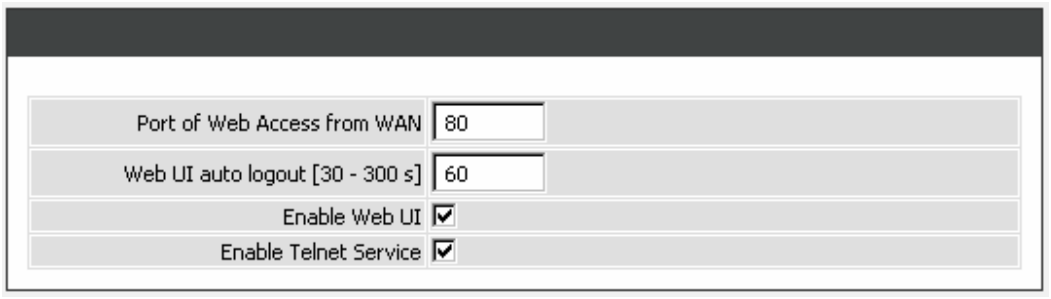


Note: There are two operating levels when entering the Web UI. Logging-in as the Administrator allows you to change all settings. A Web UI user only has access to some settings.

Administrator's Name and Password: Enter the administrator name and password, "Administrator" has the highest level of control of the gateway.

Web UI Login ID and Web UI/IVR Password: Enter log-in ID and password when you log-in to the Web interface/IVR of the gateway as a normal user.

MAINTENANCE → LOGIN ACCOUNT



Port of Web Access from WAN: Enter the port number when accessing the web-based configuration utility from the WAN port.

Web UI auto logout: Enter the effective time range when logging into the web interface, the user will be disconnected from the web page to allow others to log-in.

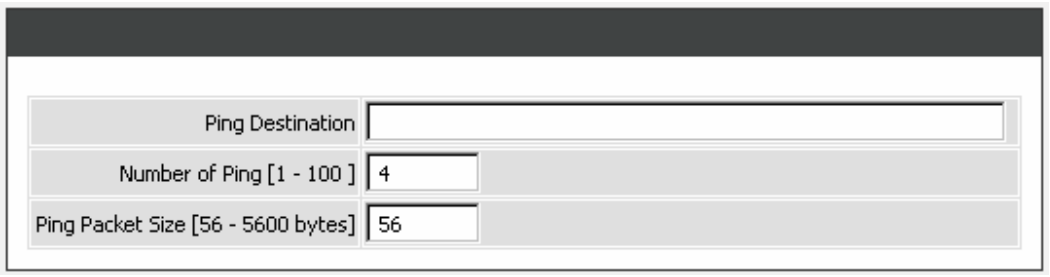
Enable Web UI: Check the box to enable WEB access from WAN or LAN.

Enable Telnet Service: Check the box to enable Telnet access from WAN or LAN.

2-3-3 Ping Test

Use "Ping" to verify if a remote peer is reachable. Enter a remote IP address and click "Test" to ping the remote host.

MAINTENANCE → PING TEST



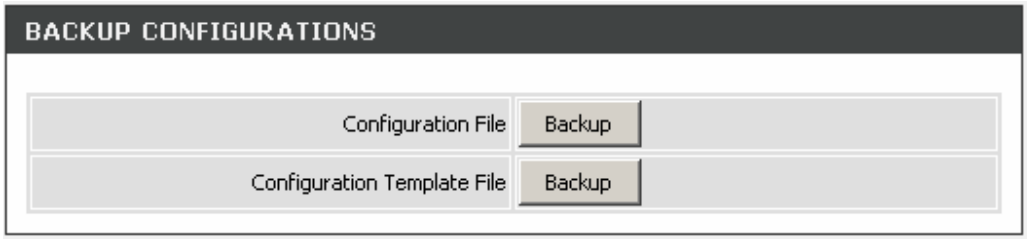
2-3-4 System

2-3-4-1 Backup/Restore

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by the DVG-G5402SP can be uploaded into the unit. To restore a system settings file, click on **Browse** to search the local hard drive for the file to be used.

Note: the gateway needs you to Save Settings and Restart so that all settings will be restored.

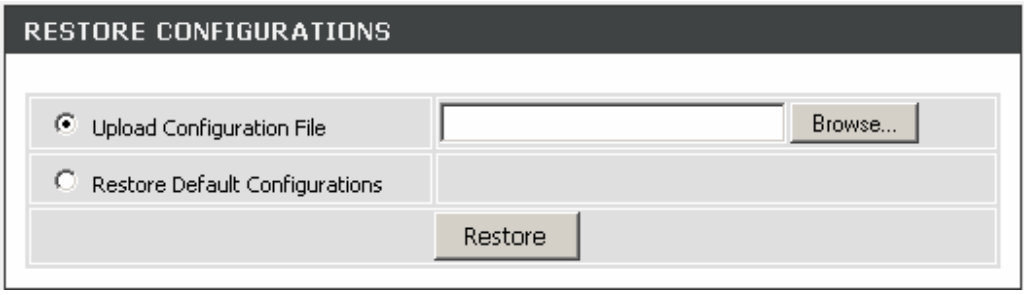
MAINTENANCE → System → BACKUP / RESTORE



Configuration File: Click the **Backup** button to your current settings to a file.

Configuration Template File: Click the **Backup** button to your current settings to a template file for editing.

MAINTENANCE → System → BACKUP / RESTORE

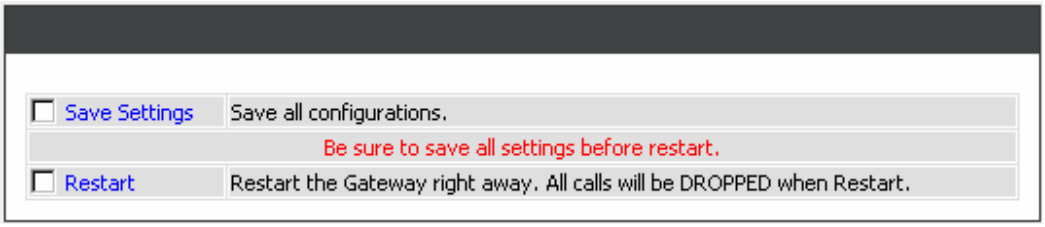


Upload Configuration File: Once you locate the file, click **Upload** to overwrite the current settings with the settings saved to the file.

Restore Default Configurations: Select **Restore Default Configurations** and click the **Restore** button to reset the DVG-G5402SP back to the factory default settings.

2-3-4-2 Save / Restart

MAINTENANCE → System → SAVE / RESTART

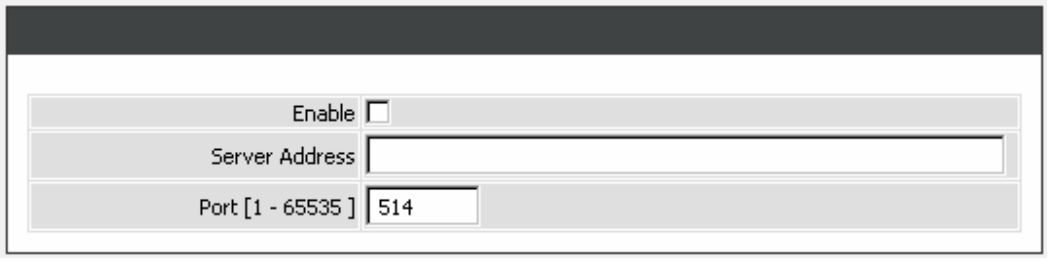


Save Settings: Check the box to save your current settings.

Restart: Check the box and click the **Accept** button to reboot your DVG-G5402SP.

2-3-5 System Log

MAINTENANCE → SYSTEM LOG



Enable: Check the box to send event notification messages across IP networks to the Server.

Server Address: Enter the System Log Server's IP address.

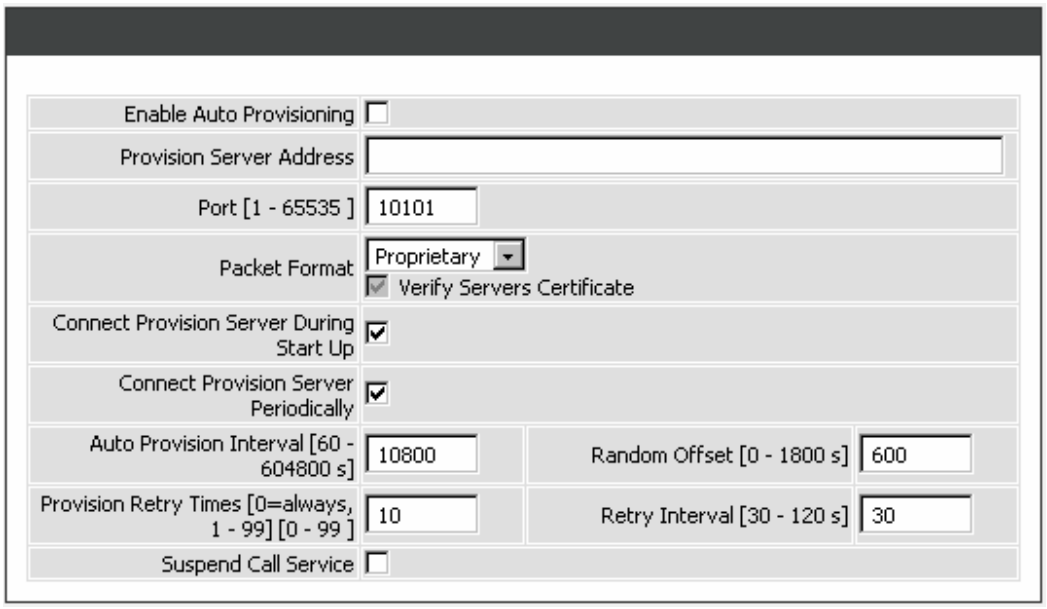
Port: Enter the System Log Server's listening port. Leave this field to the default if your VoIP Service Provider did not provide you a server port number for System Log Server.

2-3-6 Provision Settings

Provisioning is a function that automatically updates your DVG-G5402SP's VoIP configuration by using a TFTP, FTP, or HTTP server located on the Internet. If you have access to such service, you will need to know the URL or IP address of the Provisioning Server.

Note: Fill in the parameters needed by your VoIP Service Provider. Please check with your VoIP Service Provider about the availability of these services.

MAINTENANCE → PROVISION SETTINGS



Enable Auto Provisioning: Check the box to start provisioning.

Provision Server Address: Enter the Provisioning Server's IP address or URL required by your VoIP Service Provider.

Port: Enter the Provisioning Server's listening port.

Packet Format: Use the drop-down menu to choose the packet transmitting format required by your VoIP Service Provider.

Connect Provision Server During Start Up: Check the box to connect to Provisioning Server when the gateway is powered on or rebooted.

Connect Provision Server Periodically: Check the box to connect to Provisioning Server periodically.

Auto Provision Interval: Enter the time for auto provisioning.

Random Offset: Enter the offset of the time for auto provisioning.

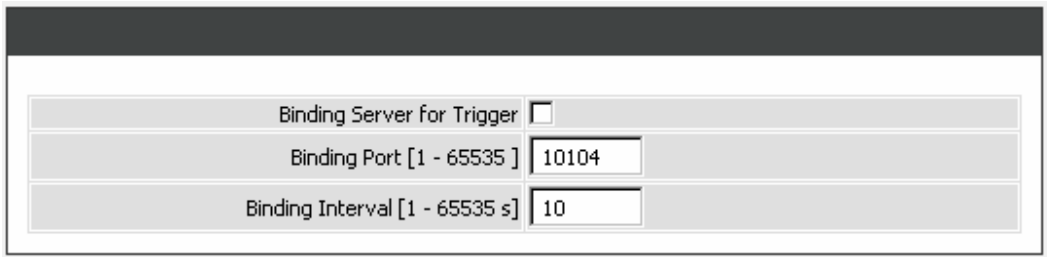
Provision Retry Times: Enter the retry time if a provisioning attempt fails.

Retry Interval: Enter the interval for retrying.

Suspend Service: Check the box to stop VoIP call service.

Note: Contact your server provider if necessary.

MAINTENANCE → PROVISION SETTINGS



Binding Server for Trigger: Check the box to trigger a connection between Provisioning Server and the gateway. Provisioning Server will bind a port for the gateway to send provision request.

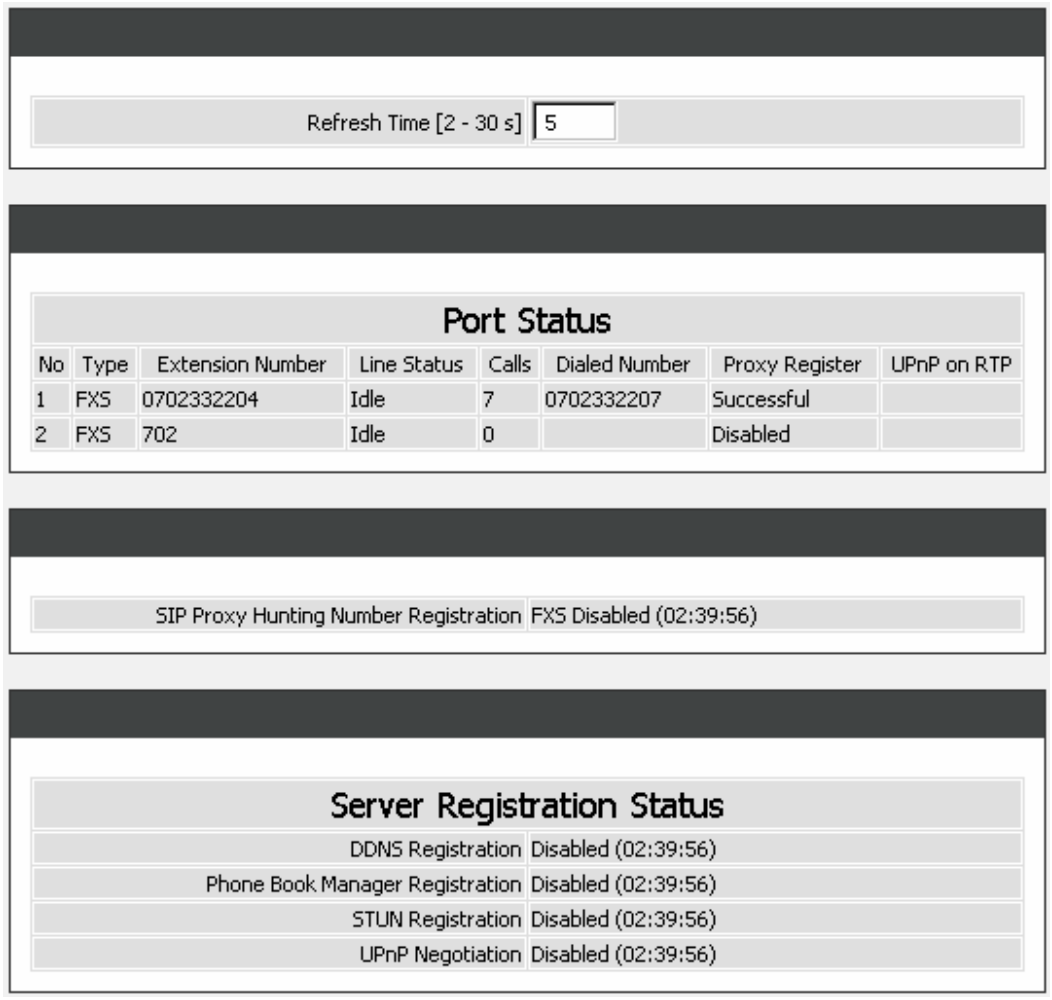
Binding Port: Enter the port number of Provisioning Server is used for binding.

Binding Interval: Enter the interval at which the gateway will keep the binding.

2-4 STATUS

2-4-1 Current Status

MAINTENANCE → CURRENT STATUS



Refresh Time [2 - 30 s] 5

Port Status

No	Type	Extension Number	Line Status	Calls	Dialed Number	Proxy Register	UPnP on RTP
1	FXS	0702332204	Idle	7	0702332207	Successful	
2	FXS	702	Idle	0		Disabled	

SIP Proxy Hunting Number Registration FXS Disabled (02:39:56)

Server Registration Status

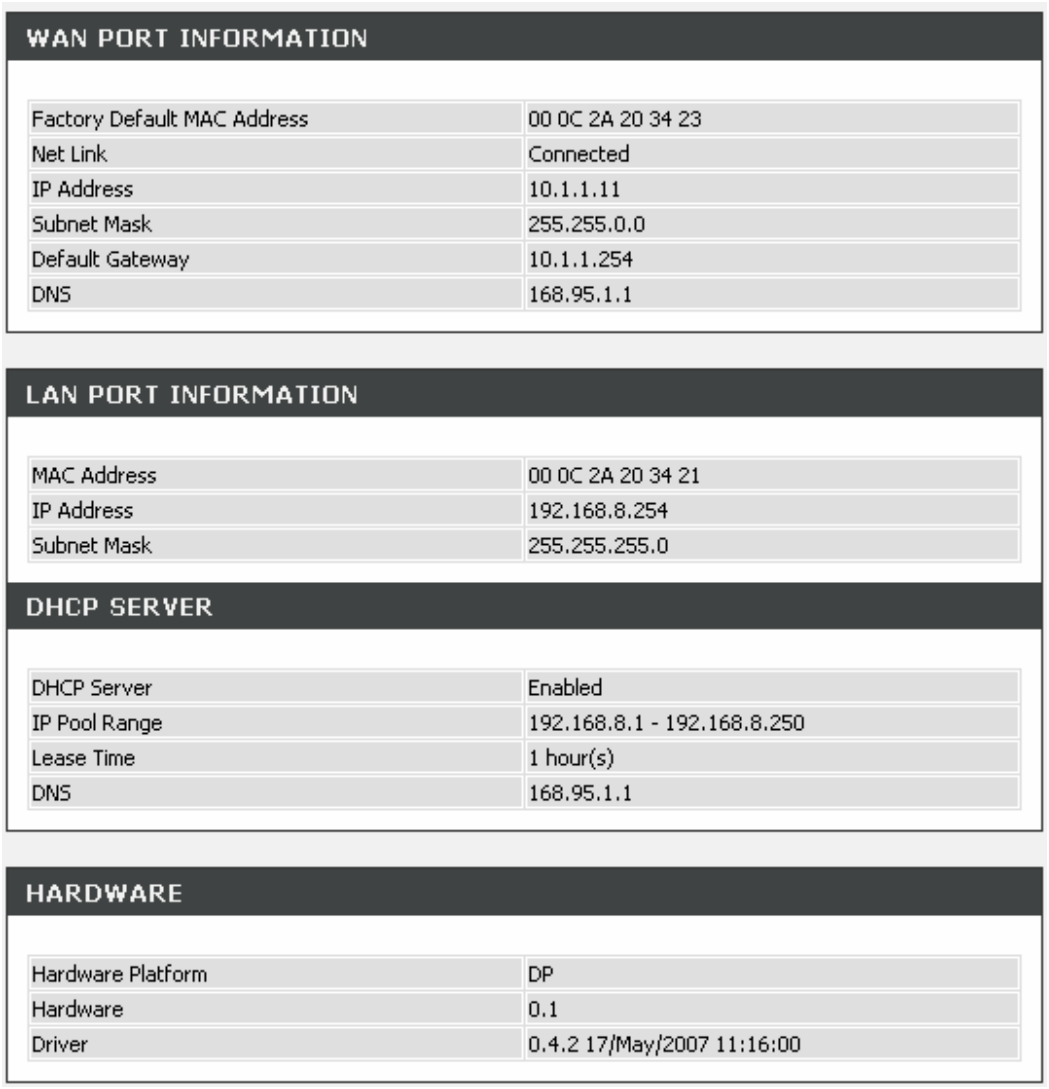
DDNS Registration	Disabled (02:39:56)
Phone Book Manager Registration	Disabled (02:39:56)
STUN Registration	Disabled (02:39:56)
UPnP Negotiation	Disabled (02:39:56)

For Port Status, it includes if each port registers to Proxy successfully, the last dialed number, how many calls each port has made since the gateway is start, etc.

For Server Registration Status, it shows the registration status of DDNS, Phone Book Manager, STUN and UPnP.

2-4-2 System Information

MAINTENANCE → SYSTEM INFORMATION



WAN PORT INFORMATION

Factory Default MAC Address	00 0C 2A 20 34 23
Net Link	Connected
IP Address	10.1.1.11
Subnet Mask	255.255.0.0
Default Gateway	10.1.1.254
DNS	168.95.1.1

LAN PORT INFORMATION

MAC Address	00 0C 2A 20 34 21
IP Address	192.168.8.254
Subnet Mask	255.255.255.0

DHCP SERVER

DHCP Server	Enabled
IP Pool Range	192.168.8.1 - 192.168.8.250
Lease Time	1 hour(s)
DNS	168.95.1.1

HARDWARE

Hardware Platform	DP
Hardware	0.1
Driver	0.4.2 17/May/2007 11:16:00

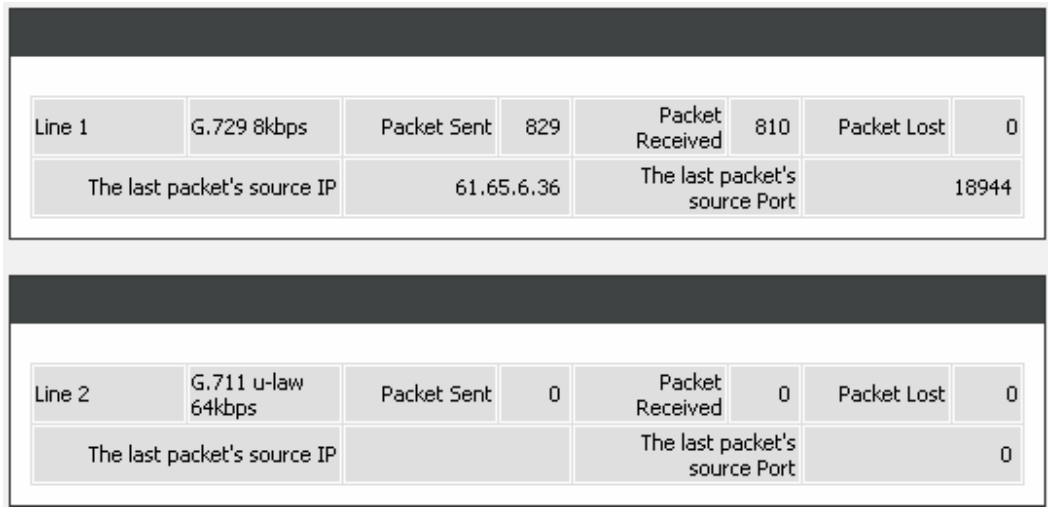
For WAN Port Information, it shows IP address, subnet mask, default gateway and DNS server. If you use PPPoE to obtain IP, you will know if the IP is obtained through this method. If IP address, subnet mask, default gateway is blank, it means that the gateway does not obtain IP.

For LAN Port Information, it shows LAN port IP, subnet mask, and the status of DHCP server.

For Hardware, it shows the hardware platform and driver version.

2-4-3 RTP Packet Summary

MAINTENANCE → RTP PACKET SUMMARY



Line 1	G.729 8kbps	Packet Sent	829	Packet Received	810	Packet Lost	0
The last packet's source IP		61.65.6.36		The last packet's source Port		18944	

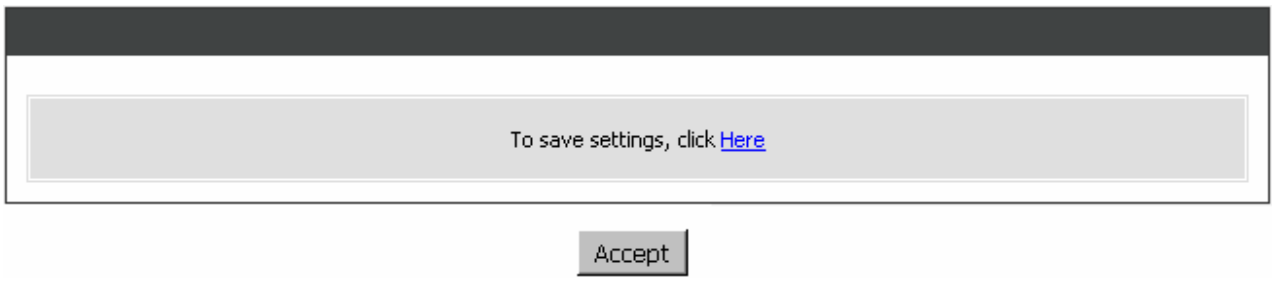
Line 2	G.711 u-law 64kbps	Packet Sent	0	Packet Received	0	Packet Lost	0
The last packet's source IP				The last packet's source Port		0	

Display the information of the last call made. Press **Refresh** button to get the latest RTP Packet Summary.

2-4-4 Logout

If setting or parameter has been changed, remember to save the changes before you logout the configuration menu.

MAINTENANCE → LOGOUT



3. Configuring the Gateway through IVR

VoIP transmits voice data (packets) via the Internet, hence the condition and status of the network environment is relatively important to the telecommunications quality. If any one of the parties involved in VoIP communications has insufficient bandwidth or frequent packet loss, the telecommunication quality will be poor. Therefore, excellent telecommunication can only happen when the gateways are connected to the Internet and when the network environment is stable.

Preparation

1. Connect the power supply, telephone set, telephone cable, and network cable properly as described in Chapter 2.
2. If a static IP is provided, confirm the correct IP settings of the WAN Port (IP address, Subnet Mask, and Default gateway). Please contact your local Internet Service Provider (ISP) if you have any question.
3. If you are using ADSL (PPPoE) for your network connection, confirm the account number and password.
4. If you intend to operate the gateway under NAT, the IP range of Gateway WAN Port and LAN Port IP Address should not be the same in order to avoid phone failures.

Basic Setup

The gateway provides two setup modes:

1. Telephone IVR Configuration Mode
2. Browser Configuration Mode

IVR configuration provides basic query and setup functions, while browser configuration provides full setup functions.

3-1 IVR (Interactive Voice Response)

The gateway provides convenient IVR functions. Users are able to get query and setup the gateway with a phone-set and function codes without turning on the PC.

Note: When finishing the setup, make sure the new settings are saved. This will enable the new settings to take effect after the system is restarted.

Instructions

FXS Port: Connect to telephones. To access IVR mode, passwords should be entered, "* * password #". Alphabets to digits conversion information is provided in the PPPoE Character Conversion Table. (Refer to Page??) When correct IVR passwords are entered and accepted, an indication tone can be heard indicates the system is in IVR setup mode. Enter function codes to check or configure the gateway. (Please refer to page 43 for function codes).

Example: If your password is "1234", enter * (star) * (star) 1 2 3 4 # (pound)**,** and now you are entering IVR setup mode. Next, enter a function code to check or configure the gateway. If your password is "admin", enter * (star) * (star) * (star) 41 44 53 49 54 # (pound). Please refer to the IVR Functions Table (page 43) for available functions and codes.

Once the setting or query has been completed, you can hear a dial tone. Use the same procedure to make a second query or setting. To exit IVR mode, simply hang up the phone.

Example: enter **"**#"** (you are now in IVR mode)→ enter **101** (to query the current IP address) → the system responds with an IP address. You can continue with more settings or queries: enter **111** (to set a new IP address) →enter **192*168*1*2** (new IP address).

Save Settings

When all setting procedures are completed, dial 509 (Save Settings) from phone keypad. Wait for about three seconds, you should hear a voice prompt "1 (one)." You can now hang up the phone and please reboot the gateway to enable the new settings.

To inquire about the current gateway WAN Port IP address setting

After completing all your settings, dial 101 from the keypad, then you can hear the system play back the current WAN Port IP address. If the system does not play back the IP address after dialing 101, this indicates that the gateway currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

3-1-1 IVR Functions Table:

Function Code	Description	Example / Notes
111/101	WAN Port IP address Set/Query	Dial function code **114** and then dial 1 for a Static IP connection then setup the IP address.
112/102	WAN Port Subnet Mask Set/Query	
113/103	WAN Port Default Gateway Set/Query	
114/104	Current Network IP Access Set/Query (1: Static IP, 2: DHCP, 3: PPPoE)	
115/105	DNS IP address Set/Query	
116/106	Phone Book manager IP address Set/Query	
117/107	Set/Query whether or not to use a Public Telephone Book (0: Disable 1: Enable)	
199/099	Set/Query whether or not this gateway acts as the Phone Book manager (0: Disable 1: Enable)	
066	Querying the connection to Phone Book manager	
118	Restart	
121	Setup PPPoE Account	Dial function code **114** and then dial 3 for a PPPoE connection.
122	Set PPPoE Password	
123	Set NAT IP address	
124	Uses NAT (0: Disable 1: Enable)	
311/301	LAN Port IP Set/Query	
312/302	LAN Port Subnet Mask Set/Query	
109	Restore factory default IP address configuration	A static IP address for WAN Port IP：192.168.1.2 Mask：255.255.255.0 Gateway：192.168.1.254
409	Restore factory default settings	
509	Save settings	
900	Set the IVR and the language used on the Web GUI (1: English, 2: Traditional Chinese, 3: Simplified Chinese)	
209	Software Upgrade	

3-2 IP Configuration Settings—Set the IP Configuration of the WAN Port

Static IP Settings

Note: Complete static IP settings should include a static IP (option 1 under 114), IP address (111), Subnet Mask (112), and Default Gateway (113). Please contact your Internet Service Provider (ISP) if you have any question.

Function	Command
Select a Static IP	• After entering IVR mode, dial 114. • When voice prompt plays "Enter value", dial 1 (to select static IP)
IP address Settings	• After entering IVR mode, dial 111. When voice prompt plays "Enter value", enter your IP address followed by "#". **Example**: If the IP address is 192.168.1.200, dial 192*168*1*200#.
Subnet Mask Settings	• After entering IVR mode, dial 112. When voice prompt plays "Enter value", enter your subnet mask followed by "#". **Example**: If the subnet mask value is 255.255.255.0, dial 255*255*255*0#.
Default Gateway Settings	• After entering IVR mode, dial 113. When voice prompt plays "Enter value", enter your default gateway's IP address followed by "#". **Example**: If the default gateway is 192.168.1.254, dial 192*168*1*254#.
Save Settings and Restart	• To save settings, dial **509** (Save Settings). The system will save the current settings. Please restart the system. Wait for about 40 seconds for the system to restart, and then enter **101** to check whether the IP address was retained. If the system does not play back the IP address after dialing 101, this indicates that the gateway currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

Dynamic IP (DHCP) Settings

After entering IVR mode, dial 114.

When voice prompt plays "Enter value", dial 2 (to select DHCP).

Saving settings –press 509 (Save Settings). Please restart the system. After the system is restarted, press 101 to check whether or not the IP address was retained.

Note: If the system does not play back the IP address, this indicates that the gateway failed to communicate with a DHCP server. Please check with your DHCP server or ISP.

ADSL PPPoE Settings

Note: Complete PPPoE settings should include: Select PPPoE (option 3 of 114), PPPoE account (121) and PPPoE password (122).

Please contact your local Internet Service Provider (ISP) if you have any questions.

Select a PPPoE

After entering IVR mode, dial 114.

When voice prompt plays "Enter value," dial 3 (to select PPPoE).

PPPoE Account Settings

After entering IVR mode, dial 121.

When voice prompt plays "Enter value", enter the account number followed by"#".

Example: If the account is "87654321@hinet.net," please enter 08 07 06 05 04 03 02 01 71 48 49 54 45 60 72 54 45 60 #.

Note: It is necessary to enter two digits for each alphabet/number; for example, you must enter "01" for "1" and "11" for "A". Using the web Interface to configure your PPPoE account details is recommended. Refer to the PPPoE Character Conversion Table on the next page for key mappings if you choose to use IVR setup.

PPPoE Password Setting

After entering IVR mode, dial 122,

When voice prompt plays "Enter value," enter the new password followed by "#".

Example: If the password is "3t2ixiae", please enter "03 60 02 49 64 49 41 45#".

Save Settings and Restart

To save settings, dial **509** (Save Settings). The system will save the settings. Please restart the system. Wait for about 40 seconds for the system to restart, then enter **101** to check whether the IP address was retained. If the system does not play back the IP address after dialing **101**, this indicates that the gateway currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

3-2-1 PPPoE Character Conversion Table:

The table below provides a list of PPPoE conversion codes. The first row (high-lighted) of each pair of the column lists the numbers, alphabets or symbols and the second row (high-lighted) of each pair of the column ("Input Key") represents the codes to be entered for the corresponding numbers, alphabets or symbols. For example, to enter "D-Link" according to the table below, enter: 148322495451

Numbers	Input Key	Upper Case Letters	Input Key	Lower Case Letters	Input Key	Symbols	Input Key
0	00	A	11	a	41	@	71
1	01	B	12	b	42	•	72
2	02	C	13	c	43	!	73
3	03	D	14	d	44	"	74
4	04	E	15	e	45	$	75
5	05	F	16	f	46	%	76
6	06	G	17	g	47	&	77
7	07	H	18	h	48	'	78
8	08	I	19	i	49	(	79
9	09	J	20	j	50	)	80
		K	21	k	51	+	81
		L	22	l	52	,	82
		M	23	m	53	-	83
		N	24	n	54	/	84
		O	25	o	55	:	85
		P	26	p	56	;	86
		Q	27	q	57	<	87
		R	28	r	58	=	88
		S	29	s	59	>	89
		T	30	t	60	?	90
		U	31	u	61	[	91
		V	32	v	62	\	92
		W	33	w	63	]	93
		X	34	x	64	^	94
		Y	35	y	65	_	95
		Z	36	z	66	{	96
						|	97
						}	98

4. Dialing Principles

4-1 Dialing Options

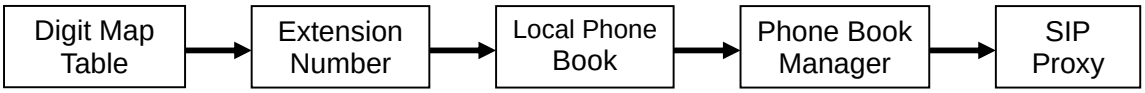
Dial the phone number which you want to call and press # to call out immediately. Note that if the "# (pound)" not dialed, the number will be called out after 4 seconds by default. The period between number dialed and call out is named "Inter Digits Timeout". (Configurable from "Advanced Options", default=4 seconds, see page 23).

If the phone number matches the setting of the Digit Map, the phone number will be dialed out through the assigned interface automatically.

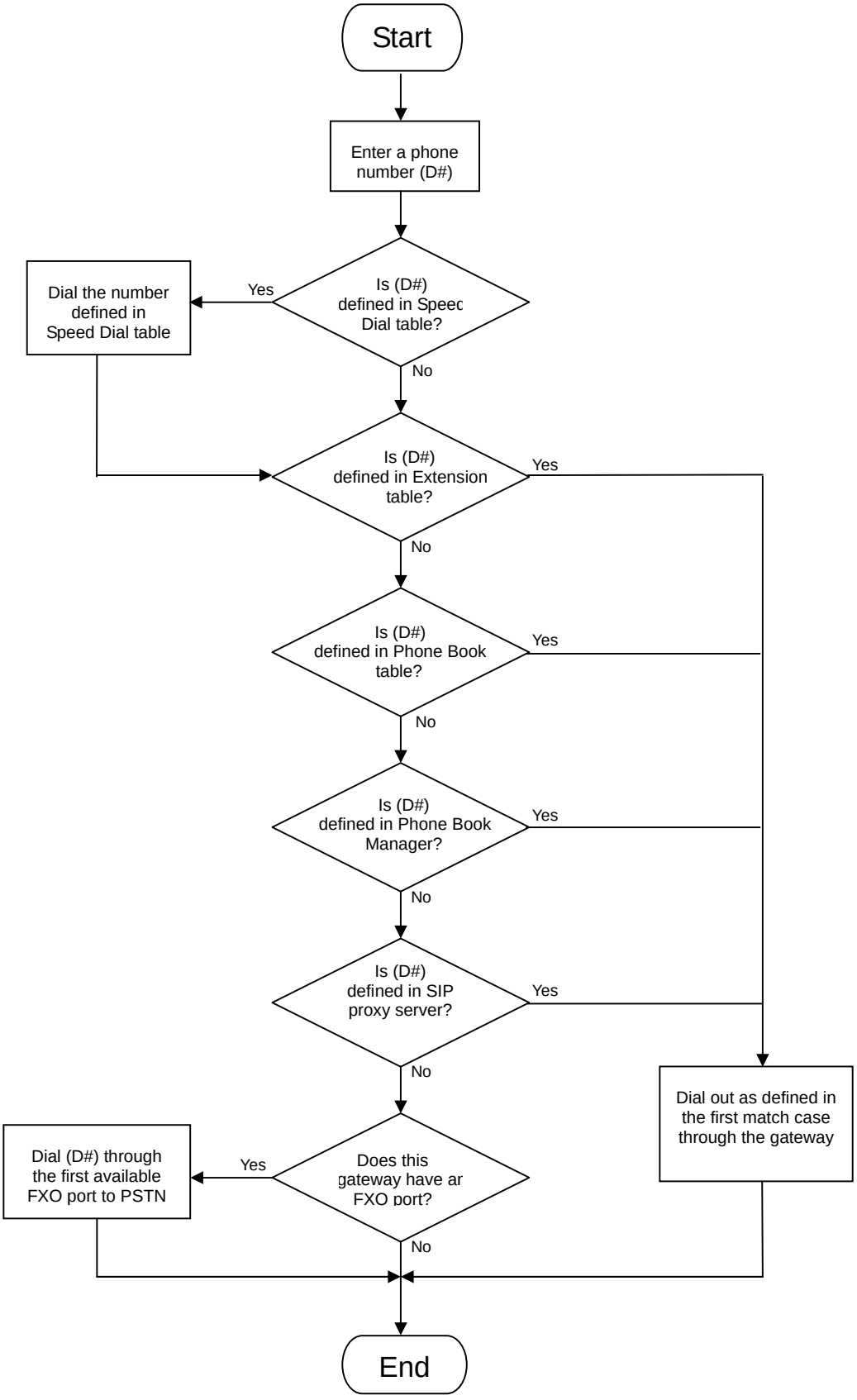
The phone number should contain at least 2 digits (not including * and #).

4-2 Dialed Number Processing Flow

To achieve maximum flexibility, the number dialed will be looked up in several tables defined by the gateway. If no match is found from Digit Map Table, it will then look up the number from another table and to the registered SIP Proxy Server. The number look up flow is shown below:



A complete flow chart is shown on the next page.


Start
Enter a phone number (D#)
Is (D#) defined in Speed Dial table?
Yes
Dial the number defined in Speed Dial table
No
Is (D#) defined in Extension table?
Yes
No
Is (D#) defined in Phone Book table?
Yes
No
Is (D#) defined in Phone Book Manager?
Yes
No
Is (D#) defined in SIP proxy server?
Yes
No
Does this gateway have an FXO port?
Yes
Dial (D#) through the first available FXO port to PSTN
No
Dial out as defined in the first match case through the gateway
End

Appendix

Product Features

WAN

- One 10/100Mbps auto-negotiation, auto-crossover RJ-45 Ethernet port
- Support static IP, PPPoE, BigPond Cable and DHCP address assignment and dynamic DNS (DDNS)
- QoS: IP TOS (Type of Services) and DiffServ (Differentiated Services) for both SIP signaling and RTP
- NAT Traversal : Port Forwarding, STUN, UPnP and Outbound Proxy
- NTP: (Network Time Protocol RFC 1305), Accepts up to 3 Time Server
- Time Zone Support
- MAC Address Clone
- RTP Packet Summary : packet sent, packet received, packet loss for voice quality analysis

LAN

- Four 10/100Mbps auto-negotiation, auto-crossover RJ 45 Ethernet ports
- Supports router and bridge mode (NAT mode and Non-NAT mode)
- DHCP server

Voice Features

- SIP (RFC3261) compatible
- Voice codecs : G.711 a /ulaw, G.726, G.729A, G.723.1
- CNG (Comfort Noise Generation)
- VAD (Voice Activity Detection)
- G.165/G.168 echo cancellation
- Adjustable Jitter Buffer and programmable Gain Control
- In-Band DTMF, Out-Of-Band DTMF relay (RFC2833, SIP INFO)
- Multiple SIP Proxy server entries with failover mechanism
- Polarity reversal detection (FXO/PSTN) and generation (FXS)
- T.30 (G.III) / Real time T.38 / Secured T.38 FAX relay
- DTMF, FSK (Bellcore & ETSI) Caller ID detection and generation.
- Support Caller ID Restriction (CLIR)
- Digit Map for dial plan
- Speed Dial
- Local phone book for peer-to-peer calling
- E.164 Numbering & ENUM support
- Hot-Line, Warm-Line support
- Single Number / Account (reprehensive number) for multiple ports
- Recordable greeting message
- Call features:
    - Call Hold, Call Waiting, Call Pickup
    - Call Forward - Unconditional, Busy, No Answer
    - Call Transfer - Unattended, Attended
    - Three Way Calling (Media Server required)
- Analogue interface
    - Connector : RJ-11
    - Signaling protocol : Loop Start

Configuration & Maintenance

- Configuration methods:
  - Web
  - IVR
  - Telnet
- Status reports:
  - Port status
  - Registration status
  - Ping tests
  - STUN/UPnP status
  - Hardware / software information
- Firmware Upgrade through TFTP, FTP and proprietary image server
- Configuration Backup/Restore
- Reset button (with restore factory default function)
- Front Panel LED : voice ports, WAN, LAN1~4, Run, Power, Alarm
- Optional Auto Provisioning Server (APS) for mass

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE 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.

CAUTION:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with 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.

RF exposure warning ·

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.