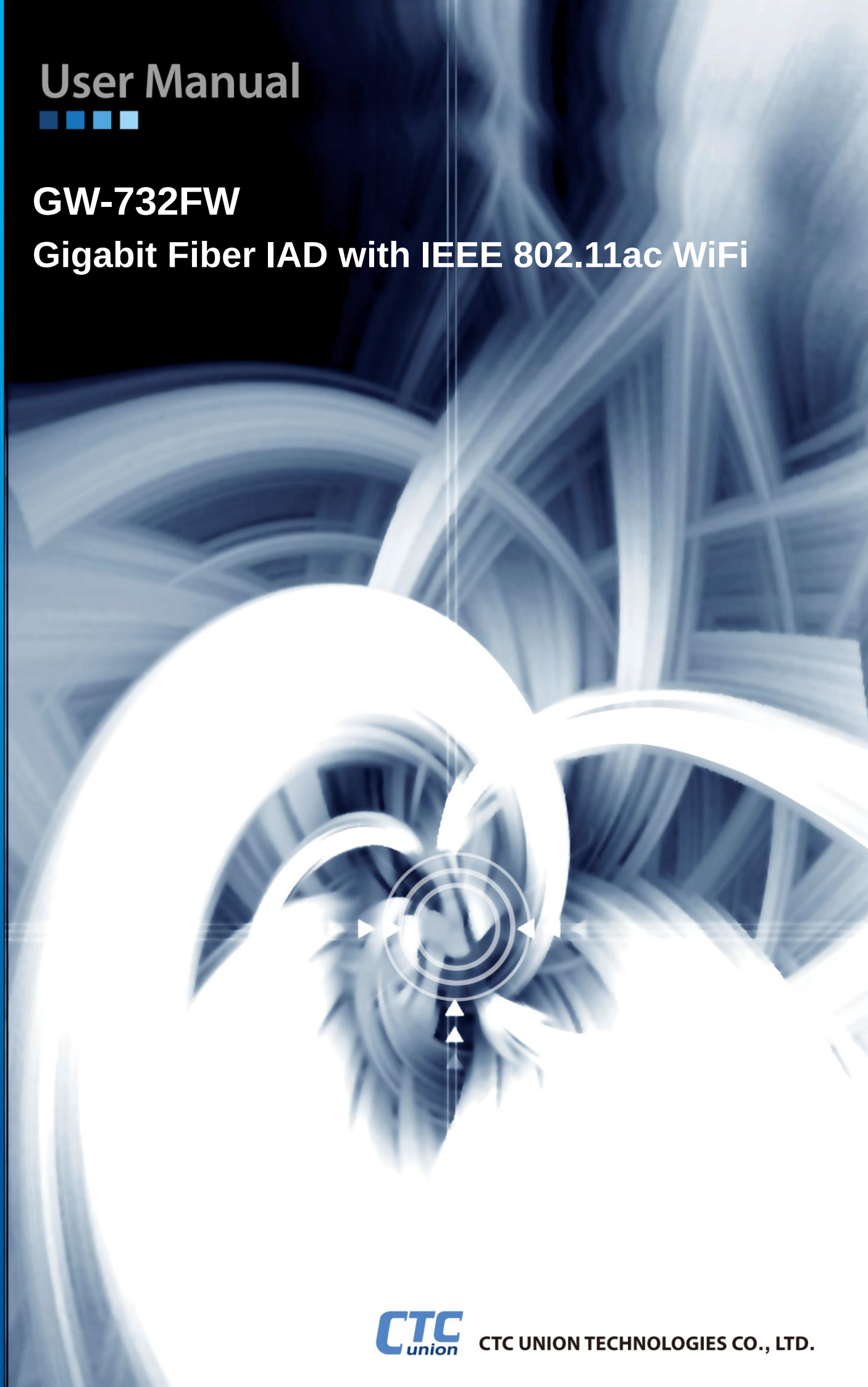
User Manual

GW-732FW

Gigabit Fiber IAD with IEEE 802.11ac WiFi



CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. Our company assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. Our company reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

Our company makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor do we assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Our products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use our product for any such unintended or unauthorized application, the Buyer shall indemnify and hold our company and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that our company was negligent regarding the design or manufacture of said product.

Federal Communications Commission (FCC) NOTICE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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 of 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.

This unit was tested with shielded cables on the peripheral devices. Shielded cables must be used with the unit to insure compliance. This statement can be deleted if unit was not tested with shielded cables.
The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications 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.
2. This device must accept any interference that may cause undesired operation.

Change or modifications that are not expressly approved by the manufacturer could void the user’s authority to operate the equipment.

CISPR PUB.22 Class B COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class B.

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.

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

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006+A1:2007, Class A, EN55024:2010.

Gigabit Ethernet Fiber IAD Gateway with IEEE 802.11ac WiFi

User Manual
Version 0.9 March 2015

Contents

1. Introduction 1
1-1 Product Overview 1
1-2 Hardware Description 2

2. VoIP Wireless Gateway Web Configuration 4
2-1 Status 5
2-1-1 Current Status 5
2-1-2 RTP Packet Summary 5
2-1-3 System Information 6
2-1-4 Routing Table 7
2-1-5 LAN Client 8
2-2 General Settings 9
2-2-1 Network operation mode 9
2-2-2 Standard WAN 9
2-2-3 Standard LAN 13
2-2-4 Multiservice WAN 14
2-2-5 Multiservice LAN 14
2-2-6 SIP 18
2-2-7 SIP Advanced 23
2-2-8 Caller ID 27
2-2-9 Hot Line 28
2-2-10 Line settings 29
2-2-11 FAX 32
2-2-12 Calling Features 34
2-2-13 Phone Book 36
2-2-14 CDR Settings 36
2-3 Wireless Settings 38
2-3-1 Basic Settings 38
2-3-2 Advanced Settings 40
2-3-3 Security Settings 41
2-3-4 Access Control 44
2-3-5 WPS 45
2-4 Advanced Settings 49
2-4-1 Codec setting 49
2-4-2 Digit Map 50
2-4-3 DTMF & PULSE 54
2-4-4 CPT / Cadence 55
2-4-5 TR069 56
2-4-6 Caller Filter 58
2-4-7 Static Route 59
2-4-8 DDNS 60
2-4-9 NAT Traversal 61
2-4-10 DoS Protection Settings 62
2-4-11 DMZ / ALG 62
2-4-12 IP Filtering 63
2-4-13 Port Filtering 64
2-4-14 MAC Filtering 64
2-4-15 Virtual Server 65
2-4-16 UPnP 65
2-5 Tools 66
2-5-1 Ping Test 66
2-5-2 STUN Inquiry 67
2-6 System Settings 68
2-6-1 NTP 68
2-6-2 Language 68
2-6-3 Login Account 69
2-6-4 Backup / Restore 70
2-6-5 System Log 71
2-6-6 Save / Restart 71
2-6-7 Software Upgrade 72
2-6-8 Logout 72

3. Configuring the VoIP Gateway through IVR 73
3-1 IVR (Interactive Voice Response) 73
3-1-1 IVR Functions Table: 74
3-2 IP Configuration Settings 75
3-2-1 Character Conversion Table: 76
4. Dialing Principles 77

1. Introduction

1-1 Product Overview

The VoIP Gateway is designed to carry both voice and facsimile over the IP network. 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 Switch and SIP proxy servers. While running optional server software, the VoIP Gateway can be configured to establish a private VoIP network over the Internet without a third-party SIP Proxy Server.

The VoIP 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 VoIP Gateway allows you to use voice and fax services over IP in order to reduce the cost of all long distance calls.

The VoIP Gateway can be configured a fixed IP address or it can have one dynamically assigned by DHCP or 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 Pannel

Indicators

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

Prov./Alm.: A blinking light indicates the VoIP Gateway can not register with SIP Server or can not get the IP address. A blinking light also indicates the VoIP Gateway is attempting to connect with the Provisioning server. Once the service connects, the LED will turn off. The LED will light solid red if the self-test or boot-up fails.

Reg.: The Register LED will turn on and continuously working when VoIP Gateway is connected to a VoIP service provider. The LED will flash if not connected to a service provider.

Phone1~2: 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.

WAN: When a connection is established the LED will light up solid. The LED will blink to indicate activity. If the LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.

WLAN 2.4G/5G: A steady light indicates a wireless connection. A blinking light indicates that the VoIP Gateway is receiving/transmitting from/to the wireless network.

LAN1~4 : When a connection is established the LED (bottom) will light up solid on the appropriate port. The LEDs will blink to indicate activity. If the LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.

USB1~2 : This indicates that VoIP Gateway detects a supported 3G modem dungle or a USB device.

WPS: Flashing in blue as wireless router processing WPS-PBC wireless connecting progress.

Rear Panel

1. **WLAN Switch:** Switch it to power on/off wireless feature.

2. **USB 1~2:** Connect to a 3G USB dongle or a printer.

3. **LAN:** 10/100/1000M Gigabit Ethernet. Connect to your Ethernet enabled computers using Ethernet cabling.

4. **WAN:** 10/100/1000M Gigabit Ethernet. Connect to your broadband modem using an Ethernet cable.

5. **Optical WAN:** Insert 155M/1.25G fiber optic SFP module and connect to a switch or router.

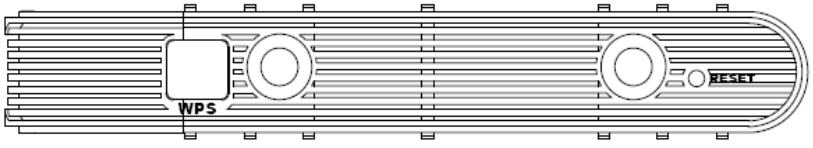
   Note: VoIP Gateway allows alternative Copper or Optical WAN at the same time.
   1. If you connect Copper WAN at first that Optical WAN will not take active unless remove RJ45 cable from Copper WAN port.
   2. If you connect Optical WAN at first that Copper WAN will not take active unless remove fiber from Optical WAN port.

6. **Phone Port (1-2):** Connect to your phones using standard phone cabling (RJ-11).

7. **Power Receptor:** Receptor for the provided power adapter.

8. **Power Switch:** Press down to turn-on VoIP Wireless Router.

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). (3) Stacking is forbidden. Doing so may damage your VoIP Gateway.



WPS: WPS button for wireless WPS-PBC setup method.

Antenna: Connect to a wireless network.

Reset button: Use to restore factory default settings.

Note: Use Reset Button to restore factory default settings:
1. Press and hold the reset button for 5 seconds.
2. As Alarm indicator is blinking, please release the reset button. Factory settings will be restored.

2. VoIP Wireless Gateway Web Configuration

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.

Instructions

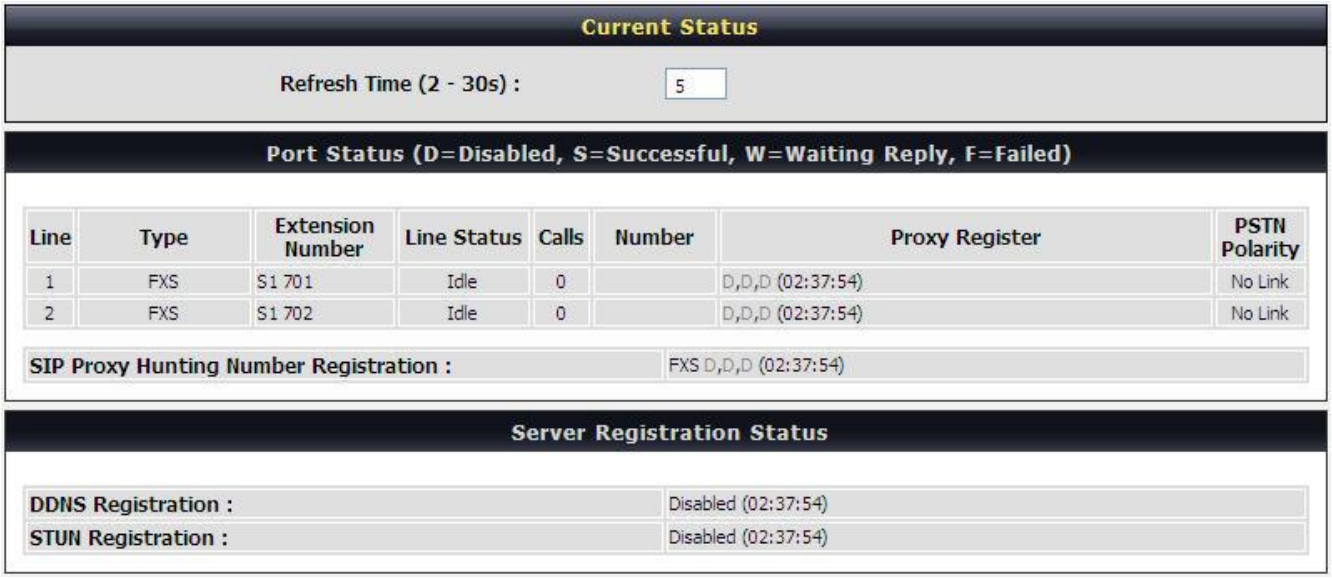
- Open a Web-Browser (e.g., Explorer, Navigator, Opera, FireFox).
- Enter the LAN port IP address in the address filed and press Enter. The default LAN port IP address is: 192.168.8.254.
- The log-in screen below will appear after you connect. (The factory default settings for **Username** and **Password** are left blank).

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

2-1 Status

2-1-1 Current Status

Status → Current Status



Current Status

Refresh Time (2 - 30s) : 5

Port Status (D=Disabled, S=Successful, W=Waiting Reply, F=Failed)

Line	Type	Extension Number	Line Status	Calls	Number	Proxy Register	PSTN Polarity
1	FXS	S1 701	Idle	0		D,D,D (02:37:54)	No Link
2	FXS	S1 702	Idle	0		D,D,D (02:37:54)	No Link

SIP Proxy Hunting Number Registration :	FXS D,D,D (02:37:54)

Server Registration Status

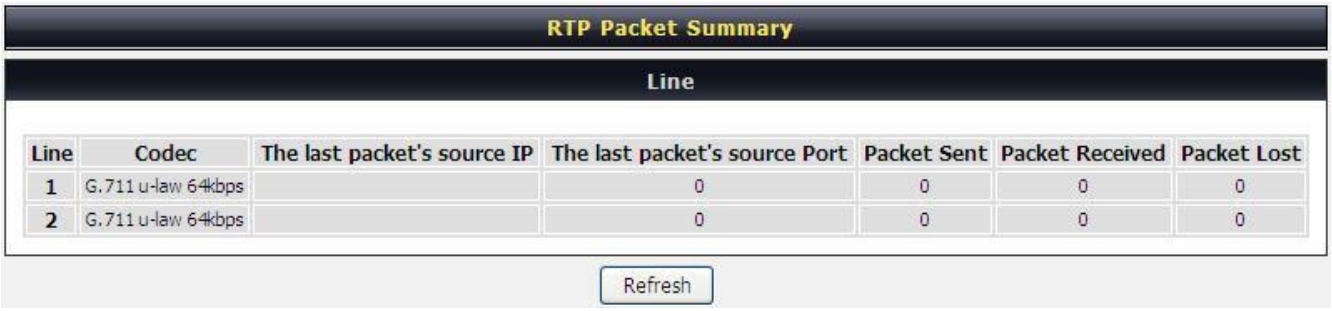
DDNS Registration :	Disabled (02:37:54)
STUN Registration :	Disabled (02:37:54)

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 VoIP Gateway starts, etc.

For Server Registration Status, it shows the registration status of DDNS, STUN and FXS Represent Number.

2-1-2 RTP Packet Summary

Status → RTP Packet Summary



RTP Packet Summary

Line

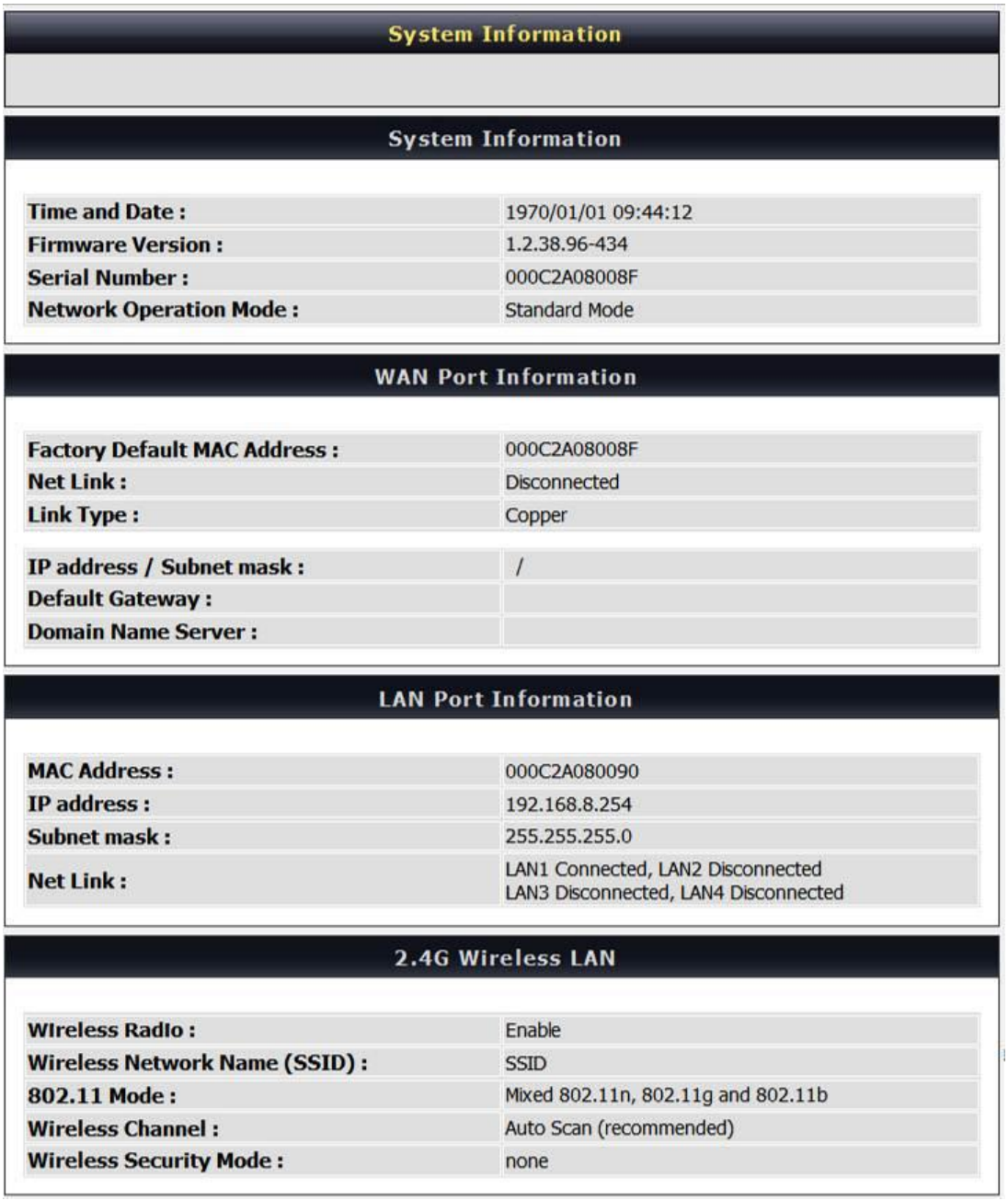
Line	Codec	The last packet's source IP	The last packet's source Port	Packet Sent	Packet Received	Packet Lost
1	G.711 u-law 64kbps		0	0	0	0
2	G.711 u-law 64kbps		0	0	0	0

Refresh

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

2-1-3 System Information

Status → System Information



System Information

System Information

Time and Date :	1970/01/01 09:44:12
Firmware Version :	1.2.38.96-434
Serial Number :	000C2A08008F
Network Operation Mode :	Standard Mode

WAN Port Information

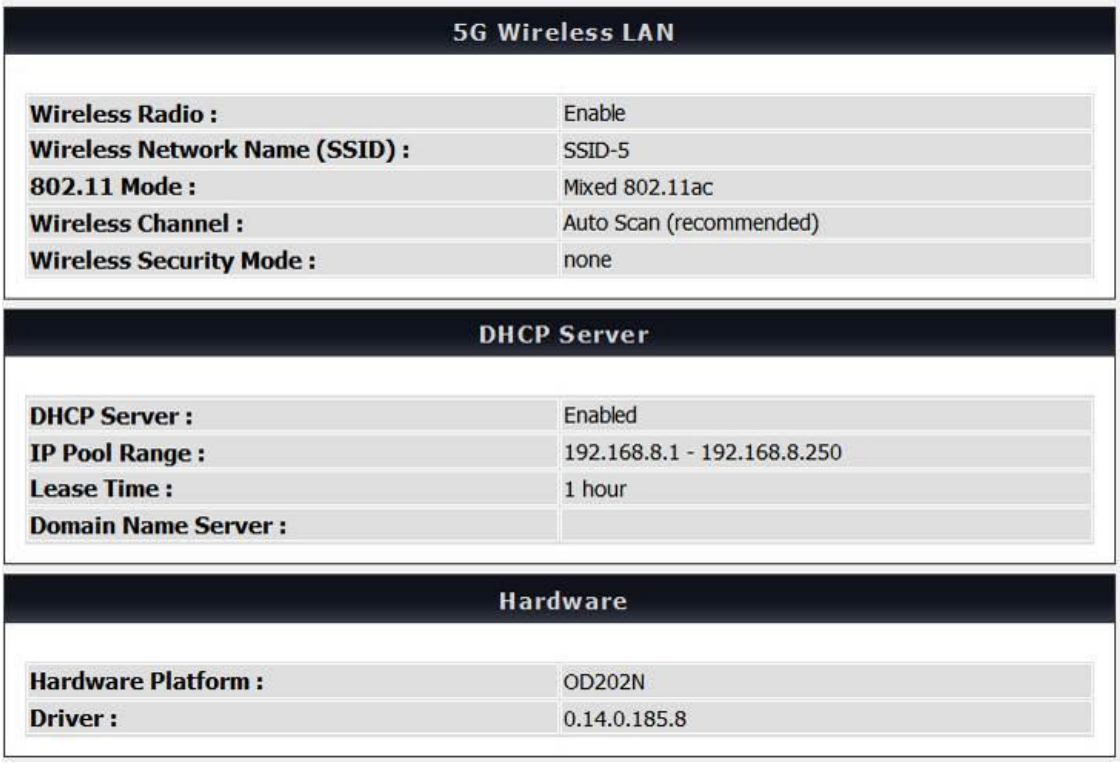
Factory Default MAC Address :	000C2A08008F
Net Link :	Disconnected
Link Type :	Copper
IP address / Subnet mask :	/
Default Gateway :	
Domain Name Server :	

LAN Port Information

MAC Address :	000C2A080090
IP address :	192.168.8.254
Subnet mask :	255.255.255.0
Net Link :	LAN1 Connected, LAN2 Disconnected LAN3 Disconnected, LAN4 Disconnected

2.4G Wireless LAN

Wireless Radio :	Enable
Wireless Network Name (SSID) :	SSID
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b
Wireless Channel :	Auto Scan (recommended)
Wireless Security Mode :	none



5G Wireless LAN	
Wireless Radio :	Enable
Wireless Network Name (SSID) :	SSID-5
802.11 Mode :	Mixed 802.11ac
Wireless Channel :	Auto Scan (recommended)
Wireless Security Mode :	none

DHCP Server	
DHCP Server :	Enabled
IP Pool Range :	192.168.8.1 - 192.168.8.250
Lease Time :	1 hour
Domain Name Server :	

Hardware	
Hardware Platform :	OD202N
Driver :	0.14.0.185.8

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 VoIP Gateway does not obtain IP.

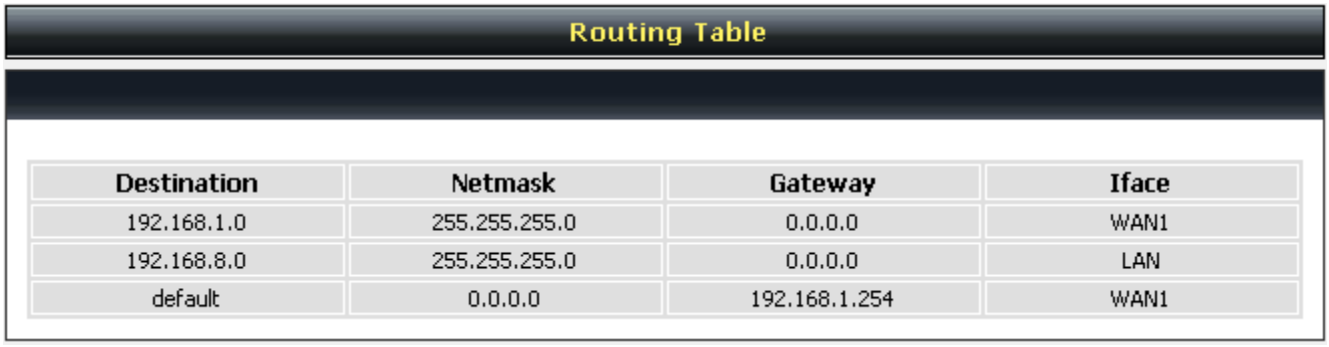
For LAN Port Information, it shows LAN port IP, subnet mask, and the status of DHCP server.

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

2-1-4 Routing Table

Status → Routing Table

It displays routing table of VoIP Gateway.



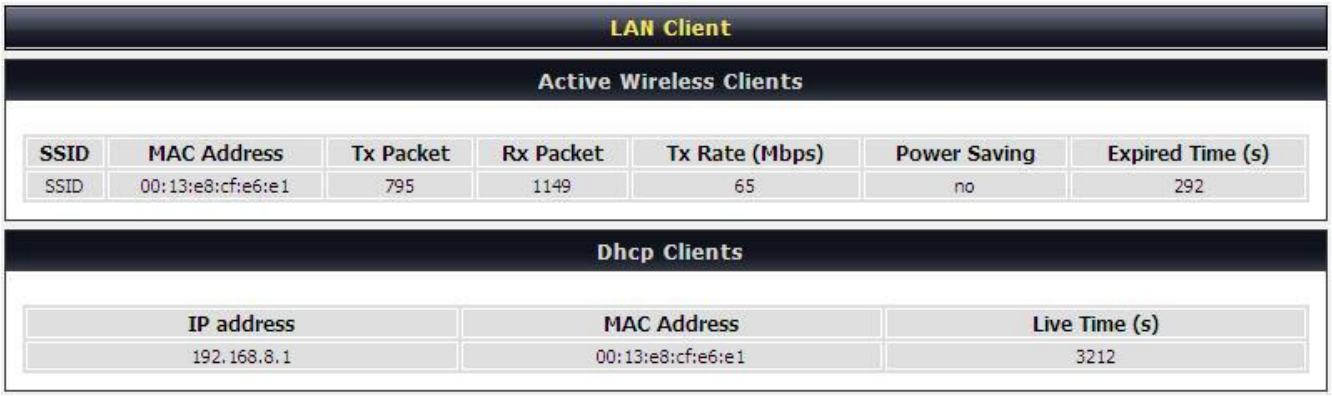
Routing Table

Destination	Netmask	Gateway	Iface
192.168.1.0	255.255.255.0	0.0.0.0	WAN1
192.168.8.0	255.255.255.0	0.0.0.0	LAN
default	0.0.0.0	192.168.1.254	WAN1

2-1-5 LAN Client

The **DHCP Clients** table displayed LAN device that has already been assigned an address from VoIP Gateway. You can check if the DHCP client has obtain an IP address.

Status → LAN Client



LAN Client

Active Wireless Clients

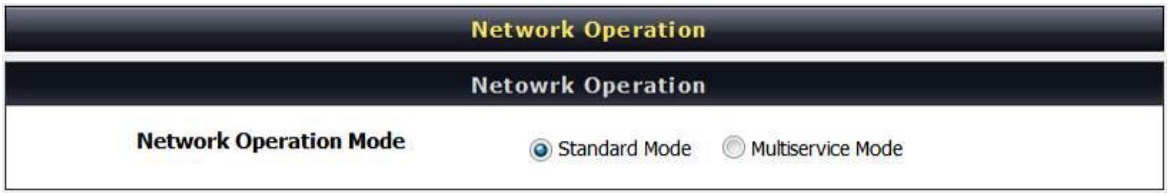
SSID	MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
SSID	00:13:e8:cf:e6:e1	795	1149	65	no	292

Dhcp Clients

IP address	MAC Address	Live Time (s)
192.168.8.1	00:13:e8:cf:e6:e1	3212

2-2 General Settings

2-2-1 Network operation mode



IAD Gateway provides 2 network operation mode: **Standard mode** and **Multiservice mode**.

2-2-2 Standard WAN

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

IP Configuration (Setting WAN Port)

There are four methods of obtaining a WAN port IP address:

1. Static IP
2. DHCP
3. PPPoE
4. PPTP
5. USB 3G

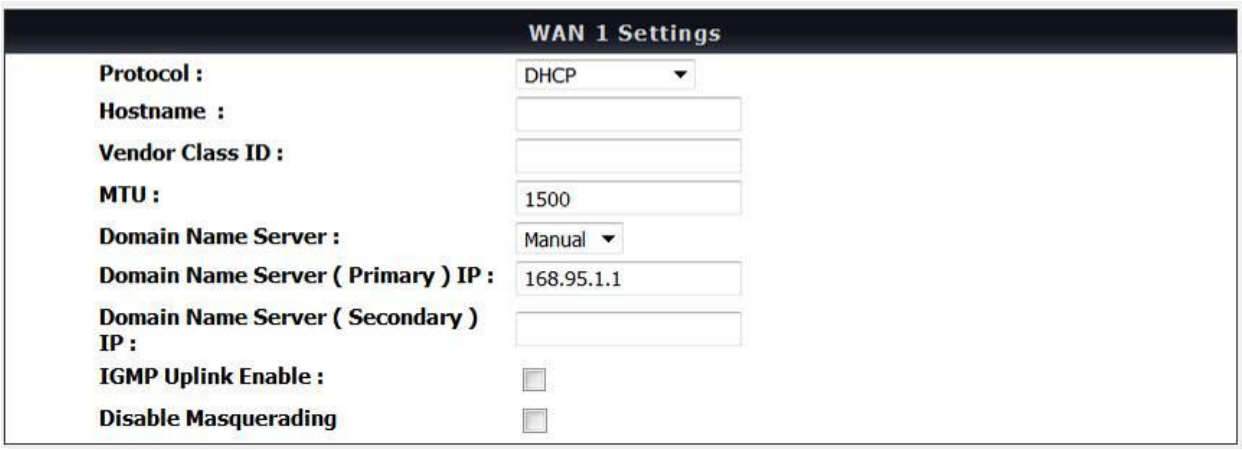
Methods for using DHCP and PPPoE for obtaining an IP address may vary. If you are not familiar with creating a network connection, please contact your local ISP.

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 VoIP Gateway to make the changes active. Enter "System Settings-> Save/ Restart" page then **Save** and **Restart**. Wait for about 50 seconds before the VoIP Gateway obtaining an IP address by the method you selected.

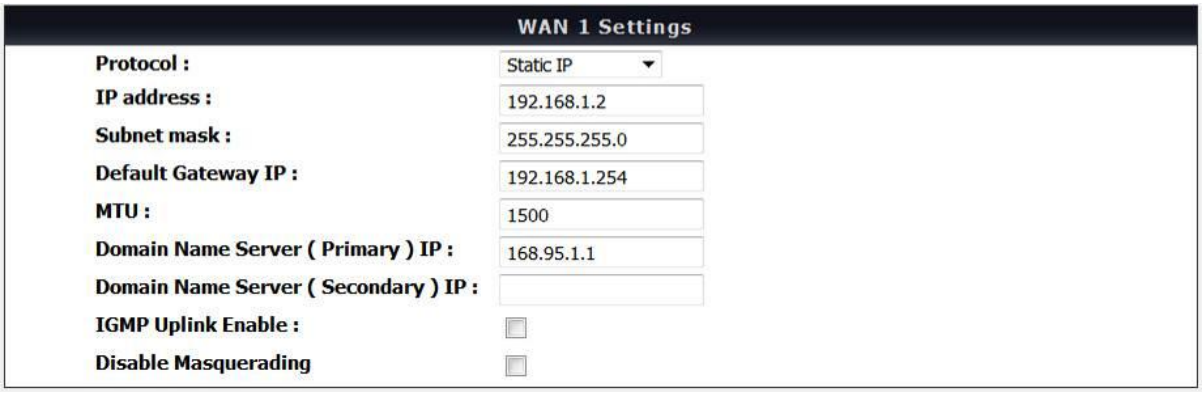
Note: When the system has obtained a new IP address, and you are using a WAN port to enter the Web Configuration Screen, the new IP address has to be used before you can get connected to the VoIP Gateway. The same principle applies to the next two settings.

General Settings → WAN



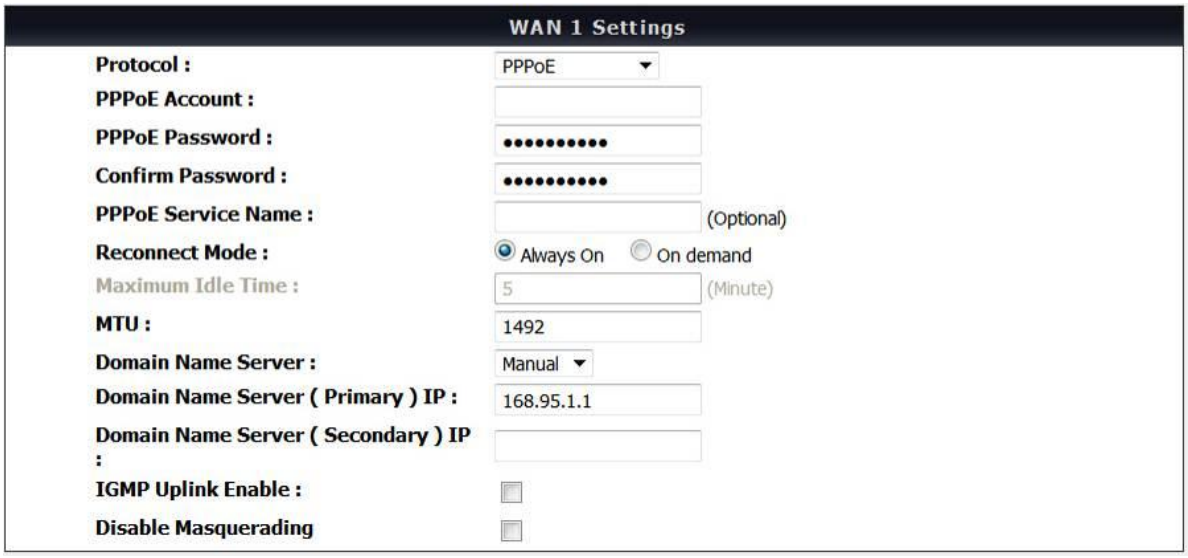
DHCP: Select this option if your ISP (Internet Service Provider) provides you an IP address automatically. Cable modem providers typically use dynamic assignment of IP Address. The Host Name field is optional but may be required by some Internet Service Providers.

General Settings → WAN



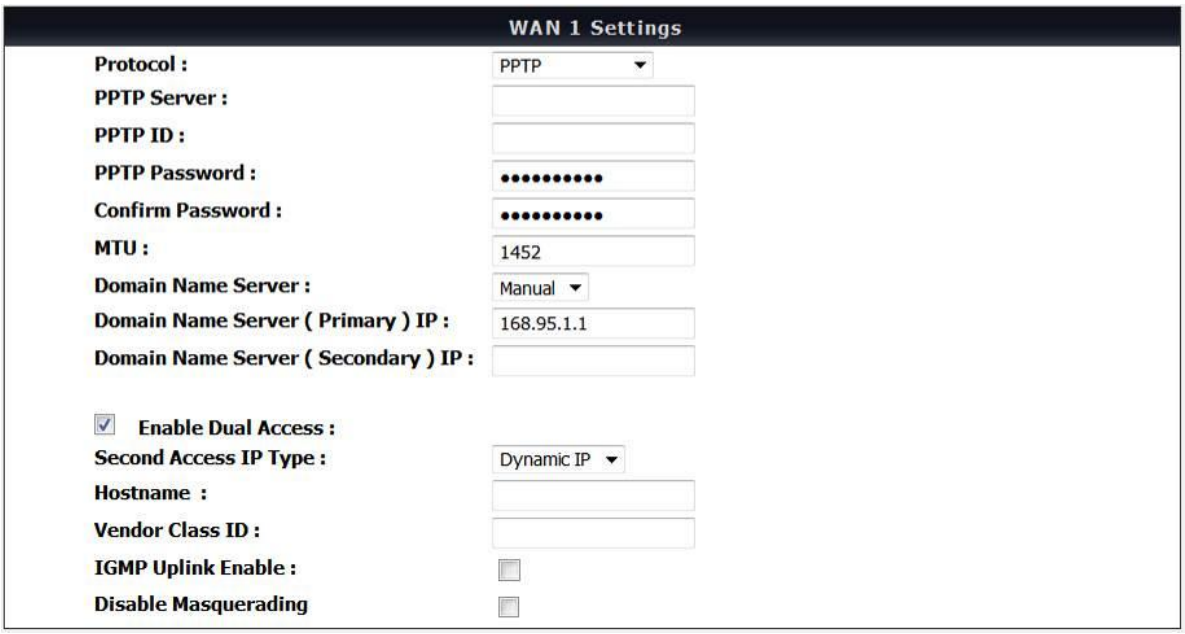
Static IP: Select this option if your ISP (Internet Service Provider) provides you a Static IP address. Enter the **IP address**, **Subnet Mask** and **Default Gateway IP**.

General Settings → WAN



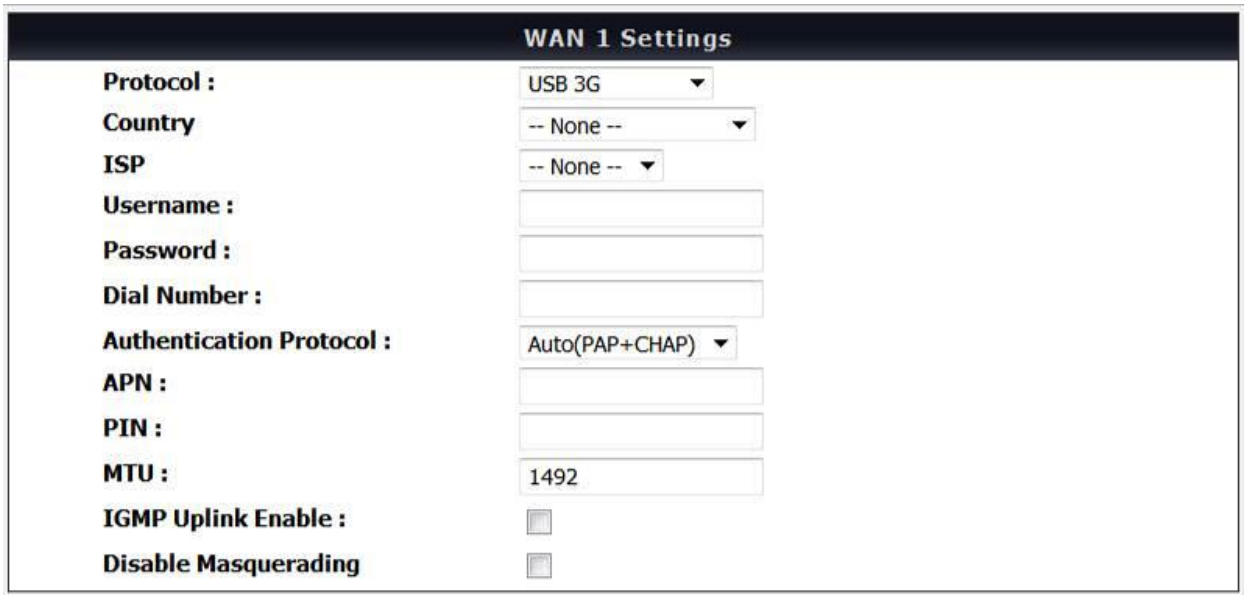
PPPoE: Select this option if your ISP requires you to use a PPPoE (Point-to-Point Protocol over Ethernet) connection. Enter the **PPPoE Account**, **PPPoE Password** and re-enter Password to confirm.

General Settings → WAN



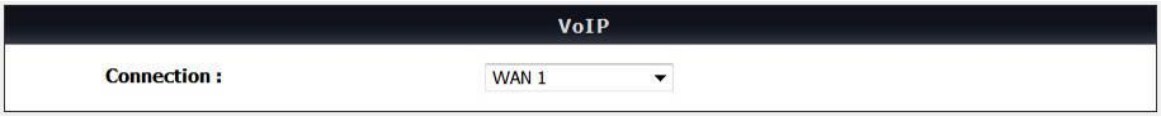
PPTP: Point-to-Point Tunneling Protocol (PPTP) is a WAN connection. Enter the **IP Address**, **Subnet mask**, **PPTP Server**, **PPTP ID** and **Password**.

General Settings → WAN



USB 3G: 3G/3.5G WISP. Enter Username, Password, Dial Number and APN to connect to Internet via 3G/3.5G WISP. Users could also select a configured WISP from the list and the gateway will fill necessary parameter automatically.

General Settings → WAN



VoIP Connection Interface: Select a WAN interface for VoIP traffic bound with as WAN 2 is enabled.

General Settings → WAN

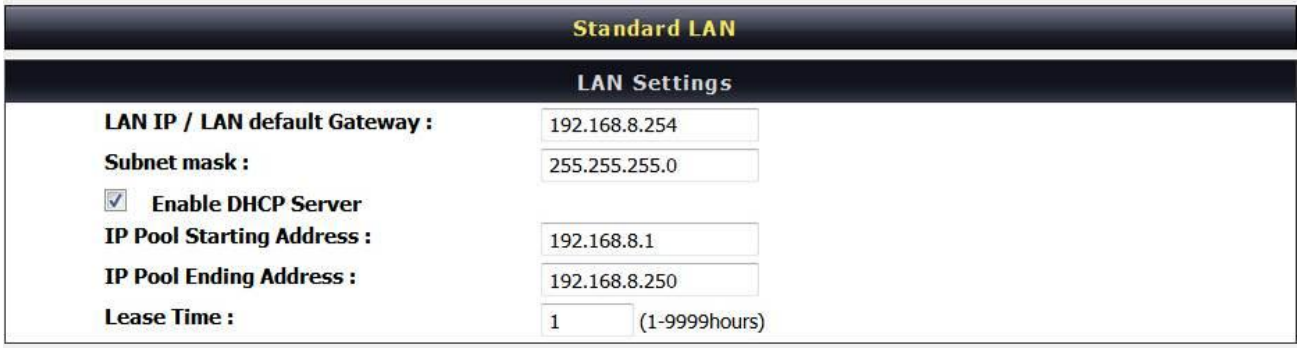
WAN Access: Check the box to enable access protocol of WAN .

General Settings → WAN

Bridge mode: check the box to set the Gateway serving as a **Bridge** between WAN port and LAN port without NAT.

2-2-3 Standard LAN

General Settings → LAN



LAN IP / LAN default Gateway: Enter the LAN IP address of the VoIP 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 VoIP 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.

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

General Settings → LAN

LAN Access: Check the box to enable access protocol of LAN.

2-2-4 Multiservice WAN

Multiservice WAN List shows the multi-WAN settings.

Multiservice WAN

WAN List

WAN	Enabled	Service	VID	Protocol	IP	DNS	Functions	Operation
1	✓	Internet		DHCP		Auto	NAPT	
2	✓	VoIP	1001	Static	192.168.1.2/255.255.255.0	168.95.1.1	NAPT	
3		UserDefined	1002	DHCP		Auto	NAPT	
4		UserDefined	1003	DHCP		Auto	NAPT	

2-2-5 Multiservice LAN

Multiservice LAN List shows the multi-LAN settings.

Multiservice LAN

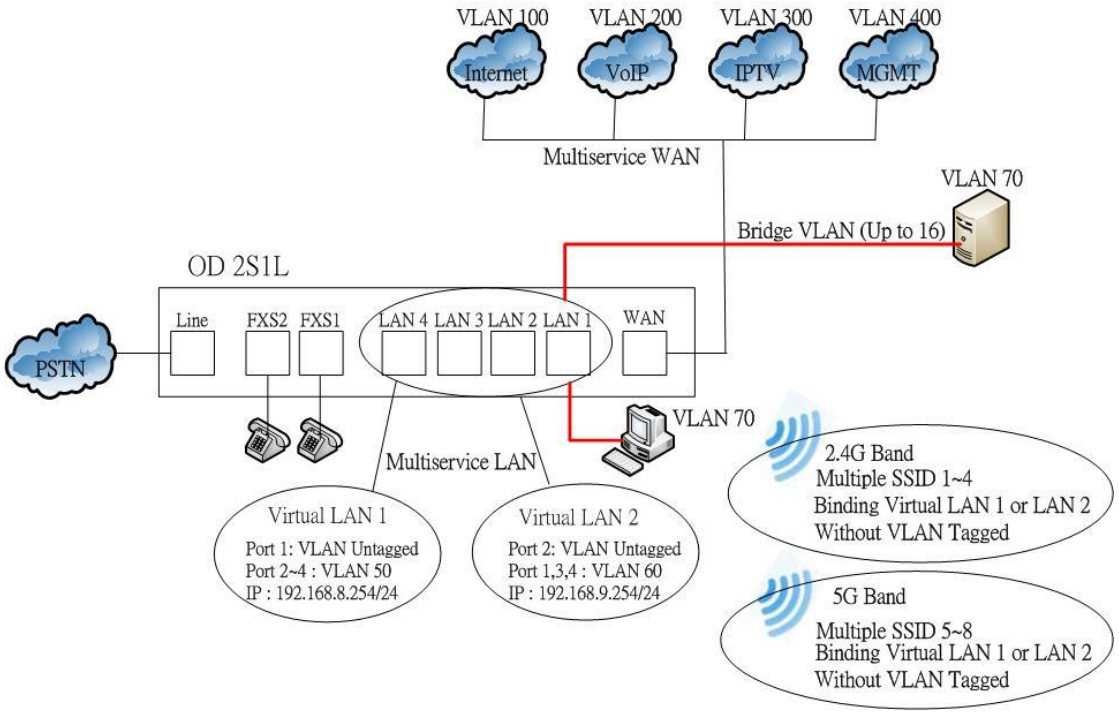
LAN List

LAN	Enabled	IP	Netmask	Port VLAN Tagging				VID	DHCP Server		Operation
				1	2	3	4		IP pool	Lease time	
1	✓	192.168.8.254	255.255.255.0	Untagged	Untagged	Untagged	Untagged		192.168.8.1 ~ 192.168.8.250	1 hour	
2			255.255.255.0	Off	Off	Off	Off		Disabled		

Below provide example for how to configure for Multiservice WAN/LAN

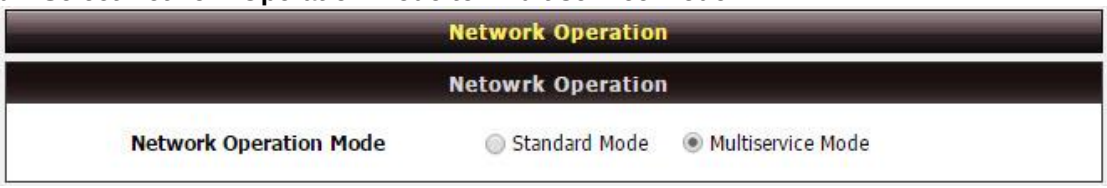
Example 1:

4 VLANs for Internet Data, VoIP, IPTV and management VLAN. And IPTV STB connected at NAT-LAN port

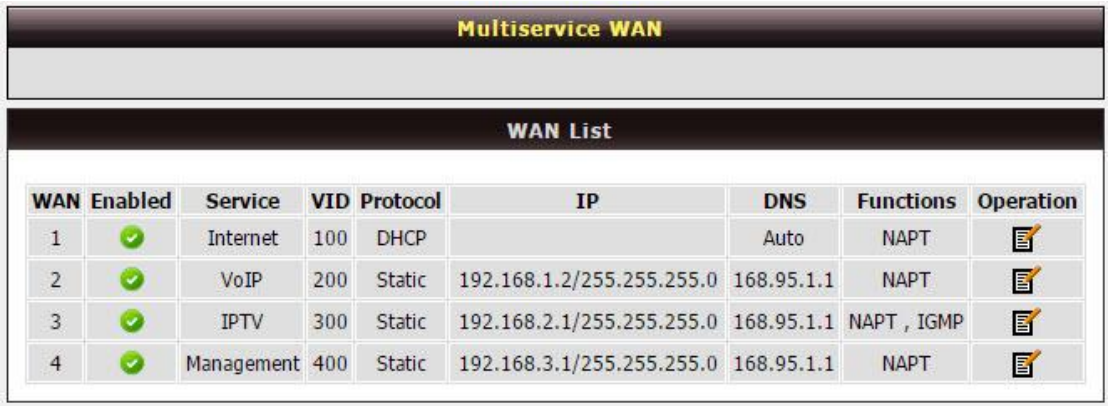


WAN setting:

Step1: Select Network Operation Mode to "Multiservice Mode"



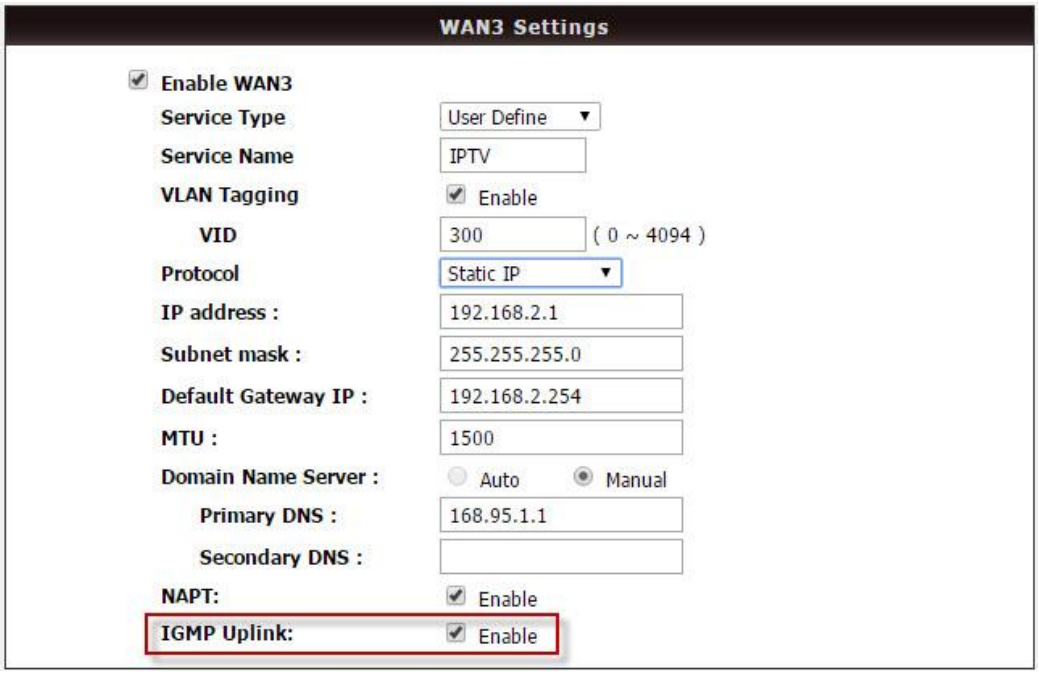
Step2: Enable Virtual WAN and Configure 4VLANs for Internet Data, VoIP, IPTV and Management VLAN



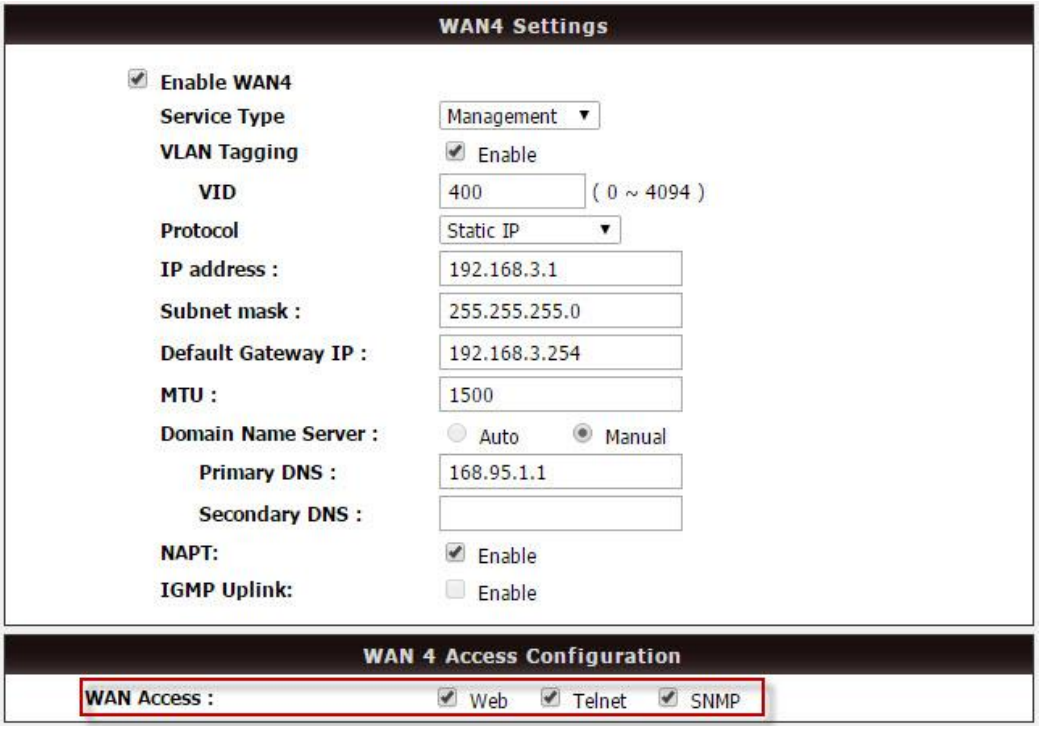
WAN	Enabled	Service	VID	Protocol	IP	DNS	Functions	Operation
1	✓	Internet	100	DHCP		Auto	NAPT	
2	✓	VoIP	200	Static	192.168.1.2/255.255.255.0	168.95.1.1	NAPT	
3	✓	IPTV	300	Static	192.168.2.1/255.255.255.0	168.95.1.1	NAPT , IGMP	
4	✓	Management	400	Static	192.168.3.1/255.255.255.0	168.95.1.1	NAPT	

2-1: Configure VALN ID 100 & 200 for Internet Data & VoIP service types

2-2: Configure VLAN ID 300 and enable "IGMP Uplink" function for IPTV service type

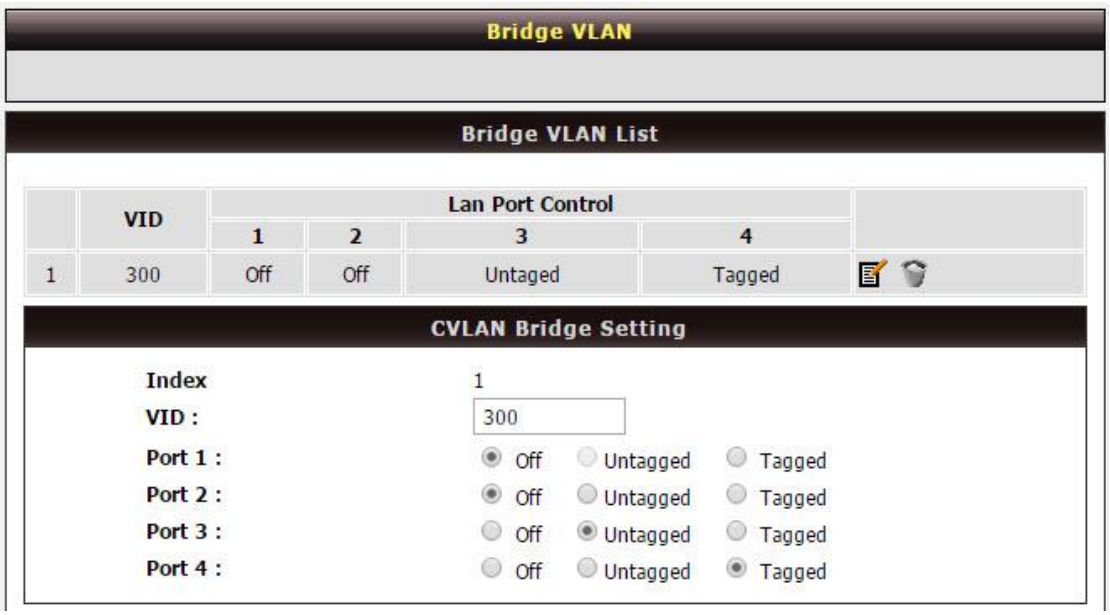


2-3: Configure VLAN ID 400 and enable WAN Access control for MGMT service type



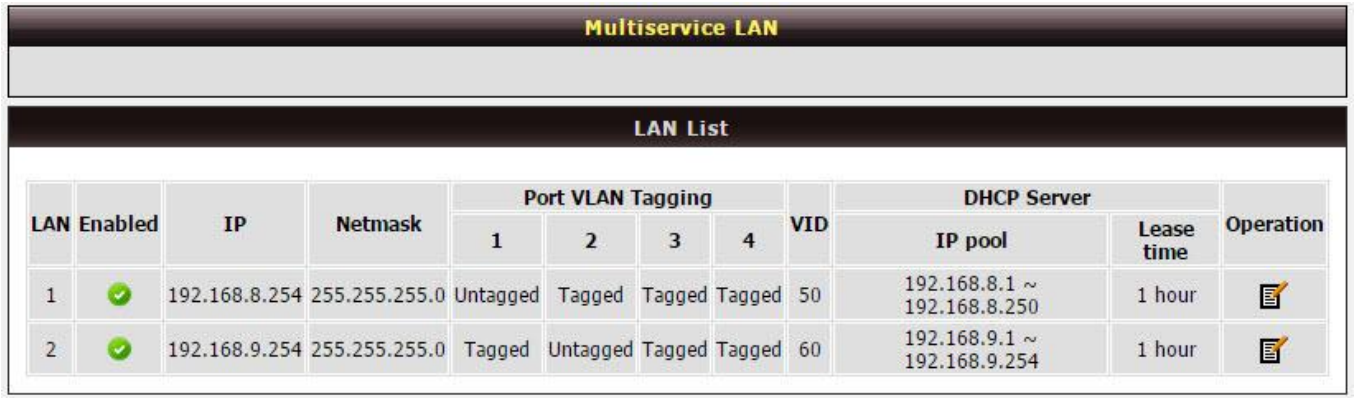
4 * VLANs for Internet Data, VoIP, IPTV and management VLAN, and IPTV STB connected at WAN-LAN bridged port

Configure Bridge VLAN ID 300 for IPTV and select LAN port to Untagged or Tagged Port



Note: Bridge VLAN can set up to 16 lists.

[LAN]: setup 2 Virtual LANs and provide configure LAN port to Untagged or Tagged with binding to different IP Pool.



Note: LAN & WAN port cannot setup to the same VLAN ID.

2-2-6 SIP

As there are various Proxy Server providers, according to RFC standard, it has designed the gateway to be compatible with them. If any registration problem occurs, please consult your Internet telephony Server Provider.

General Settings → SIP

Enable Support of SIP Proxy Server / Soft Switch: Check the box to register the VoIP Gateway with SIP proxy server or Soft Switch.

ITSP Name: Enter the name of VSP

General Settings → SIP

FXS Representative Number registers to Proxy:

Number: Enter the representative number for FXS ports. If the VoIP Gateway is configured to register with SIP proxy server, all the lines are using this number to call through SIP proxy server. It is the Caller ID for the called party when you make a VoIP call. If you register the VoIP Gateway to a SIP proxy server, then it should be the number that provided by SIP proxy server.

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

User ID/Account: User ID/Account are usually the same as Number from most SIP proxy severs.

Password: Enter password and re-enter to confirm.

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

General Settings → SIP

Each line registers to Proxy independently:

Line

Line	Type	Number	Hunt Group Port	Register	Invite with ID / Account	User ID / Account	Password and Confirm Password
FXS Representative Number				☐			••••••••• •••••••••
1	FXS	0912345678 auto	No Group	☑	☑	0912345678	••••••••• •••••••••
2	FXS	0922345678	No Group	☑	☑	0922345678	••••••••• •••••••••

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 VoIP Gateway to a SIP proxy server, then it should be the number that 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.

Hunt Group Port: It allows operators to assign multi lines for a hunting group

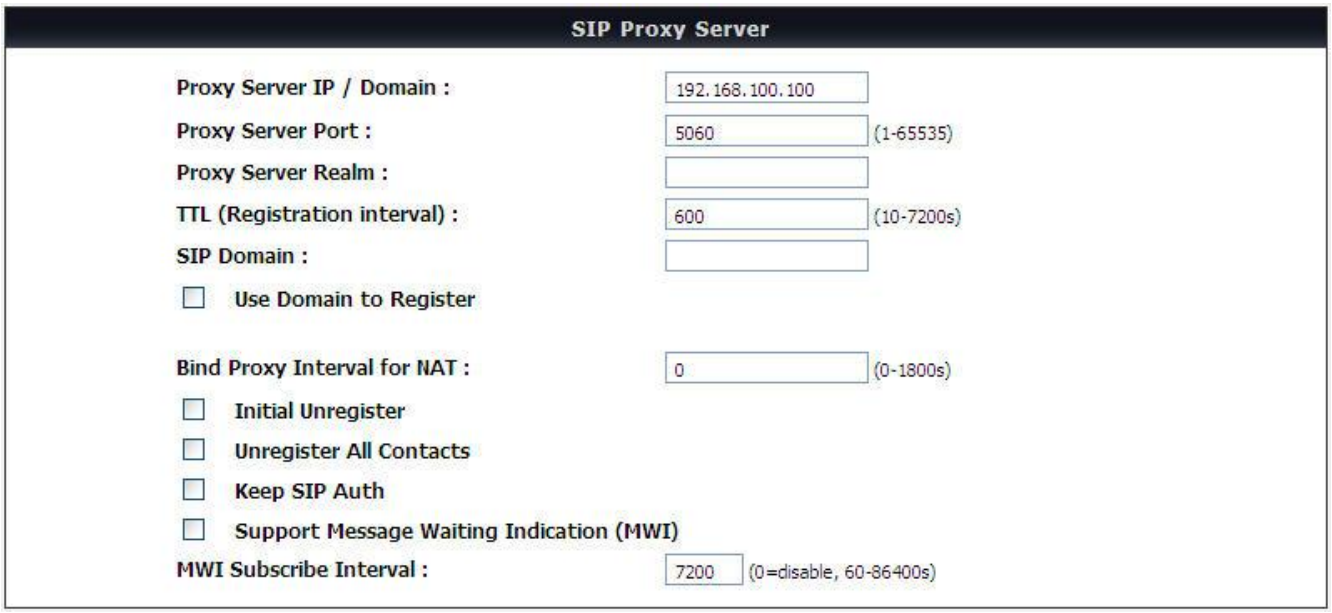
Register: Check the box to register with SIP proxy server.

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.

User ID/Account: User ID/Account is usually the same as Number from most SIP proxy severs.

Password: Enter password and re-enter to confirm.

General Settings → SIP



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 VoIP 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 in.

TTL (Registration interval) [10-7200 s]: The interval for VoIP Gateway re-report to SoftSwitch.

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

Bind Proxy Interval for NAT: Check the box to keep the binding exist by sending packets when the VoIP 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 VoIP Gateway and then it will perform a general register process.

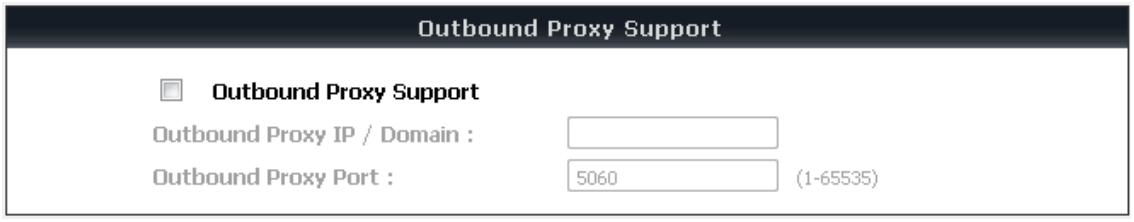
Unregister All Contacts: VoIP Gateway sends un-register request to SoftSwitch which the contact field filled with a start sign (*) to un-register all FXS in this VoIP Gateway.

Keep SIP Auth: VoIP Gateway keeps the last register SIP MD5 authentication information and re-use it for next register request.

Support Message Waiting Indication (MWI): It is used to enable/disable Message Waiting Indication. It is available only when Voice Mail Service is available from the VoIP Service Provider.

MWI Subscribe Interval: It is used to set the subscribe time for the VoIP Gateway to check the voice mail.

General Settings → SIP



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 VoIP Gateway to send and receive all SIP packets to the destined outbound proxy server rather than the remote VoIP device. 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.

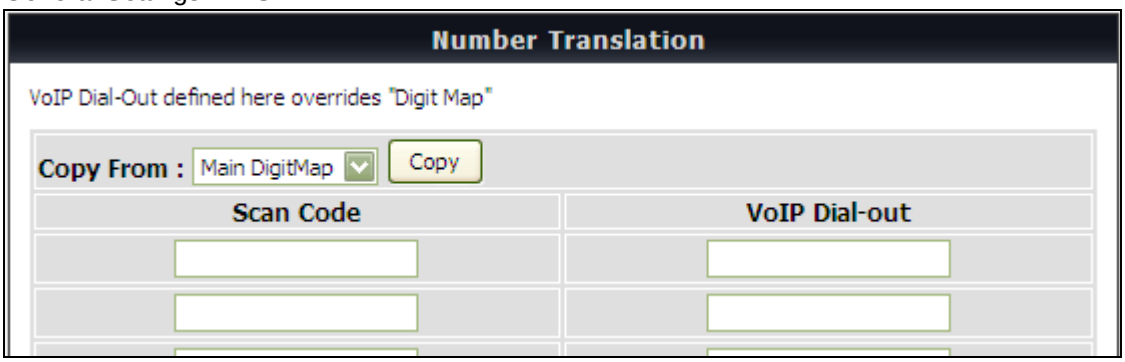
Outbound Proxy Port: Enter the outbound proxy's listening port.

General Settings → SIP

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'.

General Settings → SIP



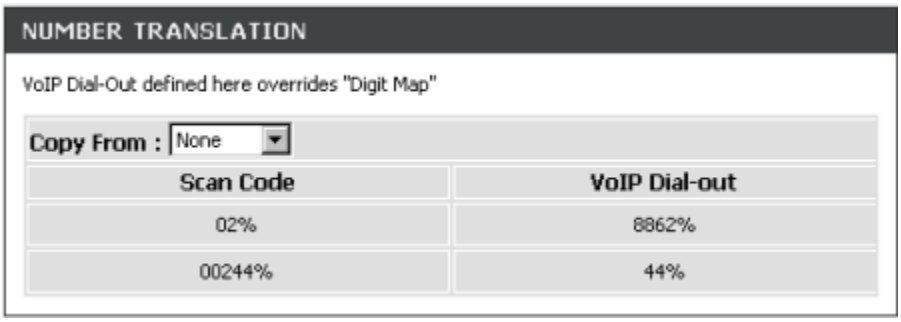
The rule of dialing of inviting to VoIP Service Providers may vary. That is, you have to configure different Digit Map for different VoIP Service Providers. In this filed, you can configure individual dialing plan for each VoIP Service Provider. The following examples introduce some cases. For general configuration, refer to **Digit Map** page. **Note: Press "Add" to add an entry. Don't forget to press "Apply" which in the above of Number Translation.**

For example (Example in Taiwan)**,**

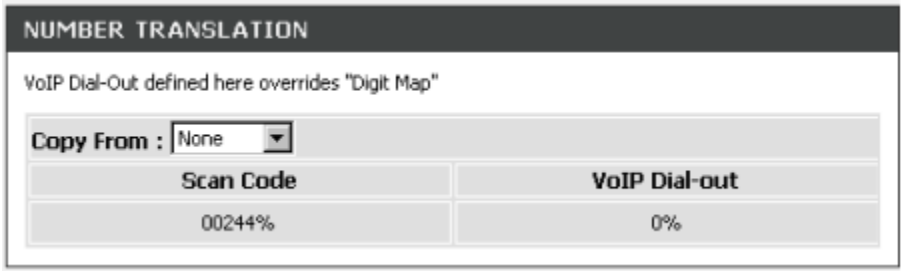
If Server 1 is local VoIP Service Provider you can refer to **Digit Map** page for general settings.

If Server 2 is global VoIP Service Provider (VoIP STUN, free to dial to some cities free charge) you can set individual dialing plan for VoIP STUN in **Number Translation** field. **Scan Code** can be your dialing custom, and **VoIP Dial-out** is the number on the basis of the dialing rule needed by VoIP STUN. Its dialing rule is Country code + Area Code + phone number. When you make calls to Taipei through VoIP STUN, you don't change the dialing custom, just dial 02xxxxxxxx, and the system will change the number from 02xxxxxxx to 8862xxxxxxxx. The same rule is for #2. When you make calls to UK via VoIP STUN, you'll dial 00244xxxxxx, and the system will change it to 44xxxxxx.

The settings for Server 2 appear like:



If Server 3 is a VoIP Service Provider in UK, you can set individual dialing plan in **Number Translation** field. As you make calls to UK through this VoIP Service Provider, "Country code" should be removed and plus "0" by the system. The settings for Server 3 appear like:



2-2-7 SIP Advanced

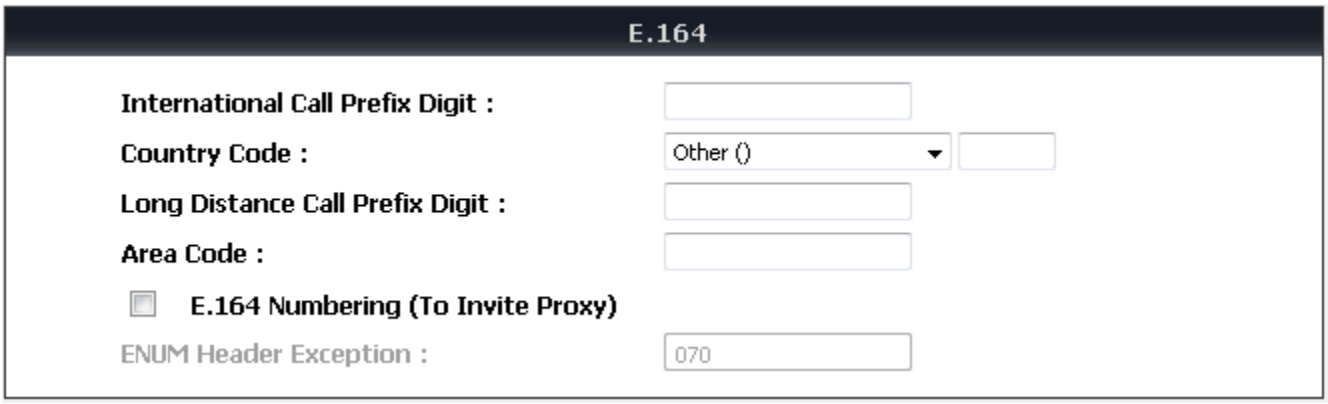
General Settings → SIP Advanced

Listen Port UDP: Enter the VoIP 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.

SIP Transport Protocol: UDP or TCP

General Settings → SIP Advanced



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.

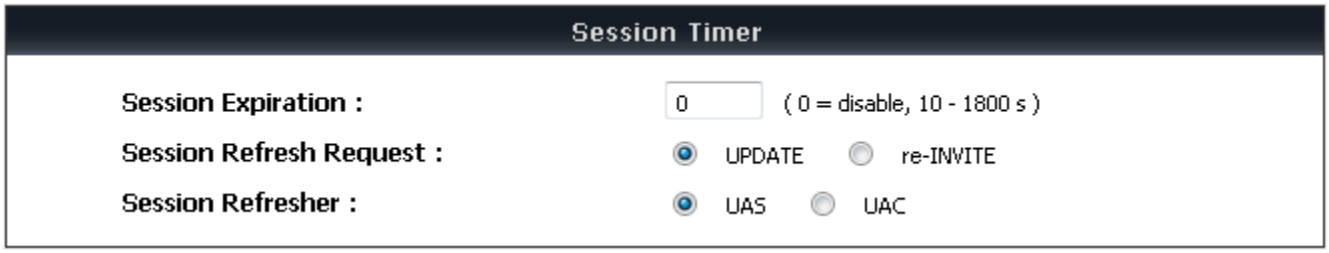
Area Code: Enter the area code.

E.164 Numbering(To Invite Proxy): This variable is followed the E.164 rule, but it depends on the SIP proxy server. Click the check box to send the number following the E.164 rule by the VoIP Gateway.

ENUM Header Exception: Enter the prefix number that the VoIP 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.

General Settings → SIP Advanced



Session Expiration: This field will set the time that the VoIP 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.

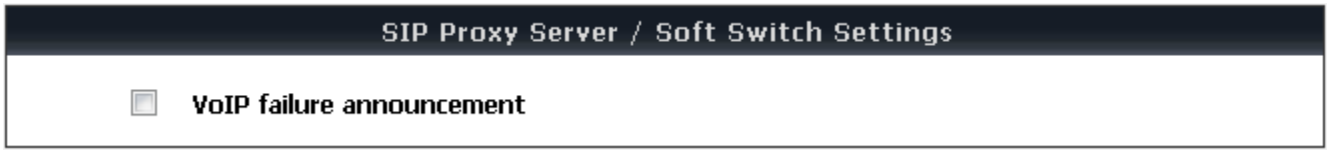
Session Refresher: This determines which side of an expired call session will initiate the session refresh. uac – specifies that the Caller side will initiate the session refresh. uas – specifies that the Call receiver (the "Callee") will initiate the session refresh.

General Settings → 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.

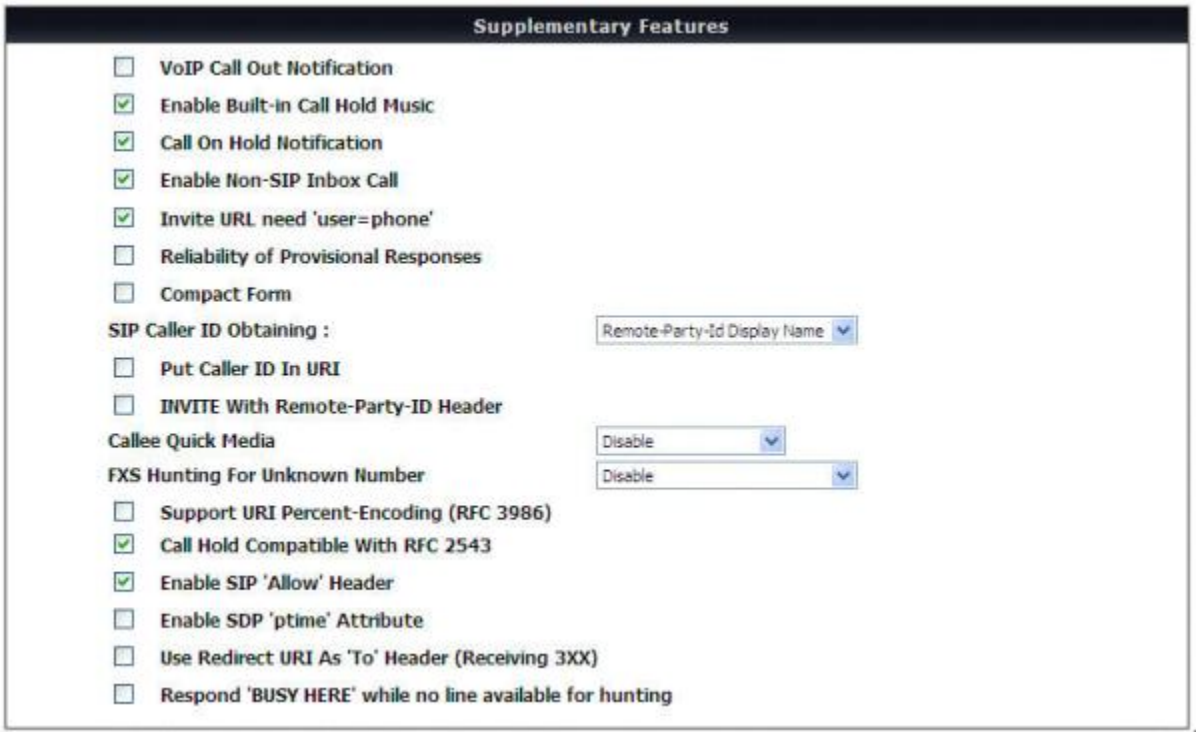
Max. Response Time for Invite: Enter the maximum response time for INVITE packet. When the destination does not reply within the set time, the call is failed.

General Settings → SIP Advanced



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

General Settings → SIP Advanced



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.

Call On Hold Notification: FXS will send alert to phone set as users hang up if there is a call still held in another line.

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.

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, i.e. 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 Caller ID Obtaining: Select the part of the SIP packet from the VoIP 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 way is in SIP → Message Header → From → SIP Display info.

From-Header User Name - It locates at SIP -> Message Header -> From -> SIP from address before [@].

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.

Callee Quick Media: VoIP Gateway will send RTP to remote party immediately as user answer an inbound call.

FXS Hunting For Unknown Number: Select the response for an incoming call which the called number is not exist in on the VoIP Gateway.

Disable –VoIP Gateway responses 404 not found.
Hunt and Transit Dial –VoIP Gateway sends alert to an available FXS port and dial the number to PBX as the FXS port picked up by PBX. It works with SoftSwitch or IPPBX to allow a remote client reach the PBX extension for one step dial. (For virtual extension)
FXS Group Hunting/ Ring Type -- VoIP Gateway sends alert to an available FXS port for hunting group.

Enable SIP "rport"(RFC 3581): ATA puts "rport" in SIP packets for SoftSwitch to deal well as ATA put under NAT.

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.

Call Hold Compatible With RFC 2543: It is used to set the procedure of Call Hold being compatible with RFC 2543.

Enable SIP 'Allow' Header: It is used to put "Allow" in SIP packets. The Allow header field lists the SIP requests supported by ITA when ticked.

Enable SDP 'ptime' Attribute: It is used to put "ptime" in SDP packets when ticked.

Use Redirect URI As 'To' Header (Receiving 3XX): It is used to change the content of 'To' header field when receiving 3XX.

Respond 'BUSY HERE' while no line available for hunting: It is used to reply 'BUSY HERE' to the calling party while no line is available for hunting.

2-2-8 Caller ID

General Settings → Caller ID

FXS Caller ID Generation:

DTMF – Sending Caller ID in DTMF signaling.

FSK – Sending Caller ID in FSK signaling.

FSK + TypeII – Send Caller ID in FSK signaling. As the phone set supports Call Waiting Caller ID that FXS will send third party's number.

Send Caller ID After the First Ring:

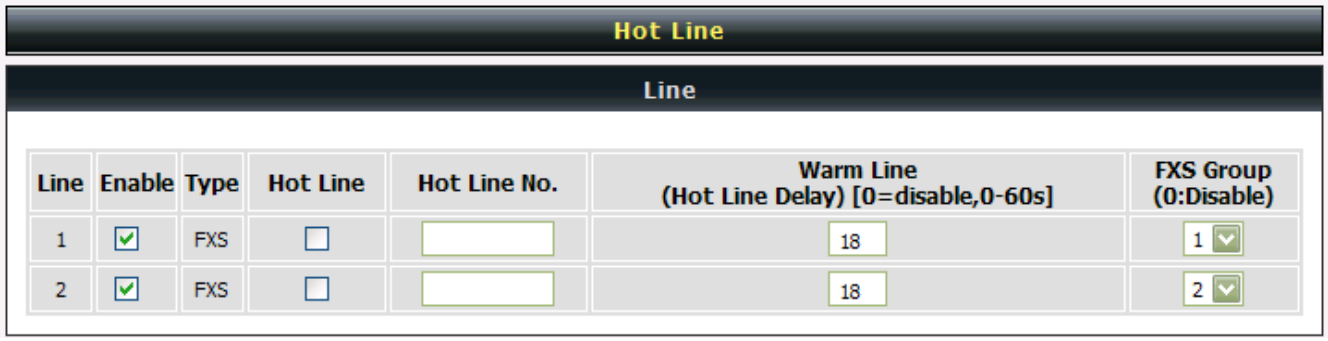
Un-Ticked – FXS sends Caller ID before the first ring. Usually it is used in DTMF mode.

Ticked – FXS sends Caller ID between the first and second ring. Usually it is used in FSK mode.

FSK Caller ID Type: Either Bellcore, ETSI or NTT could be selected.

2-2-9 Hot Line

General Settings → Hot Line



Enable: Tick the check box to enable a line. If some lines are not used, disable them (Pause Function) to avoid unnecessary waiting when an incoming call is diverting to the line.

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

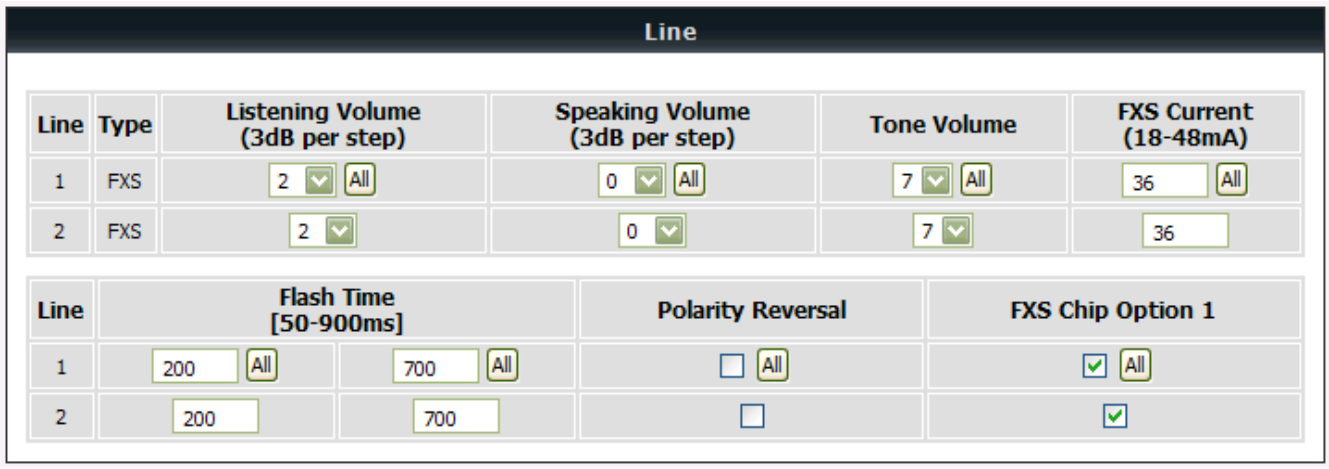
Hot Line No.: Enter the number for pre-defined destination.

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.

FXS Group: When there is an incoming call and the gateway will automatically assign an unassigned call according to the Hunting Priority. If Port 2 does not want to be set as an assigned line to receive any inbound calls, the function can be disabled.

2-2-10 Line settings

General Settings→ 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 VoIP Gateway including Dial Tone, Ring Back Tone and Busy Tone.

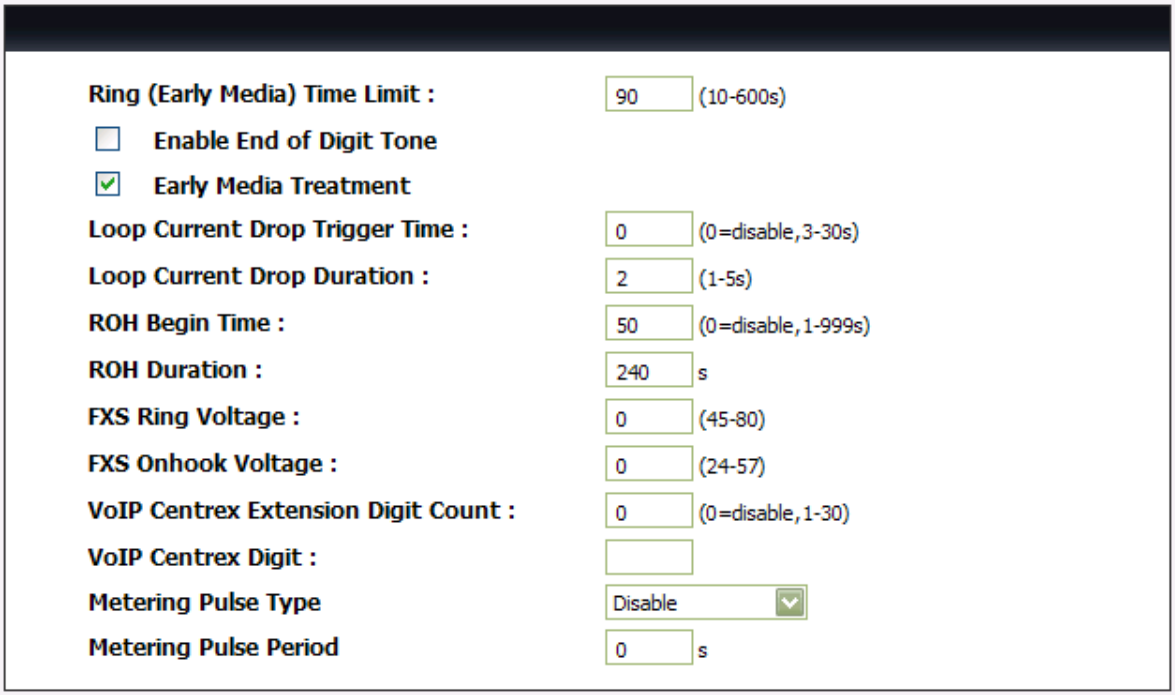
FXS Current: Set the output D.C. current of FXS port.

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.. 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.

Polarity Reversal: Check the box to activate the generation of polarity reversal from FXS.

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.

General Settings→ 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.

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.

ROH Begin Time: As users forget hang up phone set it makes FXS play loud Howler Tone to notify users put hand set correctly. If this timer is set to be 20 seconds that FXS play busy tone for 20 seconds then play ROH.

ROH Duration: It is the maximum time for FXS play ROH, then FXS will stop play ROH and keep silence.

FXS Ring Voltage: It is to set the Ring Voltage of FXS.

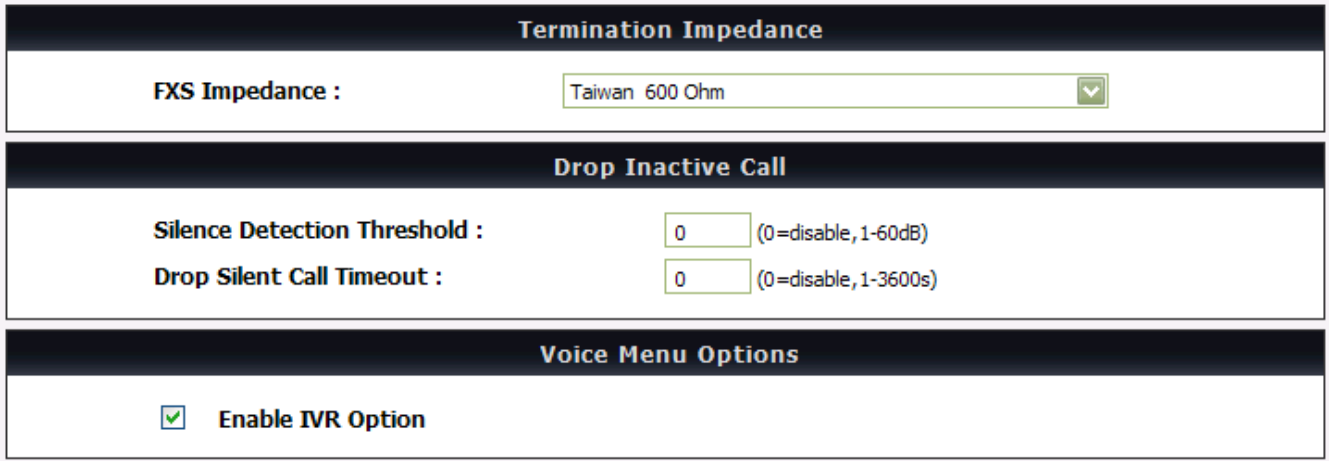
FXS Onhook Voltage: It is to set the Onhook Voltage of FXS.

VoIP Centrex Extension Digit Count: This feature is to enable and set the digit count of VoIP Centrex. The setting "0" zero is to disable this function.

VoIP Centrex Digit: Enter the digit for VoIP call. If you dial VoIP Centrex Digit first, the dialing plan is according to the Digit Map; otherwise the VoIP Gateway will send the number which digit count is the same as VoIP Centrex Extension Digit Count.

Metering Pulse Type/ Metering Pulse Period: It is used for telephony device which connected to FXS port for billing purpose. **VoIP Gateway provide Polarity Reversal、 12k Hz and 16k Hz metering capacity. The fully support for detail Metering Pulse Period is not free charge, please contact with your vendor.**

General Settings→ Line settings



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

Drop Inactive Call: This feature is a call drop standard for a VoIP Gateway to determine whether or not to hang up the phone. The VoIP 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 IP network.

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

Enable IVR Option: Check the box to enable IVR function.

General Settings→ Line settings

Hunting/Ring: It is used to set FXS group hunting mode. There are **Hunting**, **Simultaneous Ring** and **Sequential Ring**.

Hunting: When someone calls in by dialing FXS representative number, the system will always assign the call to the first line.

Simultaneous Ring: When someone calls in by dialing FXS representative number, all FXS ports will ring at the same time.

Sequential Ring: When someone calls in by dialing FXS representative number, the system will assign the call to each FXS ports in order according **Sequential Ring Time**. You can adjust **Sequential Ring Time** for the ring time of each port.

2-2-11 FAX

General Settings → FAX

Disable: Select it if you are not sending fax, but it is still accepted fax by the VoIP 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 VoIP 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 VoIP Gateway won't accept T.38 for fax transmission.

T.38 Native: Select it if you are only using T.38 for fax transmission.

T.30 V.152: As GW detect FAX tone, it will change RTP codec to be T.30 codec directly without sending Re-Invite to change codec.

Note: When a fax tone is detected from the call, the VoIP 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.

General Settings → FAX

Switch FAX On CED Detection：VoIP Gateway will send FAX Re-Invite immediately as it detect FAX CED tone, that will save handshaking time between FAX machines.

Restrict T.38：VoIP Gateway will reject T.38 Re-invite in case the FAX type contains without T.38.

FAX Detection Sensitivity：To set higher value to make VoIP Gateway to be more sensitive.

General Settings → FAX

High Speed Redundancy：Set redundancy packets for FAX image. It could repair FAX image for non-continuous packets lost. The higher redundancy the higher bandwidth required.

Low Speed Redundancy：Set redundancy packets for FAX handshaking signaling.

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

T.30 Bypass Payload Type: Fill correct payload type of T.30 bypass method.

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.

Function	Fax Detection	Content of SDP of re-INVITE	Receive re-INVITE with T.38
Disable	No	N/A	Accept and change RTP to T.38
T.38 Fax	Yes	re-INVITE with T.38 and T.30	Accept and change RTP to T.38
T.30 Fax	Yes	re-INVITE with T.30	Accept and change RTP to T.38
T.30 Fax/Modem	Detect CED only	re-INVITE with T.30	Accept and change RTP to T.38
T.30 Only	No	N/A	Accept and change RTP to T.38
T.38 Native	Yes	re-INVITE with T.38	Accept and change RTP to T.38
T.30 V.152	Yes	N/A	Accept and change RTP to T.38

2-2-12 Calling Features

General Settings → 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.

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.

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..

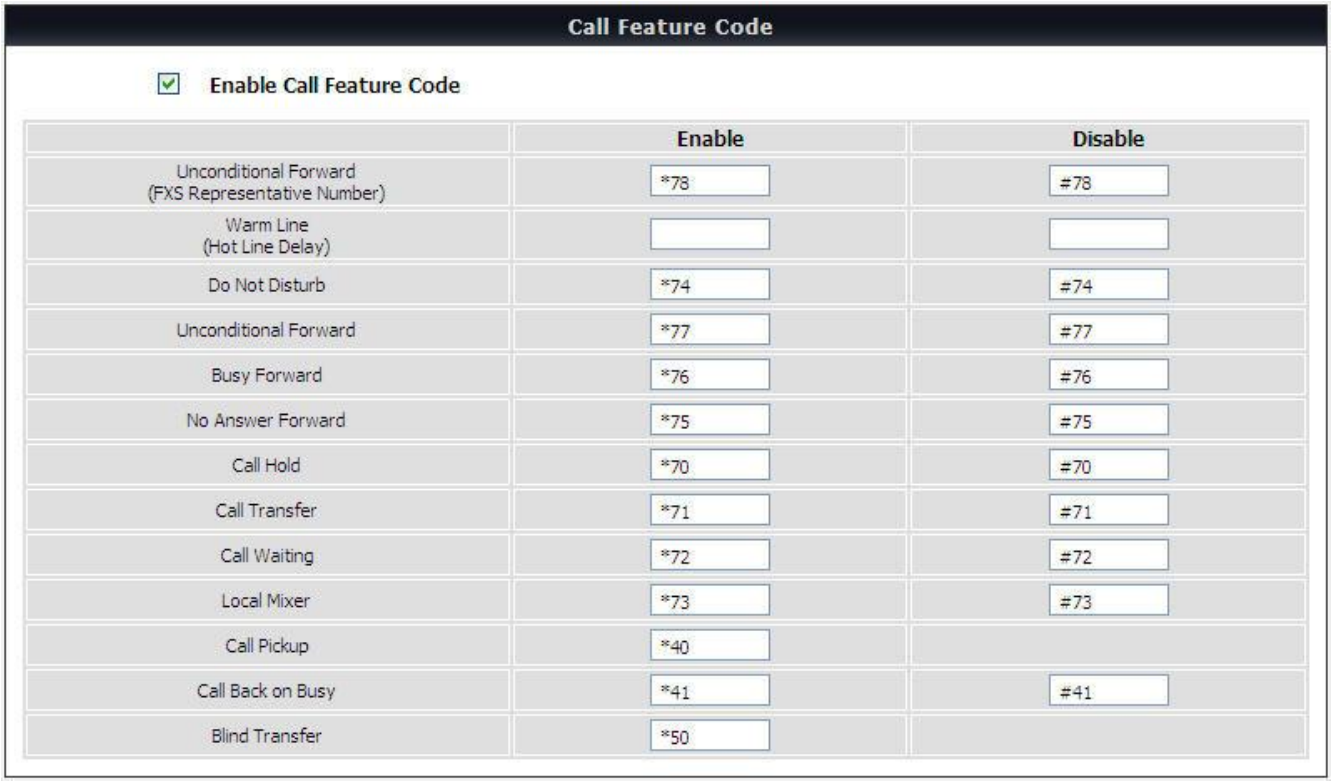
Call Transfer: Check the box to transfer the call to another destination.

Call Waiting: Check the box to accept incoming call while talking.

Three-Way Calling /Service ID: It is for conference all based on Nortel Soft Switch and must work with Proxy Server that supports Three-Way Calling service.

Local Mixer: It is used to enable build-in conference service when ticked.

Enable Call Feature Code



Call Feature Code

☑ **Enable Call Feature Code**

	Enable	Disable
Unconditional Forward (FXS Representative Number)	*78	#78
Warm Line (Hot Line Delay)		
Do Not Disturb	*74	#74
Unconditional Forward	*77	#77
Busy Forward	*76	#76
No Answer Forward	*75	#75
Call Hold	*70	#70
Call Transfer	*71	#71
Call Waiting	*72	#72
Local Mixer	*73	#73
Call Pickup	*40	
Call Back on Busy	*41	#41
Blind Transfer	*50	

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

Calling Feature Instructions:

Call Hold: The call will be held after the FLASH button is pressed on the phone set. The VoIP Gateway will play music on hold (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 VoIP 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 VoIP Gateway must support FLASH features in order to use this function. If a phone set is connecting directly to the FXS port of the VoIP 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 presses Flash to start the conference call.
   Or
4. Phone1 dials to Phone2, Phone2 answers the call.

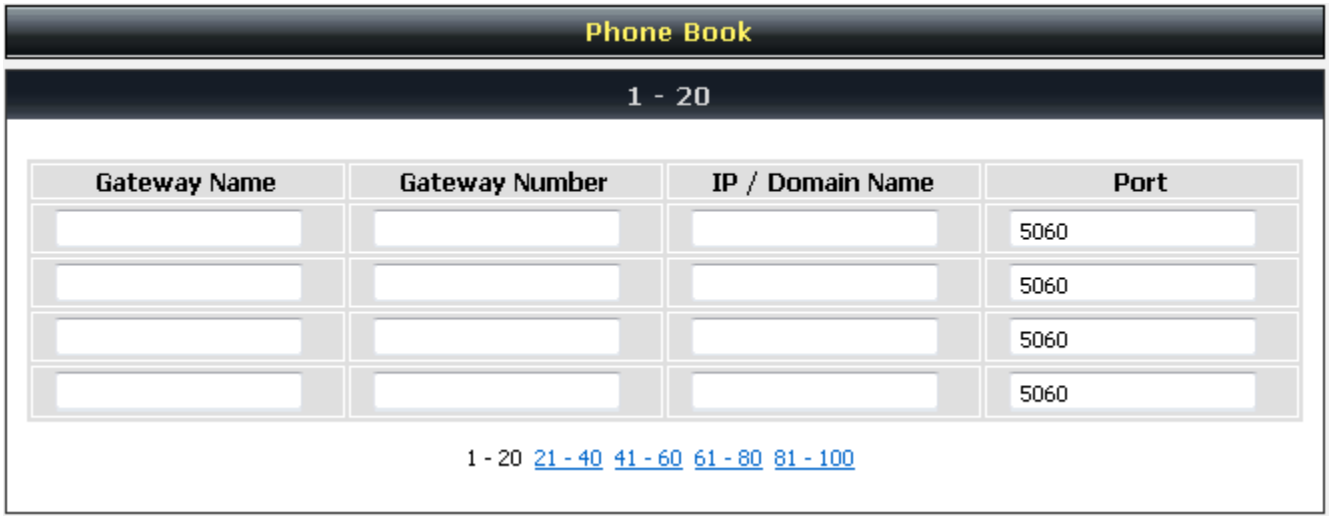
5. Phone1 presses Flash then calls Phone3 (Phone2 is on hold) and Phone3 answers the call.
6. Phone1 presses Flash and dial 3 to start the conference call.

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

2-2-13 Phone Book

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.

General Settings → Phone Book



Gateway Name: Enter the alias of the remote peer.

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

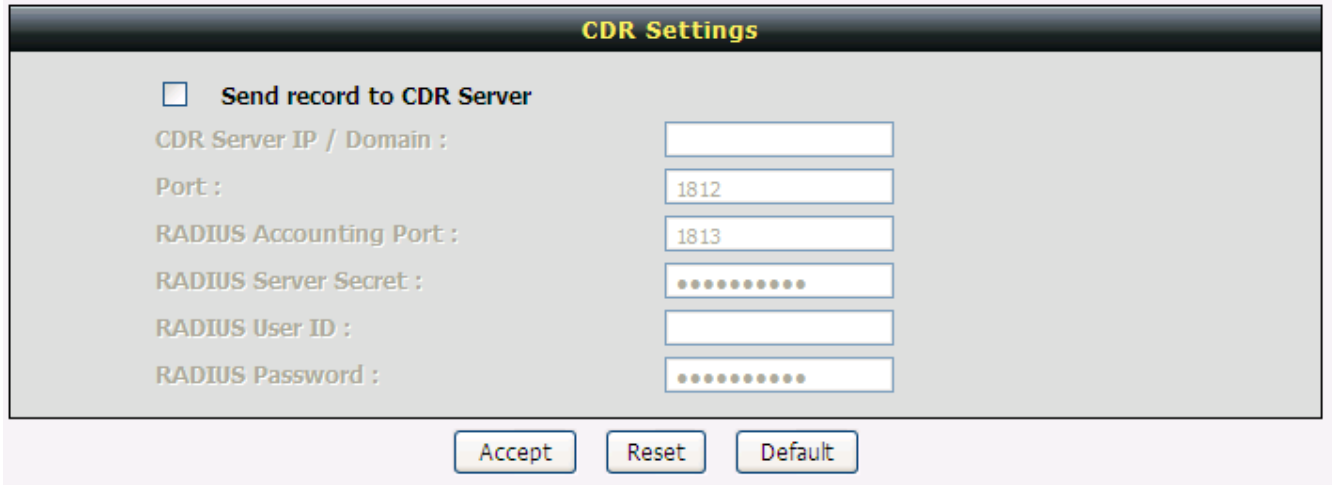
IP / Domain Name: Enter the IP address or URL (Uniform Resource Locator) of the remote peer.

Port: Enter the listen port of the remote peer.

2-2-14 CDR Settings

The user can set up a CDR Server to record call details for every phone call.

General Settings → CDR



Send record to CDR Server: Tick the check box to enable the call detail recording.

CDR Server IP / Domain: Enter the IP address of the CDR server.

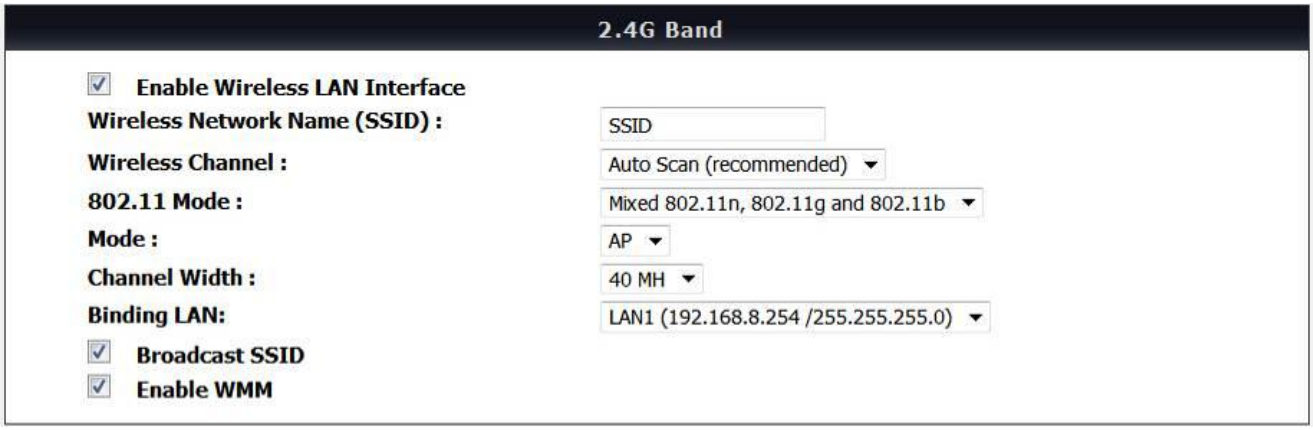
Port: Enter the listen port of the CDR server.

RADIUS: Tick the checkbox to enable RADIUS as database and enter the information of RADIUS needed. It includes RADIUS Accounting Port, RADIUS Server Secret, RADIUS User ID and RADIUS Password.

2-3 Wireless Settings

2-3-1 Basic Settings

Wireless Settings → Basic Settings



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

Wireless Network Name (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.

Wireless Channel: 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.

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

802.11b only - Allow all 802.11b compliant wireless devices to associate with the wireless AP.

802.11g only - Allow all 802.11g compliant wireless devices to associate with the wireless AP.

802.11n only - Allow all 802.11n compliant wireless devices to associate with the wireless AP.

Mixed 802.11g and 802.11b - Allow a mix of both IEEE802.11g and 802.11b compliant wireless devices to associate with the wireless AP.

Mixed 802.11n and 802.11g - Allow a mix of both IEEE802.11n and 802.11g compliant wireless devices to associate with the wireless AP.

Mixed 802.11n, 802.11g and 802.11b - Allow a mix of both IEEE802.11n, 802.11g and 802.11b compliant wireless devices to associate with the wireless AP.

Mode: The VoIP Gateway has ability to serve as four operating modes in wireless network separately.

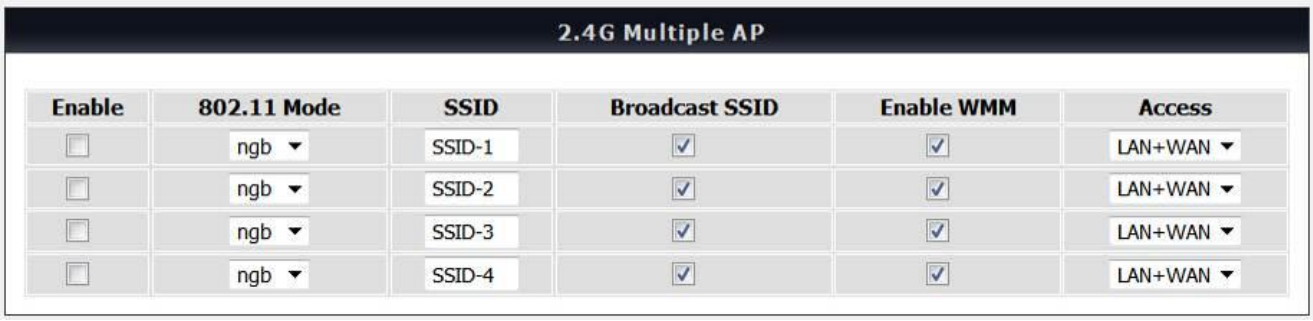
AP: As a wireless AP that allows wireless-equipped stations to communicate with a wired network and the other wireless network for Internet access and resources sharing.

Channel Width: Wireless channel width for 802.11n. Select 40 MH for higher speed.

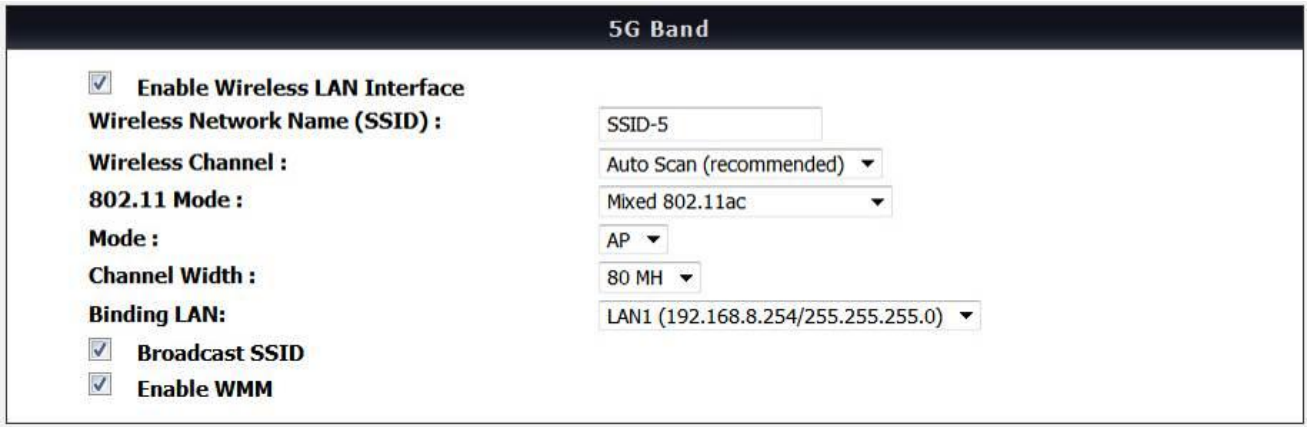
Broadcast SSID: Broad AP's SSID for convent usage. To hid SSID for more security.

Enable WMM: Wi-Fi Multimedia. It provides higher priority for multimedia stream to get better quality.

Wireless Settings → Basic Settings



Multiple AP: It is used for different level of clients. Such as different departments or guests. And you could assign different password for each SSID.



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

Wireless Network Name (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.

Wireless Channel: 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.

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

802.11a only - Allow all 802.11a compliant wireless devices to associate with the wireless AP.

802.11n only - Allow all 802.11n compliant wireless devices to associate with the wireless AP.

Mixed 802.11a and 802.11n - Allow a mix of both IEEE802.11a and 802.11n compliant wireless devices to associate with the wireless AP.

Mixed 802.11ac - Allow a mix of both IEEE802.11ac compliant wireless devices to associate with the wireless AP.

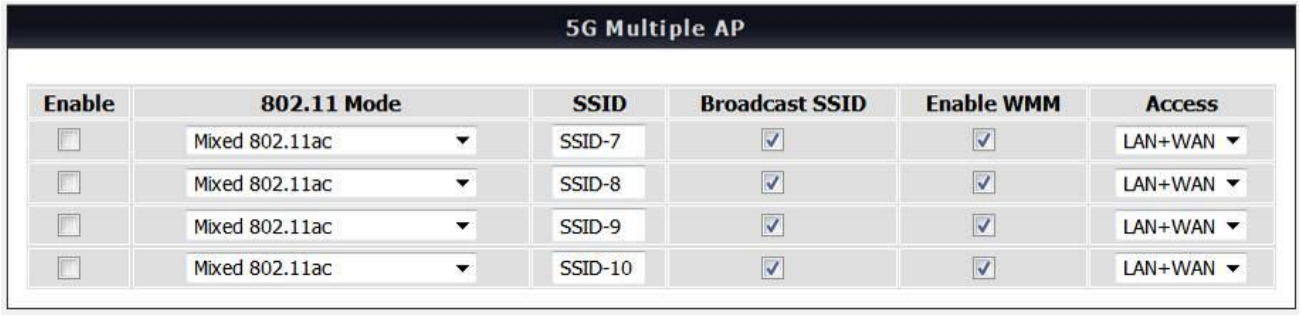
Mode: The VoIP Gateway has ability to serve as four operating modes in wireless network separately.

AP: As a wireless AP that allows wireless-equipped stations to communicate with a wired network and the other wireless network for Internet access and resources sharing.

Channel Width: Wireless channel width for 802.11ac. Select 80 MH for higher speed.

Broadcast SSID: Broad AP's SSID for convent usage. To hid SSID for more security.

Enable WMM: Wi-Fi Multimedia. It provides higher priority for multimedia stream to get better quality.



2-3-2 Advanced Settings

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 Settings

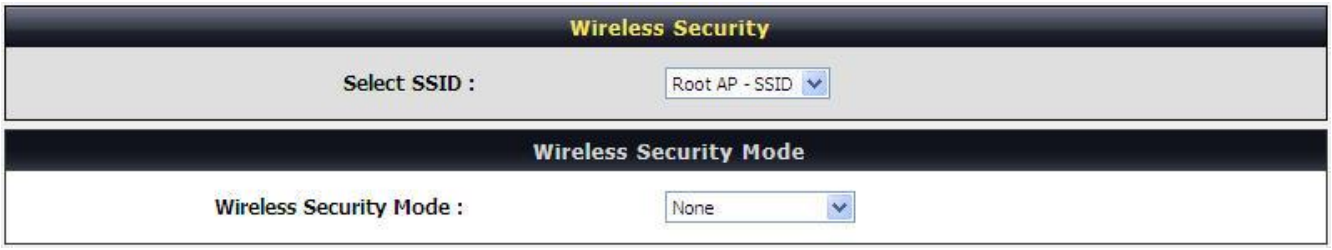
Fragmentation: A packet can be fragmented into small units to pass over a network medium that can not support the original packet size. If you encounter a busy network, a lower value of Fragment Threshold could improve performance. If the traffic flows are not very busy, a higher Fragment Threshold provides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

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

2-3-3 Security Settings

Wireless Settings → Security Settings



Select SSID: Select an SSID to configure wireless security mechanism.
Security Mode: Select the encryption/authentication type: None, WPA, WPA2 and WPA / WPA2 Mixed.

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

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

WPA Authentication Mode: Select **Personal (Pre-Shared Key).**

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 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.

Wireless Settings → Security Settings

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

WPA Authentication Mode: Select **Enterprise (RADIUS).**

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.

RADIUS Server:

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.

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

RADIUS server key - Enter the password such as a security Key.

2-3-4 Access Control

Wireless Settings → Access Control

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

Comment: The space is reserved for comment or notation.

2-3-5 WPS

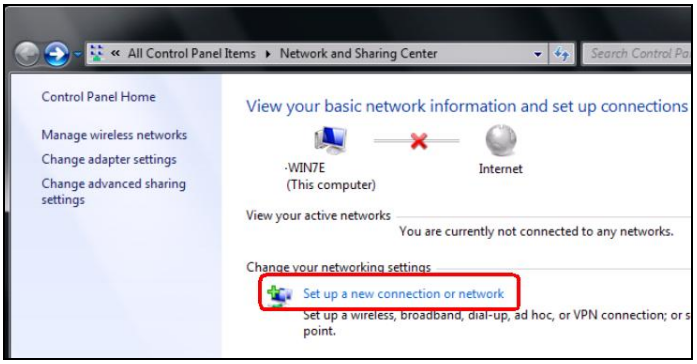
Wireless Settings → WPS

It allows users establish wireless connect between VoIP Gateway and computers via WPS(Wireless Protect Setup) method.

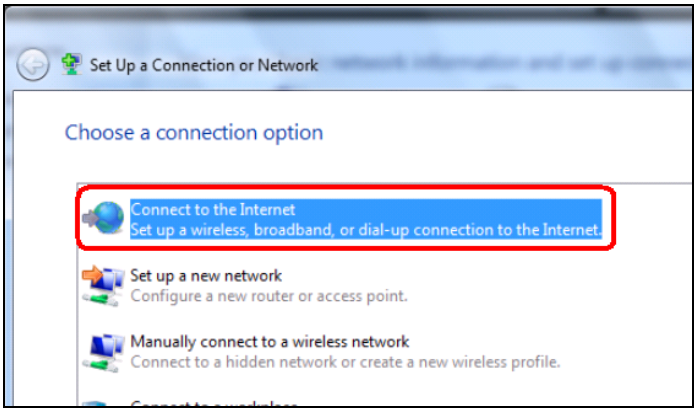
Example for setting Wireless profile via WPS method on Windows 7.

Enter [Network and Sharing Center]

Click [Set up a new connection or network]

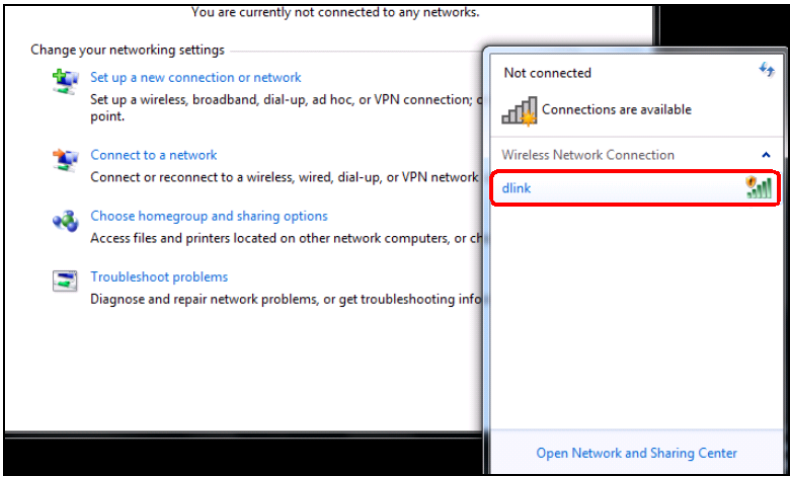


Click [Connect to the Internet]

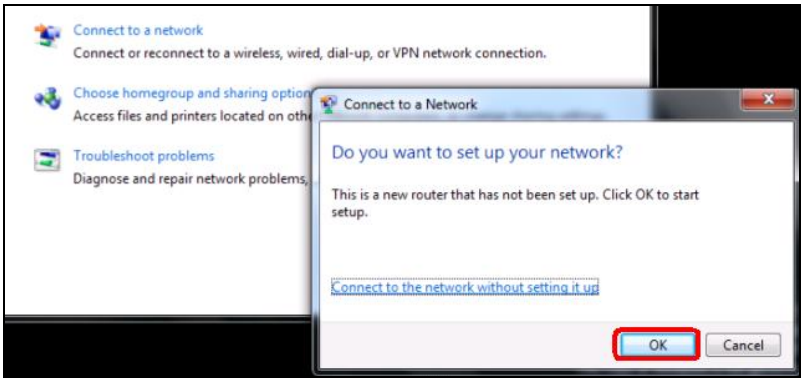


Click [Wireless]

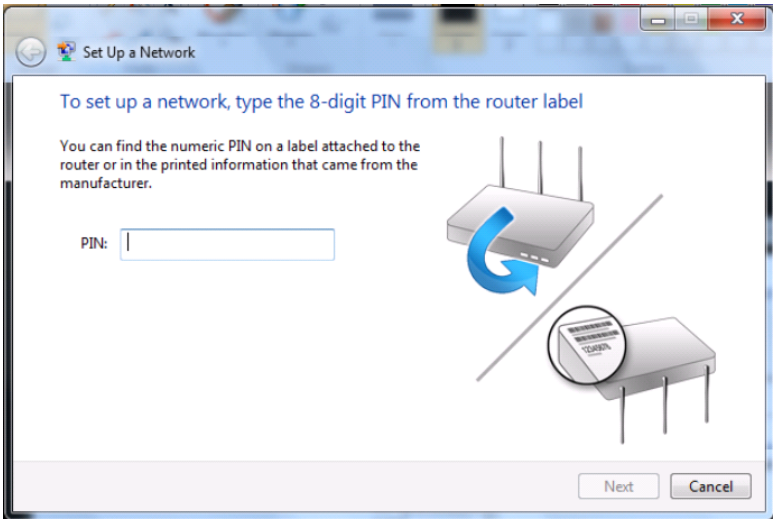
Select a Wireless AP.



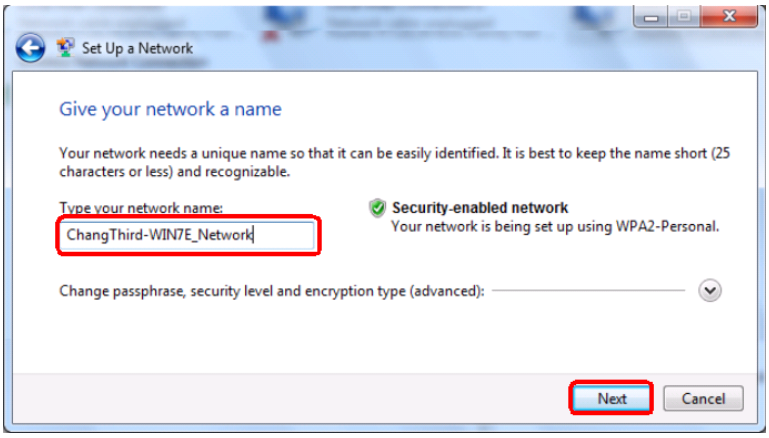
Click [OK] to start setup.



Enter the 8-digit PIN from VoIP Gateway label then click Next.

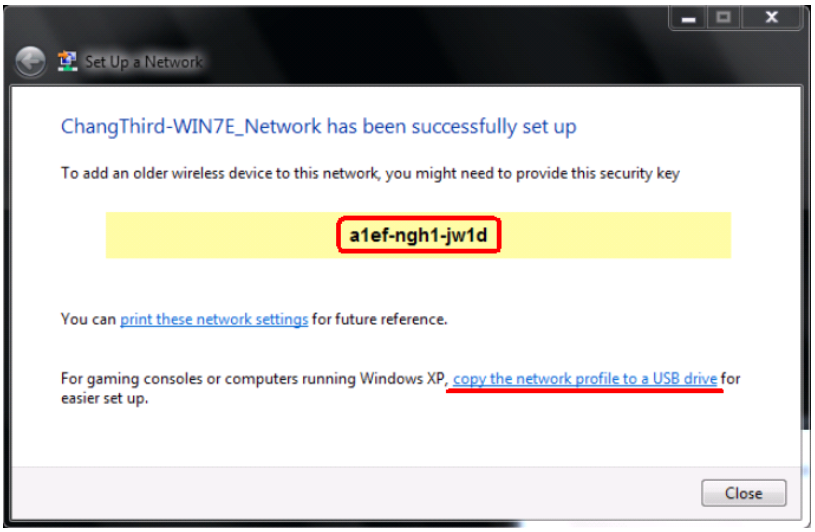


Type network name(SSID) then click Next.



Wait for Windows 7 setting up wireless network.

Configuration finished, you could connect to VoIP Gateway at present. You could also print security key of save this profile for another computer to add this wireless network manually.

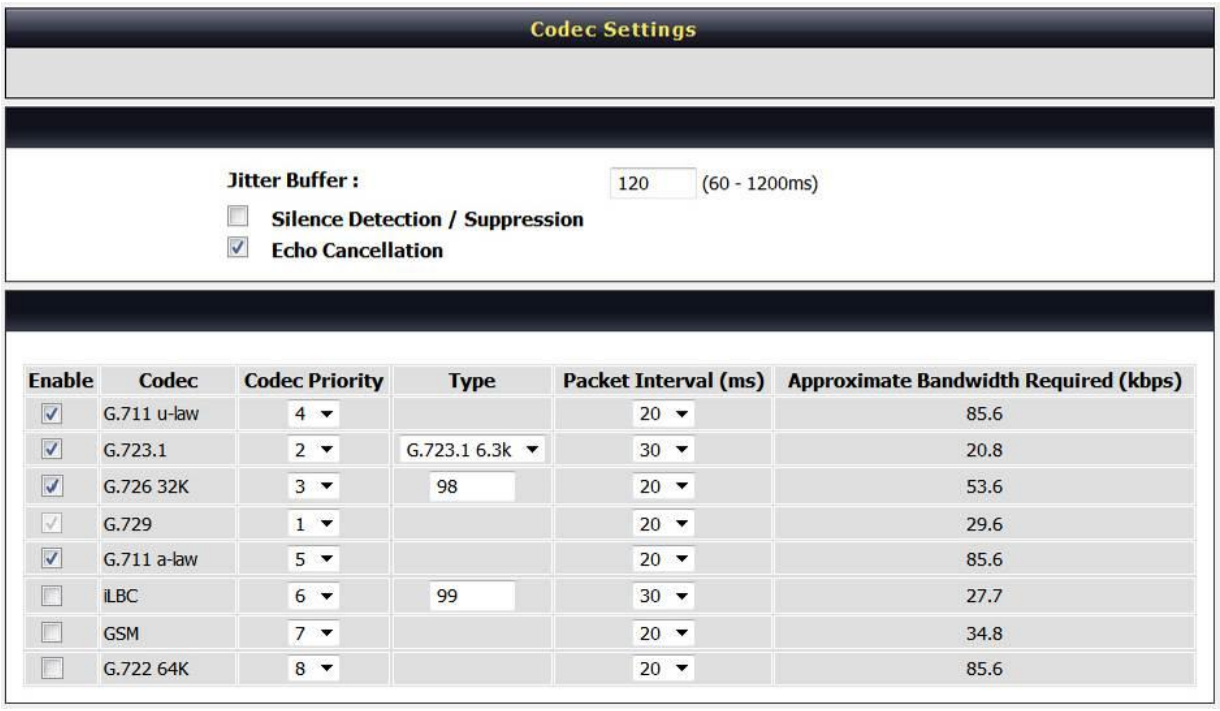


Note: VoIP Gateway supports WPS work with Windows® Vista and Windows® 7 only.

2-4 Advanced Settings

2-4-1 Codec setting

Advanced Settings→ Codec settings



Enable	Codec	Codec Priority	Type	Packet Interval (ms)	Approximate Bandwidth Required (kbps)
☑	G.711 u-law	4		20	85.6
☑	G.723.1	2	G.723.1 6.3k	30	20.8
☑	G.726 32K	3	98	20	53.6
☑	G.729	1		20	29.6
☑	G.711 a-law	5		20	85.6
☐	iLBC	6	99	30	27.7
☐	GSM	7		20	34.8
☐	G.722 64K	8		20	85.6

Jitter Buffer: Enter the jitter of receiving packets.

Silence Detection / 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 VoIP Gateway to support. All codecs are selected and supported by default. You can un-check the box that is not used.

Codec Priority: The priority of code for communication.

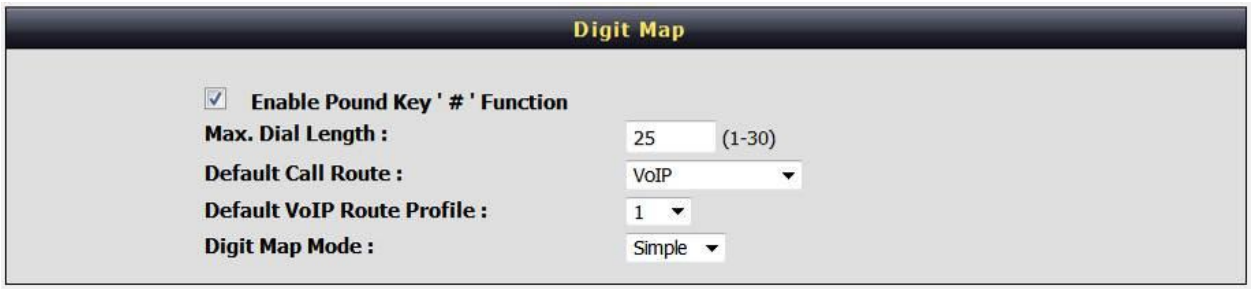
Packet Interval: Select the frame size of voice package from different codec. It defines the time interval for the VoIP Gateway to send a RTP packet or voice packet to the receiving side. The smaller the value, the greater the bandwidth takes, and larger values might cause voice delay.

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

2-4-2 Digit Map

Digit Map supports multiple dial plans which help users to arrange least cost route. Each Proxy Server has individual dial plan which combines the original feature of Digit Map and Speed Dial. You can use "?" or "%" in the column of Scan Code and VoIP 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, users 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 Settings → 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 VoIP Gateway.

Default Call Route: Defines the default call route of the VoIP Gateway.

VoIP: The call route is VoIP only.

Deny: The call will be denied.

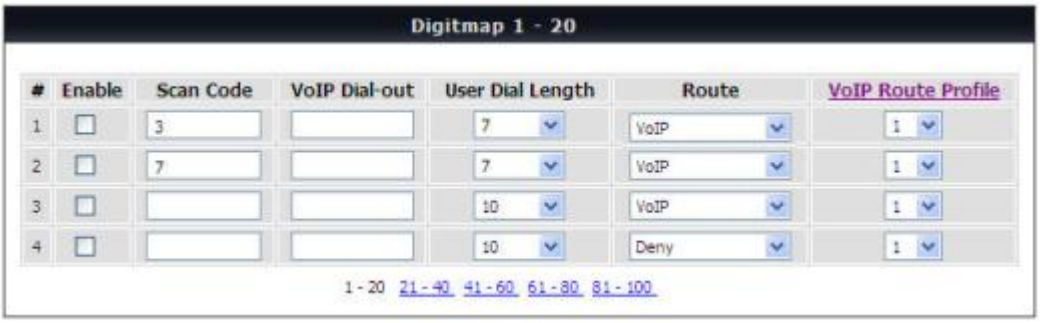
Default VoIP Route Profile: Enter the Profile ID (ranging from 1-10) for the Default VoIP routing.

Advanced Settings → Digit Map

Test Dial No.: You have to set some rules in Digit Map Setting first and enter the number for test.

Result: The gateway will show the number for VoIP Dial-out and PSTN Dial-out according to the Digit Map Setting as below

Advanced Settings → Digit Map



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

VoIP Dial-out: Enter the actual dialing number rule for the VoIP 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.

VoIP Route Profile: Choose the proper Profile ID and click the **VoIP Route Profile** to set the priority of VoIP Route Profile

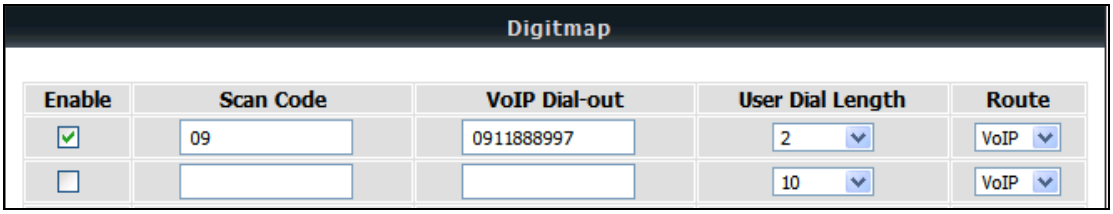
VoIP Gateway Profile

There are 10 VoIP route profiles. Each VoIP route profile provides four routes to select. **Server 1**, **Server 2**, **Server 3**, **Phone Book** and **None** can be selected for each route.

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.

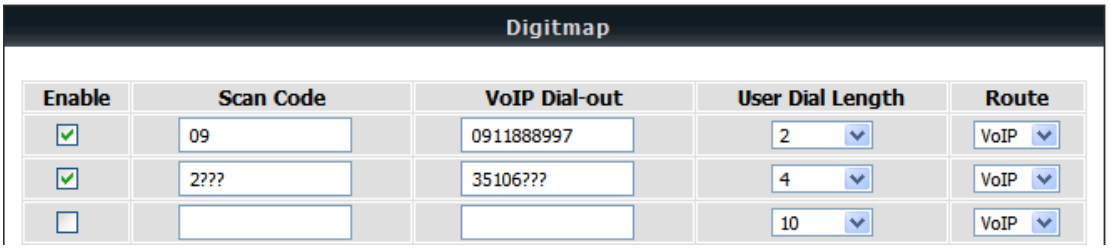
For example,
Scan Code: 09
VoIP Dial-out: 0911888997
User Dial Length: 2
Route: VoIP
VoIP Route Profile: Route # 1



Pick up the handset and dial 09, the VoIP Gateway will dial 0911888997 and follow Route # 1.

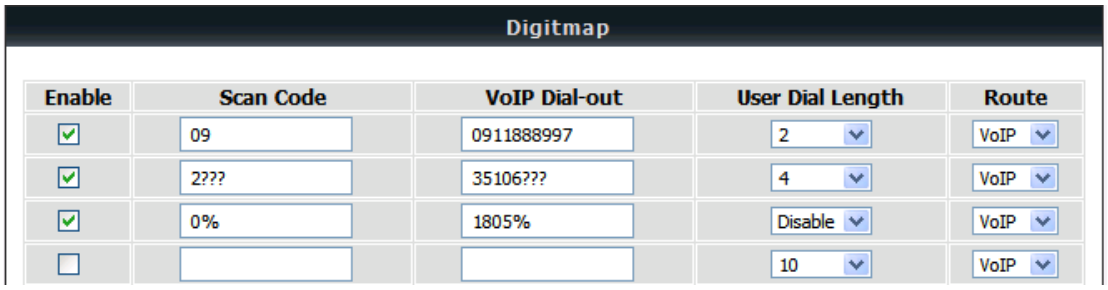
Method 2- Multi mapping: Fill the prefix code into the Scan Code column and the format to transfer into the VoIP Dial-out column.

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



Pick up the handset and dial 2301. The VoIP Gateway will dial 35106301 and follow Route # 2.

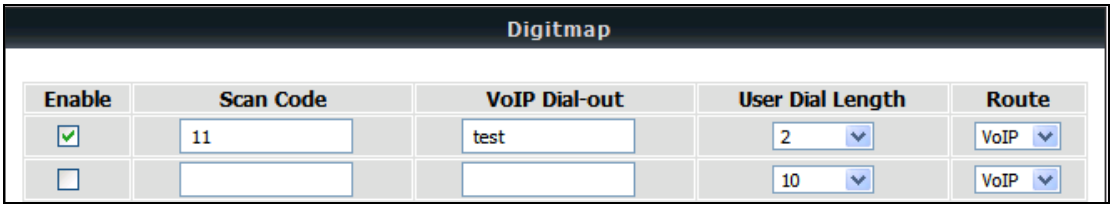
For example,
Scan Code: 0%
VoIP Dial-out: 1805%
User Dial Length: Disable
Route: VoIP
VoIP Route Profile: Route # 3



Pick up the handset and dial 0423456789. The VoIP Gateway will dial 1805423456789 and go through Internet first and follow Route # 3.

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.

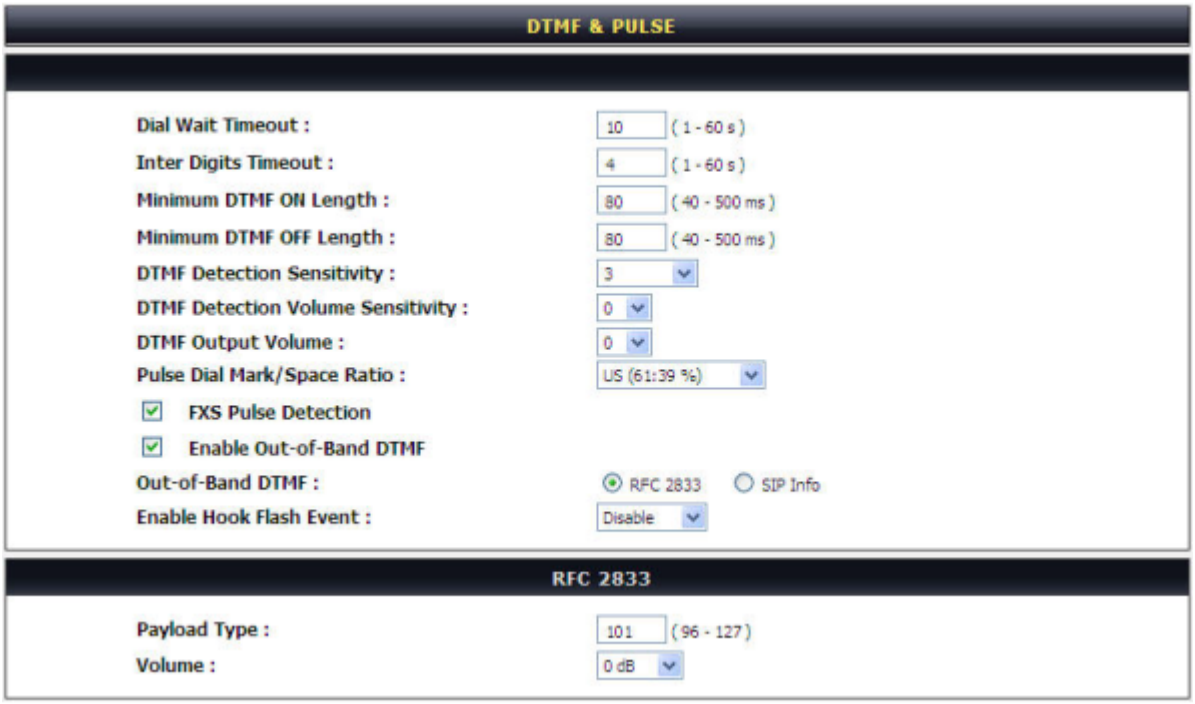
For example,
Scan Code: 11
VoIP Dial-out: test
User Dial Length: 2
Route: VoIP
VoIP Route Profile: Route # 1.



Pick up the handset and dial 11. The VoIP Gateway will dial "test" and go through Internet and follow Route # 1.

2-4-3 DTMF & PULSE

Advanced Settings → 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.

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 VoIP Gateway to detect the DTMF.

DTMF Output Volume: Adjust the Tx volume of FXS port for DTMF Caller ID or Out of Band DTMF.

Pulse Dial Mark/Space Ratio: Duration and break of pulse dial ration.

FXS Pulse Detection: It allows FXS detect PULSE dial method sends from a phone set.

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.

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

Payload Type: payload type of RFC2833.

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

2-4-4 CPT / Cadence

Advanced Settings → CPT / Cadence

CPT # 1 Default

Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2	T_ON_3	T_OFF_3
Dial Tone	350	440	3000	0	0	0	0	0
Congestion Tone	480	620	250	250	0	0	0	0
Busy Tone	480	620	500	500	0	0	0	0
Ring-Back Tone	440	480	1000	2000	0	0	0	0

☑ **CPT # 2** Default

Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2	T_ON_3	T_OFF_3
Dial Tone	400	0	300	100	3500	100	0	0
Congestion Tone	400	0	250	250	0	0	0	0
Busy Tone	400	0	500	500	0	0	0	0
Ring-Back Tone	400	0	500	100	500	2000	0	0

Default

Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2	T_ON_3	T_OFF_3
FWD/DND Dial Tone	400	0	800	80	0	0	0	0

CPT # 1 Enable Setting 1: The CPT has a set of parameter table. Please adjust the CPT based on the local PSTN or PBX settings and requirements.

Advanced Settings → CPT / Cadence

FXS Ring Cadence Settings Default

Range	ON_1 [250-8000ms]	OFF_1 [200-8000ms]	ON_2 [0,250-8000ms]	OFF_2 [0,200-8000ms]	ON_3 [0,250-8000ms]	OFF_3 [0,200-8000ms]
1	1000	2000	0	0	0	0
2	500	500	500	1500	0	0
3	500	500	500	1500	0	0

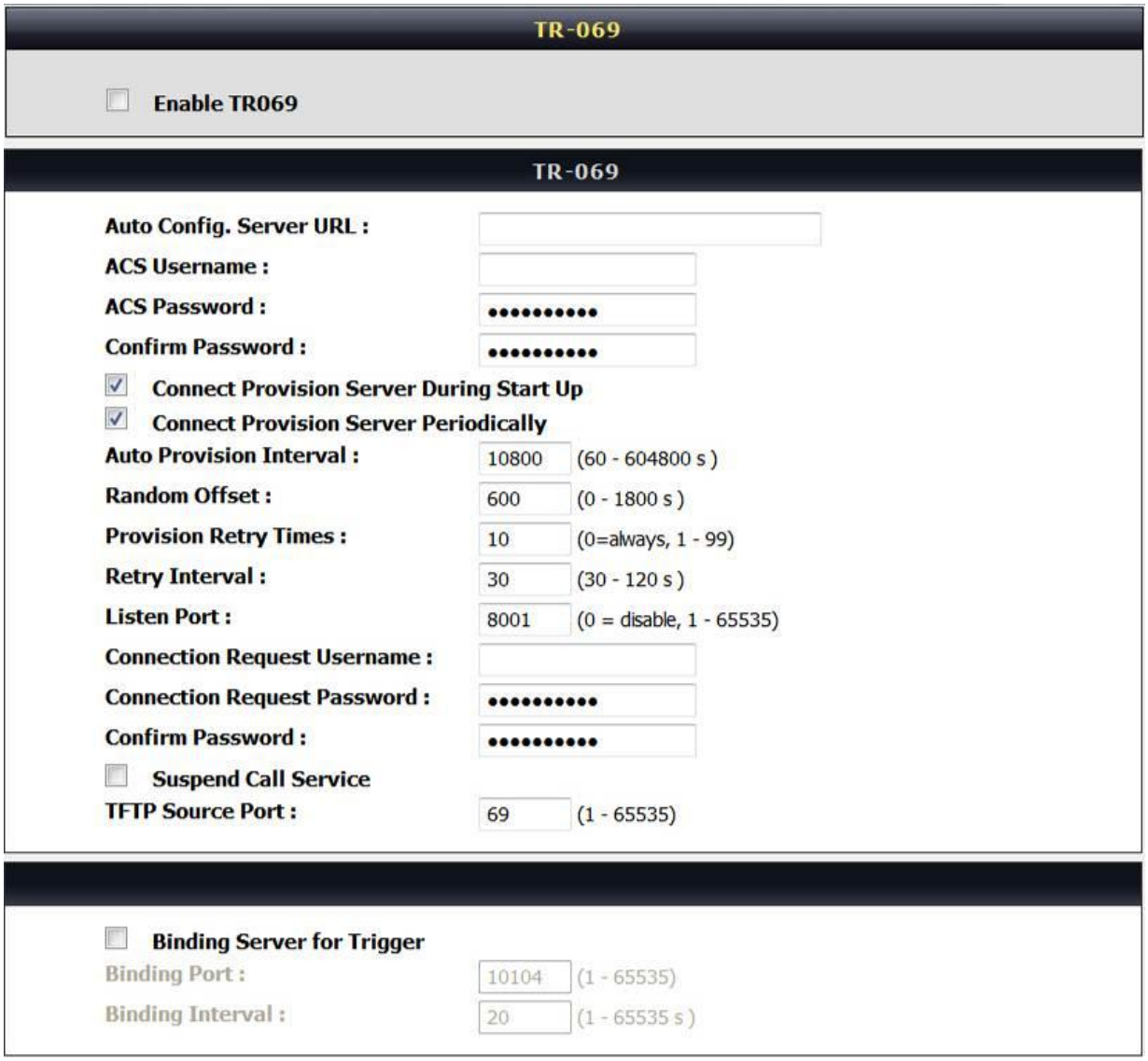
FXS Ring Cadence Settings: Specify the ring cadence for the FXS port. In this field, you specify the on and off pulses for the ring. The ring cadence that should be configured differs depending on local PSTN or PBX settings and requirements.

2-4-5 TR069

TR069 allows operator to manage the VoIP Gateway with a TR069 standard protocol.

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

Advanced Settings → TR069



Enable TR069: Check the box to start TR069 service.

Auto Config. Server URL: Enter the TR069 Server's IP address or URL required by your VoIP Service Provider.

ACS Username: Enter an available ACS user name.

Password: Enter the ACS password.

Connect Provision Server During Start Up: Check the box to connect to Provisioning Server when the VoIP 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.

Listen Port: TR069 listen port for remote trigger.

Connection Request Username: Enter username for remote trigger.

Connection Request Password: Enter password for remote trigger**.**

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

TFTP Source Port: Assign TFTP source port for TFTP download

Note: Contact your server provider if necessary.

Binding Server for Trigger: Check the box to trigger a connection between Provisioning Server and the VoIP Gateway. Provisioning Server will bind a port for the VoIP 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 VoIP Gateway will keep the binding.

2-4-6 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 Setting → Caller Filter

Caller Filter: It is to allow or deny the filter rule.

Status: It is to show the status of enable or disable.

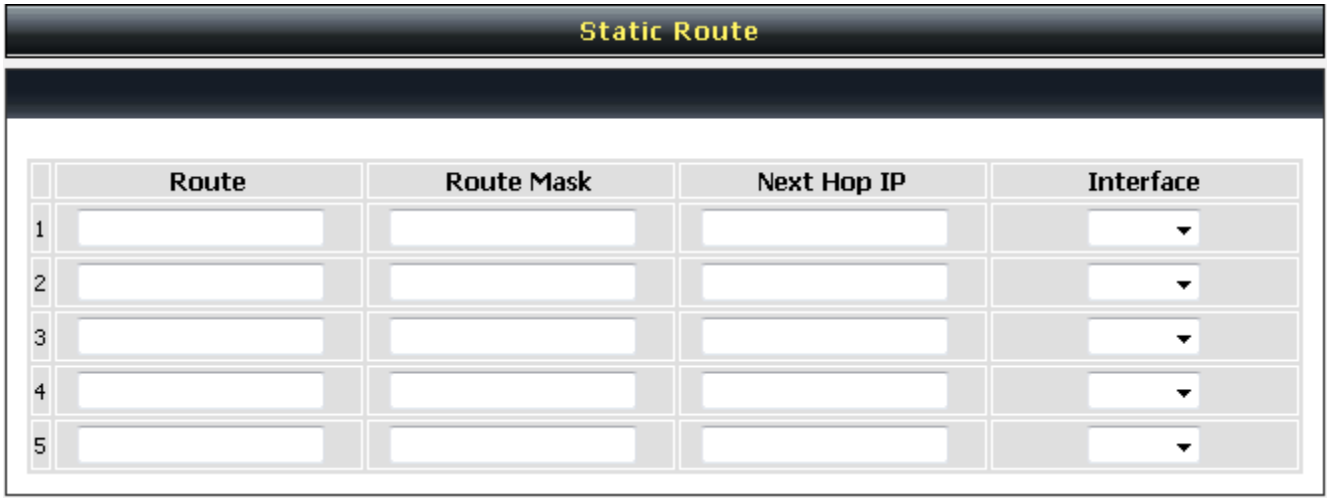
Filter IP Address: Enter the start IP address which you would like to Allow or Deny.

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

2-4-7 Static Route

Build static routes within an internal network. These routes will not apply to the Internet.

Advanced Settings → Static Route



Route: Destination network of the route.

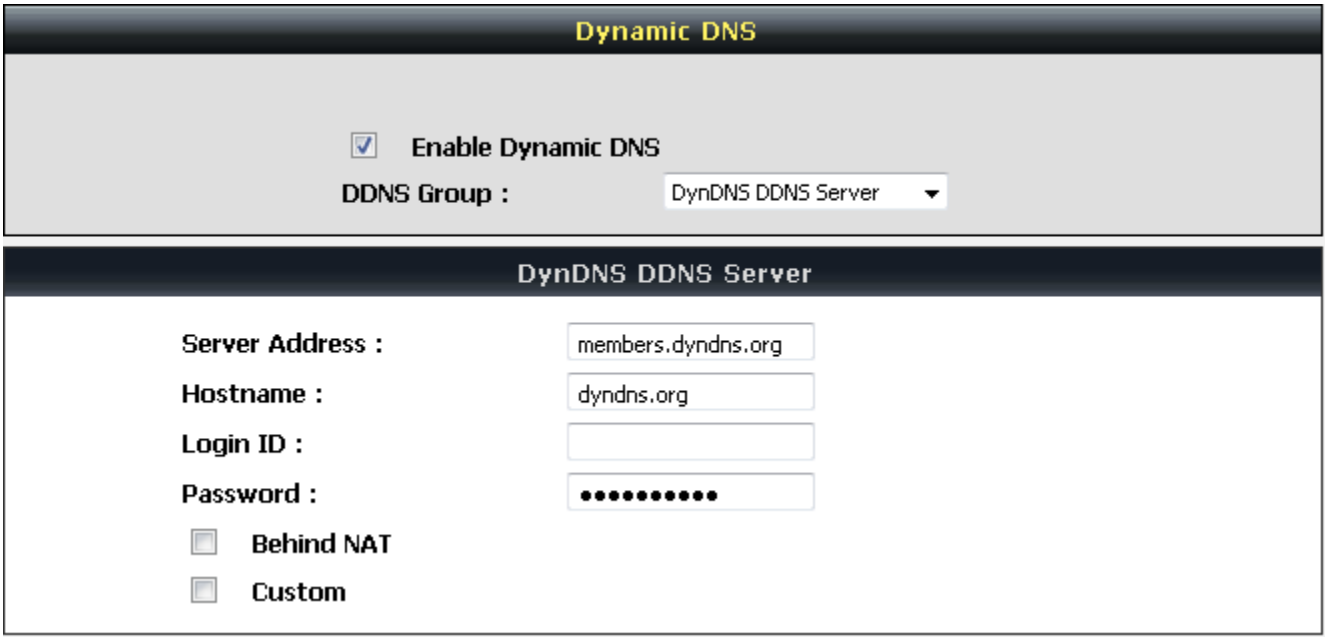
Route Mask: Subnet mask to apply on destination network.

Next Hop IP: The next hop IP address to the specified network.

Interface: The interface attached to this route.

2-4-8 DDNS

Advanced Settings → DDNS



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

Server address: Accept the default setting or fill a correct DDNS Service FQDN.

Hostname: Enter the URL of the system (or NAT) – applied from domain name registration providers (e.g. VoIPGateway01.dyndns.org).

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

> **Note:** If the VoIP 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.

2-4-9 NAT Traversal

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

Advanced Settings → NAT Traversal

Enable(NAT Public IP): Check the box to use the IP address of the Internet sharing device if the VoIP Gateway is set up behind an Internet sharing device. Also the VoIP 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 VoIP 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 VoIP Gateway is not able to traverse the NAT. It is not a flaw of the VoIP 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.

2-4-10 DoS Protection Settings

Advanced Settings → DoS Protection Settings

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

2-4-11 DMZ / ALG

Advanced Settings → DMZ /ALG

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.

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.

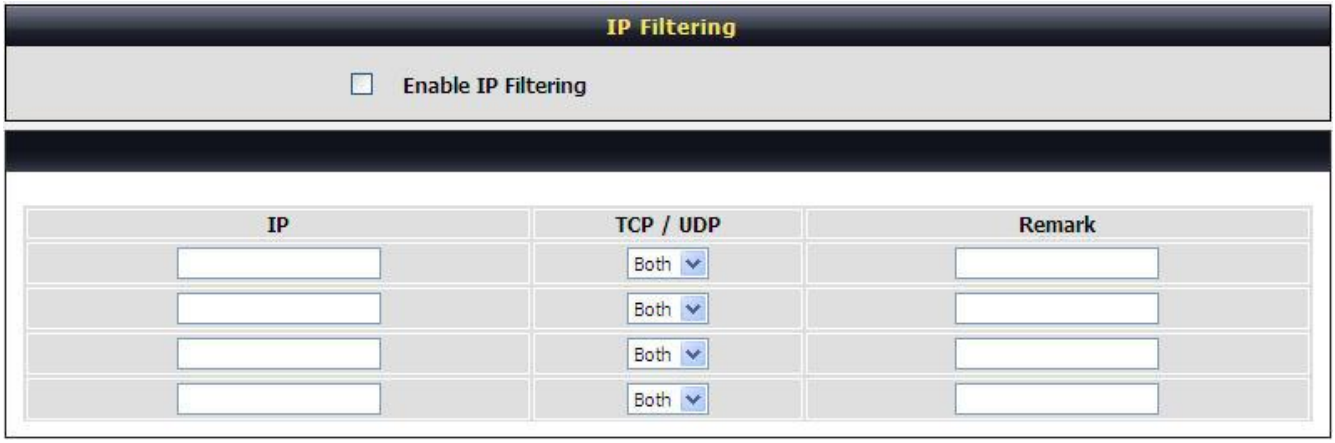
RTSP ALG: Enable ALG for RTSP multimedia stream.

2-4-12 IP Filtering

Advanced Settings → 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 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.

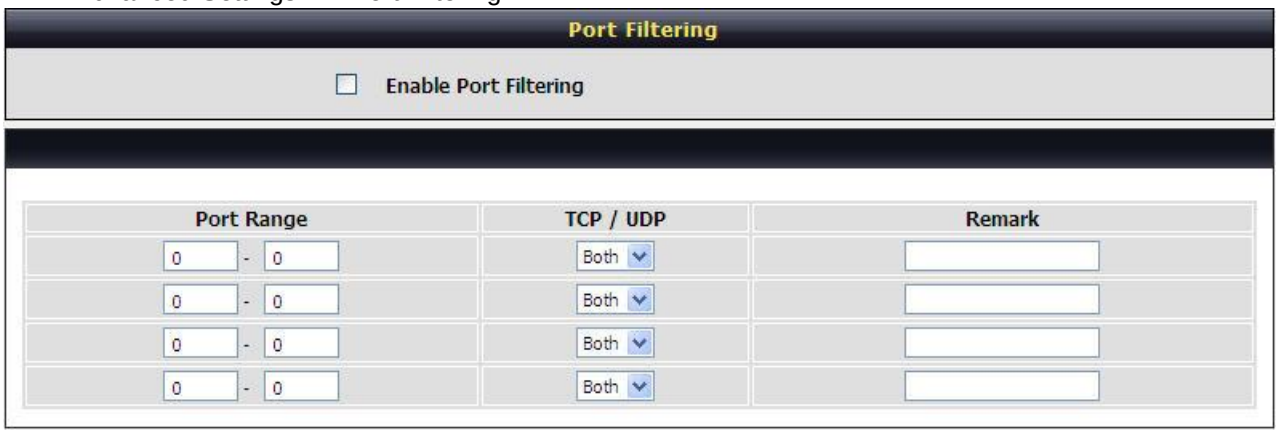
Remark: Enter comments.

2-4-13 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.

Note: When the port used at the source end is within the limited scope, it will be filtered without transmission.

Advanced Settings → Port Filtering



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

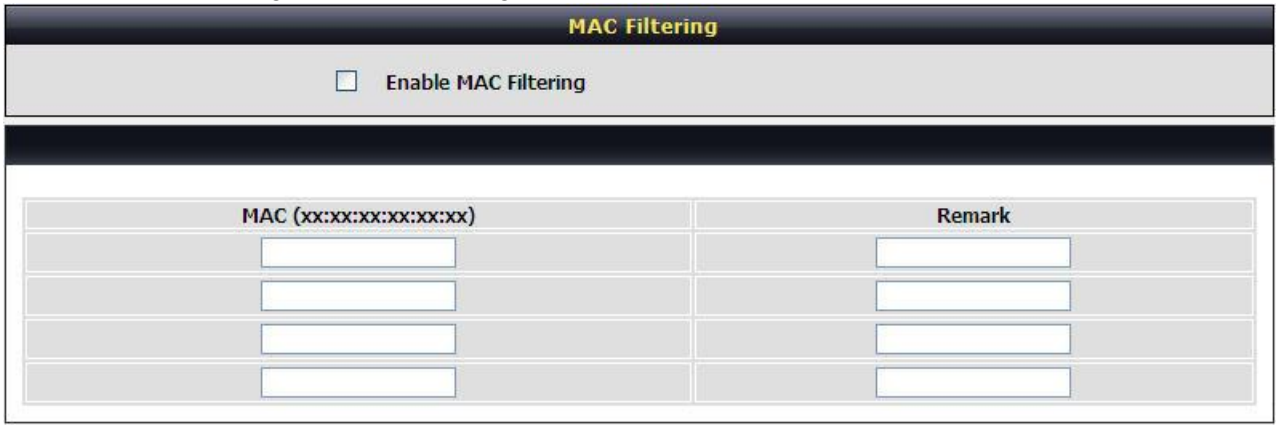
Port Range: Enter the port range that will be denied access to the Internet.

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

2-4-14 MAC Filtering

MAC (Media Access Control) address filtering allows you to filter the transmission of data by network card physical address.

Advanced Settings → MAC Filtering



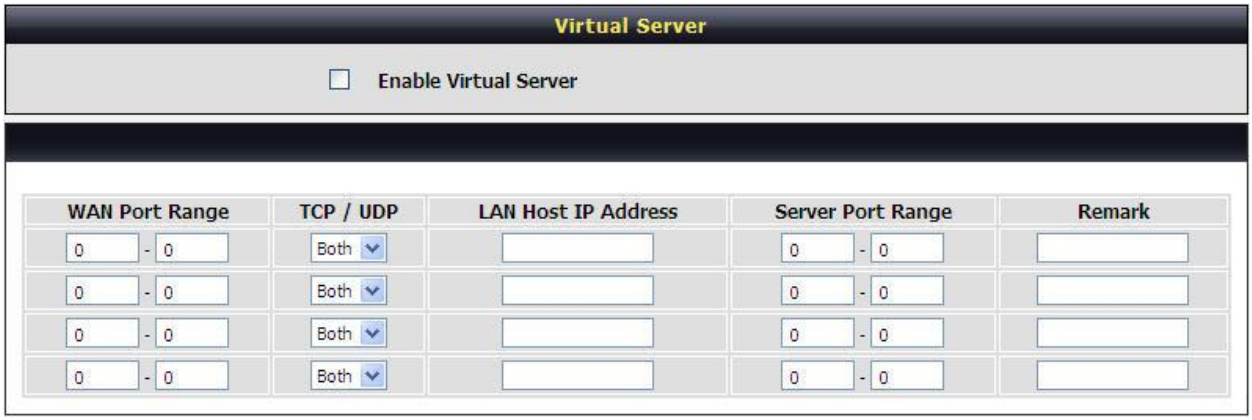
Enable MAC Filtering: Enter a MAC address to prevent the particular device from accessing the Internet.
MAC: Enter a MAC address to prevent the particular device from accessing the Internet.

Remark: Enter comments

2-4-15 Virtual Server

Enable users on Internet to access the WWW, FTP and other services from your NAT. It is also known as port forwarding. When remote users are accessing Web or FTP servers through WAN IP address, it will be routed to the server with LAN IP address

Advanced Settings → Virtual Server



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

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

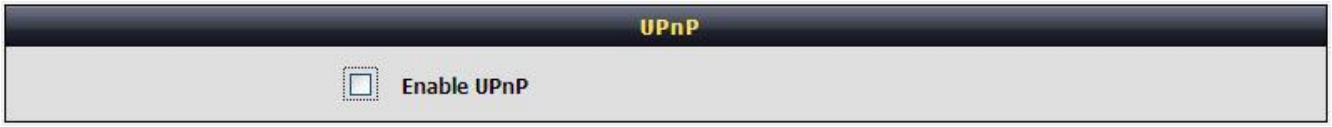
TCP/UDP: Select the communication protocols used by the server, **TCP**, **UDP** or **Both**.

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.
Remark: Enter comments

2-4-16 UPnP

Advanced Settings → UPnP



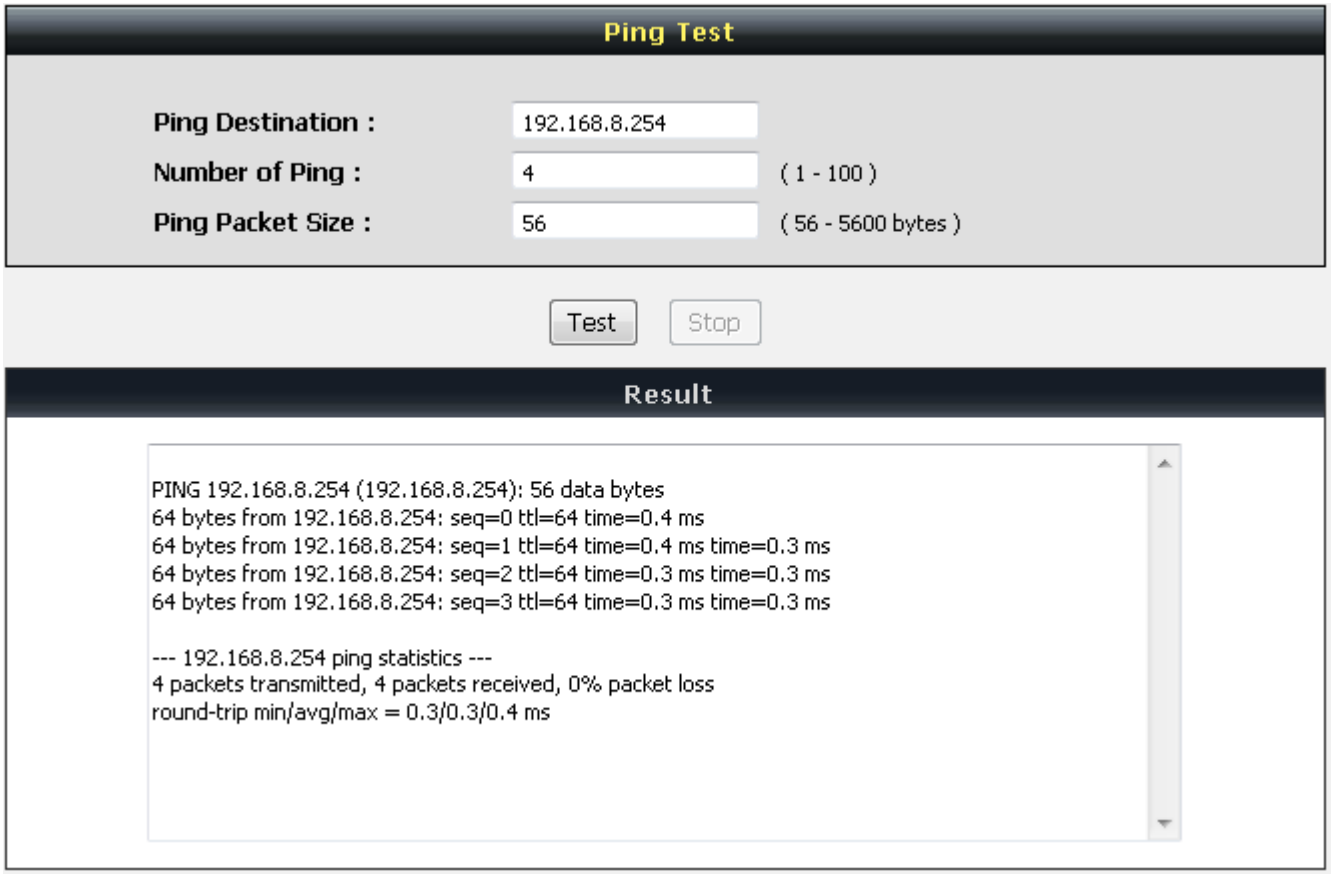
Enable UPnP Server: UPnP is a network standard, enables the auto discovery the devices on the network. It only works with the device that supports UPnP

2-5 Tools

2-5-1 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. The result would be shown on **Result** Table

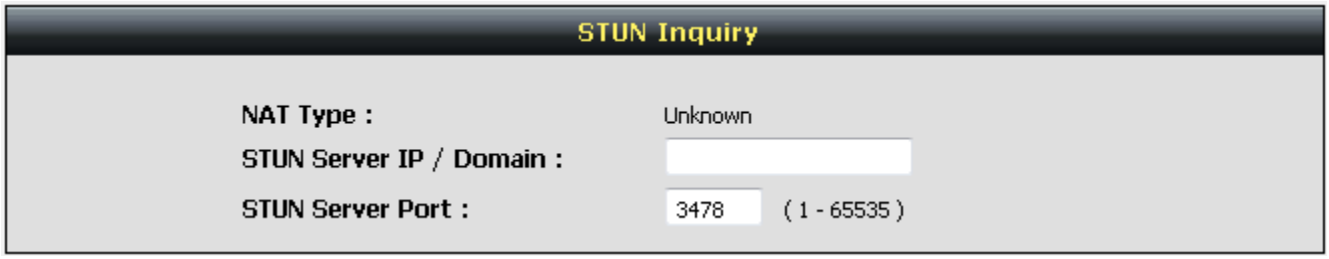
Tools → Ping Test



2-5-2 STUN Inquiry

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

Tools → 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.

2-6 System Settings

2-6-1 NTP

System settings → NTP

Automatically synchronize with Internet time servers: The VoIP Gateway should automatically sync up with time servers.

First NTP time server: Select the desired domain name of a NTP server as first priority.

Second NTP time server: Select the domain name of a NTP server as second priority.

Current Router Time: It shows the current time of the VoIP Gateway.

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

Enable Daylight Saving: To enable/disable daylight saving time.

Daylight Saving Offset: Set the current time zone offset for your location.

Daylight Saving Dates: Set the start and end dates for daylight saving time.

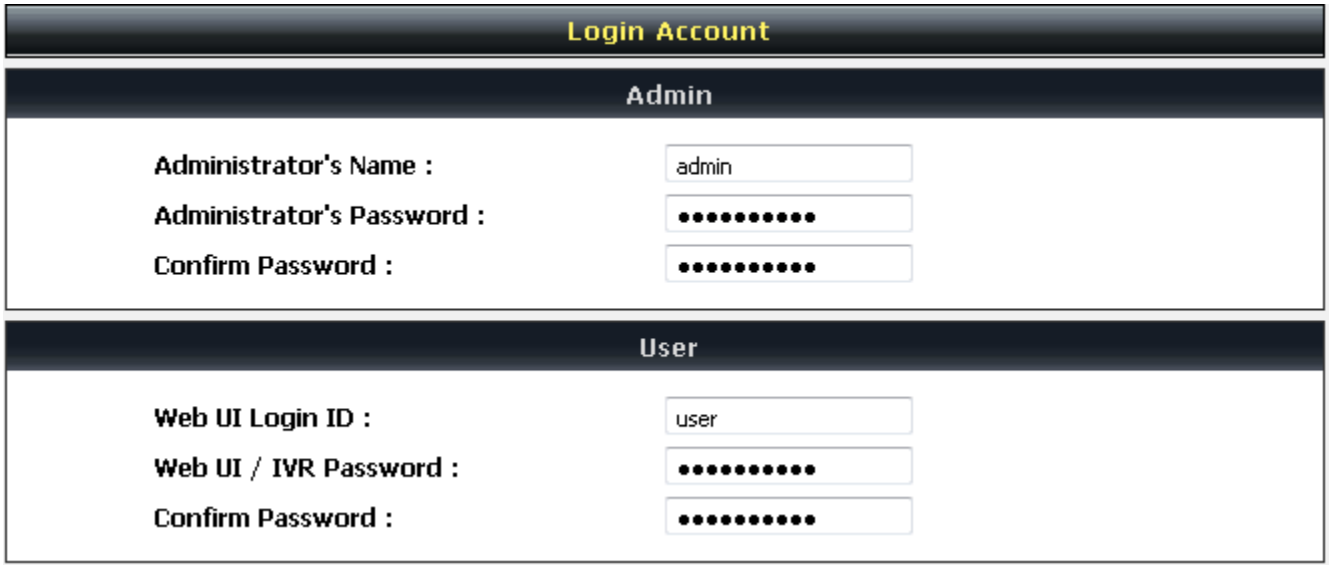
2-6-2 Language

The system provides English, Traditional Chinese, and Simplified Chinese for displaying text on web pages. Changing the language setting also changes the language for IVR (Interactive Voice Response).

System settings → Language

2-6-3 Login Account

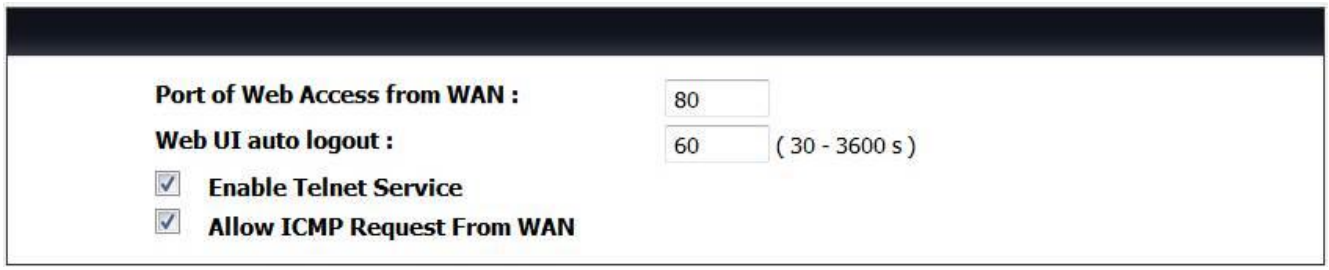
System settings → Login Account



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

Password: It is highly recommended that you create a password to keep your VoIP Gateway secure.

System settings → Login Account



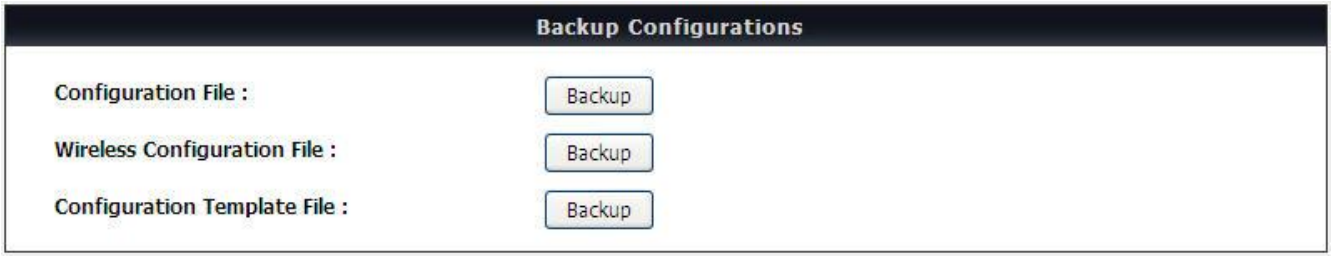
Port of Web Access from WAN: Enter the port number when accessing the web-based configuration utility from the WAN port.

Web Idle Time Out: Enter the range of effective time when log-in the web interface. The user will be disconnected from the web page to allow others to log-in.

2-6-4 Backup / Restore

Backup Configurations File

System settings → Backup and Restore



The current system settings can be saved as a file onto the local hard drive. Click the **Backup Settings** button to save your current settings to a file.

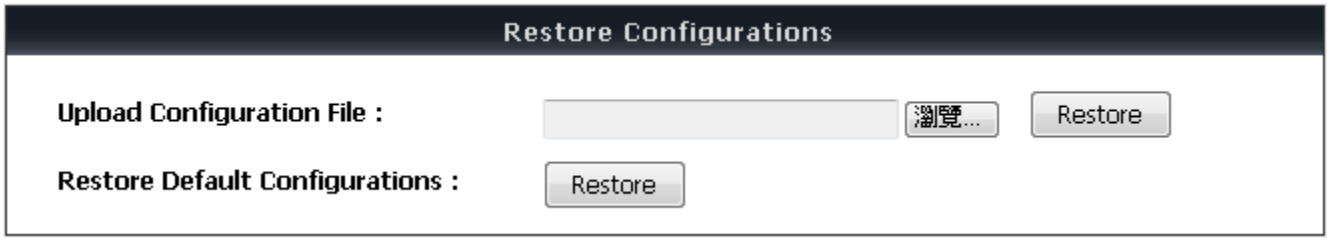
Configuration File: It is to backup the all settings.

Wireless Configuration File：It is to backup the Wireless settings.

Configuration Template File: It is to backup the settings as template file for editing.

Restore Default Settings

System settings → Backup and Restore

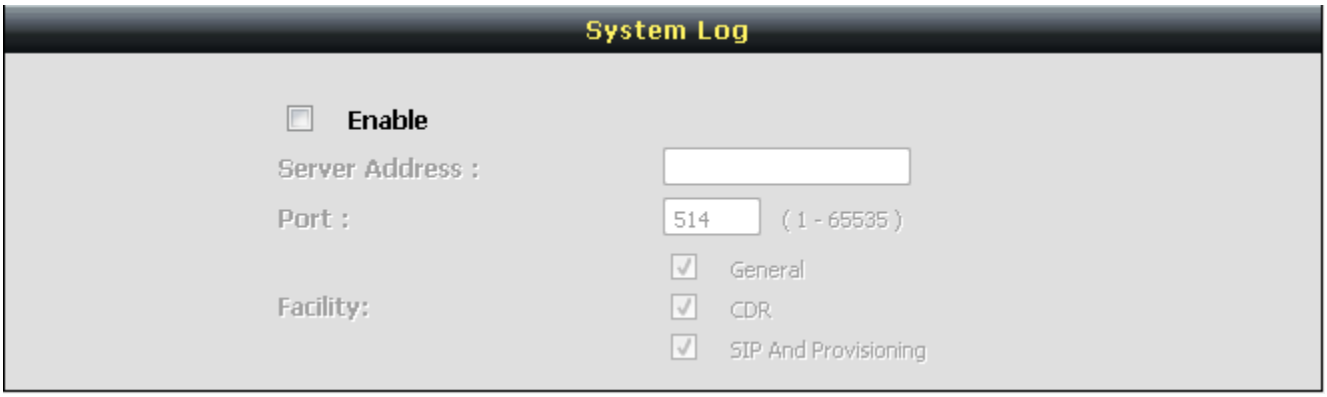


You can backup settings to a file and restore settings from that file. You also can restore all settings back to default by selecting **Restore Default Configurations** and click **Restore**.

Note: You have to save settings and restart, and all settings will take effect.

2-6-5 System Log

System settings → System log



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

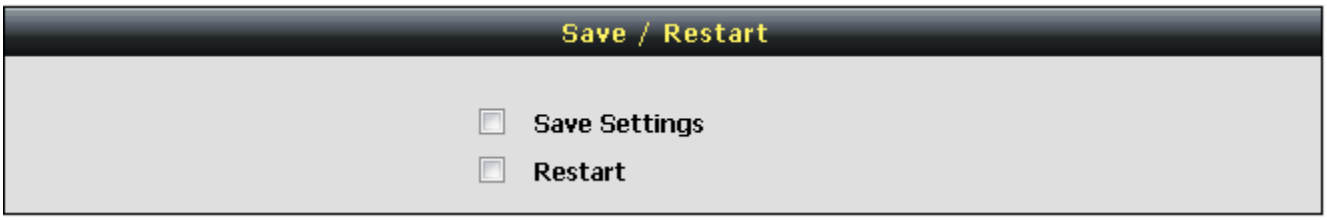
Server Address: Enter the System Log Server's IP address.

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.

2-6-6 Save / Restart

Save and Reboot

System settings → Backup and Restore



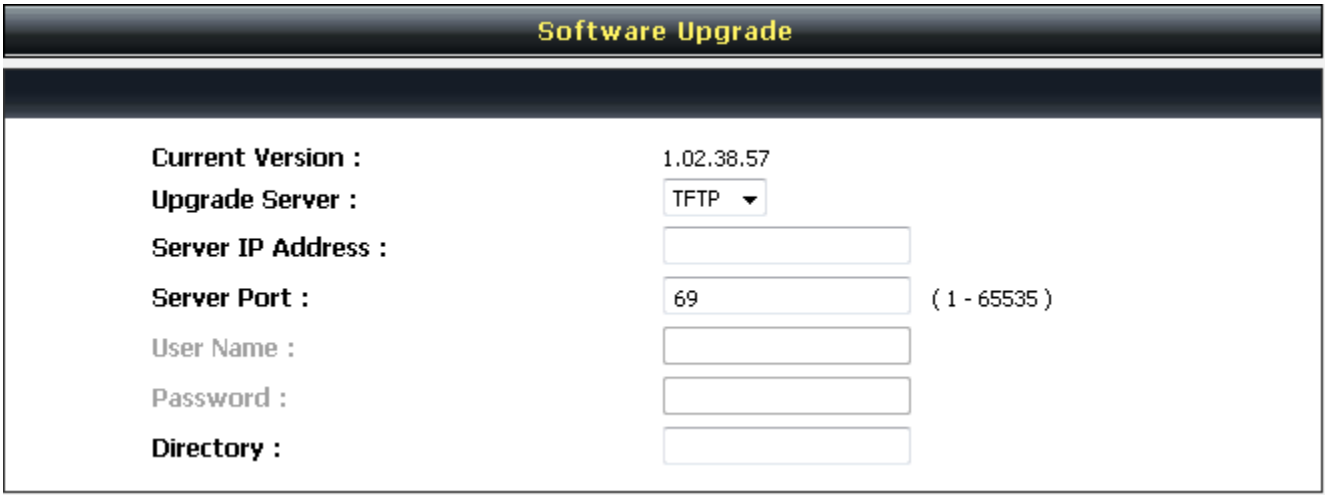
Save All Settings: Click the **Save All Settings** check box and reboot the system after completing changes. The new settings will take effect after the VoIP Gateway is restarted.

Restart: Click the **Reboot** button to reboot the system.

2-6-7 Software Upgrade

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

System settings → Software 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.

2-6-8 Logout

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

Logout

3. Configuring the VoIP Gateway through IVR

Preparation

1. Connect the power supply, telephone set, telephone cable, and network cable properly.
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 intend to operate the VoIP Gateway under NAT, the IP range of VoIP Gateway WAN Port and LAN Port IP Address should not be the same in order to avoid phone failures.

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

3-1 IVR (Interactive Voice Response)

The VoIP Gateway provides convenient IVR functions. Users are able to get query and setup the VoIP 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. 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 VoIP Gateway.

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 VoIP Gateway. If your password is "admin", enter * (star) * (star) * (star) 41 44 53 49 54 # (pound). Please refer to the IVR Functions Table (page 68) 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 VoIP Gateway to enable the new settings.

To inquire about the current VoIP 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 VoIP 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)	
116/106	Phone Book manager IP address Set/Query	
118	Restart	
311/301	LAN Port IP Set/Query	
312/302	LAN Port Subnet Mask Set/Query	
109	Restore factory default IP address configuration	
409	Restore factory default settings	
509	Save settings	

3-2 IP Configuration Settings

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 VoIP 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 VoIP Gateway failed to communicate with a DHCP server. Please check with your DHCP server or ISP.

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 VoIP 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 Character Conversion Table:

The table below provides a list of 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 "admin" 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

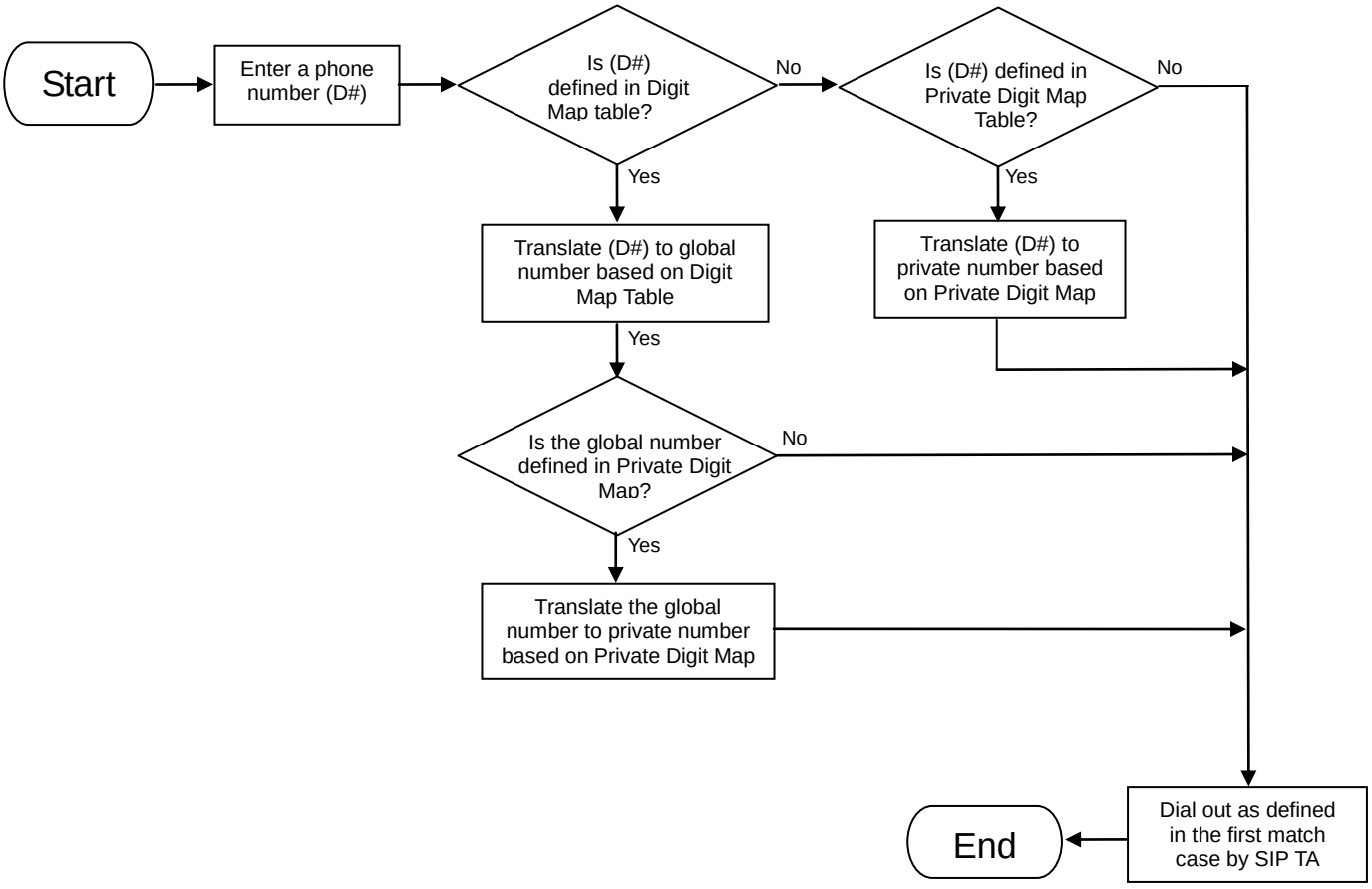
The VoIP Gateway provides the registration for multiple VoIP Service Providers, and each VSP has a private digit map. Hence, the routing and number translation may vary. We use two part, Routing and Number Translation, to explain the dialing principle of the VoIP Gateway.

Dialing Options

1. 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 "DTMF", default=4 seconds, see page 55).
2. If the phone number matches a rule of Digit Map Table, the phone number will be routed the assigned VSP or Phone Book according VoIP Route Profile automatically.

Number Translation

Phone number is dialed by user. The system will check if the phone number is matched Digit Map Table. If no matched is found from Digit Map Table, it will use the phone number to look up private digit map of the server set in VoIP Routing Profile. The system will translate the phone number to global number used to look up private digit map of the server set in VoIP Routing Profile.



Routing

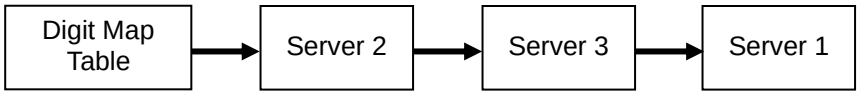
To achieve maximum flexibility, the number dialed will be looked up in several tables defined by the VoIP Gateway. If no match is found from Digit Map Table, it will then look up the number from another table and to the registered VSP.

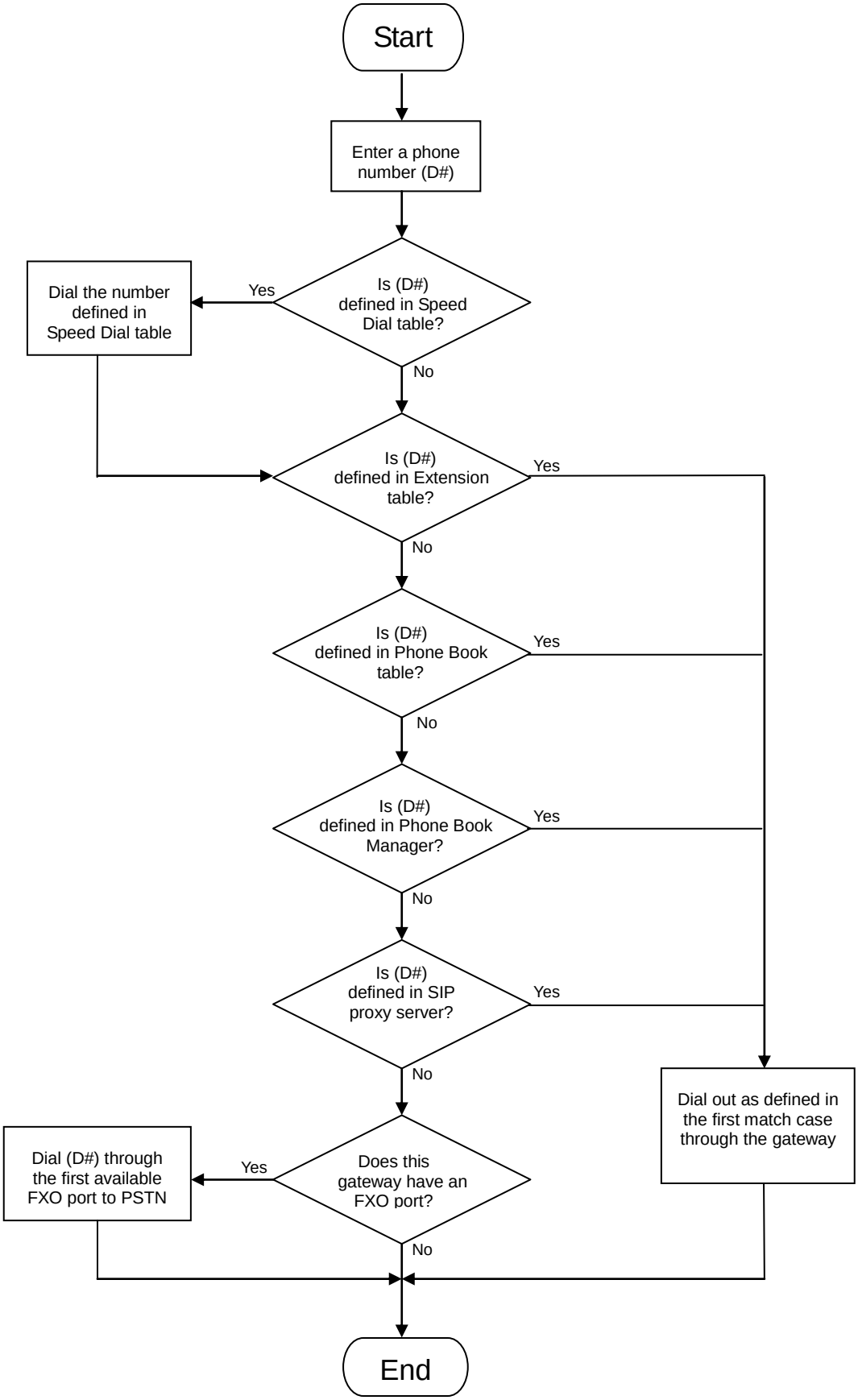
Routing Processing Flow

The routing after checking Digit Map Table may be vary. The routing is accord with VoIP Route Profile. By default, Phone Book is the first route of VoIP Route Profile. The second and third route is Server 1 and Server 2. Server 3 is the last route. Each server has a Private Digit Map, and the number will be translated according the Private Digit Map before dialing out. For default setting, the number look up flow appears like:

The routing after checking Digit Map Table may be vary. The routing is accord with VoIP Route Profile. By default, Phone Book is the first route of VoIP Route Profile. The second and third route is Server 1 and Server 2. Server 3 is the last route. Each server has a Private Digit Map, and the number will be translated according the Private Digit Map before dialing out. For default setting, the number look up flow appears like:

Assume that the route of Default Route Profile is Server 2 as the first route, Server 3 as the second route and Server 1 as the last route. The number look up flow appears like:




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
Dial out as defined in the first match case through the gateway
Does this gateway have an FXO port?
Yes
Dial (D#) through the first available FXO port to PSTN
No
End

This page is intentionally left blank.

CTC union®

www.ctcu.com

T +886-2 2659-1021 **F** +886-2 2659-0237 **E** sales@ctcu.com