Powered by Accton

SIP Gateway
VG3300 Series

User Guide

www.edge-core.com

SIP Gateway VG3300 Series

User Guide

Update: 2005/06/20

Contents

1. Safety Instructions

WARNING

1. Do not attempt to service the product yourself. Any servicing of this product should be referred to qualified service personnel.
2. To avoid electric shock, do not put your finger, pin, wire, or any other metal objects into vents and gaps.
3. To avoid accidental fire or electric shock, do not twist power cord or place it under heavy objects.
4. The product should be connected to a power supply of the type described in the operating instructions or as marked on the product.
5. To avoid hazard to children, dispose of the product's plastic packaging carefully.
6. The phone line should always be connected to the LINE connector. It should not be connected to the PHONE connector as it may cause damage to the product.
7. Please read all the instructions before using this product.

2. Preface

The VG3300 unit is a personal SIP VoIP gateway developed using the latest in VoIP technology. It is also very simple to install and easy to operate.

2.1. What is SIP

Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFC 2543& RFC 3261) that can be used to establish, maintain, and terminate calls between two or more end points. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* provides the ability to control the attributes of an end-to-end call.

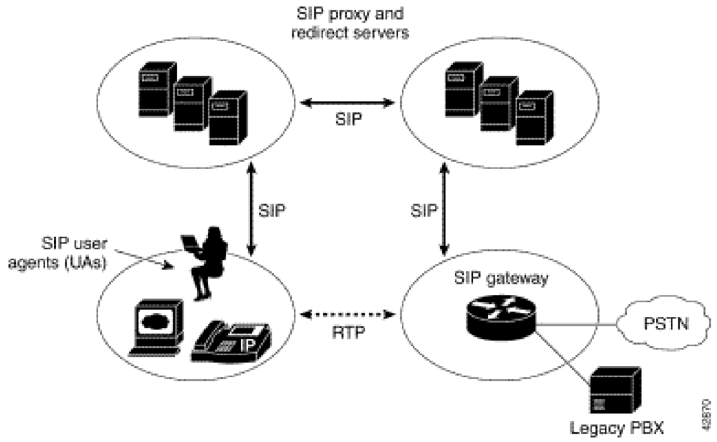
SIP provides the following capabilities:
Determine the location of the target end point—Supports address resolution, name mapping, and call redirection.
Determine the media capabilities of the target end point—By using Session Description Protocol (SDP), SIP determines the highest level of common services between the end points. Conferences

are established using only the media capabilities that can be supported by all end points.
Determine the availability of the target end point—If a call cannot be completed because the target end point is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target end point is unavailable.
Establish a session between the originating and target end point—If the call can be completed, SIP establishes a session between the end points. SIP also supports mid-call changes, such as the addition of another end point to the conference or the changing of a media characteristic or Codec.
Handle the transfer and termination of calls—SIP supports the transfer of calls from one end point to another. During a call transfer, SIP simply establishes a session between the transferee and a new end point (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

2.1.1. Components of SIP

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:
User agent client (UAC)—A client application that initiates the SIP request.
User agent server (UAS)—A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.
Typically, a SIP end point is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.
From an architecture standpoint, the physical components of a SIP network can be grouped into two categories: clients and servers.

Architecture



SIP Clients

SIP clients include the following:

Phones—Can act as either a UAS or UAC. Soft phones (PCs that have phone capabilities installed) and SIP IP phones can initiate SIP requests and respond to requests.

Gateways—Provide call control. Gateways provide much functionality. The most common one is a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway also translates between audio and video Codec and performs call setup and clearing on both the LAN side and the switched-circuit network side.

SIP Servers

SIP servers include the following:

Proxy server—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on behalf of the client's. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

Redirect server—Provides the client with information about the next hop or hops that a message should take, then the client contacts the next hop server or UAS directly.

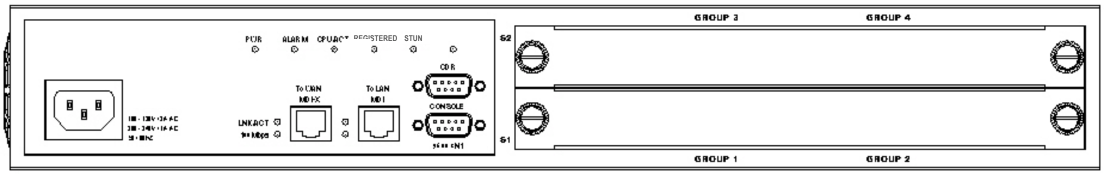
Registrar server—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

3. Package Contents

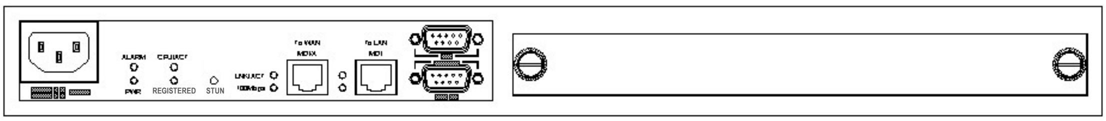
The VG3300 Gateway	X	1	
Power Cord	X	1	
Accessories for fixing support	X	1	(For VG3310/3318)
System CD-ROM	X	1	
5 IDC Connector	X	4	(For VG3310/3318)
Rubber footer			
RJ-45 Ethernet Cable	X	1	
RJ-11 Telephone Cable	X	1	

4. Panel Descriptions

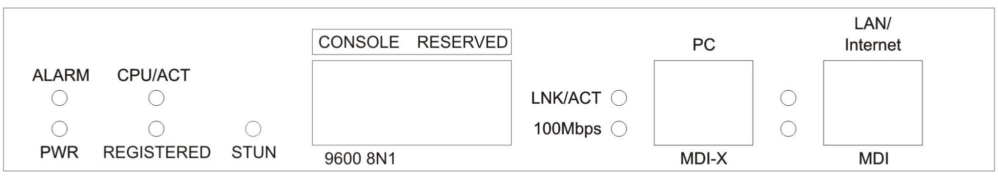
4.1. Front Panel



VG3318 Front Panel



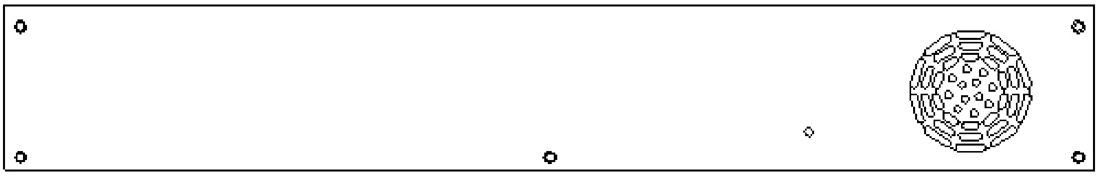
VG3310 Front Panel



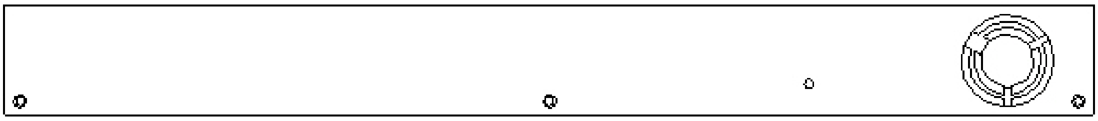
VG3306 Front Panel

4.2. Rear Panel

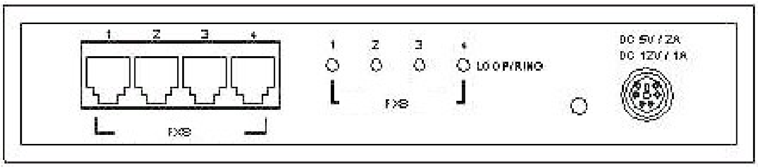
There is a button on the rear panel of gateway for special maintenance. Please don't touch this button under normal operation.



VG3318 Rear Panel



VG3310 Rear Panel



VG3306 Rear Panel

5. LED Indicators

LED	Label	Description	
10/100 Ethernet	LNK/ACT	On	Link up
		Off	Link down
		Flash	Sending/Receiving data packets
	100Mbps	On (LNK is on)	100Mbps
		Off (LNK is on)	10Mbps
LOOP/RING	FXS	On	Off hook
		Off	On hook
		Flash	Ringing out
	FXO	On	Line is active
		Off	Line is inactive
		Flash	Ringing in
Device	Alarm	The red light "On" indicates that system has some problem; please contact your vender.	
	Power	"On" indicates that the power supply is working normally.	
	CPU/ACT	"On" indicates that the CPU is working normally.	
	Registered	"On" indicates that all SIP entities are registered successful. "Off" indicates that all SIP entities are registered fail. "Flash" indicates that one of these SIP entities is registered fail.	
	STUN	"On" indicates communicate with STUN Server once. "Off" indicates never communicate with STUN Server.	

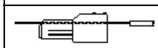
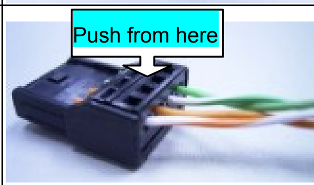
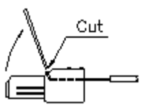
6. Connectors

Ports	Label	Description
Voice Ports	FXS	Connects to a telephone set or fax machine
	FXO	Connects to the phone line
Ethernet Ports	LAN/Internet	RJ-45 connector MDI-X connects to a Modem
	PC	RJ-45 connector MDI connects to a PC
Console Port (Only VG3306/3310/3318)	Console	RJ-45 connector/RS-232 Interface

7. IDC Connectors (Only for VG3310/3318)

IDC connector is used for the voice interface (FXS and FXO) on the frame model. IDC connector can easily connect PBX line and telephone wire together to the gateway.　No special tools are required; please follow the instruction to install:

(Remarks: For IDC connector, it's better to use No. 24 wire, e.g. CAT 5)

Get the material ready	 
 Insert the insulated wires directly into the block for wire insertion	
 Push the block down until it is locked to flush the conductor with the probe	
Cut off the conductor outside the edge to avoid from causing the circuit shortage	

8. Information required before Installation

You need to prepare the following information before installing the gateway.

8.1. IP Address

The gateway requires an IP address for operation. Before installation you need to know how to obtain an IP address from your local ISP. Static IP, DHCP or PPPoE can be used. The following table helps you to decide what information you need. If your ISP offers static IP, you may need to obtain an IP from MIS personnel in order to prevent an IP conflict. Otherwise DHCP (most cable broadband providers offer this) and PPPoE (most ADSL broadband providers offer this) will work fine.

IP Environment		Requiring information
Static IP	Public IP Address	IP Address Subnet Mask ***Default Gateway*** It is strongly suggested that you obtain an IP address from MIS personnel in order to prevent an IP conflict.
	Private IP Address	IP Address Subnet Mask Default Gateway It is strongly suggested that you obtain an IP address from MIS personnel in order to prevent IP conflicts. Your private IP requires an IP Sharing device and you must configure the IP Sharing device to treat the gateway and the IP that it is using as a virtual server.
Dynamic IP address (DHCP)		DHCP mode
PPPoE		Account Number Password Your ISP normally provides this information. If you don't have this information please contact your ISP.

8.2. SIP Information

Before configuring SIP, the VG3300 requires SIP information for operation. The following table helps you to decide what information you need.

Items	Description
1. SIP Proxy	If you want to make SIP calls through SIP proxy server, you will need to know the IP address or domain name of SIP proxy server. The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. If you don't know which SIP proxy for setting, contact your SIP service provider.
2. Public Address (SIP Account) Example: sip@edge-core.com	The public address is like phone number, you can get the account from your SIP service provider.
3. Outbound Authentication	You will need the information when the SIP proxy server requires authentication. You can get this authentication information from SIP service provider when you apply for the service.

8.3. Prepare a password for Web Management

You will need to prepare a password for Web based Management. It can be a digit and/or letter combination ranging from 1 to 6 digits (E.g. 123). For security reason, password must be set to enter the Web Management page.

9. Installation and Configuration

After preparing the information you need as specified in section 5, follow the following steps to do the basic configuration. You can use either a telephone or a system console to perform basic configurations. It is simple to connect a telephone set to FXS port and configures the system. If you want to use system console to configure the system (Only VG3306/3310/3318 support), you have to configure your VT100 terminal to match the settings of the gateway's console port. The console port's terminal connection is set to 9600 baud, 8 data bits, 1 stop bit and no parity. Turn on the gateway's power and wait for the terminal to display "Press Enter…" follow the directions to begin.

Here are several procedures to do:

1. Confirming the Region ID.
2. Configure IP address of gateway.
3. Enter into the WEB page.
4. Plan and configure the channels into SIP entity.
5. Configure SIP proxy and register information.
6. Configure SIP entity information.
7. Configure Outbound Authentication (If needs).
8. Configure STUN (If your gateway is behind NAT).
9. Check the SIP entity if is registered successful.
10. Configure Phone book (If needs)
11. Make a SIP call.

9.1. Confirming the Region ID

About the Region ID, please refer to Section 15.5 Region ID.

9.1.1. Phone Setting

1. Connect the power.
2. Connect the phone cable to the "Phone" socket on the rear panel as pictured above.
3. When the CPU/ACT LED is on, pick up the handset and listen for the dialing tone.
4. Dial "##0000" and listen for 3 short beep.
5. Dial "95<u>07</u>#"；Assuming you are modifying for China (The last 2 digits are the regional ID)
6. Dial "97<u>1</u>#"；Sets the new regional ID.
7. Hang up the phone. The device will be updated with the new region setting after it restarts (restart time is about 10 seconds)

9.1.2. System console settings (Only VG3306/3310/3318)

SIP-RG>enable

SIP-RG #configure

Enter configuration commands, one per line. End with CNTL/Z

SIP-RG(config)#regional_id *07*

SIP-RG(config)#exit

SIP-RG#delete nvram

This command resets the system with factory defaults.

All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

Reset system with factory defaults, [Y]es or [N]o? Yes

Attention:

Before Changing the Region ID, the system has to be reset to the default value. Therefore this step should be done first.

The following instruction may keep the IP address unchanged after reset:

"delete nvram keep_ip"

9.2. IP Address Settings

We recommend using a traditional phone to configure the unit's parameters, as this is the easiest way. The following two sections contain the procedures used to configure the gateway according to how you obtain your IP address (Static IP; DHCP or PPPoE).

Every time you set a parameter item and press the "#" key to complete it, a successful setting will be confirmed by three equal tones in succession. If your setting is unsuccessful you will be prompted with one long tone.

9.2.1. Static IP Mode

The following table shows an example.

IP Address	210.67.96.121
Subnet Mask	255.255.255.248
Default Gateway	210.67.96.120
Web Management Password	123

Using the information contained in the example above. The procedure is as follows:

1. Connect the gateway to a suitable Power source.
2. Connect a traditional phone set to the "FXS" connector located on the rear panel.
3. When the CPU/ACT light is on, pick up the phone to hear the dialing tone.
4. ##0000 ; you should hear three short tones.
5. 010# ; the digit "0" is used to enable "manual" IP mode.
6. 02210*67*96*121# ; IP address.
7. 03255*255*255*248# ; Subnet Mask.
8. 04210*67*96*120# ; Default Gateway.
9. 15123# ; "123" is the web management password.
10. 981# ; Warm-restarts.
11. Hang up the phone. The system should now restart.

You can also use console to configure IP address. But phone number can't be configured by console.(Only VG3306/3310/3318)

SIP-RG>enable

SIP-RG#configure

Enter configuration commands, one per line. End with CNTL/Z

SIP-RG(config)#ip state user

SIP-RG(config)#ip address 210.67.96.121 255.255.255.248

System need to restart

SIP-RG(config)#ip default-gateway *210.67.96.120*

SIP-RG(config)#exit

SIP-RG#restart

This command resets the system. System will restart operation code agent.

Reset system, [Y]es or [N]o? Yes

9.2.2. DHCP Mode

1. Connect the gateway to a suitable Power source.

2. Connect a traditional phone set to the “FXS” connector located on the rear panel.
3. When the CPU/ACT light is on, pick up the phone to hear the dialing tone.
4. ##0000 ; you should hear three short tones.
5. 011# ; the digit “0” is used to enable “manual” IP mode.
6. 15123# ; “123” is the web management password.
7. 981# ; Warm-restarts.
8. Hang up the phone. The system should now restart.

You can also use console to configure IP address.

SIP-RG>enable
SIP-RG#configure
Enter configuration commands, one per line. End with CNTL/Z
SIP-RG(config)#ip state dhcp
SIP-RG(config)#exit
SIP-RG#restart
This command resets the system. System will restart operation code agent.
Reset system, [Y]es or [N]o? Yes

9.2.3. PPPoE Mode

If your network environment is using PPPoE, you need to prepare the information as specified in section 8. Information required before Installation.

The following table shows an example.

PPPoE Account	83721@hinet.net
PPPoE Password	123ab
Web management password	123

There are three ways to configure user name and password of PPPoE

1. Use phone set to configure:

You can configure the user name and password by using phone set. The command ‘09’ is used for username and ‘10’ is for password of PPPoE. Since the user name and password use characters and digits are accepted by phoneset only, you need a mapping between characters and digits. You can find them at section 15.4

Mapping table of characters used in PPPoE.

Example user name：83721@hinet.net，Password：123ab，The procedure is below

1. Connect the phone to the gateway
2. When CPU/ACT is light, pick up the phone and press
3. ##0000 ；You will hear 3 short tones.
4. 0938333732314068696*465742*46*46574# ；Set user name：83721@hinet.net
5. 103132336162# ；Set password is 123ab
6. 981# ；Save and restart.

2. Use Console to configure (Only VG3306/3310/3318)

SIP-RG>enable

SIP-RG#configure

Enter configuration commands, one per line. End with CNTL/Z

SIP-RG(config)#pppoe username 83721@hinet.net

SIP-RG(config)#pppoe password 123ab

SIP-RG(config)#exit

SIP-RG#restart

This command resets the system. System will restart operation code agent.

Reset system, [Y]es or [N]o? Yes

3. Use WEB Interface to configure:

You can configure the user name and password by using WEB interface. Follow the steps to finish configuration.

Step 1: Using a traditional phone set to configure the web management password and phone number

You will need to use a web browser to perform the PPPoE settings through the gateway's web based management interface. To enter the web based management interface you must have a previously configured password. Follow the next procedure to setup your password and phone number.

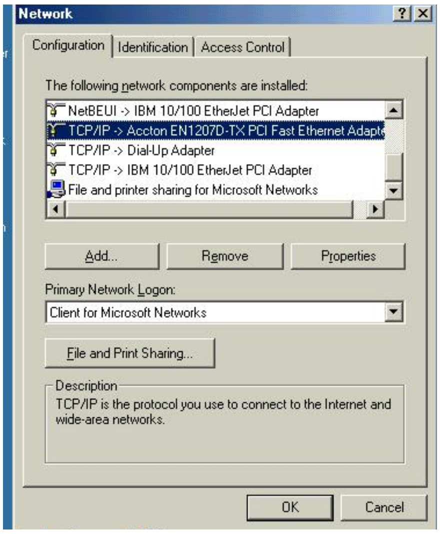
1. Connect the gateway to a suitable Power source.
2. Connect a traditional phone set to the "Phone" connector located on the rear panel.
3. When the CPU/ACT light is on, pick up the phone. You should hear the dialing tone.
4. ##0000 ; you should hear three short tones.
5. 15123 ; "123" is the web management password.

6. 010# ; "0" is to enable "manual" IP mode.
7. 02192*168*0*2# ; IP address.
8. 03255*255*255*0# ; Subnet Mask .
9. 981# ; Used to restart the gateway.
10. Hang up the phone to complete the configuration.

Step 2：Configure IP address of PC

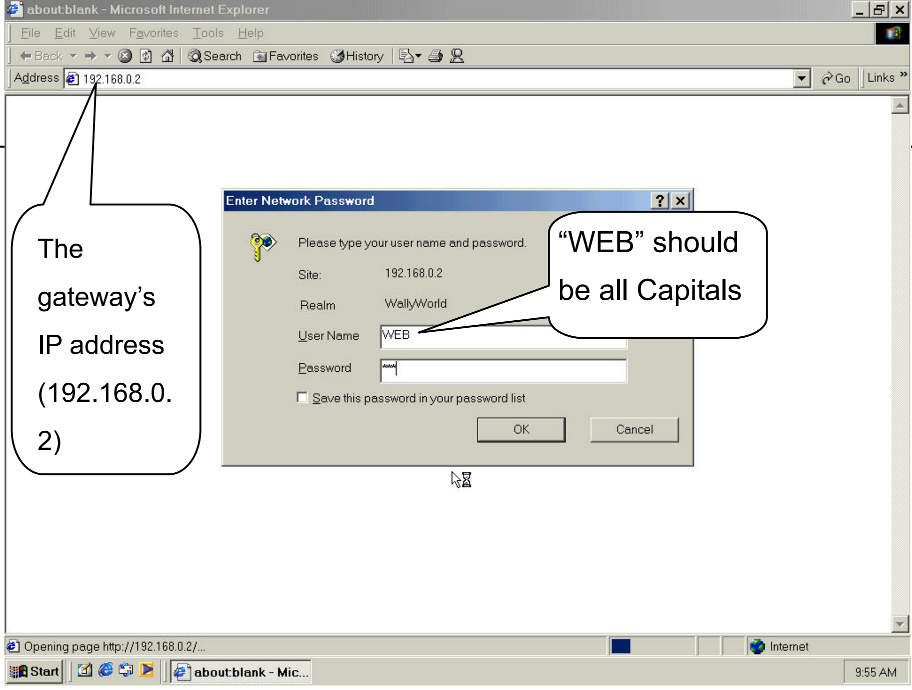
Use the provided Ethernet cable to connect your PC to the port labeled "PC", located on the rear panel of the gateway. For VG3306, VG3310, and VG3318, it is located on the front panel.

Because the gateway's default IP setting of this is 192.168.0.2, you must configure your PC to the same subnet. "192.168.0.x" for example. The following example uses 192.168.0.5 for the IP address and 255.255.255.0 for the subnet mask.



After you have completed the PC's IP address setting, you will be required to restart the PC in order for the new settings to take effect.

Step 3: Using the browser to configure the PPPoE Parameters of the gateway.



On the PC that is connected to the gateway, enter the gateway's IP address (Default 192.168.0.2) and press enter. The gateway will then prompt you with a dialogue box requesting that you enter a password. Use "WEB" (all capitals), for the User field and "123" for the password field that you have previously configured. Click the OK button; you should now have access to the gateway's web based management interface page.

Upon entering the web based configuration interface.

Click on "IP SETTING" at the top of the page and you will see the page as shown in the following image.

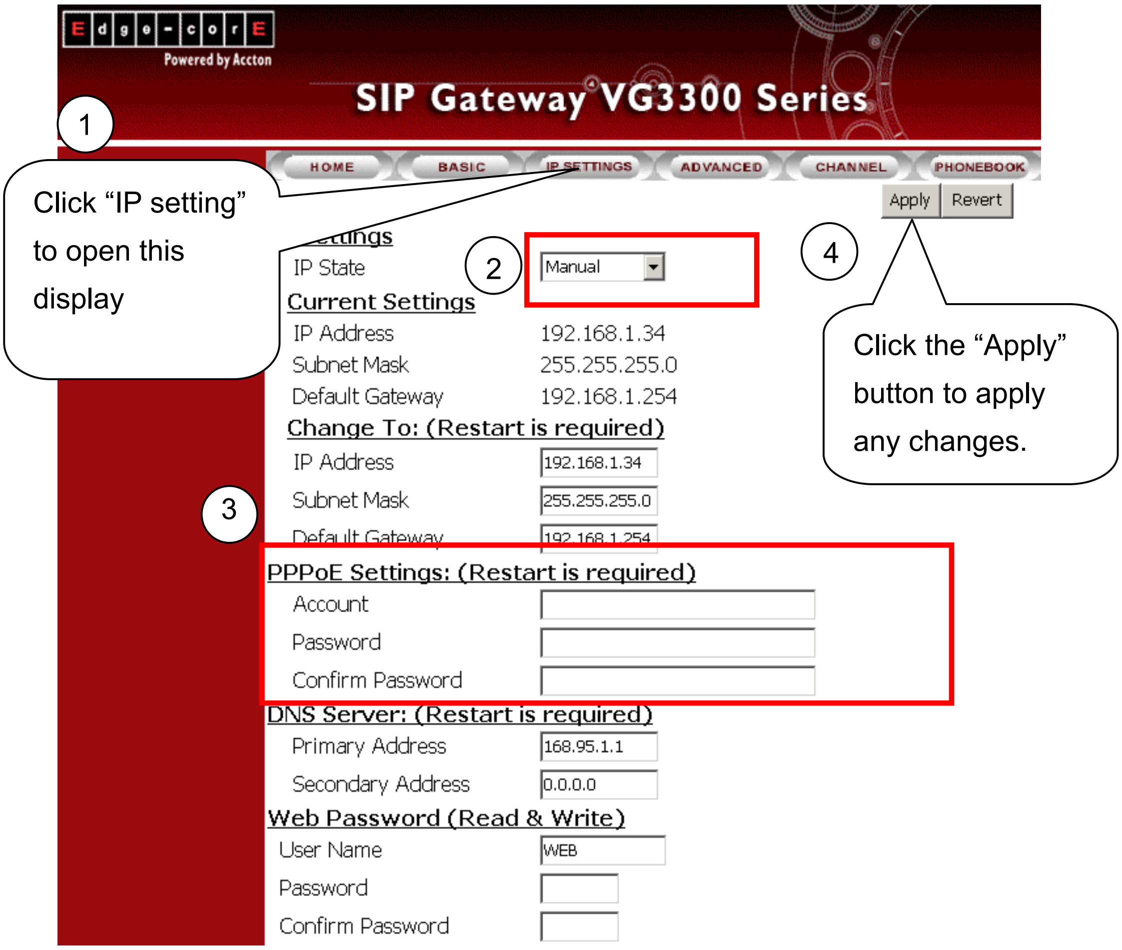
Select PPPoE from the "IP State" pull down menu.

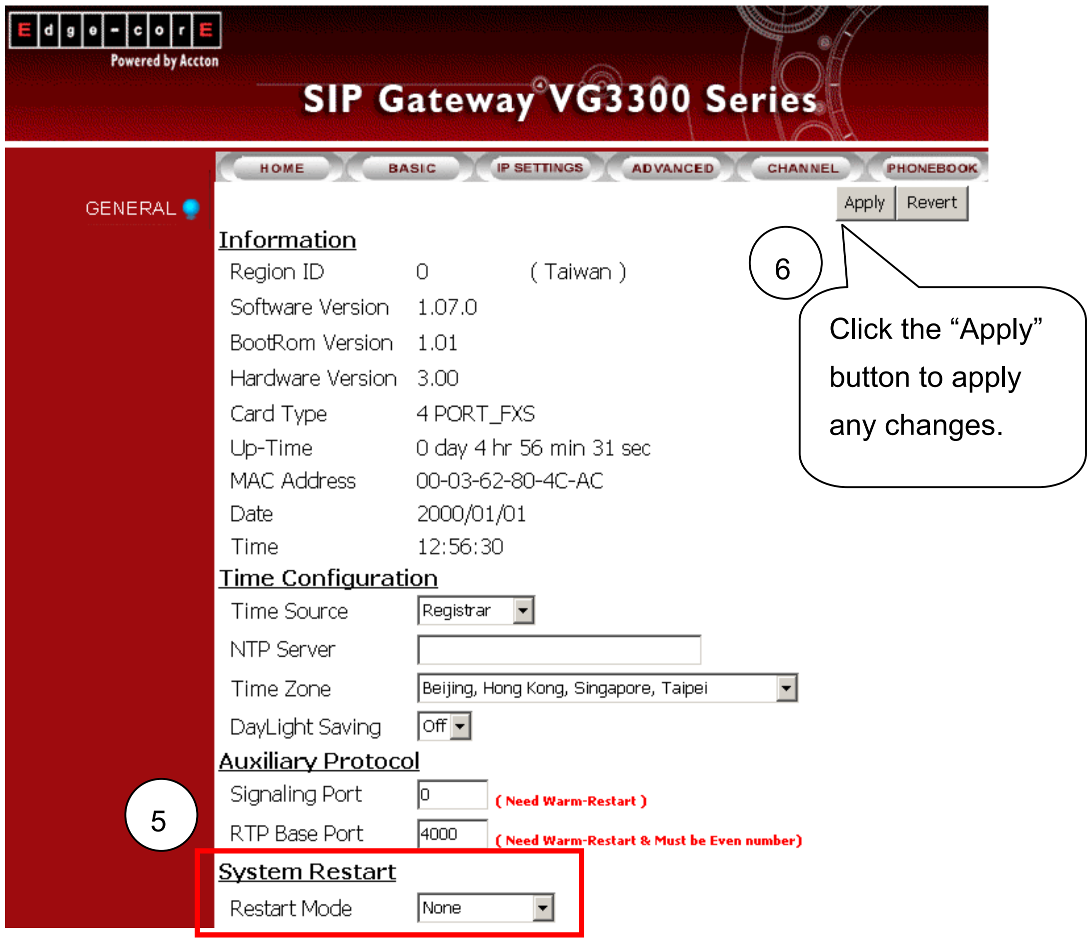
Fill in the "Account", "Password", and "Confirm Password" under the PPPoE Settings. You can obtain this information from your ISP.

Click on the Apply button.

Click the "BASIC" button at the top to go to the BASIC page and select "Warm Start" to restart the gateway. You can also perform a warm start using the phone by picking up the handset and dialing "##0000" then "981#".

After restarting, the gateway will use PPPoE to obtain it's IP address.

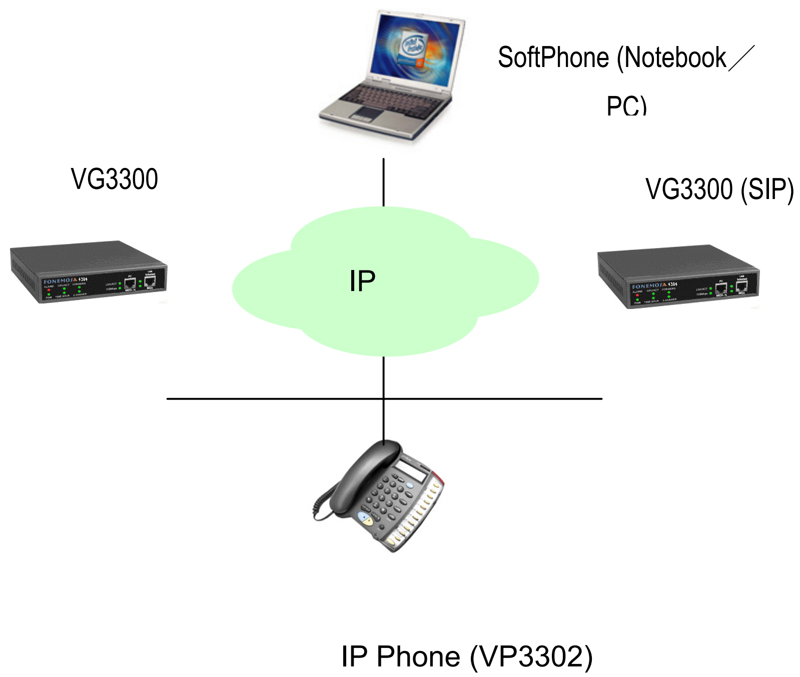

Powered by Accton
SIP Gateway VG3300 Series
HOME
BASIC
IP SETTINGS
ADVANCED
CHANNEL
PHONEBOOK
Apply
Revert
1
Click "IP setting" to open this display
IP State
2
Manual
4
Click the "Apply" button to apply any changes.
Current Settings
IP Address 192.168.1.34
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.254
Change To: (Restart is required)
IP Address 192.168.1.34
Subnet Mask 255.255.255.0
3
PPPoE Settings: (Restart is required)
Account
Password
Confirm Password
DNS Server: (Restart is required)
Primary Address 168.95.1.1
Secondary Address 0.0.0.0
Web Password (Read & Write)
User Name WEB
Password
Confirm Password



At this stage, your gateway should be able to use PPPoE to access the Internet. However, if you configured a wrong account number or password, your gateway cannot access the Internet. You are not able to use PC to access the gateway by using the IP address of 192.168.0.2 because the gateway has been set in PPPoE mode. You have to use phone set to configure the gateway back to fix IP mode (##0000 010#) and use PC browser to configure correct parameters.

10. SIP Configuration

VG3300 not only can make regular PSTN calls, it also can communicate with IP Phones or Soft-Phones by using SIP protocol. Previous paragraphs have described the way to make regular IP calls. This section shows you what parameters you need to configure for SIP calls and how to make the SIP calls.



Notice: These configurations on WEB page, after select or input value in the field, please press "Apply" button to save and confirm the setting. Some parameters need "Warm-restart", please process the restart action, thanks.

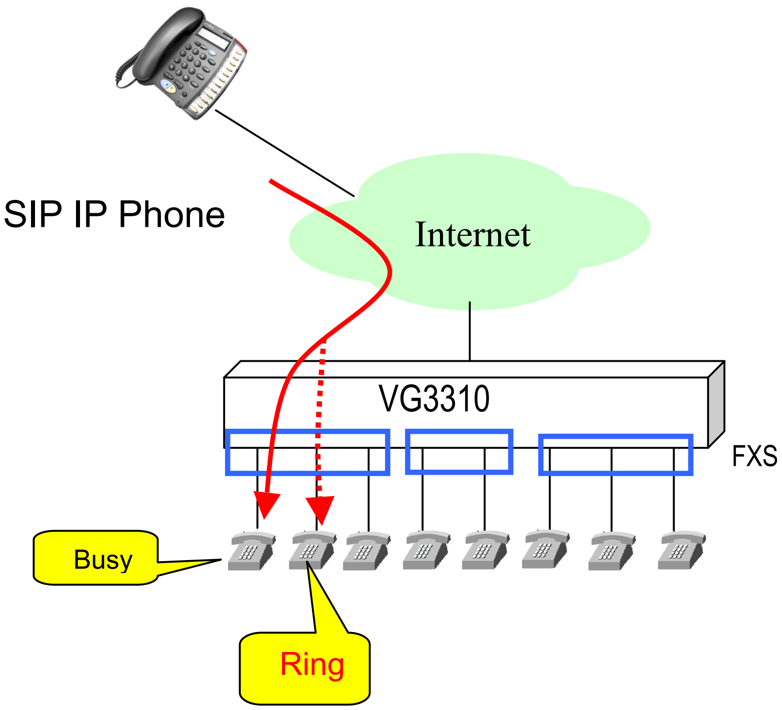
10.1. Channels and SIP entity

Many Channels can be assigned as on SIP Entity. Single Channel also can be assign as on SIP Entity.

Application example:

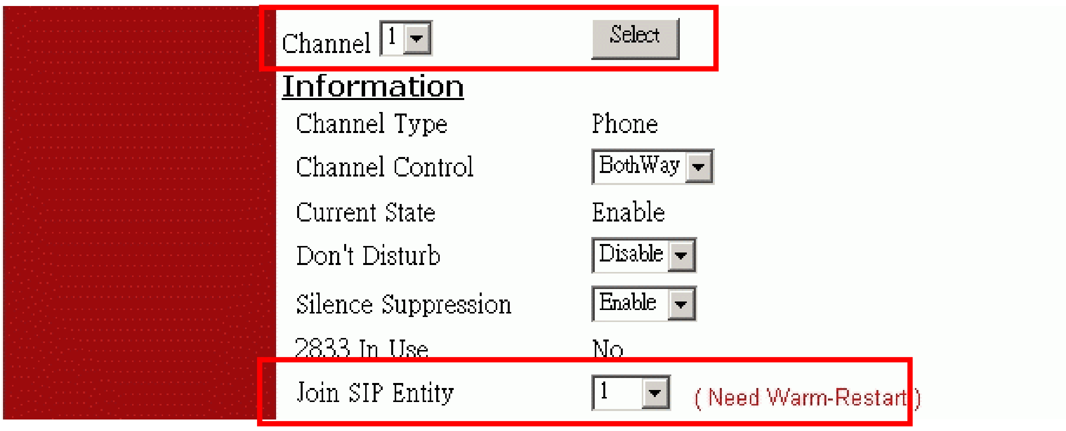
As the figure below, Channel 1-3 belongs to SIP Entity 1: 001@edge-core.com. Channel 4 and Channel 5 belongs to SIP Entity 2: 002@edge-core.com. and Channel 6-8 belongs to SIP Entity 3: 003@edge-core.com. When other device under SIP network dial into 001@edge-core.com, the phone connect to Channel 1 is ringing. If Channel 1 is under conversation (busy), the line will be switched to Channel 2, and so on. So Channel 1~3 become a simple Hunting Group. (This feature needs the support of SIP Proxy Server).

Figure:



Configuration:

WEB page: CHANNEL\



Notice: Each channel must belong to a SIP entity.

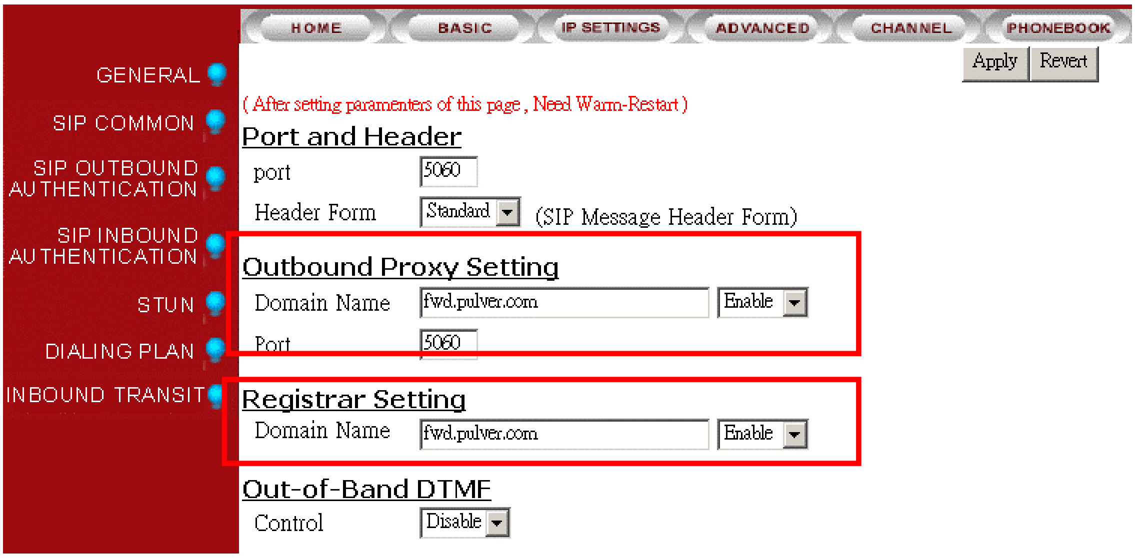
10.2. SIP Proxy and Register Parameters

You need to configure IP address or Domain name of Registrar and Outbound Proxy server, please check the information is right.

SIP service provider will give you an IP address or Domain name of Registrar and Outbound proxy when you apply for the service.

Configuration

WEB Page: ADVANCED\SIP COMMOM



Notice: The Registrar Server is only for SIP entity registering. If the SIP entity register is fail, please check the item. SIP calls are all through Outbound Proxy Server, if the parameter is not configured, the SIP call will fail. So the two parameters must be configured. If Outbound Proxy Setting is Enabled and Registrar Setting is Disabled, then all SIP call is routed to Outbound Proxy.

10.3. SIP Entity

SIP service provider will assign one or more SIP accounts for you when you apply for the service. In standard, the SIP account is called ‘Public Address’, so you need to configure the account information in ‘Public Address’ item. The format is like an E-mail address such as mary@edge-core.com.

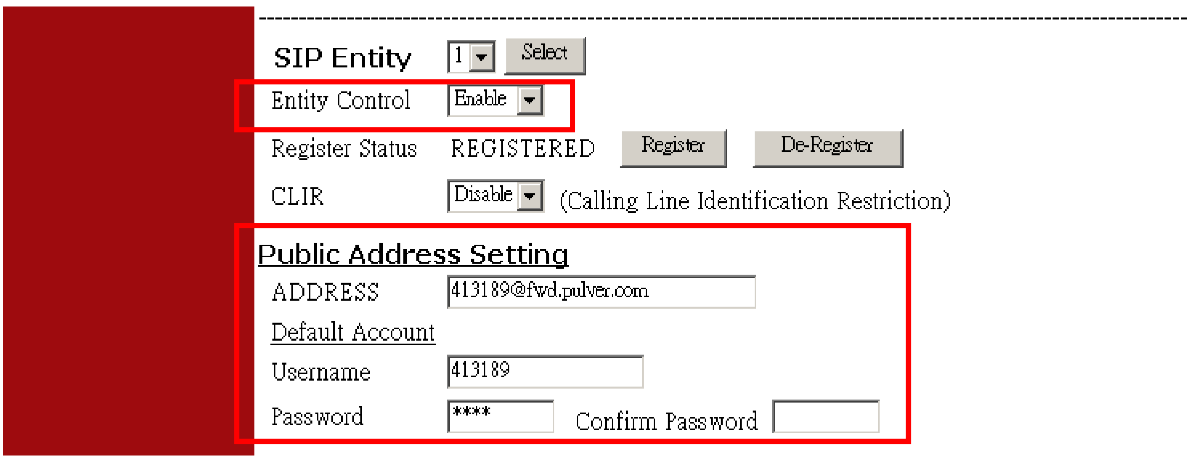
The Public Address will be generated automatically with the format below if user keeps the Public Address empty.
"Default account's username" @ "Registrar" if you had enter the information below

1. Registrar Setting. For example: fwd.pulver.com, which configured at 10.2 SIP Proxy and Register Parameters
2. Username of Default Account. For example: 413189, which is configured at below graph

For example: If the two data above is created, then the Public Address will be 413189@ fwd.pulver.com

Input Username and Password here if SIP Proxy needs it for authentication. This account information also helps you to create Realm for SIP Outbound Authentication and Public Address.

Configuration
WEB Page: ADVANCED \ SIP COMMON



You can control the SIP entity on WEB page, just select ‘Enable’ or ‘Disable’.

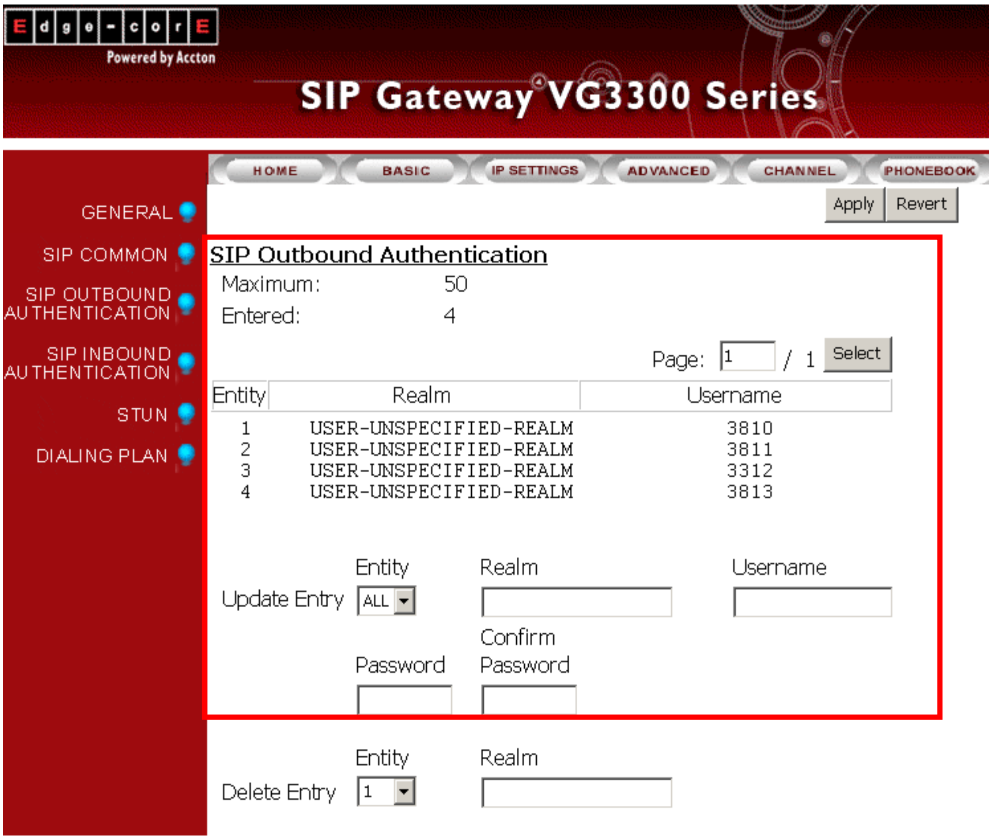
10.4. SIP Outbound Authentication

You need to configure outbound authentication for each SIP entity if SIP proxy server or other SIP phone request for authentication. Please check with SIP service provider if you need the setting. Please select the entity then input information includes realm, username, and password.

"Realm" is a kind of verification for SIP Outbound Authentication. If SIP service provider does not provides this information. The gateway will create a default Realm (by string USER-UNSPECIFIED-REALM) automatically with your Username and Password mentioned on last section for SIP Outbound Authentication. If there are more than one SIP entity is registered on this gateway. The gateway creates Realm for each entity. The default Realm helps you to register the SIP server successfully.

Configuration

WEB Page: ADVANCED \ SIP OUTBOUND AUTHENTICATION



10.5. Configure STUN

The STUN (Simple Traversal UDP through NAT) server is an implementation of the STUN protocol that enables STUN functionality in SIP-based systems. The STUN server also includes a client API to enable STUN functionality in SIP endpoints.

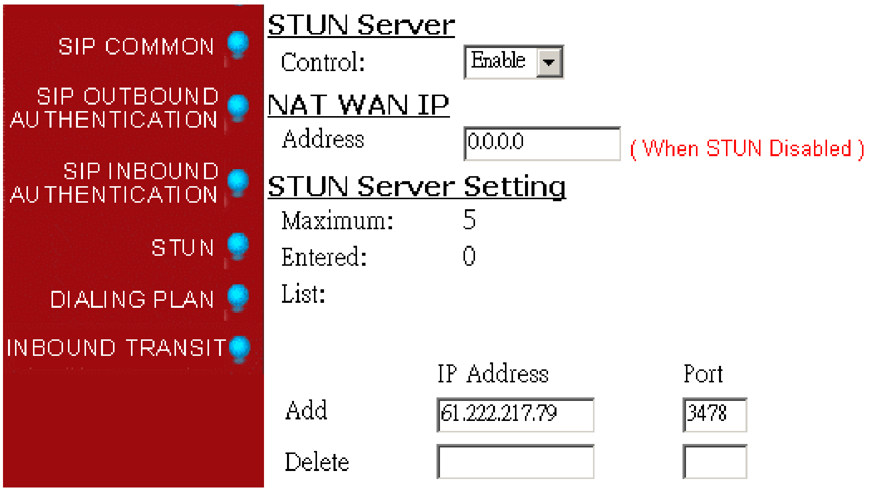
STUN is an application-layer protocol that can determine the public IP and nature of a NAT device that sits between the STUN client and STUN server.

Notice: If your gateway is behind NAT (Use Private IP), must configure the parameter.

After configuring the parameters of STUN, please act Warm-Restart.

Configuration

WEB Page: ADVANCED\STUN



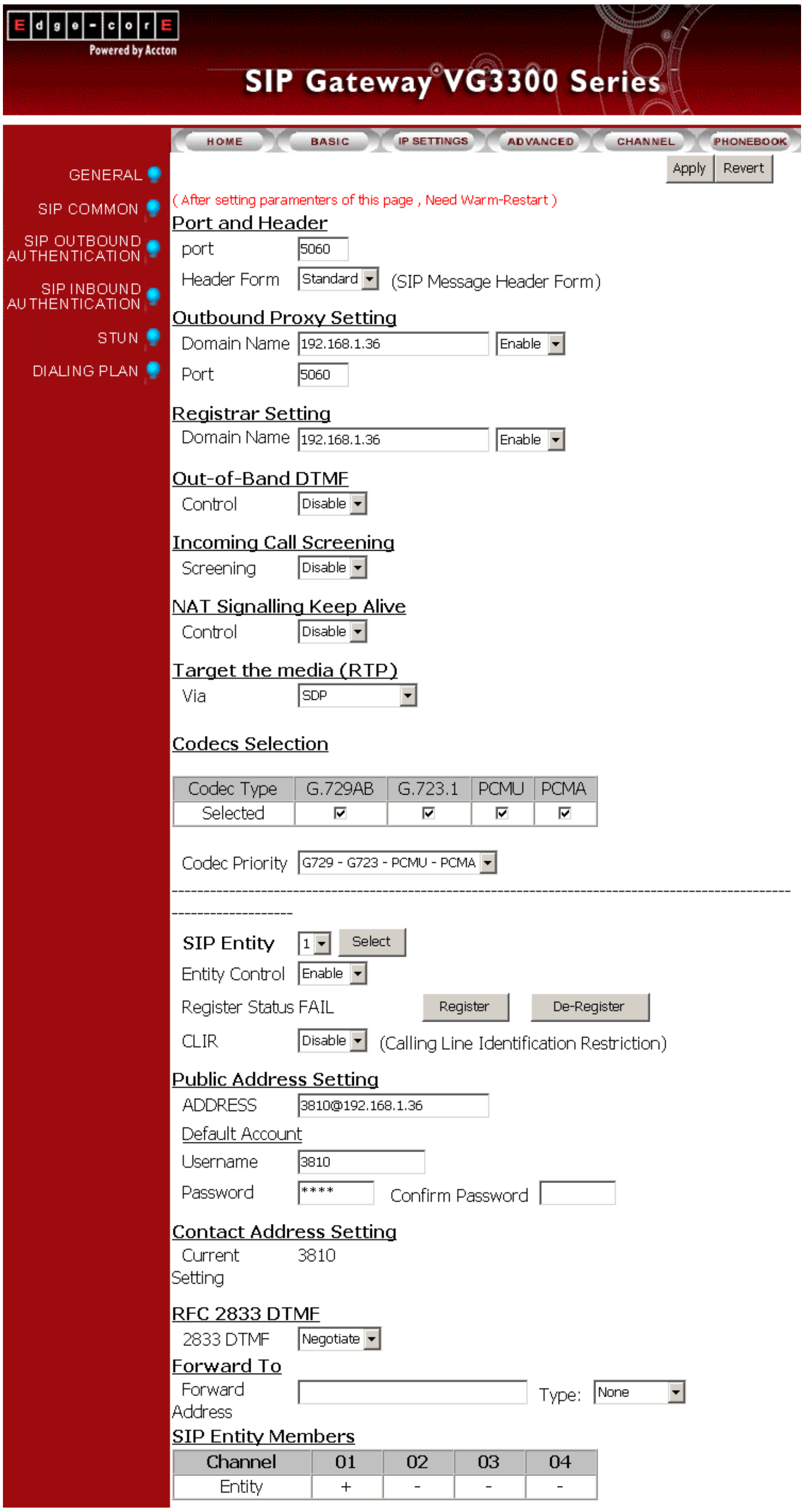
You can enable and disable the service on WEB page.

The STUN refresh time defines how long the device will send a binding request packet with discard flag on to STUN server. A binding packet with discard flag off will be sent each time when the number of binding request packet with discard flag on reach the Rebinding counts. The binding request packet is used to let the STUN server keep the most fresh client information.

10.6. Check SIP entity Status

You can use the WEB page to check the SIP entity is registered successful or unsuccessful.

WEB Page: ADVANCED\SIP COMMOM



If the status shows “REGISTERED” means successful, otherwise means fail; please notice that.

When you find the registration is fail, first check the “Registrar Setting” configuration is normal, or not “Enable”.
Then check the “Public Address” and “Outbound Authentication” configuration is in normal status.
If the configurations are all right, please check the situation with your SIP service provider.

10.7. Phone Book

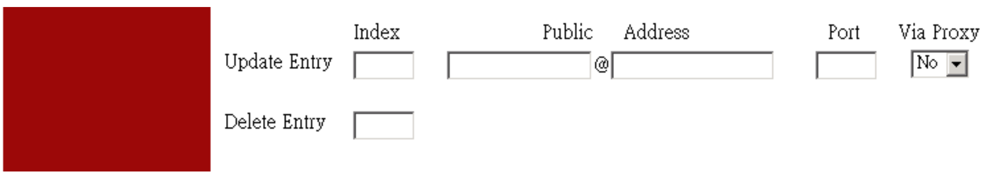
10.7.1. General Phone Book

Since the SIP phone number is not easy for regular phone to dial, VG3300 provide a SIP phone book to let standard phone to make a SIP call easier. The phone book uses index number to map SIP account. User also can configure this index number to build the route by SIP Proxy or build the route without Proxy if destination gateway use fixed IP (Public IP or private IP in VPN)
For instance if the phone book is configure as below:

Index	Public Address	Port	Via Proxy	
100	01@61.220.145.70	5060	No	<-- GW1
200	73797@fwd.pulver.com	5060	Yes	<-- GW2
201	abcd@61.222.217.5	5060	No	<-- GW2

Notice: If your SIP account is digit type like 234@edge-core.com or 456@edge-core.com, you don’t need to configure the items.

Configuration
WEB page: PHONEBOOK \



10.7.2. Hotline Function

A new Hotline function is added for VG3300 Firmware Version 1.07 or above
When hotline function is enabled, the FXS channel is connected to specified SIP device or VES3302 (if the VG3300 is configured and register to VES3302 as a client) automatically when user of VG3300 FXS channel picks up hand-set.

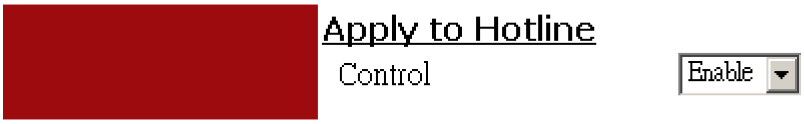
- If the FXS channel is Hotlined to other SIP device (SIP Phone, Softphone), other SIP device rings immediately when FXS channel user of VG3300 picks up hand-set.

- If the FXS channel is Hotlined to VES-3302 Line, FXS channel user of VG3300 hear dialing tone from VES3302 when pick up hand-set, and then he/she can dial extension number to other SIP device.

Configuration of Hotline

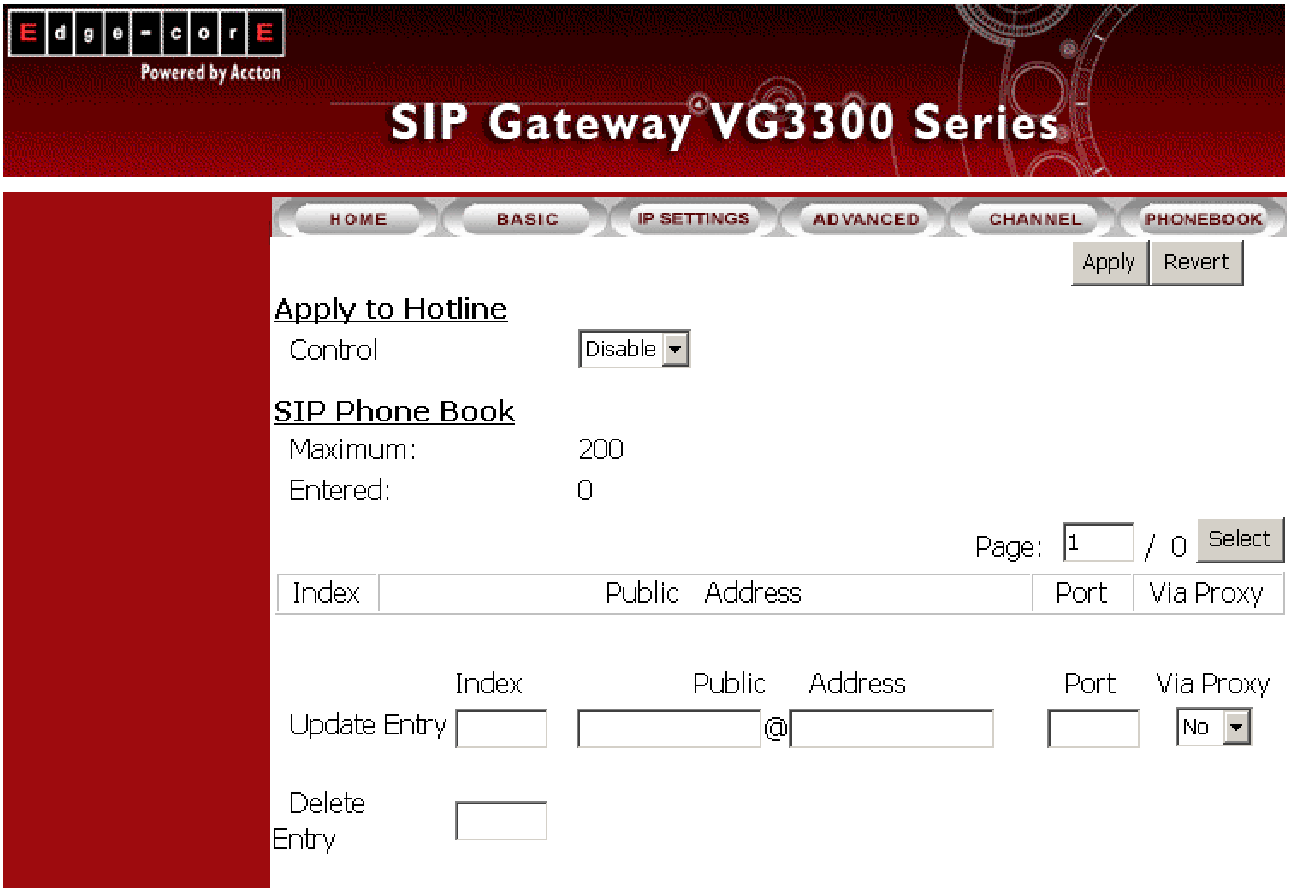
- Enable Hotline function

WEB page: PHONEBOOK \



- Setup index number

WEB page: PHONEBOOK \



When Hotline function is enabled, user also needs to specify which channels (FXS only) should join Hotline function and which SIP number (Public Address) the channel is hotlined to.

Hotline mapping table

Channel (FXS) only	Index Number	Description
1st FXS channel	1	Index number "1" maps the 1st FXS channel
2nd FXS channel	2	Index number "2" maps the 2nd FXS channel
….	….	…
16th FXS channel	16	Index number "16" maps the 16th FXS channel

Available Hotline index number

Model	Available Hotline Index Number	Note
VG3306	1, 2, 3, 4	
VG3310	Depends on module used. Please refer to table below.	Only FXS channel can be counted as index number
VG3318	Depends on module used. Please refer to table below.	Only FXS channel can be counted as index number

VG3310/VG3318 channel mapping number

Model	Group	Location	Channel Number (Please select FXS port only)			
3318	Group 1	Lower module(S1), 4 ports of left side	1	2	3	4
	Group 2	Lower module(S1), 4 ports of right side	5	6	7	8
	Group 3	Upper module(S2), 4 ports of left side	9	10	11	12
	Group 4	Upper module(S2), 4 ports of right side	13	14	15	16
3310	Group 1	4 ports from left	1	2	3	4
	Group 2	4 ports from right	5	6	7	8

Any index number that is not listed in **Available Hotline Index Number** is recognized as normal index number and they are not used as hotline function and not all of the channels have to join hotline function. Please see the example below

Example Model: VG3306

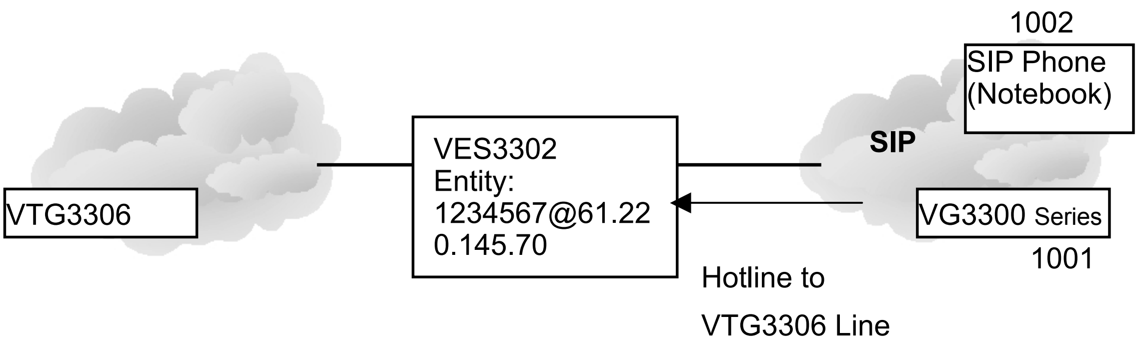
Index	Public Address	Port	Via Proxy	Description
1	01@61.220.145.70	5060	No	Channel 1 Hotline to 01@61.220.145.70 without proxy
2	73797@fwd.pulver.com	5060	Yes	Channel 2 Hotline to 73797@fwd.pulver.com by proxy,
100	jack@fwd.pulver.com	5060	Yes	No hotline function for channel 3, 4 to dial
200	mike@fwd.pulver.com	5060	Yes	

300	Jason@fwd.pulver.com	5060	Yes	

User of 1st FXS channel picks up hand set, and then 01@61.220.145.70 rings immediately
User of 2nd FXS channel picks up hand set, and then 73797@fwd.pulver.com rings immediately

Hotline to VES3302

Assume the Public Address of VES3302 is 1234567@61.220.145.70 and it has extension number 1001 to 1002.



So we configure the Phone Book as below

Index	Public Address	Port	Via Proxy	Description
1	1234567@61.220.145.70	5060	Yes	Channel Hotline to 1234567@61.220.145.70 VES3302 directly
2	1234567@61.220.145.70	5060	Yes	Channel Hotline to 1234567@61.220.145.70 VES3302 directly

User hears dial tone from VES3302 when pick up hand set and then dial extension no. for example 1002, to other SIP device

10.8. Make SIP Calls

After you have configured the SIP phone on the SIP phone book, you can easily make SIP calls.

You can select one way to make SIP call following these ways:

Standard Call: Dial <numbers>+<#>.

1. Compare dialing plan, check the number if it is in setting. Example 050.
2. If the number is in setting, send the call to proxy. If the calls does not match dialing plan or the registration to the proxy is fail, then the call will be sent to PSTN.

3. If the number is not in dialing plan, the call will be sent to PSTN.

Phone Book Call: Dial <#>+ <index>+<#>.

1. Compare SIP Phone books; check the number if it is in phone book.
2. If the number is configured in Phone Book and Proxy selection is set to "No", you will hear a busy tone. If Proxy selection is set to "Yes", then send the call to proxy.
3. If the index number you had configured to use **Via Proxy** but it communicates with proxy failed, you will hear busy tone.
4. If the number is not in phone book, you will hear busy tone.

Force PSTN Call: Dial <*>+<numbers>.

Always go through PSTN

Hotline Call:

If the channel is configured to use Hotline function, any dialing above is disabled. If the channel is hotlined to other SIP device, no dialing is needs after user picks up handset. Other SIP device rings immediately.

Hotline Call to VES3302:

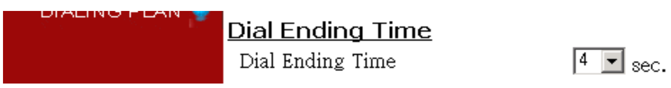
Dial <SIP extension number> or

<Prefix number (configured in VES-3302 Line)>

1. If you dial SIP extension number, other SIP device that register to VES-3302 Line with that SIP extension number will ring.
2. If you dial Prefix number, the call is relay to the IP-PBX network according to the Prefix Map specified in VES-3302 Line.

Notice: If you do not want to dial "#" after numbers, please configure the 'Dial Ending Time' item. After the seconds, the call will be sent automatically.

WEB Page: ADVANCED\GENERAL

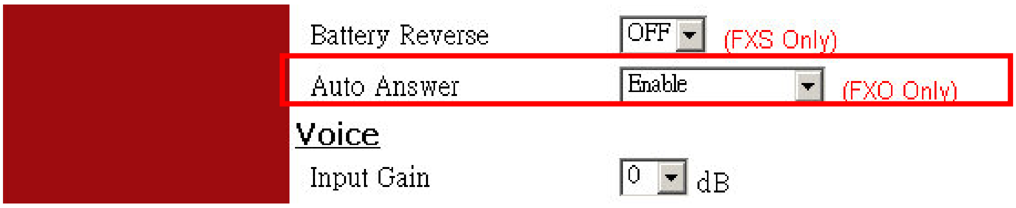


10.9. Make Inbound Transit Call

To make an inbound transit call from PSTN to SIP, you have to enable Auto Answer function of this gateway

Please enable Auto Answer configuration at

WEB Page: CHANNEL



If you don't enable the Auto Answer configuration, the inbound call from PSTN will be assigned to a free FXS port of this gateway directly. It makes Inbound Transit Call impossible.

When Auto Answer function is enabled, the gateway will answer the call and calling side will hear the second dial tone. For the Auto Answer function, it is also divided into **Enable** and **Enable w/ Pincode** options. The configuration page is the same as above.

Dial Inbound Transit Call when Auto Answer is configured as Enable

Please dial the number below after the second dial tone:
1. SIP Number + ‘#’, Example: 73797# or
2. ‘#’ + Index Number + ‘#’, Example: #123#

If you still need to make a call to the FXS port of this gateway, please press "*" to seize a free FXS port.

Dial Inbound Transit Call when Auto Answer is configured as Enable w/ PIN code

This Auto Answer mode provides security control for the Inbound Transit call

Please dial the number below after the second dial tone:
1. PIN code + ‘#’+ SIP Number + ‘#’, Example: 7742#73797# or
2. PIN code + ‘#’+ ‘#’ + Index Number + ‘#’, Example: 7742##123#

If you still need to make a call to the FXS port of this gateway, please press "*" to seize a free FXS port.

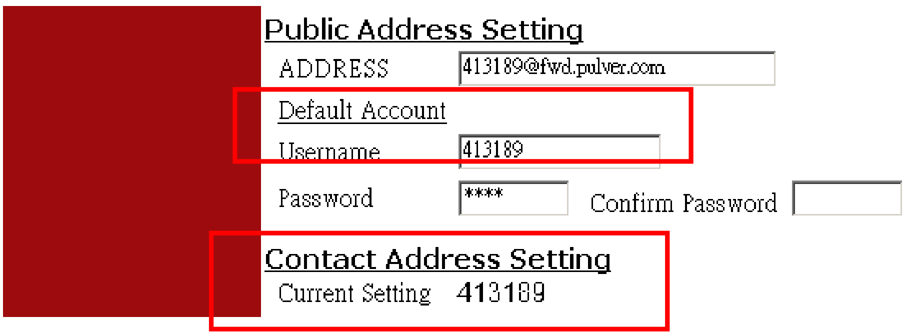
Notice for the Inbound Transit Call

1. If the SIP number that user dial does not match any prefix code configured in Dialing Plan page, the call is disconnected.
2. If the PIN code does not match any passwords configured in Password For Inbound Transit page, the call is terminated.
3. If the Index Number does not match any pre-configured Phonebook Index in Phone Book page, the Index Number will be regarded as SIP number and create a IP call without applying any match rule configured in Dialing Plan.

For which free FXS port that this gateway will seize, please refer to 11.5 Non-SIP Call port seizure preference
The PIN code (Password for Inbound Transit) is configured at chapter 12.8 Inbound Transit
The Dialing Plan is configured at chapter 11.1 Dialing Plan
The Index Number is configured at chapter 12.11 PHONE BOOK

10.10. Contact Address

The main purpose of Contact Address is making SIP calls without proxy.
The Contact Address is the same as the "Username" of Public Address if that field is configured. For S/W version above 1.05, the value is read only. Generally speaking, "Username" of Default Account are digits and it is regarded as SIP number.
WEB Page: ADVANCED\SIP COMMOM

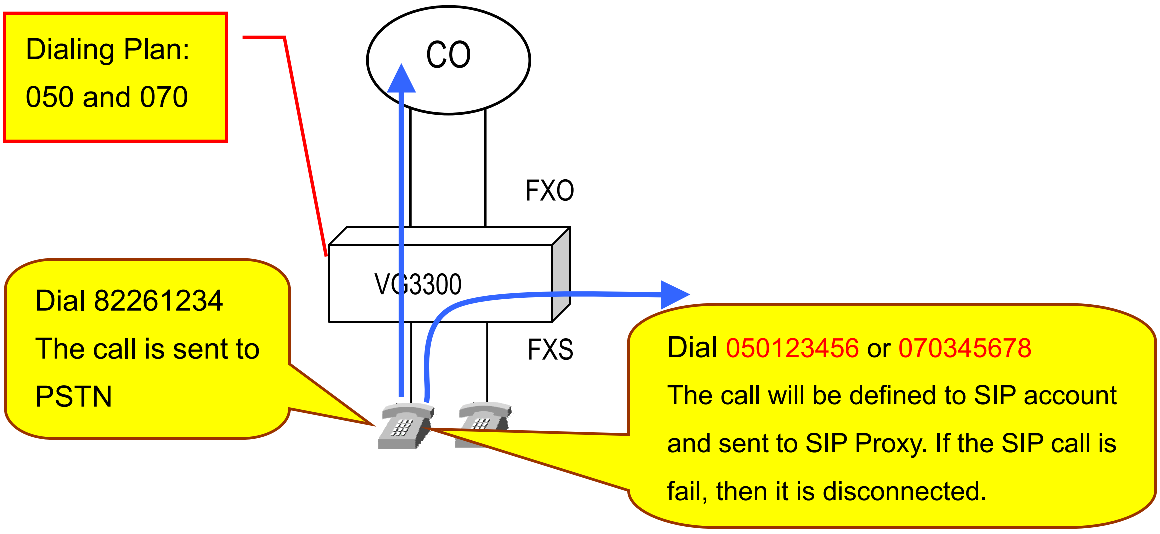


Making SIP calls without proxy server:
The SIP protocol allows you to make SIP calls directly to the destination number without through the proxy server. You can simply dial the SIP number to connect other SIP gateway. The typical example is: 413189@fwd.pulver.com. Other SIP gateway that had already configured 413189@fwd.pulver.com in Phone Book can connect this gateway by number 413189 without routing through SIP Proxy.
Notice: For this type of SIP calls, the destination device's IP address is already known and fixed.

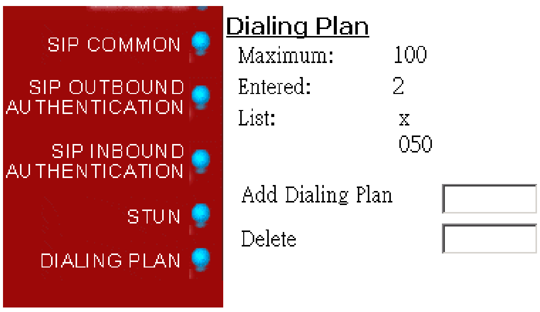
11. Other Parameters

11.1. Dialing Plan

X means all calls will be sent to SIP proxy, if the SIP call is fail, it is disconnected. Only if Outbound Proxy is disabled, then the gateway will try to connect the number by PSTN. Outbound Proxy Setting can be configured on Web Page: SIP Common. Please refer to 12.4 SIP COMMON
If the configuration is only '050' means the numbers like 050xxxxx will send to SIP proxy, if you dial any other numbers like 100, the number will send to PSTN immediately.



Configuration
WEB Page: ADVANCED\Dialing Plan



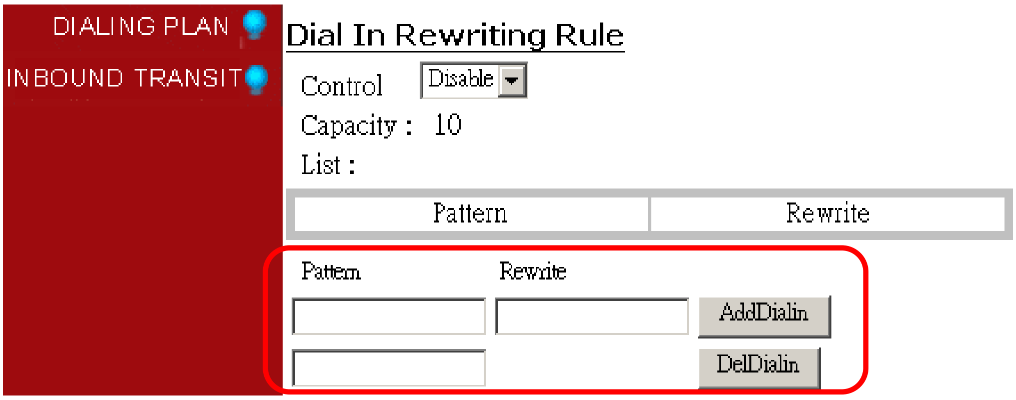
Dial In Rewriting Rule

Number dialed from VG3300 can be converted to different number and sent to SIP Proxy. User can pre-define maximum 10 sets of prefix rewriting rule to convert the number that user dials before build the connection to SIP Proxy. It is useful to create a user-friendly dialing behavior and also can limit user to dial certain number. The rules below explain the judgment.

1. System will check the dialing plan on last page in advance to decide whether it is PSTN call or SIP call.
2. If the call will be send to SIP Proxy, then system will exams the number to see if it meets Rewriting Rule.
3. If the SIP call does not meets any Rewriting Rule, system will build the SIP call with the number that user dials.
4. If the numbers of the SIP call meets any Rewriting Rule, then the numbers is converted (or limited if it meets barring rule) and system build the SIP call by converted number.

Here is the example

Web Folder: ADVANCED \ DIALING PLAN



Pattern: Add the pattern that user may dial

Rewrite: Add the converted number if user dials the same digits in pattern column.

Fill in digits and click the AddDialin button

By the operation above, we create a Rewriting Rule table below and it controls all SIP call.

Pattern	Rewrite	X means any digits. ! means the call is terminated.
00x		If the prefix number dials from user are 001~009, then the 3 digits are removed. For example, if user dials 0028621123456, then the system dials 86211123456 to build SIP call.
0	886	If the prefix number dials from user are 0, then the digit is replaced with 886. For example, if user dials 0921123456, then the system dials 886921123456 to build SIP call.

x	8862x	If the prefix number dials from user are 1~9, then add 8862 in front of the original number. For example, if user dials 82263368, then the system dials 886282263368 to built SIP call.
0204	!	If the prefix number dials from user are 0204, then the call is terminated.

Matching Rule

1. Best Match rule, the longest digits match first.
2. Wildcard (x digits) match last

11.2. Call Forward

There are three forward types:

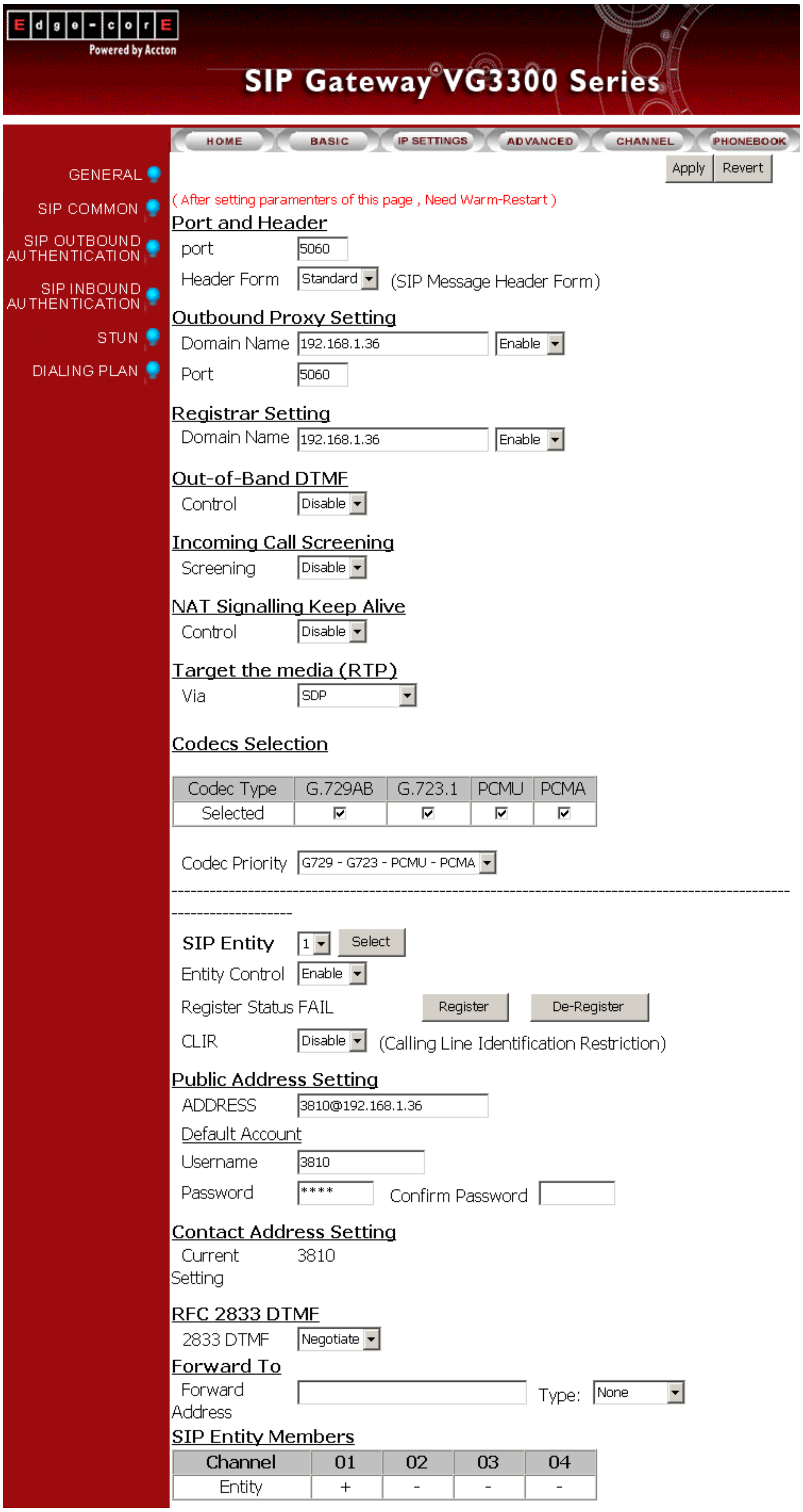
1. All: All incoming VoIP call to the SIP entity will be forward.
2. Busy: When the SIP entity is busy, the incoming VoIP call will be forward.
3. No Answer: When the SIP entity is no answer and after 30 seconds, the incoming VoIP call will be forward.

Notice:

- In order to let the caller identify the port has been configured ”forward”; the caller will hear second dial tone, rather than normal dial tone.
- If Auto Answer function is disabled, incoming call from PSTN seizes a free FXS port. The call is not forwarded even the seized FXS port is part of Call Forward SIP Entity.
- If Auto Answer function is enabled, Incoming PSTN call dials "*" to seize a free FXS port after second dial tone. The call is not forwarded even the seized FXS port is part of Call Forward SIP Entity.
- If Auto Answer function is enabled, Incoming PSTN call dials "SIP phone number" of the gateway itself after second dial tone. The call is forwarded to other VG3300 or SIP device.

Configuration

WEB page: ADVANCED\SIP COMMOM



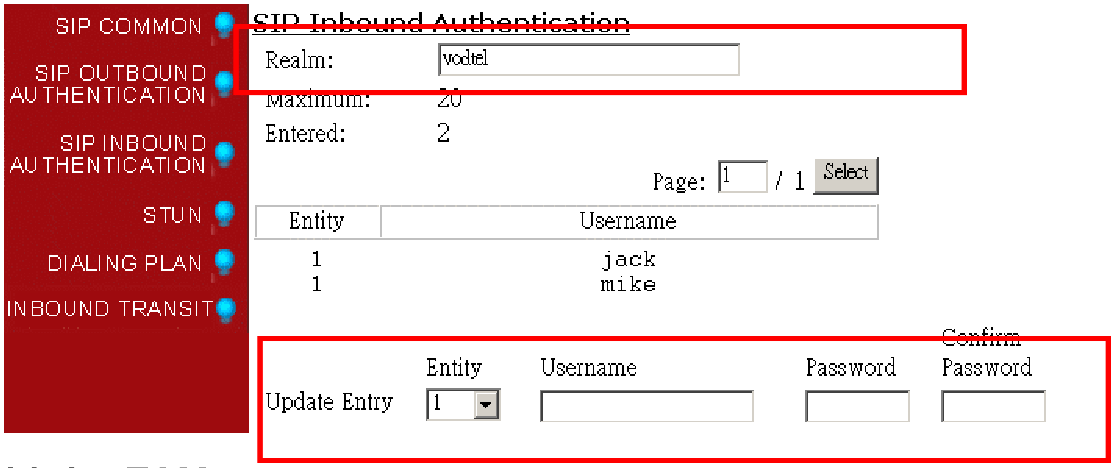
Phone Set: Please refer to section Appendix A: Phone-Set Command.

11.3. Inbound Authentication

You need to configure inbound authentication if you request authentication for other SIP phone to call you.

Configuration

WEB Page: ADVANCED \ SIP INBOUND AUTHENTICATION



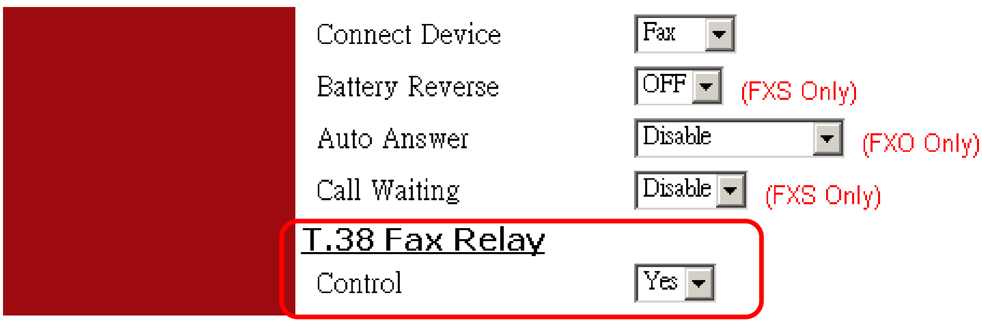
11.4. FAX

For VG3300 software version 1.05 or above, SIP-based T.38 Fax protocol is applied. Any brand SIP gateway with SIP-based T.38 Fax protocol can transmit FAX with each other. T.38 is FAX protocol and it has better performance and better successful transmission rate. However, SIP device that does not support SIP-based T.38 still can transmit and receive FAX with VG3300 by G.711 codec. G.711 codec uses more bandwidth, so it may not as good as SIP-based T.38 protocol if bandwidth control is the key factor of the network.

Setup method is listed below:

1. Web folder: “Channel”

   Enable T.38 Fax Relay support. Configure it to Yes



2. Warm-Restart the system

Note: For FAX transmission, two gateways will change to SIP-Based T.38 Protocol automatically if both sides support SIP-based T.38.

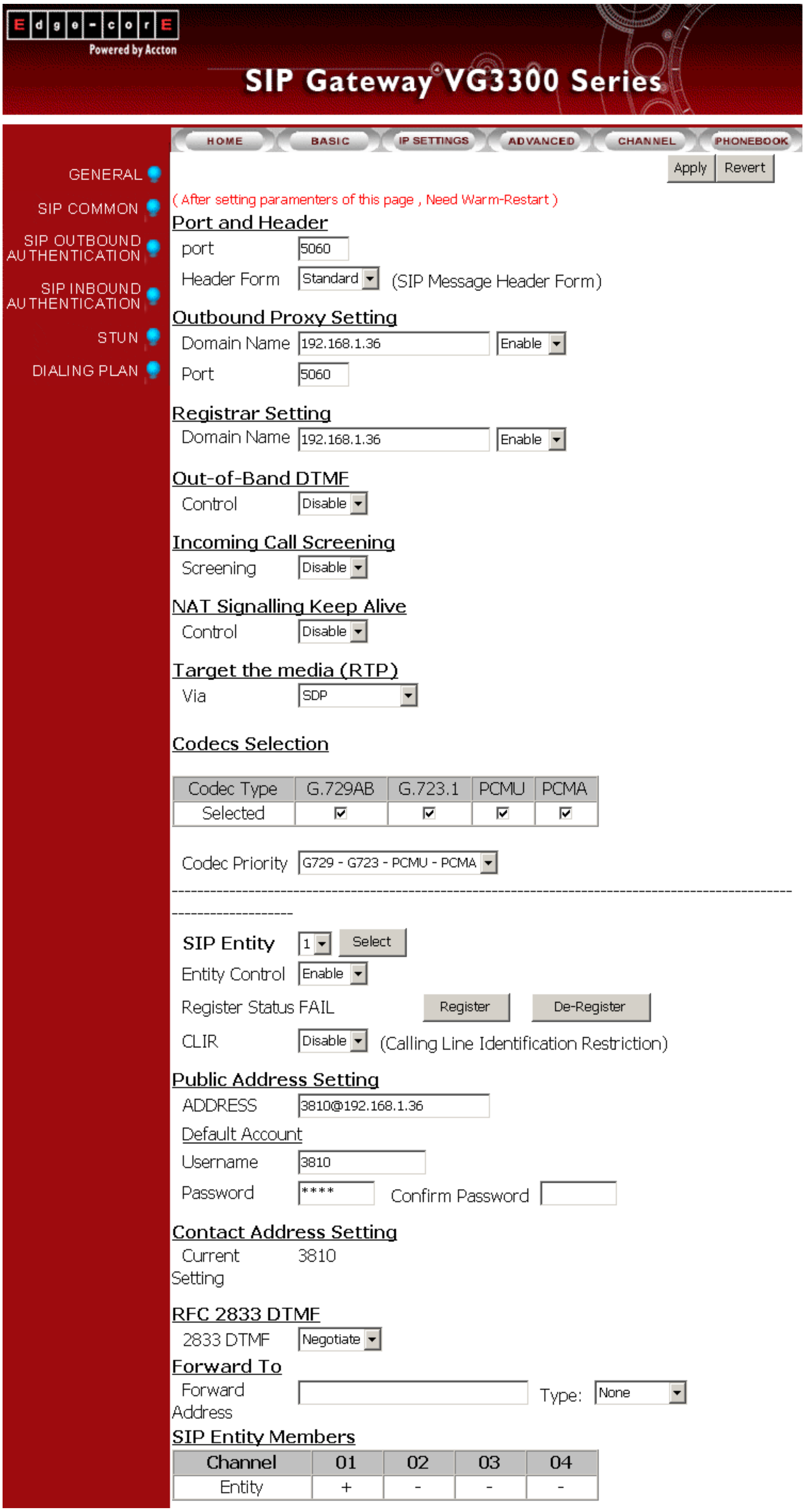
Note:

If VG3300 connects different SIP devices, some have T.38, but some use G.711 codec only, then user should enable G.711 codec support for FAX. Setup method is listed below:

1. The same step as above set Connect Device to Fax

2. Setup “Codecs Type“, Web Folder: ADVANCED\SIP COMMON

Select and mark “PCMU” and “PCMA” Codecs (G.711 Standard), than click “Apply” button



3. Warm-Restart the system

11.5. Non-SIP Call port seizure preference

For non-SIP Calls, the port seizure preference is listed below

1. Inbound from PSTN

If the inbound FXO port was configured as "Fax" device, it will also seize only FXS ports that "Connect Device" is configured as Fax. The Voice devices behave the similar way.

From FXO port to FXS port		Note
Connect Device at FXO port	Connect Device at FXS port	
VOICE port	Select VOICE port only	From the lowest port number upward
FAX port	Select FAX port only	From the lowest port number upward

2. Outbound to PSTN

For the calls from FXS to FXO, the ports of the same "Connect Device" type will be the prior selection for the calls.

If there is no correct configured port is available, it will ignore the "Connect Device" setting and create a call as the rule below.

From FXS port to FXO port		Note
Connect Device at FXS port	Connect Device at FXO port	
VOICE port	Select VOICE port (1st priority)	From the highest port number downward
	Select FAX port (2nd priority)	
FAX port	Select FAX port (1st priority)	From the highest port number downward
	Select VOICE port (2nd priority)	

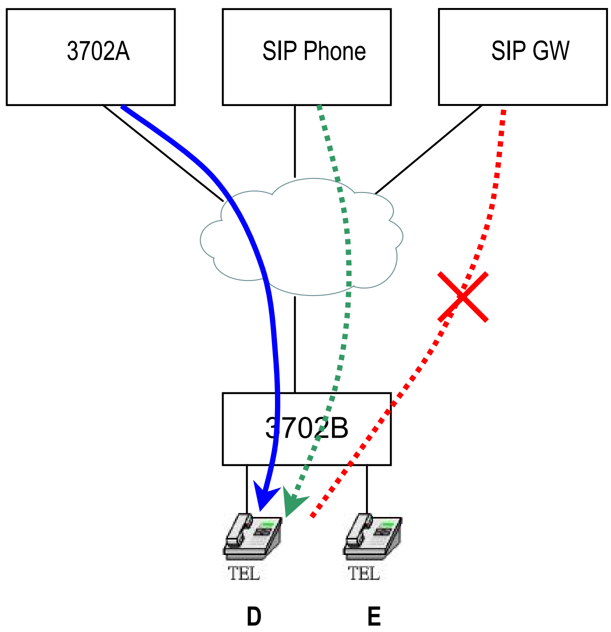
For the setting of "Connect Device", please refer to 12.10 CHANNEL

11.6. Call Waiting

Call waiting function for a FXS port to answer two SIP calls.

When D answer a SIP call from other SIP phone or gateway, such as A. In normal condition, another incoming call dial to D will be busy, such as B to D. With Call Waiting function, the phone call dials from B to D will not be busy. Here is the possible situation.

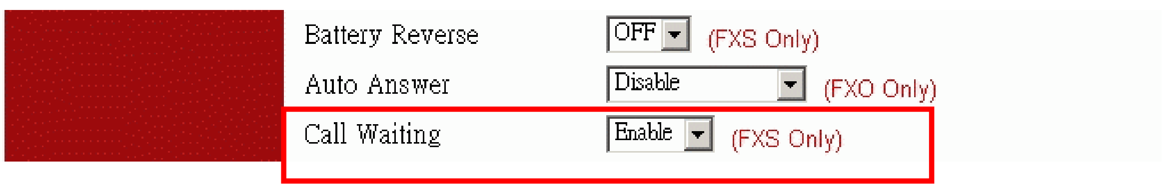
- D keeps talking with A and hears Call Waiting Tone if B calls D.
- B hears normal ring back tone without sense any different.
- If D keep talking with A and ignore the Call Waiting Tone for more than 30 seconds, Call Waiting Tone stop and the phone call return to normal condition
- If D keep talking with A and ignore the Call Waiting Tone for more than 30 seconds, B keep hearing ring back tone for 30 seconds and listen busy tone finally.
- D can talk to B if D presses Flash button when hearing the Call Waiting Tone. Phone A is silent when D talk to B.
- D can talk to A or to B by keep pressing Flash button to switch the two side.
- C will hear busy tone when C call to D if there is one line in call waiting status for A.



Configuration

Enable the Call Waiting function of the FXS port (D) of VG3300 gateway. This function can be configured for each FXS port individually.

Web Folder: Channel\



Connection Type
A: FXS port of VG3300 Series
B, C: SIP Device (VG3300 Series, other brand SIP gateway. SIP phone...), Normal PSTN phone call (special condition is described below)

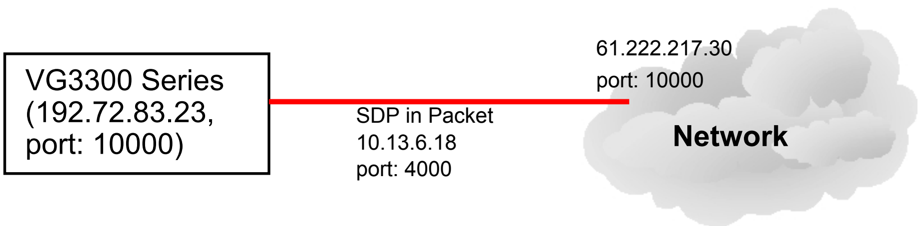
Call waiting function works only on SIP call. So PSTN call works when it is transited as SIP call. If Inbound transit call is configured on VG3300 (please refer to 10.9 Make Inbound Transit Call), then Call Waiting function is available when user dials the SIP number of this VG3300 gateway itself. If no inbound transit call function is configured, it is impossible to do call waiting function.

11.7. Target the Media (RTP)

For the SIP call passing through NAT, it is possible that the media would not deliver properly; owing to the RTP contact information (IP address, port number) is different from original RTP packet. This function selects different contact information for VG3300 to send RTP Packets to other SIP device within far-end NAT. It designates whether to use the source contact information from the UDP/IP header (Symmetric RTP) or the contact information specified within the packet (SDP) when the gateway send RTP packet

Web Folder：ADVANCED\SIP COMMON, Default Value is SDP

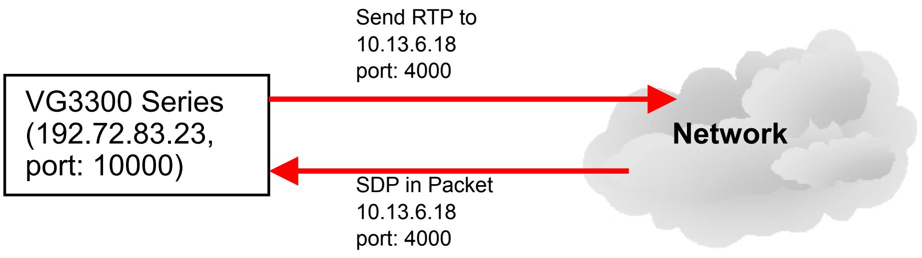
Example 1: Via Symmetric RTP
The source contact information (IP, port number) of RTP packet is IP: 61.222.217.30, port number: 10000, but the SDP in the packet is IP: 10.13.6.18, port: 4000. In this case, please Use **Symmetric RTP**



VG3300 tries the contact information from SDP first (IP:10.13.6.18, port number: 4000). If VG3300 finds that the contact information from SDP is different from the source contact information, then it will try the source contact information, as the example above, use IP:61.222.217.30, port number:10000. It makes SIP call successful.

Example 2: Via SDP (Default)

This selection ignores the source contact information (IP, port number) which VG3300 received. It always sends the RTP packet to the contact information (IP, port number) described in the packet (SDP) received.

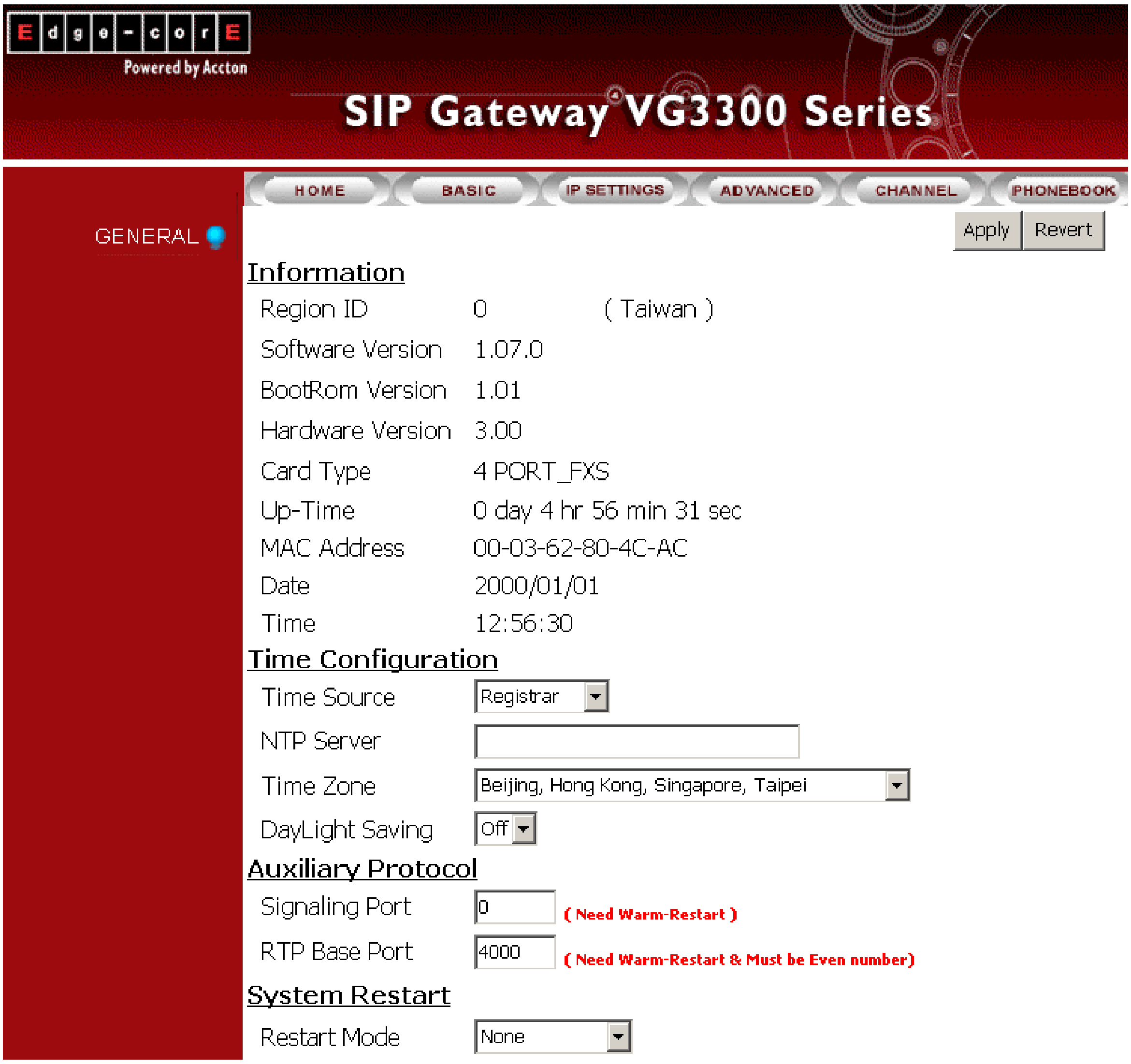


12. WEB MANAGEMENT INTERFACE

The Tree Architecture of Web Management is shown below

HOME	BASIC	GENERAL
	IP SETTING	
	ADVANCED	General
		SIP COMMON
		SIP OUTBOUND AUTHENTICATION
		SIP INBOUND ATHENTICATION
		STUN
		Dialing Plan
		Inbound Transit (for gateway has FXO port. Gateway without FXO port does not have this page)
	CHANNEL	
	PHONE BOOK	
	ACCESS CODE	

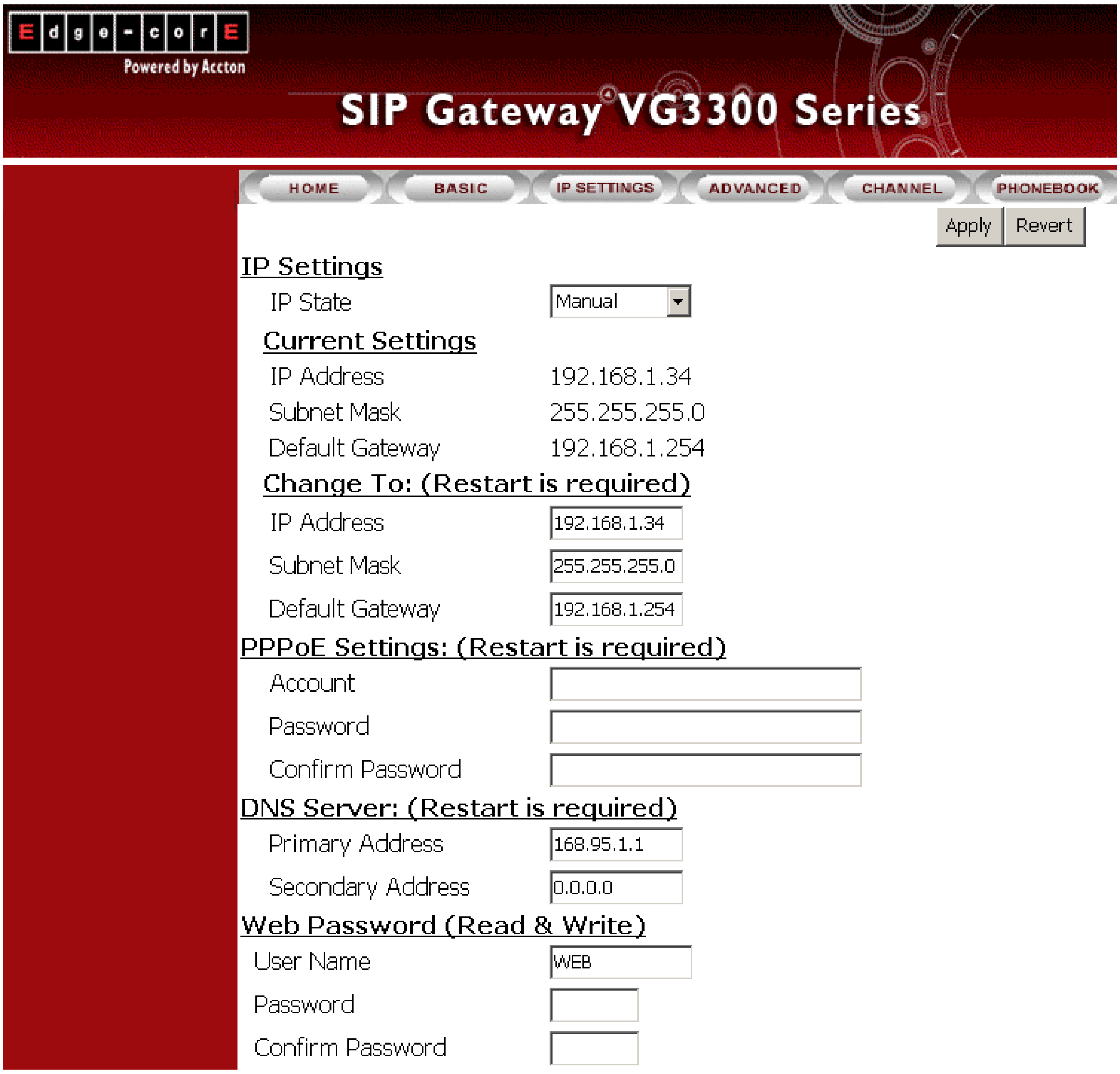
12.1. BASIC / GENERAL



Category	Section	Description	Default Setting
Information	Region ID	Display region ID.(Read only)	0
	Software Version	Display software version.(Read only)	
	BootRom Version	Display BootRom Version.(Read only)	
	Hardware Version	Display hardware Version.(Read only)	
	Card Type	Display card type. (Read only)	
	Up-Time	Display the use time since from system reboot.(Read only)	
	MAC Address	Display MAC address.(Read only)	
	Date	Show the date	
	Time	Show the time	
Time Configuration	Time Source	Select the time server to synchronize the time of this gateway ♦ Registrar: Get the time data from the Registrar Server. ♦ NTP Server: Get the time data from the NTP Server	Registrar
	NTP Server	Input the address if the system use NTP server as time synchronization source. The gateway will synchronize with the NTP Server once a day. If the NTP server inputted here is not available or fail to response, the gateway will retry it every 5 minutes. The gateway has its own clock, so the clock will keep going according to last synchronization time. For NTP server information, please refer to http://www.ntp.org	
	Time Zone	Select local system time zone. Select correct Time Zone.	

	Daylight saving	ON: Enable daylight saving. OFF: Disable daylight saving.	OFF
Auxillary protocol	Signaling Port	UDP port to transfer signal packets. It can be setting in the range of 0 to 65535. (Must reboot system to apply changes)(Only support VG and VTG devices)	0
	RTP Base Port	Base of UDP port to receive RTP packets. It can be setting in the range of 0 to 65534.(Must be Even, after setting this item, please reboot system to apply changes)	4000
System Restart	Restart Mode	None: Not to restart system. Cold restart: Cold restart. Warm restart: Warm restart.	None

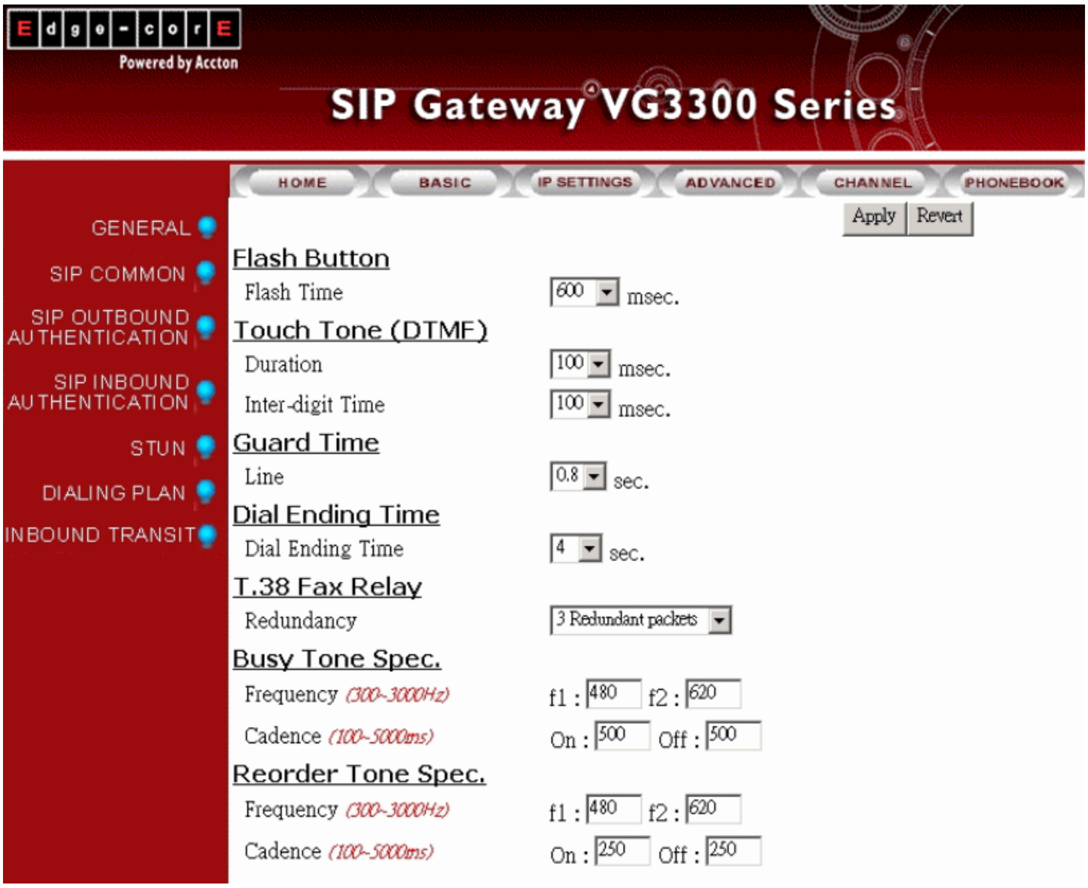
12.2. IP SETTING



Category	Section	Description	Default Setting
IP Settings	IP State	The way to obtain IP address: Manual: Entered by user (Static IP) Auto(DHCP): Assigned by DHCP server PPPoE: Assigned by PPPoE of ISP	Manual

	Current Setting	Display the configured IP address, subnet mask address and default gateway. (Read only)	192.168.0.2 255.255.255.0 192.168.0.1
	Change To	Enter the IP address that will be used after next restart, Including: IP Address Subnet Mask Address Default Gateway (This item is used only on Manual mode of IP Setting.)	
PPPoE Settings	Account	The user's account of PPPoE protocol, provided by ISP.	
	Password	The user's password of PPPoE protocol.	
	Confirm Password	Confirm the user's password of PPPoE protocol.	
	Service Name	The service name of PPPoE account, provided by ISP. (Most ISP doesn't need this)	
DNS Server	Primary Address	The primary address of DNS server. The default setting would be different according to the local area. In Taiwan, the default setting is 168.95.1.1.	168.95.1.1
	Secondary Address	The secondary address of DNS server.	
Web Password	User Name	The user's name of Web Management Interface.(12 character)	WEB
	Password	The password of Web Management Interface.(6 character)	
	Password Confirm	Enter the password again to confirm it.	

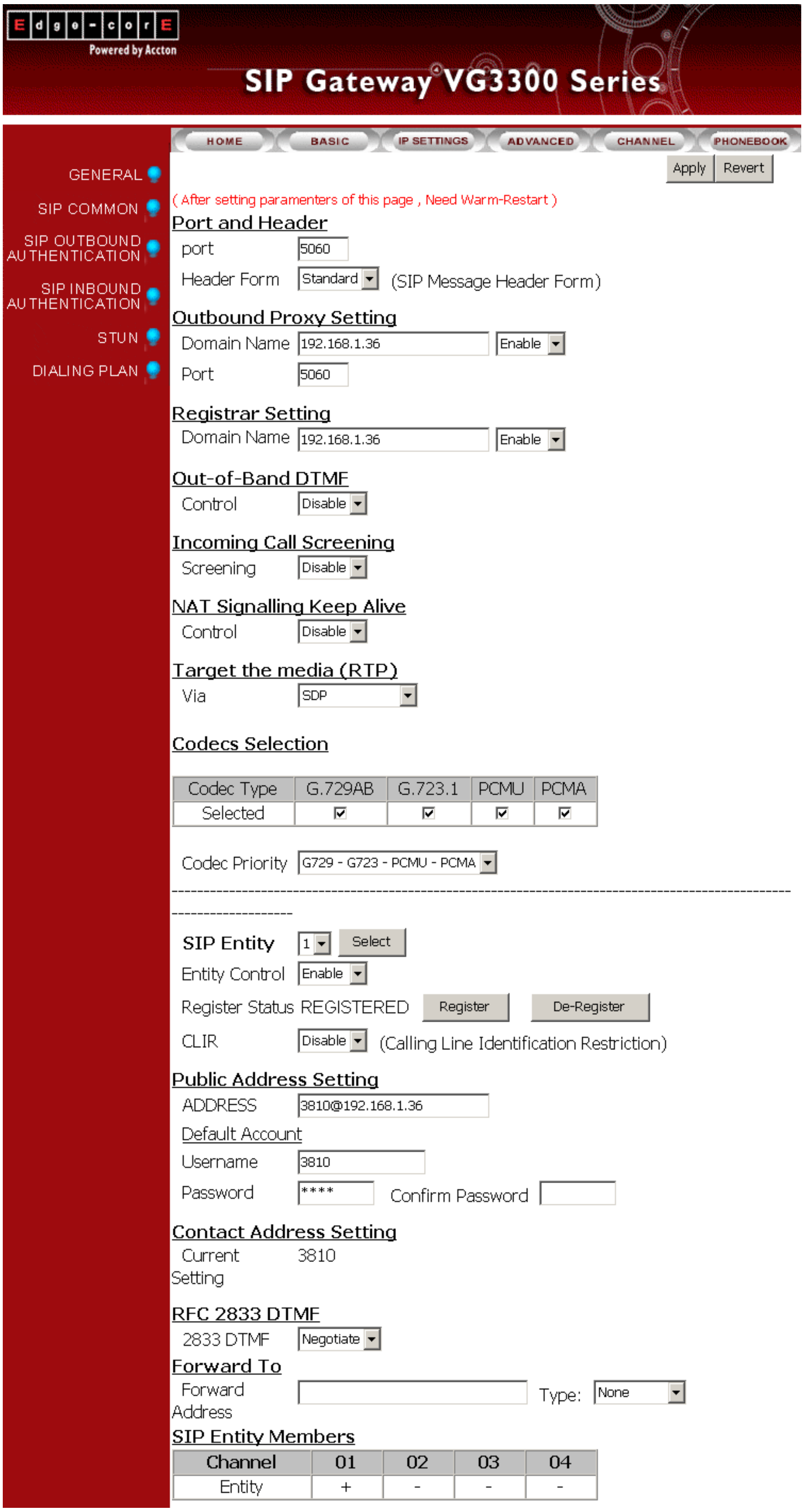
12.3. ADVANCED / GENERAL



Category	Section	Description	Default Setting
Flash Button	Flash Time	System confirmed "Flash" time.	200 msec
Touch Tone (DTMF)	Duration	The duration to send a DTMF.	100 msec
	Inter-digit	The inter-digit time of sending string of DTMF digits.	100 msec
Guard Time	Line	The time defines how long the system will not take incoming call after call has been disconnected.	0.8 sec
Dial Ending Time	Dial Ending Time	The time specifies how long to end the dialing	4 1-10 (seconds)

		number if a '#' digit is missing.	
T.38 Fax Relay	Redundancy	Number of times to retry T.38 Fax protocol. Use more Redundant packet when network is unstable. No Redundant packet 1 Redundant packet 2 Redundant packets 3 Redundant packets 4 Redundant packets	
Busy Tone Spec	Frequency	f1, f2	(300 ~ 3000Hz)
	Cadence	on, off. The on and off duration in playing the tone	(100 ~ 5000ms)
Reorder Tone Spec	Frequency	f1, f2	(300 ~ 3000Hz)
	Cadence	on, off. The on and off duration in playing the tone	(100 ~ 5000ms)

12.4. SIP COMMON



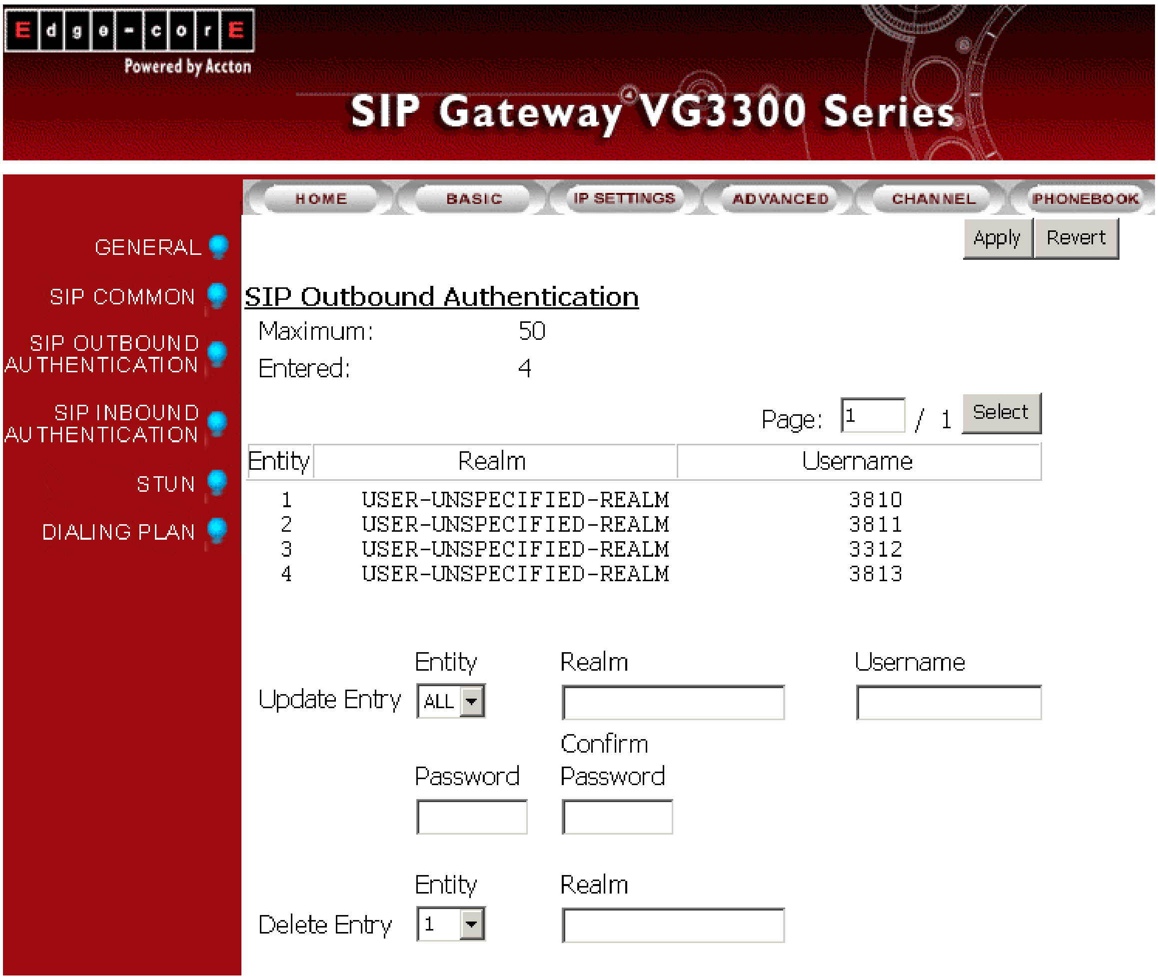
Section	Item Field	Description	Default
Port and Header	Port	The control port number of SIP protocol.	5060
	Header Form	Select 'Standard' or 'Compact' to be the header format of SIP packet. When Compact is selected, the header will be shorter and it saves bandwidth.	Standard
Outbound Proxy Setting	Domain Name	Domain name or IP address of proxy.	Empty Disable
	Port	Control port number of SIP protocol.	5060
Registrar Setting	Domain Name	Domain name or IP address of proxy that you want to register.	Empty Disable
Out-band DTMF	Control	Enable/Disable Enable: It "Disable" RFC 2833 DTMF	Disable
Incoming Call Screening	Screening	Disable: Accept all incoming SIP call Enable: This gateway only accepts incoming call through SIP Proxy.	Disable
NAT Signalling Keep Alive	Control	Port number mapping may change if the connection to pass through some NAT device is timeout. This function sends Dummy Packet to Proxy server every 50 seconds to keep the port number via NAT intact. Disable: Does not send Dummy Packet Enable: Send Dummy Packet	Disable
Target the media (RTP)	Via	Select the contact information (IP Address, Port Number) to pass through NAT device. Please refer to 11.7 Target the Media SDP: via SDP Symmetric RTP: via Symmetric RTP	SDP
Codecs Selection	Codec Type	G.729AB: Mark the selection to Enable G.729AB Codec	Enable
		G.723.1: Mark the selection to Enable G.723.1 Codec	Enable

Section	Item Field	Description	Default
		PCMU: Mark the selection to Enable PCMU Codec (G.711 u Law)	Enable
		PCMA: Mark the selection to Enable PCMA Codec (G.711 A Law)	Enable
	Codec Priority	You can select the codec priority for your requirement.	G729-G723-PCMU-PCMA
SIP Entity	SIP Entity	Select an entity and click Select button to display follow items' setting of SIP entity section. Select: Select Button Register: Register Button De-Register: Cancel Register Button	1
	Entity Control	Select Enable/Disable	Enable
	Register Status	Show the register status, if it shows Registered means successful. (Read only) Register: Register Button De-Register: Cancel Register Button	Empty
	CLIR	Calling Line Identification Restriction Disable: Send caller ID to SIP proxy when user make SIP call Enable: Don't send caller ID when user make SIP call. Note that for some SIP Proxy Server, the SIP call is failed if no caller ID is sent. Please set "CLIR" Disable for this case. That's the reason why default value is disable.	Disable
Public Address Setting	Address	Enter SIP phone number of the port. The phone number general assigned by SIP service provider.	Empty

Section	Item Field	Description	Default
	Default Account	Account information for registering SIP Proxy Username: It may the same as your SIP number Password: Password for Authentication Confirm Password: Reconfirm Password	
Contact Address Setting			
	Current Setting	Display current setting of (Read Only) Contact Address. It will be the same as the **Username** of Public Address Setting at this page of web if that field is configured	
RFC 2833 DTMF	2833 DTMF	Enable: Enable RFC 2833 DTMF. Negotiate: Encode DTMF to message and decode it back at destination. Never: Convert DTMF to voice and sent by RTP packets.	Never
	2833 In Use	Display current status of (Read Only) DTMF configuration.	
Forward To	Forward Address	Enter a SIP account (Public Address) forward. When users dial into the SIP Entity, the call will be forwarded to the number. Only SIP calls can be forwarded.	Empty
	Type	N/A: All incoming calls are forward. Busy: When the SIP entity is busy, the calls will be forward. No Answer: When the SIP entity is no answer about 30 seconds, the calls will be forwarded.	N/A
SIP Entity Members	Channel	Show the all channels	Depend on gateways

Section	Item Field	Description	Default
	Entity	Show '+ ' means the SIP entity is for the channel.	Empty

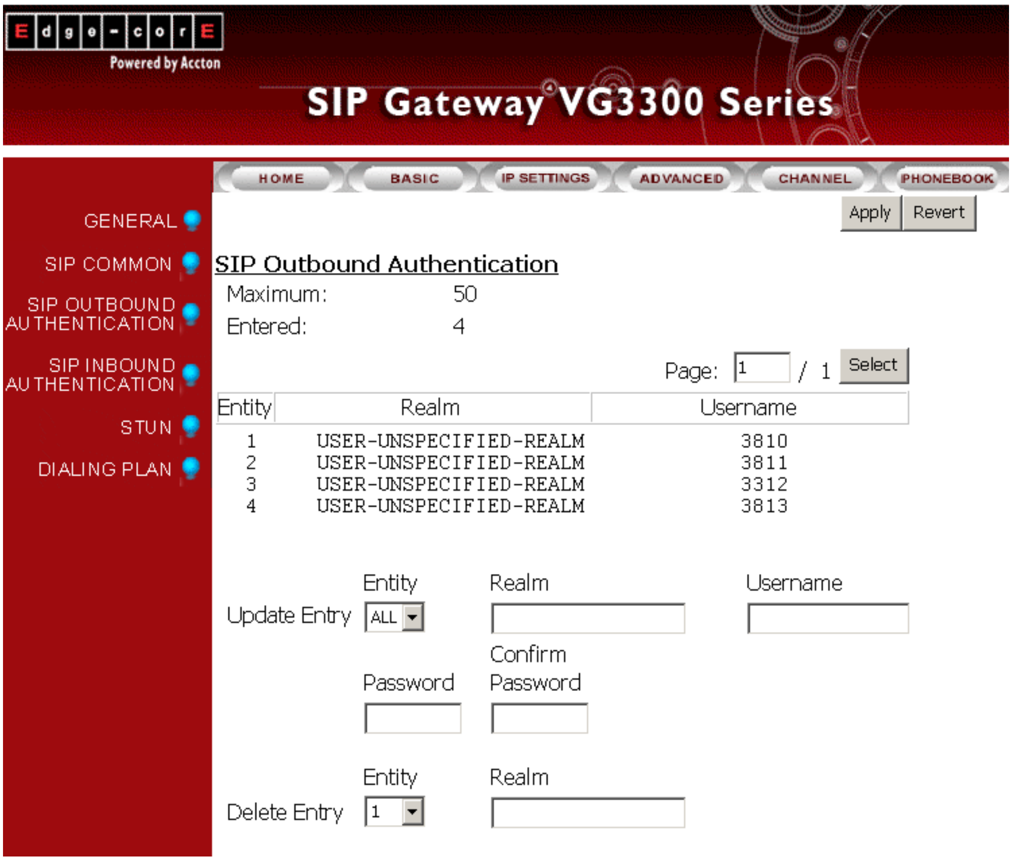
12.5. SIP OUTBOUND AUTHENTICATION



Section	Item Field	Description	Default
SIP Outbound Authentication	Maximum	Maximum number of entries (Read Only) allowed	50
	Entered	Number of entries of (Read Only) authentication entered.	0
	Entries	List of entries (Read Only)	Empty

Section	Item Field	Description	Default
	List	Entity: Which entity that you select. Realm: Domain name or IP address. Username: Username of authentication. The gateway creates default entry according to the Public Address Setting for easy registration. Please refer to 10.3 SIP Entity and 10.4 SIP Outbound Authentication	
	Update Entry	Enter the information of outbound authentication Entity: Select an entity. Realm: Domain name or IP address. Username: Enter Username of authentication. Password: Enter password of authentication. Confirm Password: Enter password again for confirmation.	Empty
	Delete Entry	Delete the information of outbound authentication Entity: Select an entity. Realm: Domain name or IP address.	Empty

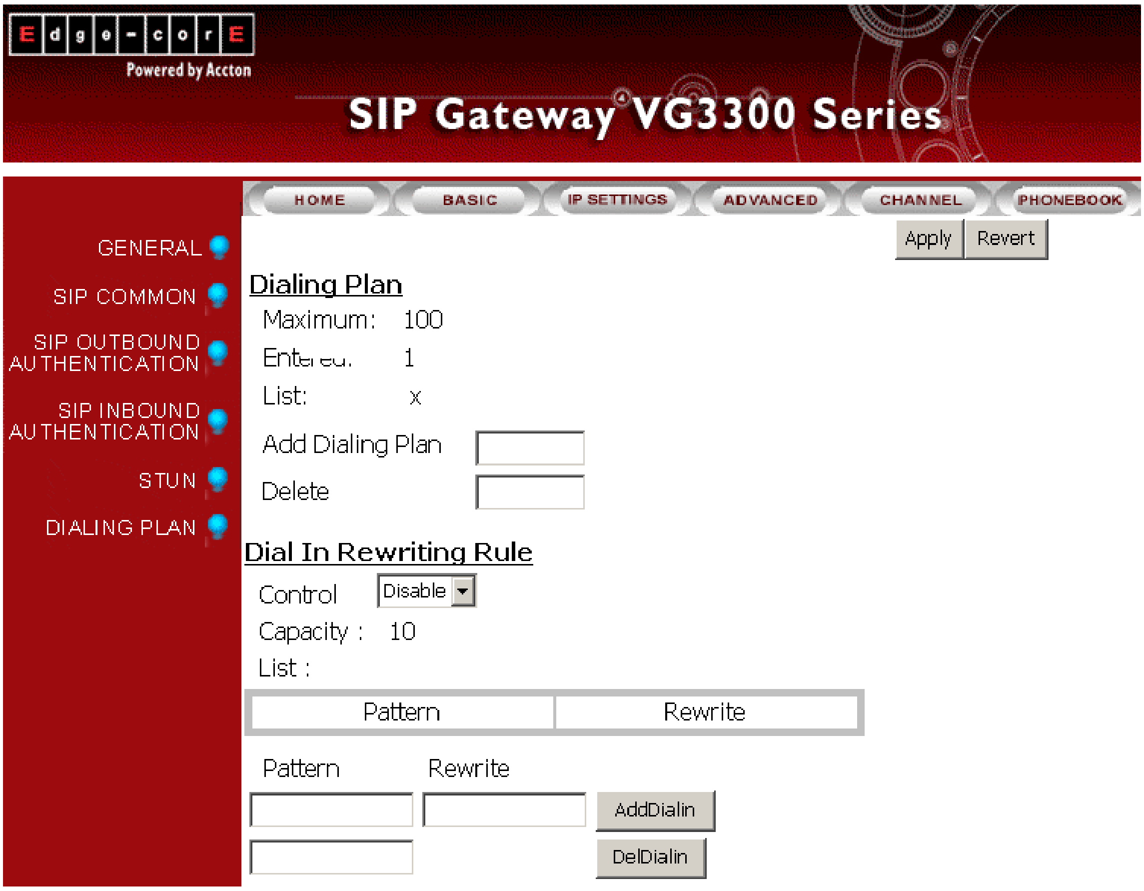
12.6. SIP INBOUND ANTHENTICATION



Section	Item Field	Description	Default
SIP Inbound Authentication	Realm	Enter domain name, IP address or word string.	Empty
	Maximum	Maximum number of entries allowed (Read Only)	20
	Entered	Number of entries of authentication entered. (Read Only)	0
	Entries List	Display the entries (Read Only) Entity: Which entity that you select. Username: Username of authentication.	Empty

Section	Item Field	Description	Default
	Update Entry	Enter entries of authentication Entity: Which entity that you select. Username: Username of authentication. Password: Password of authentication. Confirm Password: Enter password again for confirmation.	Empty
	Delete Entry	Delete entries of authentication Entity: Which entity that you want to delete. Username: Username of authentication.	Empty

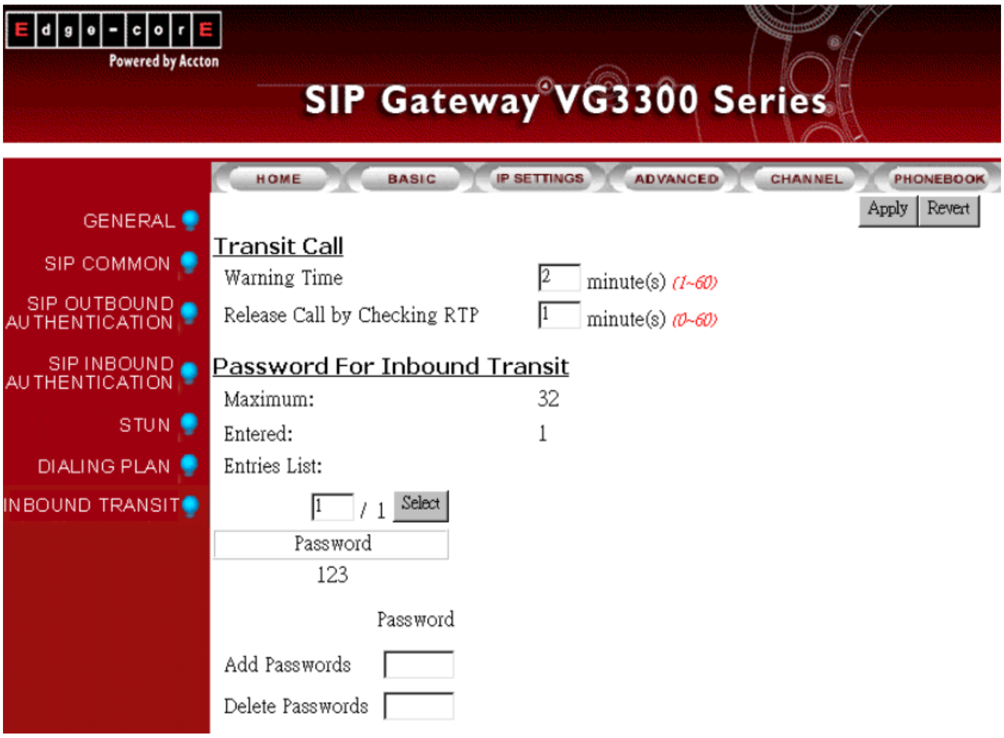
12.7. Dialing Plan



Section	Item Field	Description	Default
DIALING PLAN	Maximum	Maximum number of (Read Only) entries allowed	100
	Entered	Number of entries of (Read Only) authentication entered.	1
	List	Display the entries (Read Only) The default value "x" means that all numbers that you dial will first go through SIP proxy.	x
	Add Dialing Plan	Enter numbers. Example: 050.	Empty
	Delete Entry	Enter numbers for delete.	Empty
Dial In Rewriting Rule	Control	Digits dialed from VG3300 can be rewrite to different digits and sent to SIP Proxy. Enable/Disable	Disable
	Capacity	The max set of rewrite number	
	List	List the entries of original digits and the rewrite digits Pattern: the pattern that user may dial Rewrite: the converted number if user dials the same digit in pattern column.	
	Add Dialin (button)	Pattern: Add the pattern that user may dial Rewrite: Add the converted number if user dials the same digit in pattern column. Fill in digits and click the Add Dialin button	
	Del Dialin (button)	Fill in the Pattern digit that will be deleted and click Del Dialin button	

12.8. Inbound Transit

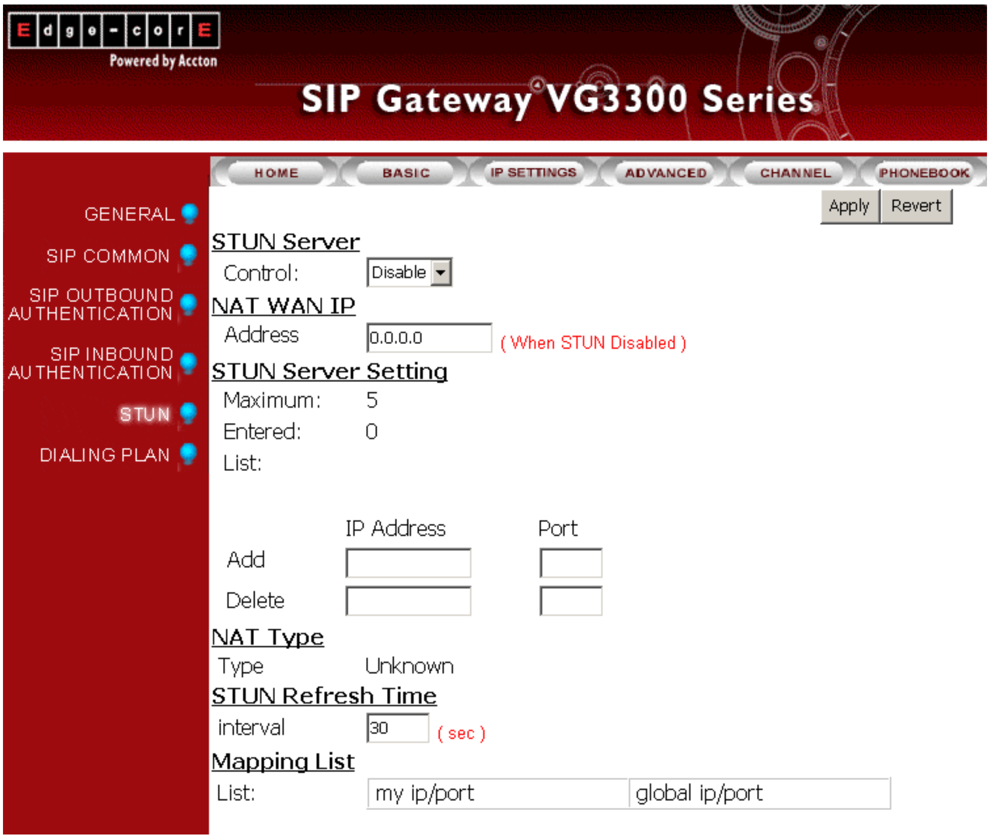
Only VG3300 gateway with FXO port has this web page.



Group	Field	Description	Default Value
Transit call	Warning Time	This gateway will send warning tone periodically to check if the line is still alive. If calling side fail to press any key after hearing the warning tone, the line will be disconnected.	60
	Release Call by Checking RTP	This gateway will check the RTP packet periodically to verify if the line is still alive. If no RTP packet is found, the gateway will disconnect the call. When this value is set to "0", means the gateway will not check the RTP packet	0
Password For Inbound Transit	Maximum	Display no. of password can be accepted (Read only)	32
	Entered	Display the no. of password had been entered (Read only)	0
	Entries List	List the detail data of password had been entered (Display) Only)	Blank

Group	Field	Description	Default Value
	Add Passwords	Enter a new password, any combination of digits (0~9), less than 9 characters. The password will be used at PINcode for auto answer function	Blank
	Delete Passwords	Enter the password to be deleted, refer the detail data under Entries List	Blank

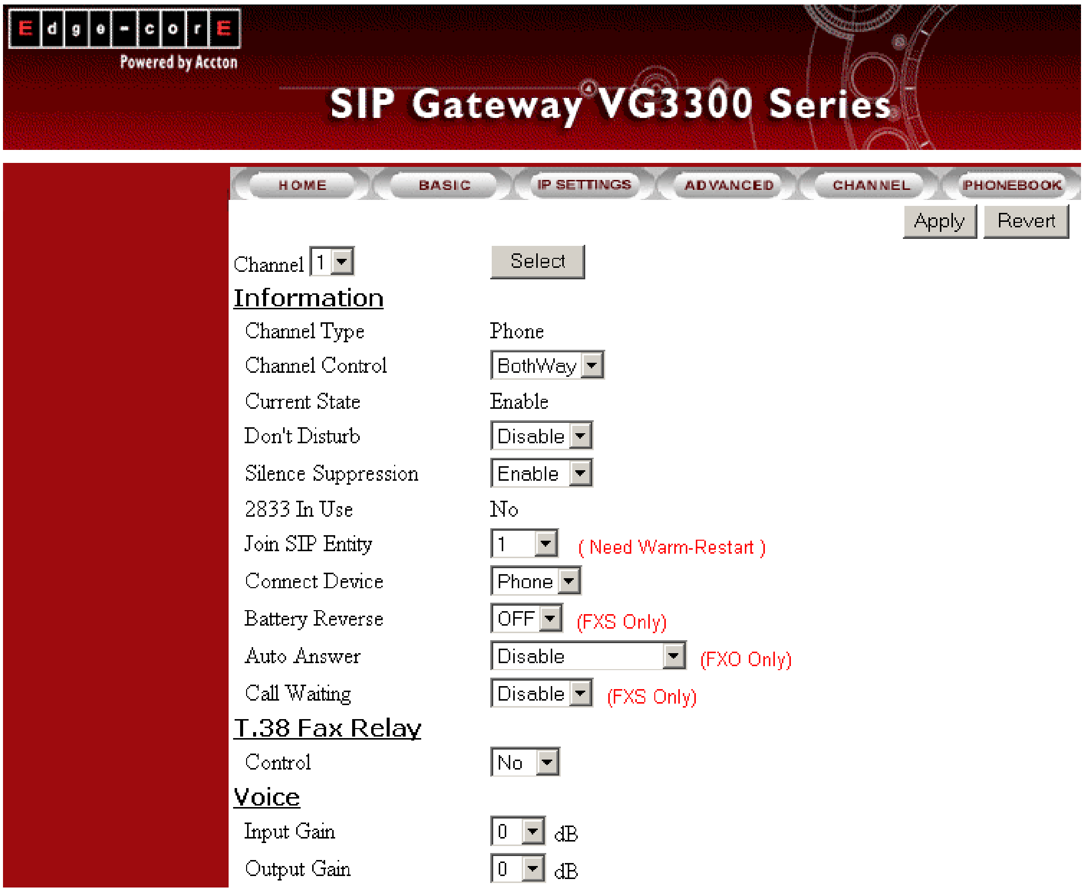
12.9. STUN



Section	Item Field	Description	Default
STUN Server	Control	Enable or Disable STUN Server service.	Disable

Section	Item Field	Description	Default
NAT WAN IP	Address	Input this NAT WAN IP helps you to pass through NAT without using STUN server. The port number inside and outside NAT should be the same. NAT WAN IP is the Public IP that used on NAT device **Note**: If you disable STUN server and input NAT WAN IP here, the RTP (normally 4000) and Signaling (normally 5060) port number inside and outside NAT must be the same, and Server Port need to be configured on NAT device.	
STUN Server Setting	Maximum	Maximum number of entries allowed (Read Only)	5
	Entered	Number of entries of STUN server that have been entered. (Read Only)	0
	List	Display all of servers that have been entered. (Read Only)	
	Add	Add a stun server IP Address: Enter IP address or Domain Name Port: Enter port number of service.	Empty
	Delete	Delete a stun server IP Address: Enter IP address. Port: Enter port number of service.	Empty
NAT Type	Type	Display NAT type (Read Only)	Unknown
Stun Refresh Time	Interval	It defines how long the device will send a binding request packet with discard flag on to STUN server.	30
Mapping List	List	My ip/port: shows the private IP and port number. (Read Only) Global ip/port: Display public IP and port number.	Empty

12.10. CHANNEL

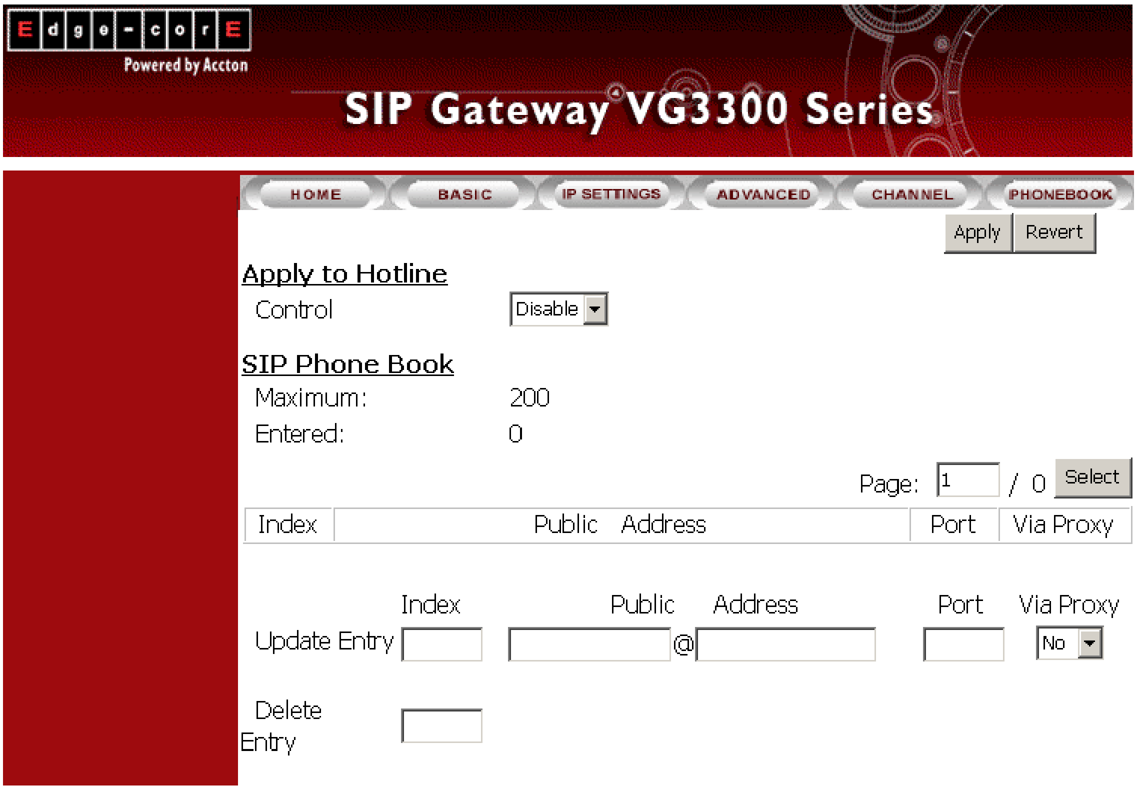


Category	Section	Description	Default Setting
	Channel	Channel number:	1
Information	Channel Type	Display port type. (Read only) Phone: FXS Interface, connect to telephone set or Fax machine. Line: FXO Interface, connect to phone line.	

	Channel Control	For FXS port: Bothway: Can make and accept IP call and PSTN call from this channel Disable Disable all functions of this port. For FXO port: IN_Only: Accept calls from PSTN only Bothway: Accept call from PSTN or call dial from FXS Disable: Disable all functions of this port.	Enable
	Current State	Display the current state of this port. (Read only) Enable/ Disable.	
	Do not Disturb	Enable/Disable does not disturb function	Disable
	Silence Suppression	Enable/Disable the function.	Enable
	2833 In use	Yes (Read only) No	
	Join SIP Entity	Select an Entity for SIP. Both FXS and FXO ports can join SIP Entity	1
	Connect Device	Phone: Connect to this port is regular phone FAX: Connect to this port is FAX machine. Codec will be fixed on G.711 if SIP-based T.38 codec negotiation fails. Both FXS and FXO ports can select their Connect Device	Phone

	Battery Reverse	This mechanism will reverse the polarity promptly that help some PBX to identify the start and end of each call ON: Enable the function OFF: Disable the function	OFF
	Auto Answer	This unit auto answer the call from FXO Disable: Disable Auto Answer Enable: Enable Auto Answer Enable w/ Pincode: Enable Auto Answer and Pincode verification.	Disable
	Call Waiting	Call waiting function for answering two incoming SIP VoIP phone calls Enable: Enable call waiting Disable: Disable call waiting	Disable
T.38 FAX Relay	Control	Yes: Use T.38 as FXS protocol No: Don't use T.38 as FAX protocol. If user send or receive FAX by this port, gateway can use G.711 (PCMU, PCMA) to pass-through FAX, please refer to 11.4 FAX	No
Voice	Input Gain	Adjust Voice input Gain	0
	Output Gain	Adjust Voice output Gain	0

12.11. PHONE BOOK



Section	Item Field	Description	Default
Apply to Hotline	Control	Enable or Disable the hotline function to VES-3302 Line or other SIP device to make hotline call.	Disable
SIP Phone Book	Maximum	Maximum number of entries allowed (Read Only)	200
	Entered	Number of entries of phone books entered. (Read Only)	0
	Entries List	Display phone books (Read Only) Index: Dialing number Public Address: SIP account. Port: Port number. Via Proxy: Via proxy or not.	Empty

Section	Item Field	Description	Default
	Update Entry	Enter entries Index: Enter dialing number Public Address: Enter SIP account. Port: Enter port number Via Proxy: Select via Proxy or not	Empty
	Delete Entry	Delete entries Index: Enter the index for delete.	Empty

13. Use Private IP (Behind NAT)

Using a Private IP in a NAT Environment
The gateway is able to communicate with other gateways under a NAT environment using Private IP addresses on the LAN side of your IP Sharing device. However you must configure the IP Sharing device to treat the gateway as a Virtual Server using UDP port 5060,2000.

You will have to ask MIS personnel to enable the ports listed in the following table.

Packet Modes	Using Ports
SIP Signal Packets	UDP 5060
Gateway Signaling Port	UDP 2000
Gateway RTP Base Port	UDP 4000
FTP software upgrade	TCP 21
Web management	TCP 80

If you want to use private IP behind NAT and Proxy Server is in Internet, you must need to enable STUN service. If the system is installed in VPN, it is not necessary to Enable Stun.

14. File Management

14.1. File Types

The naming convention to the file type of VPS3302 is listed in the following table:

File Name	File Type	Description
SIP3302.CFG SIP3304.CFG SIP33XX.CFG	System configuration file	File of system configuration
SIP3302.RUN SIP3304.RUN SIP33XX.RUN	Executing file	System Software
SIP3302.WEB SIP3304.WEB SIP33xx.WEB	Web file	Page for web browser

14.2. Software Update

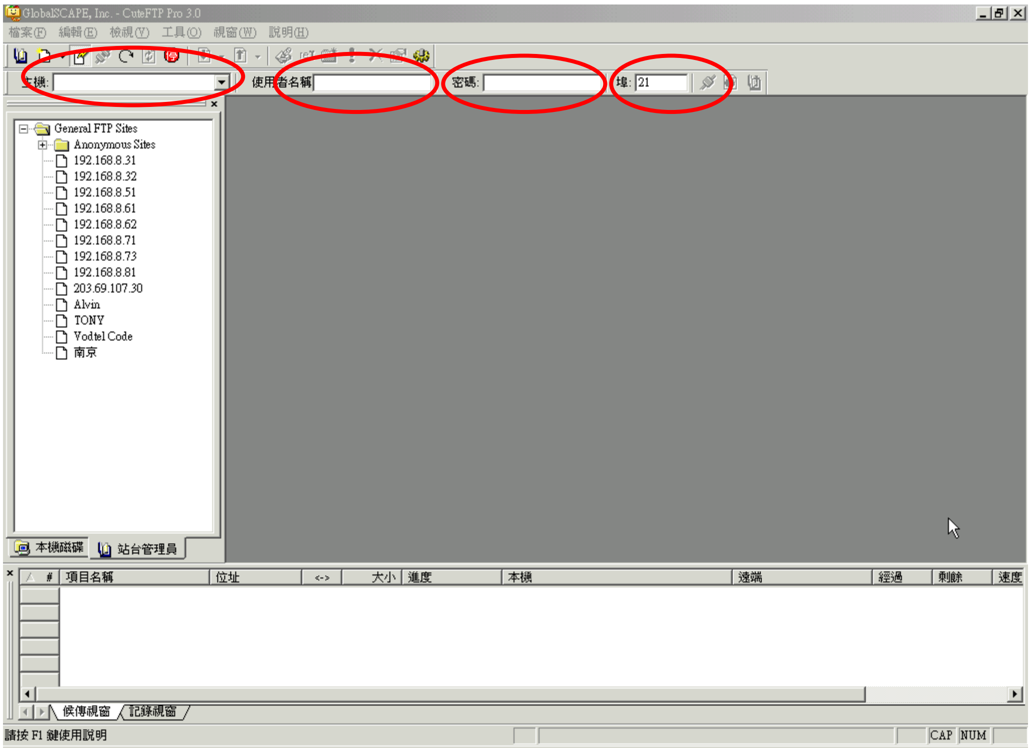
14.2.1. Software update via FTP

Preparation before Updating FIRMWARE

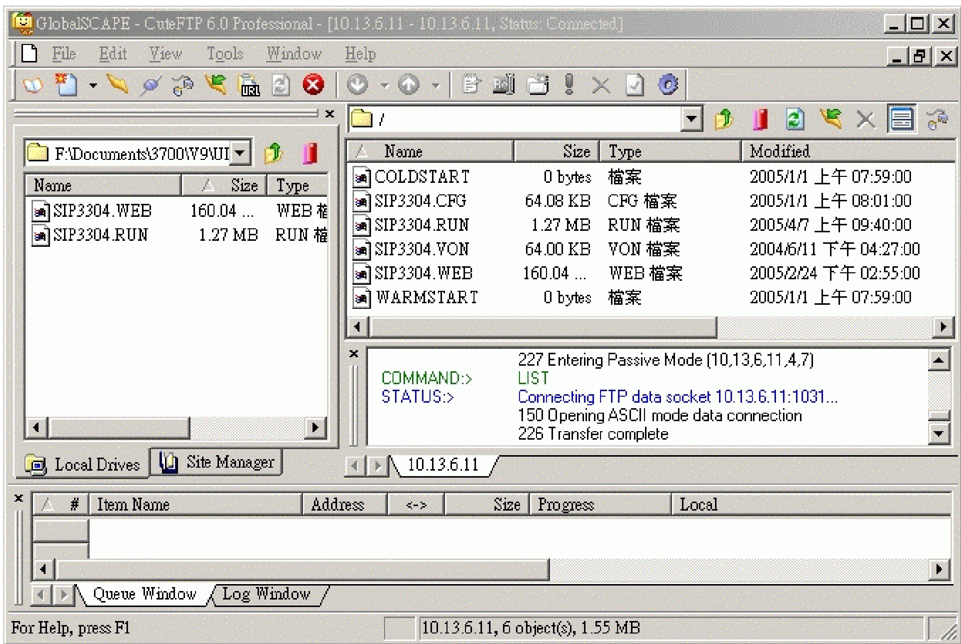
1. Power on the Conference Bridge
2. Get Windows based PC ready
3. LAN cable is well connected (for FTP)
4. Configure the IP, Subnet, and Default Gateway of this gateway and PC
5. Get the file of update “GW FIRMWARE” ready

Software Update by FTP for File Type RUN and WEB

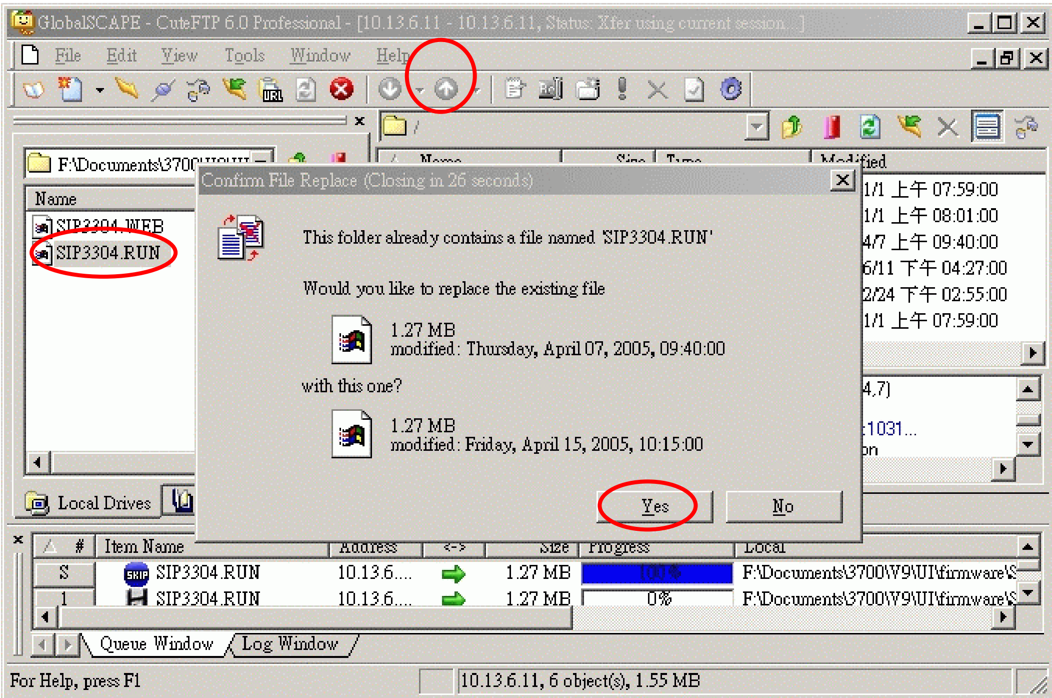
1. Execute FTP Client Software, e.g. CuteFTP
   Enter IP Address, User Name (default is FTP), Password (the password of FTP and Console is same, and the default is blank), and the Port Number to 21



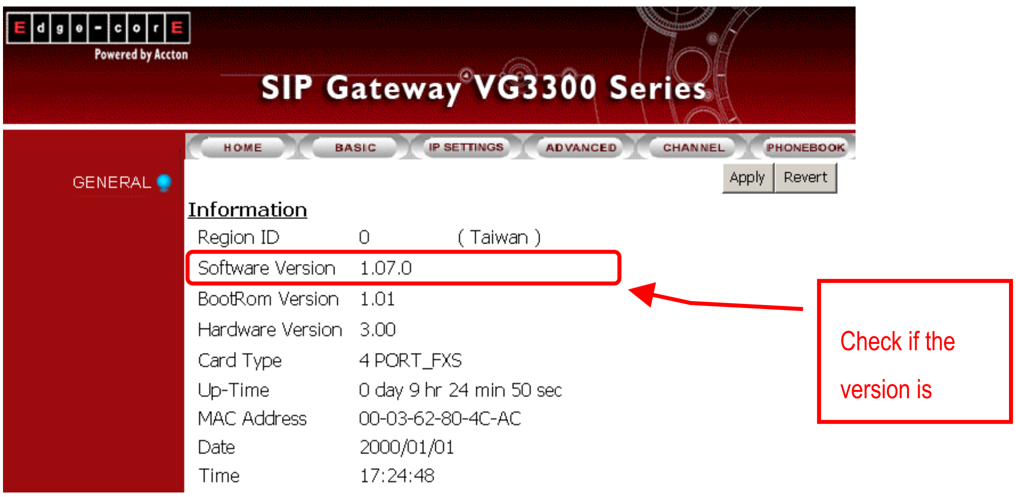
2. Click button **Connect** to get connection between gateway and FTP Client. The files of the gateway will be displayed on the window if the connection is successful.



3. Select the file with extension of .RUN and click button **Upload** and then **Yes** to overwrite. (Please notice that the file name must be same as the file name in the Gateway, e.g. SIP3304.RUN).



4. After the file is overwritten (you may check if the time of the file is updated), Gateway has to run Cold Start to store the configure file, then the updating is effective.
5. Select the file with extension of .WEB and click button **Upload** (Please notice that the file name must be same as the file name in the Gateway, e.g. SIP3302.WEB). And repeat the step 3 ~ 4.
6. Check if the uploading is successful, you enter the Web Management Page to examine the version of software. (Web Folder: BASIC\GENERAL)



15. Appendix

15.1. Appendix A: Phone-Set Command

Pick up the handset and listen for the dialing tone. Dial “##0000 and listen for three consecutive tones before setting the following parameters. After input the parameters, please dial ‘# to end the configuration.

Command	Description	Parameters
01	IP State	0 : static; 1: DHCP; 2: PPPoE
02	IP Address	xxx*xxx*xxx*xxx
03	Subnet Mask	xxx*xxx*xxx*xxx
04	Default Gateway	xxx*xxx*xxx*xxx
05	Primary DNS Server IP	xxx*xxx*xxx*xxx
06	Second DNS Server IP	xxx*xxx*xxx*xxx
07	Select Signaling Port	0~65535
08	Select RTP Base Port	0~65534 (limit to even port number only)
09	PPPoE username	User name (use the mapping table to map character into digits)
10	PPPoE password	Password (use the mapping table to map character into digits)
11	DND	Do not Disturb, this line accept dial out call only. All incoming call is terminated. 0 : Disable ; 1: Enable
12	SIP Forward State	0 : Disable ; 1: Enable; 2: Busy; 3: No Answer
13	SIP Forward To Number	The SIP number that this line will forward to. The Forward To address is "key in phone-set number@SIP proxy registered". For example, 73796@fwd.pulver.com, 73796 is the number you key-in by phone-set. fwd.pulver.com is the registered proxy of this gateway.
14	Change Service Port	1:FTP; 2:HTTP 3:Telnet (Port: 0-65535)
15	Change WEB	6 digits

	Password	
16	Change FTP Password	6 digits
40	Listen for the IP Address	(ending ”#” is not required)
41	Listen for the Subnet Mask	(ending ”#” is not required)
42	Listen for the Default Gateway	(ending ”#” is not required)
46	Listen for WEB, FTP, Telnet Port	1:FTP; 2:HTTP 3:Telnet
47	Listen for Current Public Address	(ending ”#” is not required)
95	Region ID	2 digits
97	Reset unit to Factory Default values	1: reset all; 2: keep IP
98	System Warm Restart	1: do it

15.2. Appendix B: Console Command

User Exec commands

Enable	Turn on privileged commands
Exit	Exit from the EXEC
Help	Description of the interactive help system
Show	Show running system information

show

Dns	Show the IP address of domain name server
ethernet	FastEthernet port status and configuration
history	Display the session command history
Ip	Display IP configuration
running-config	Show current operating configuration
version	System hardware and software status

Privileged Mode

Configure	Enter configuration mode
Delete	Reset configuration
Disable	Turn off privileged commands
Exit	Exit from the EXEC
Help	Description of the interactive help system
Ping	Send echo request to destination
Probe-hook	probe busytone cadence
Probe-remove	stop probe busytone cadence
Reload	Halt and perform cold start
Restart	Halt and perform warm start
Show	Show running system information

Global Mode

Dbflush	DataBase flush
Dns	Set the IP address of domain name server
End	Exit from configure mode to privileged mode
Exit	Exit from configure mode
Help	Description of the interactive help system
Ip	Global IP configuration subcommands
Log	Control log output
No	Negate a command or set its defaults
pppoe	PPPoE configuration subcommands
regional_id	Set regional id
service_port	Set service port number

15.3. Specifications

Voice Interface	
FXS interface	Loop start, 2 wire Feeding Voltage: 20V Feeding Current: 30 mA
FXO interface	Loop start, 2 wire
Connectors	RJ-11 Connectors (3304/3306) IDC Connectors (3310/3318)
Voice compression	G.711/G.723/G.729AB
Silence suppression	VAD, CNG
Echo cancellation	G.165/G.168 16ms
Jitter buffer	Adaptive jitter buffer management
Gain control	In/Out +/-6db
Transport protocols	RTP, RTCP
Call control protocol	Pure SIP
Network Interface	
Number of ports	Two Ethernet ports
Interface	10BASE-T/100BASE-TX Auto-negotiation
Connectors	RJ-45 Connectors
General Spec	
Dimension	VG3306: 172mm x 177mm x 35 mm VG3310: 440mm x 44mm x 254 mm VG3318: 440mm x 66mm x 254 mm
Power	Voltage: 100-240 VAC, Frequency: 50/60 Hz
Power consumption	VG3306: 12W VG3310/3716: 70W
Working environment	Operating temperature: 0 to 50℃ Storage temperature: -10 to 70℃
EMI	FCC part 15 Class B . CE Mark
PTT	FCC part 68 , NALTE , iDA , JATE
Safety	cUL , CCIB , CB

15.4. Mapping table of characters used in PPPoE

Character	Digits to key-in	Character	Digits to key-in
0	30	X	58
1	31	Y	59
2	32	Z	5*0
3	33	a	61
4	34	b	62
5	35	c	63
6	36	d	64
7	37	e	65
8	38	f	66
9	39	g	67
@	40	h	68
A	41	i	69
B	42	j	6*0
C	43	k	6*1
D	44	l	6*2
E	45	m	6*3
F	46	n	6*4
G	47	o	6*5
H	48	p	70
I	49	q	71
J	4*0	r	72
K	4*1	s	73
L	4*2	t	74
M	4*3	u	75
N	4*4	u	76
O	4*5	w	77
P	50	x	78
Q	51	y	79
R	52	z	7*0
S	53	=	3*3
T	54	.	2*4
U	55		

V	56		
W	57		

15.5. Region ID

Country	Region ID	Country	Region ID	Country	Region ID
Argentina	01	France	12	Singapore	36
Australia	02	Germany	13	Slovenia	38
Philippines	03	Hong Kong	15	South Africa	39
Portugal	04	India	18	Spain	40
Brazil	05	Italy	22	Switzerland	42
Canada	06	Japan	23	Taiwan	43
China	07	Korea	24	Thailand	44
Russia	08	Malaysia	26	British	46
Sweden	09	Mexico	27	USA	47
Vietnam	10	Netherlands	28		
Belgium	11	New Zealand	29		

V	56		
W	57		

15.5. Region ID

Country	Region ID	Country	Region ID	Country	Region ID
Argentina	01	France	12	Singapore	36
Australia	02	Germany	13	Slovenia	38
Philippines	03	Hong Kong	15	South Africa	39
Portugal	04	India	18	Spain	40
Brazil	05	Italy	22	Switzerland	42
Canada	06	Japan	23	Taiwan	43
China	07	Korea	24	Thailand	44
Russia	08	Malaysia	26	British	46
Sweden	09	Mexico	27	USA	47
Vietnam	10	Netherlands	28		
Belgium	11	New Zealand	29		