



USER MANUAL

IPG-200/IPG-110

VoIP ATA w/router function



Table of Contents

TABLE OF CONTENTS	1
1.1 OVERVIEW	5
1.2 AUDIENCE	5
1.3 ACRONYMS TABLE	5
1.4 INTRODUCTION	5
1.5 FRONT PANEL LED INDICATORS & REAR PANELS	6
1.6 IPG-200/IPG-110 SPECIFICATION	7
INSTALLATION AND SETUP.....	10
2.1 PACKAGE CONTENT	10
2.2 HARDWARE INSTALLATION	11
2.4 WIZARD SETUP	13
NETWORK SETTING.....	18
3.1 WAN INTERFACE	18
STATIC IP	18
DHCP CLIENT	19
PPPoE	20
PPTP WITH WAN (STATIC 、DHCP 、PPPoE)	21
L2TP WITH WAN (STATIC 、DHCP 、PPPoE) – ONLY IPG-110	21
3.2 LAN INTERFACE	22
3.3 NAT	23
PORT FORWARDING	24
VOIP SETTING (IPG-200/IPG-110)	25
QoS	31
4.2 PHONE	32
COMMON	35
REGION	36
4.3 PHONE BOOK	36
SPEED DIAL	36
DIAL PLAN WITH URL	37
SECURITY.....	38
5.1 FIREWALL	38
IP FILTERING	38

MAC FILTERING	38
PORT FILTERING	39
CONTENT FILTERING	40
MAINTENANCE	41
6.1 SYSTEM	41
GENERAL	41
TIME SETTING	42
AUTO PROVISION	42
DDNS	42
6.2 TOOLS	43
CONFIGURATION	43
UPGRADE FIRMWARE	44
PING TEST	44
PING FUNCTION YOU CAN PING IP OR DOMAIN.	44
6.3 LOG	46
LOGOUT	47
INFORMATION.....	48
SYSTEM STATUS	48
IVR COMMAND.....	49
APPENDIX	50
A - FAQ LIST	50
B - SCENARIO APPLICATION SAMPLES	51

COPYRIGHT & TRADEMARKS

We reserve the right to change the product specification without notification. **8level** is a registered trademark of 8level. No part of the manual may be reproduced, translated or processed in any other form without permission from 8level NEXT LEVEL IN NETWORKING. All rights reserved. Copyright © 2011 8level.

SAFETY NOTICE

Do not use this product near water. Using the product during a thunderstorm should be avoided. Do not place heavy objects on the casing.

RECYCLING NOTICE



The symbol of the crossed-out wheeled bin on this product means that it is forbidden to place the equipment waste together with other waste (under penalty of fine). Detailed information about recycling of the product can be obtained at local authorities, local waste treatment plants or local distributors. Forwarding the equipment waste to recycling or recovery points helps to avoid the negative influence of the harmful components present in the equipment on the environment and human health; in this scope the primary role is played by each household.

8level NEXT LEVEL OF NETWORKING

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **VoIP ATA / Router**

Model No.: **IPG-200**

Trademark: **8level**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

EMC 2004/108/EC

LVD 2006/95/EC

The above product is in conformity with the following standards or other normative documents:

EN55022:1998+A1:2000+A2:2003

EN61000-3-2:2000

EN61000-3-3:1995+A1:2001

EN55024:1998+A1:2000+A2:2003

Person is responsible for marking this declaration:

Mariusz Hofman
CEO



20.02.2012

SUNNYLINE COMPUTER PRODUCTS POLAND SP. Z O.O.
ul. Graniczna 588, 62-081 Przeźmierowo – POLAND

Introduce

IPG-200/IPG-110 series are the low cost VoIP Solutions. This document describes the usage of IPG-200/IPG-110 (Analogue Telephone Adapter)

1.1 Overview

- An Analogue Telephone Adapter, or IPG-200/IPG-110, is a device that allows one to connect a normal PSTN telephone to the Internet in order to make or place telephone calls.
- IPG-200/IPG-110 provides a direct analog interface for PSTN, PBX, fax machines, analog telephones, and other devices that require an analog port.

1.2 Audience

This document is intended for system vendor who are using IPG-200/IPG-110 to build an Internet telephony gateway or server application. It is assumed that the reader has the general knowledge of VoIP applications and products.

1.3 Acronyms Table

Acronym:	Full Name:	Acronym:	Full Name:
API	Application Interface	CODEC	Coder / Decoder
ADC	Analog to Digital Converter	DC	Direct Current
DAC	Digital to Analog Converter	DHCP	Dynamic Host Configuration Protocol
DDNS	Dynamic Domain Name System	DNS	Domain Name System
DTMF	Dual Tone Multi Frequency	MAC	Media Access Control
FXS	Foreign Exchange Station	NAT	Network Address Translation
WAN	Wide Area Network	PPTP	Point-to-Point Tunneling Protocol
NTP	Network Time Protocol	RTCP	Real-Time Transport Control Protocol (also known as RTP control protocol)
RTP	Real-Time Transport Protocol	SLIC	Subscriber Line Interface Circuit
SIP	Session Initiation Protocol	URI	Uniform Resource Identifier
STUN	Simple Traversal of UDP through NATs	UDP	User DSR-100gram Protocol
TCP	Transmission Control Protocol	VoIP	Voice Over Internet Protocol

1.4 Introduction

This Analogue Telephone Adapter (IPG-200/IPG-110) provides a total solution for integrating voice-data network and PSTN.

The **IPG-200** Analogue Telephone Adapter (IPG-200) support SIP VoIP Protocol. The **IPG-200** Analogue Telephone Adapter (IPG-200) allows 1~2 lines analog voice and fax communication over a traditional data communications/data networking digital Internet.

Model	FXO Port(PSTN)	FXS Port	WAN Port	LAN Port	RJ-11 port	SIP
IPG-200	0	2	1	1	2	√

The **IPG-110** Analogue Telephone Adapter (IPG-110) support SIP VoIP Protocol. The **IPG-110** Analogue Telephone Adapter (IPG-110) allows 1~2 lines analog voice and fax communication over a traditional data communications/data networking digital Internet.

Model	FXO Port(PSTN)	FXS Port	WAN Port	LAN Port	RJ-11 port	SIP
IPG-110	1	1	1	1	2	√

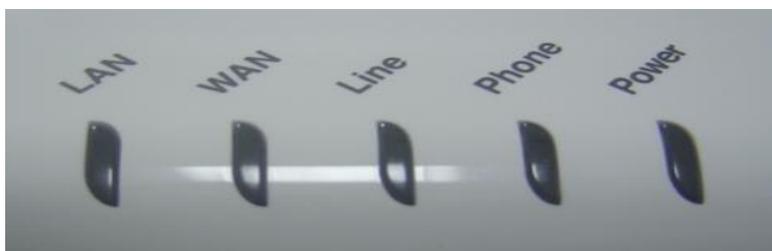
1.5 Front Panel LED Indicators & Rear Panels

IPG-200



LED	State	Description
1. POWER	On	IPG-200 is power ON
	Off	IPG-200 is power Off
2. LAN port	On	LAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC
3. WAN port	On	IPG-200 network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection
4. FXS (Phone)	Off	Telephone Set is On-Hook
	Flashing	Ring Indication
	On	Telephone Set is Off-Hook

IPG-110



LED	State	Description
1. POWER	On	IPG-110 is power ON
	Off	IPG-110 is power Off
2. LAN port	On	LAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC
3. WAN port	On	IPG-110network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection
4. FXS (Phone)	Off	Telephone Set is On-Hook
	Flashing	Ring Indication
	On	Telephone Set is Off-Hook
5. FXO (Line)	Off	Line is On-hook
	On	Line is In-Use

1.6 IPG-200/IPG-110 Specification

VoIP Key Features:

- Support SIP protocols: SIP Registration and Digest Authentication.
- Smart VoIP call Dialing Book: VoIP call Book could provide any application VoIP call to any type destination (Domain name/IP address, PSTN or PBX) or hunting number setting.
- Voice channels status display: This function display each port status like as On-hook, Off-hook, calling number caller's number, talk duration, codec.

Telephony Specification:

- Voice Codec: G.711(A-law / μ -law), G.729 AB, G.723 (6.3 Kbps / 5.3Kbps), G.726 (16,24,32,40 Kbps).
- Call Waiting
- Call Forward: Immediate /On Busy Forward / No Answer Forward
- Speed Dial
- Dial Plan With URL
- Multi-Line Appearance

-  DTMF Relay : PCM/SIP INFO / Out-of-band DTMF Relay (RFC2833)
-  DND
-  Hot-Line
-  Jitter Buffer Control
-  DNS Server
-  FAX T.38
-  Session Timer
-  MWI (Message Waiting Indicator)

IP Specification:

-  SIP (RFC 3261) , SDP (RFC 2327), Symmetric RTP,
-  STUN (RFC3489), ENUM (RFC 2916), RTP Payload for DTMF Digits (RFC2833), Outbound Proxy Support,
-  WAN: PPPoE client, DHCP client, Fix IP Address, PPTP/L2TP with WAN (Static 、 DHCP 、 PPPoE)
-  DDNS: DynDNS,TZO
-  QoS : IP TOS (IP Precedance) / DiffServ / SIP DSCP/RTP DSCP
-  VLAN

Call Features:

-  Volume : - 32 db ~ 30 db
-  VAD (Voice Activity Detection)
-  Caller ID Generation: DTMF CID / Bellcore CID / ETSI CID / BT CID / NTT CID
-  Peer to Peer Call by Dial Plan
-  Different Country Tone Table(Region)
-  G.168 Echo cancelation
-  Hook-Flash Timing
-  Call Transfer
-  Pulse Dial Detection
-  Auto Dial
-  Off-Hook Alarm

Configuration & Management:

-  Web-based Graphical User Interface
-  Remote management over the IP Network
-  Web Base firmware upgrade
-  Backup and Restore Configuration file
-  Different Account Login
-  Back to Factory Default
-  Time setting
-  Auto Provision(Auto config /Auto FW updrade)
-  Ping Test

Security (Firewall):

-  IP Filter
-  MAC Filter
-  URL Filter
-  Port Filter

General Specification:

-  AC power : AC100V-240V, DC12V/1A, 50/60 Hz
-  Temperature: 0°C ~ 40°C (Operation)

-  Humidity: up to 90% non-condensing
-  Emission: FCC Part 15 Class B, CE Mark
-  RoHS Compliant
-  Dimension : 115 x 85 x 29 mm
-  Weight: 165 g

Installation and Setup

2.1 Package Content

Please check enclosed product and its accessories before installation. (Refer to the item number). These contents are from pre-released product. The contents for the final product might change a little bit.

IPG-200 Package



The IPG-200 packet contents:

VoIP ATA IPG-200	X1
RJ-45	X1
AC Power Adapter (DC12V 1A)	X1
QIG	X4
CD-Rom(User manual)	X1

IPG-110 Package



The IPG-110 packet contents:

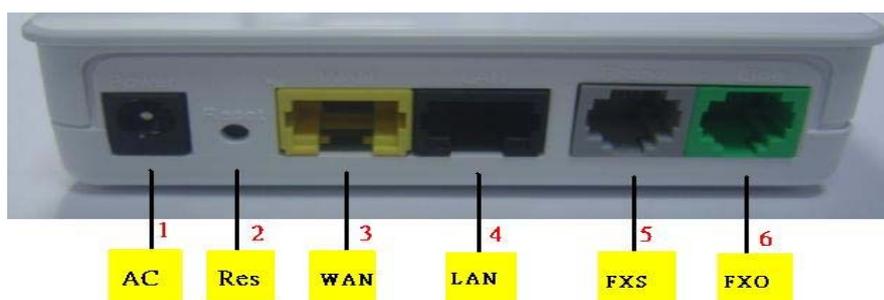
VoIP ATA IPG-110	X1
RJ-45	X1
AC Power Adapter (DC12V 1A)	X1
QIG	X4
CD-Rom(User manual)	X1

2.2 Hardware Installation

Port Description: DEMO Model IPG-200



Port Description: DEMO Model IPG-110



Item	Port	Description
1	FXS(Foreign Exchange Station)	FXS port can be connected to analog telephone sets or Trunk Line of PBX.
2	PSTN(FXO)	Connect to PBX or CO line with RJ-11(Gray) analog line. FXO port was connected to the extension port of a PBX or directly connected to a PSTN line of carrier.
3	WAN(Wide Area Network)	Connect to the network with an Ethernet cable. This port allows your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
4	LAN(Local Area Network)	Connect to PC with Ethernet cable. 1 port allows your PC or Switch/Hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
5	RES(Reset button)	Push this button until 3 seconds, and ATA will be set to factory default configuration.
6	AC power(DC in 12V)	A power supply cable is inserted

Installation:

- 1 Connect the 12V DC IN to the power outlet with power adaptor.
- 2 Connect FXO to PSTN.
- 3 Connect FXS to a telephone jack with the RJ-11 analog cable.

Connecting to a PC:

- 1 Connect the Ethernet cable (with RJ-45 connector) to any LAN port.
- 2 Connect the other end of the Ethernet cable to your PC's installed network interface card (NIC).

Connecting to an External Ethernet Hub or Switch:

- 1 Connect the Ethernet cable (with RJ-45 connector) to WAN port.
2. Connect the other end of the Ethernet cable to DSL/Cable modem or the external Ethernet hub or switch.

2.3 Quick Start

How to set your network environment?

IPG-200/IPG-110 default network environment:

For WAN:

Wan type: DHCP client

For LAN:

IP: 192.168.1.1

Subnet mask: 255.255.255.0

How to configure IPG-200/IPG-110?

1. Configure your PC or NB to the same subnet with IPG-200/IPG-110.
2. Use web browser (IE/Firefox) link to url: <http://192.168.1.1> (If you connect to LAN port, link to url: <http://192.168.1.1>)
3. Login user name: admin
4. Login password: admin
5. Use this web configuration interface to configure all system functionality; firstly you should change the WAN network environment to yours.

8level
NEXT LEVEL IN NETWORKING

Analog Telephony Adapter

Welcome to your ATA Configuration Interface

Enter your password and click "Login"

Username :

Password :

(max. 30 alphanumeric, printable characters and no spaces)

Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.

Login Reset

How to use VoIP?

1. Configure SIP user account to register your SIP proxy, use web configuration:
"SIP Settings" -> "Account Setting"
 - a. Port Phone Number
 - b. Port Authentication User Name
 - c. Port Authentication Password
 - d. Confirmed Password
2. Configure SIP registrar server and proxy server, use web configuration:
"SIP Settings" -> "Server Setting"
 - a. Registrar Server Address
 - b. Outbound Proxy Address
3. Make sure IPG-200/IPG-110 has already registered to your proxy, and then you can make a call

2.4 Wizard Setup

Wizard for Quick Setup TA20/IPG-110 after finishing the authentication, the Main menu will display 2 parts of configuration, please click "Connection wizard" to enter quick start:

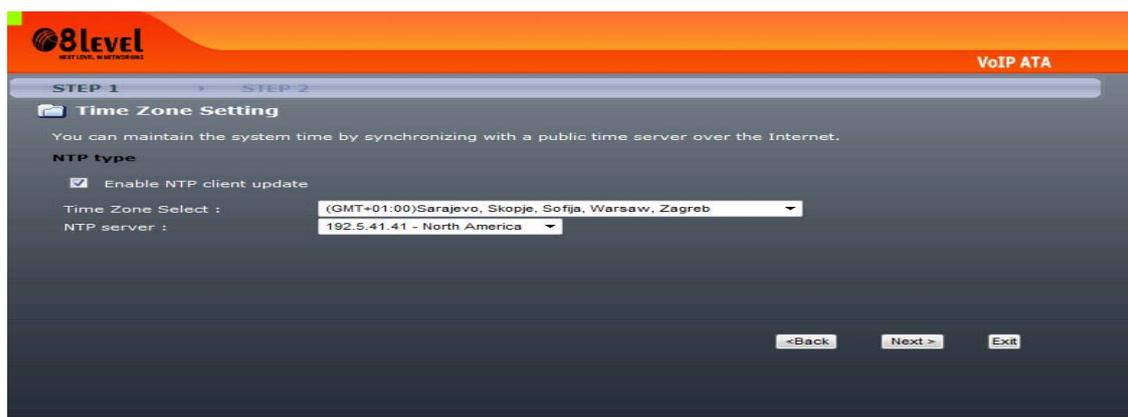
Step 1. Connection wizard



Step 2. Welcome to the VOIP ATA Connection Wizard



Step 3. Time Zone Setup



Time Zone Select : Choose your time zone
NTP Server : Select NTP server.

Step 4. WAN Port Type Setup:

For most users, Internet access is the primary application. The IPG-110/IPG-200 support the WAN interface for Internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click “**WAN Port Type Setup**” from within the Wizard **Setup**, the following setup page will be show.

Three methods are available for Internet Access:

Fixed IP User: If you are a leased line user with a fixed IP address, fill out the following items with the information provided by your ISP.

The screenshot shows the 'WAN Interface Setting' page for a Static IP configuration. The page title is '8level VoIP ATA' and it is on 'STEP 2'. The 'WAN Access Type' is set to 'Static IP'. The configuration fields are as follows:

WAN Access Type:	Static IP
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.2.1
DNS :	192.168.2.1

Navigation buttons at the bottom right include '<Back', 'Finished', and 'Exit'.

-  **WAN IP Address:** check with your ISP provider
-  **Subnet mask:** check with your ISP provider
-  **Default Gateway:** check with your ISP provider

DHCP Client (Dynamic IP):

Get WAN IP Address automatically

The screenshot shows the 'WAN Interface Setting' page for a Dynamic IP configuration. The page title is '8level VoIP ATA' and it is on 'STEP 2'. The 'WAN Access Type' is set to 'Dyamic IP'. The configuration fields are as follows:

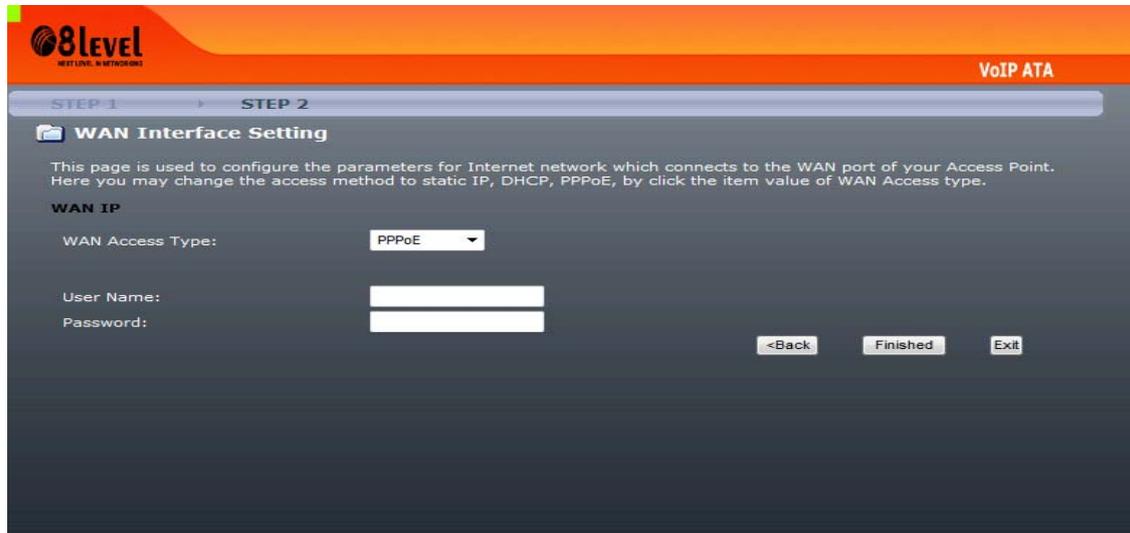
WAN Access Type:	Dyamic IP
------------------	-----------

Navigation buttons at the bottom right include '<Back', 'Finished', and 'Exit'.

ADSL Dial-Up User (PPPoE Enable)

Some ISPs provide DSL-based service and use PPPoE to establish communication link with end-users. If

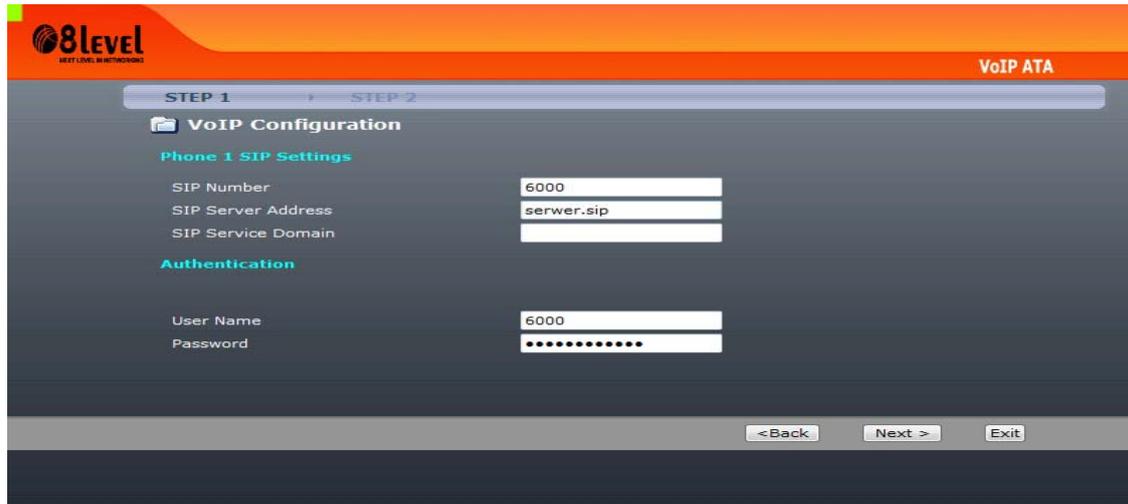
you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to select this item.



-  **PPPoE User Name:** Enter User Name provided by your ISP
-  **PPPoE Password:** Enter Password provided by your ISP.
-  **Confirmation Password:** Enter Password to confirm again.

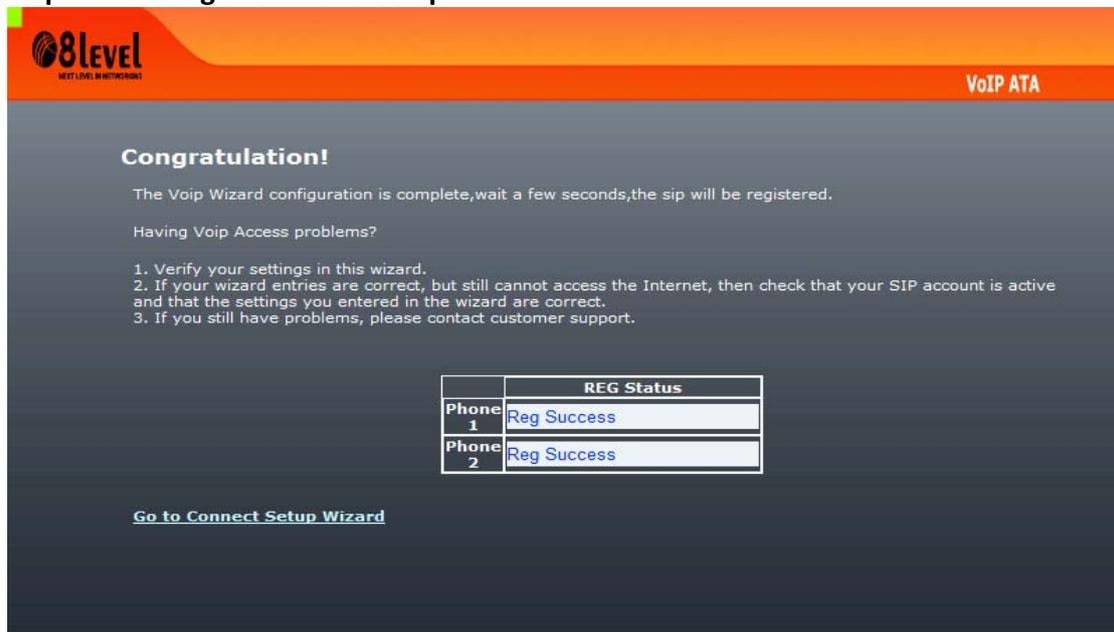
Step 6.Voip Setup





- SIP Number: you need to input the User Name get from your ISP.
- SIP Server add: you need to input the Proxy add get from your ISP.
- SIP Server Domain: you need to input the SIP Domain get from your ISP.
- User Name: you need to input the Register User Name get from your ISP.
- Password: you need to input the Register Password get from your ISP.

Step 7. Finishing the Wizard Setup



Network Setting

-  WAN Interface
-  LAN Interface
-  NAT

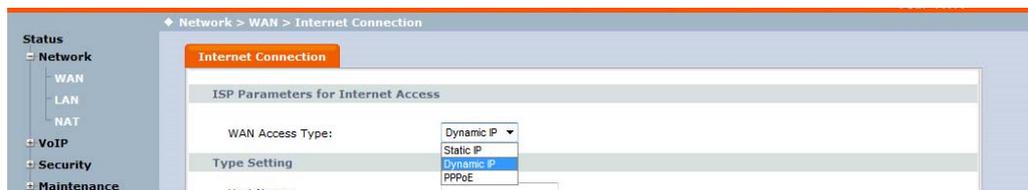
3.1 WAN Interface

WAN (Wide Area Network) is a network connection connecting one or more LANs together over some distance. For example, the means of connecting two office buildings separated by several kilometers would be referred to as a WAN connection. The size of a WAN and the number of distinct LANs connected to a WAN is not limited by any definition. Therefore, the Internet may be called a WAN.

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

For most users, Internet access is the primary application. IPG-200/IPG-110 supports the WAN interface for internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click "WAN Setting", the following setup page will be shown. Three methods are available for Internet Access.

-  Static IP
-  DHCP
-  PPPoE
-  PPTP with WAN (Static \ DHCP \ PPPoE)



Static IP

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

Example: 168.95.1.1

- IP Address: Check with your ISP provider.
- Subnet Mask: Check with your ISP provider.
- Default Gateway: Check with your ISP provider.

The screenshot shows the 'Internet Connection' configuration page. The breadcrumb trail is 'Network > WAN > Internet Connection'. The page title is 'Internet Connection'. The configuration is organized into several sections:

- ISP Parameters for Internet Access:** WAN Access Type is set to 'Static IP'.
- Type Setting:** IP Address, Subnet Mask, and Default Gateway are all set to '0.0.0.0'. MTU Size is set to '1500' (with a note '(1400-1500 bytes)'). There is an unchecked checkbox for 'Enable PPTP'.
- DNS Servers:** First DNS Server is '0.0.0.0' and Second DNS Server is '0.0.0.0'.
- Clone MAC Address:** There are two radio button options: 'Clone the computer's MAC address-IP Address:' (selected) with a value of '0.0.0.0', and 'Use specified MAC Address:' with a value of '000000000000'.
- Other Setting:** There is an unchecked checkbox for 'Enable uPNP'.

At the bottom of the form, there are 'Apply' and 'Reset' buttons.

DHCP client

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

Note: WAN port gets the IP Address, Subnet Mask and default gateway IP address automatically, if DHCP client is successful.

◆ Network > WAN > Internet Connection

Internet Connection

ISP Parameters for Internet Access

WAN Access Type:

Type Setting

Host Name:

MTU Size: (1400-1492 bytes)

Enable PPTP

DNS Servers

Assign DNS Dynamically

User-Defined DNS

First DNS Server:

Second DNS Server:

Clone MAC Address

Clone the computer's MAC address-IP Address:

Use specified MAC Address:

Other Setting

Enable uPNP

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE). Some ISPs provide DSL-based services and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to make sure the following items, PPPoE User name: Enter username provided by your ISP. PPPoE Password: Enter password provided by your ISP.

◆ Network > WAN > Internet Connection

Internet Connection

ISP Parameters for Internet Access

WAN Access Type:

Type Setting

User Name:

Password:

Service Name:

Connection Type:

Idle Timeout: (1-1000 minutes)

MTU Size: (1360-1492 bytes)

Enable PPTP

DNS Servers

Assign DNS Dynamically

User-Defined DNS

First DNS Server:

Second DNS Server:

PPTP with WAN (Static、DHCP、PPPoE)

Some ISPs provide DSL-based service and use PPTP with Static, DHCP or PPPoE to establish communication link with end-users.

The screenshot shows the 'Internet Connection' configuration page. Under 'ISP Parameters for Internet Access', the 'WAN Access Type' is set to 'Static IP'. In the 'Type Setting' section, the following fields are visible: IP Address (0.0.0.0), Subnet Mask (0.0.0.0), Default Gateway (0.0.0.0), MTU Size (1500 bytes), 'Enable PPTP' (checked), Server IP Address, User Name, Password, and MTU Size (1400 bytes). 'Request MPPE Encryption' is also checked.

- PPTP Server IP Address: check with your VPN /PPTP Server provider
- PPTP User Name: PPTP Dial-in account
- PPTP Password: PPTP Dial-in Password
- PPTP MTU Size
- Request MPPE Encryption
- Remote LAN setting: select SIP Call by LAN IP Address or not

L2TP with WAN (Static、DHCP、PPPoE) – only IPG-110

Some ISPs provide DSL-based service and use L2TP with Static, DHCP or PPPoE to establish communication link with end-users.

The screenshot shows the 'VPN Type Setting' page. The 'Enable L2TP' checkbox is checked. Below it, the following fields are visible: L2TP Server IP Address (0.0.0.0), L2TP User Name, L2TP Password, and L2TP MTU Size (1412 bytes). The 'Remote LAN setting' section has the 'SIP Call by LAN IP Address' checkbox unchecked.

- L2TP Server IP Address: check with your VPN /PPTP Server provider
- L2TP User Name: L2TP Dial-in account
- L2TP Password: L2TP Dial-in Password
- L2TP MTU Size
- Request MPPE Encryption
- Remote LAN setting: select SIP Call by LAN IP Address or not

3.2 LAN Interface

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 192.168.1.1 with a subnet mask of 255.255.255.0.

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

- LAN IP Address: Assign the IP address of LAN server, default is 192.168.1.1
- Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0.

DHCP Server Setting

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is starting up and request an IP address to be logged on to the network. The device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled in the unit. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP client computers connected to the unit will have their information displayed in the DHCP Client List table. The table will show the Type, Host Name, IP Address, MAC Address, Description, and Expired Time of the DHCP lease for each client computer.

DHCP Server is a useful tool that automates the assignment of IP addresses to numbers of computers in your network. The server maintains a pool of IP addresses that you use to create scopes. (A DHCP scope is a collection of IP addresses and TCP/IP configuration parameters that are available for DHCP clients to lease.) Then, the server automatically allocates these IP addresses and related TCP/IP configuration settings to DHCP-enabled clients in the network. The DHCP Server leases the IP addresses to clients for a period that you specify when you create a scope. A lease becomes inactive when it expires. Through the DHCP Server, you can reserve specific IP addresses permanently for hardware devices that must have a static IP address (e.g., a DNS Server).

An advantage of using DHCP is that the service assigns addresses dynamically. The DHCP Server returns addresses that are no longer in use to the IP addresses pool so that the server can reallocate them to other machines in the network. If you disable this DHCP, you would have to manually configure IP for new computers, keep track of IP addresses so that you could reassign addresses that clients aren't using, and reconfigure computers that you move from one subnet to another. The DHCP Static MAP table lists all MAC and IP address which are active now.

When you enable the DHCP server,

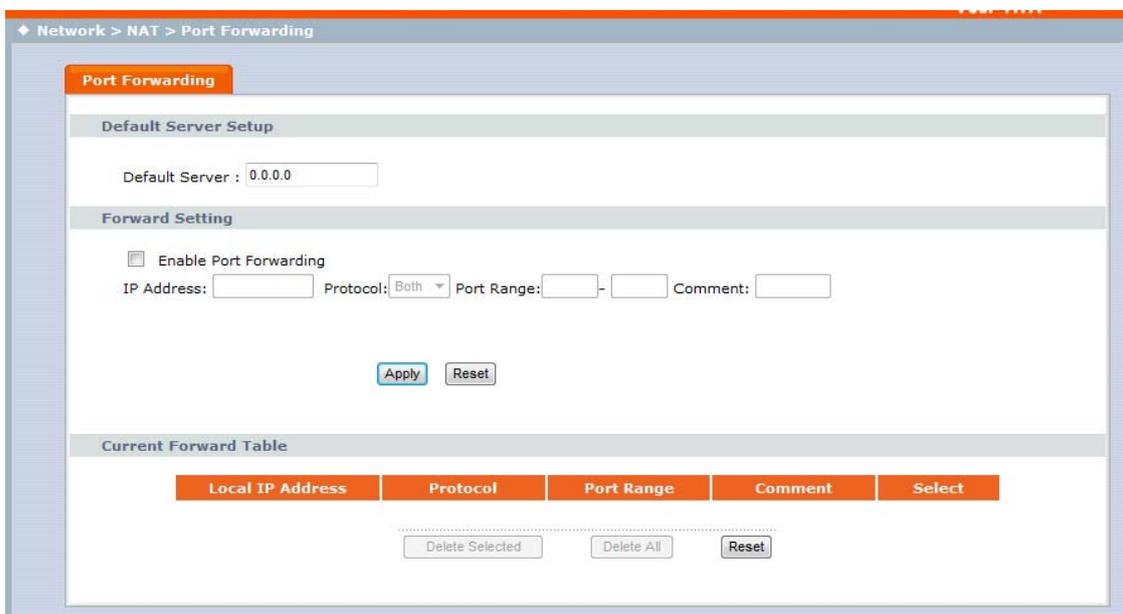
- Assigned DHCP IP Address: Enter the starting IP address for the DHCP server’s IP assignment and the ending IP address for the DHCP server’s IP assignment.
- DHCP IP Lease Time - Assign the length of time for the IP lease, default setting is 86400 seconds.

DHCP Table



3.3 NAT

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



DMZ - In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Think of DMZ as the front yard of your house. It belongs to you and you may put some things there, but you would put anything valuable inside the house where it can be properly secured. Setting up a DMZ is very easy. If you have multiple computer s, you can choose to simply place one of the computers between the Internet connection and the firewall.

If you have a computer that cannot run Internet applications properly from behind the device, then you

can allow the computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ host with unrestricted Internet access. 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.

Port Forwarding

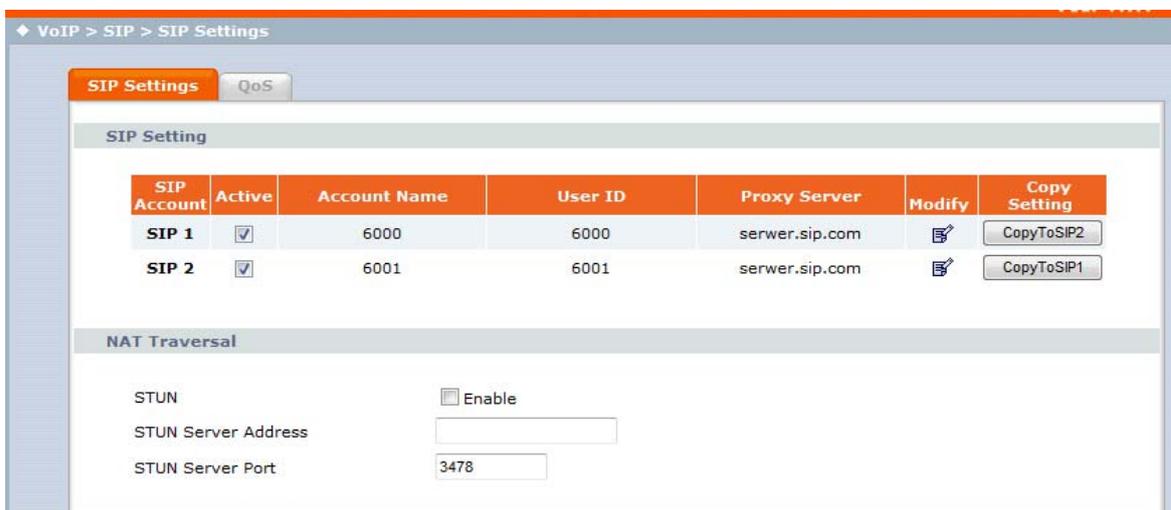
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

VOIP Setting (IPG-200/IPG-110)

SIP is a request-response protocol, dealing with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

-  SIP Setting
-  Phone
-  Phone book
-  PSTN Line (IPG-110 only)

IPG-200



The screenshot displays the 'SIP Settings' configuration page. At the top, there are tabs for 'SIP Settings' and 'QoS'. Below the tabs is a table with the following columns: SIP Account, Active, Account Name, User ID, Proxy Server, Modify, and Copy Setting. Two SIP accounts are listed: SIP 1 and SIP 2. Below the table is a section for NAT Traversal with fields for STUN (checked), STUN Server Address, and STUN Server Port (3478).

SIP Account	Active	Account Name	User ID	Proxy Server	Modify	Copy Setting
SIP 1	<input checked="" type="checkbox"/>	6000	6000	server.sip.com		<input type="button" value="CopyToSIP2"/>
SIP 2	<input checked="" type="checkbox"/>	6001	6001	server.sip.com		<input type="button" value="CopyToSIP1"/>

NAT Traversal

STUN Enable

STUN Server Address

STUN Server Port

IPG-110

Account	Active	Account Name	User ID	Proxy Server	Modify	Copy Setting
Phone	<input checked="" type="checkbox"/>	6000	6000	server.sip.com		CopyToSP2
Line	<input checked="" type="checkbox"/>	6001	6001	server.sip.com		CopyToSP1

Advanced Setting

PSTN Call ByPass To Phone Enable

NAT Traversal

STUN Enable

STUN Server Address

STUN Server Port

4.1 SIP Setting

Sip setting

In SIP Settings you can setup the Service Domain, Port Settings, Codec Settings, Codec ID Settings, RTP Setting, RPort Setting and Other Settings. If the VoIP service is provided by ISP, you need to setup the related information correctly then you can register to the SIP Proxy Server correctly.

In Service Domain Function you need to input the account and the related information in this page, please refer to your ISP provider. You can register three SIP account in the VoIP Phone. You can dial the VoIP phone to your friends via first enable SIP account and receive the phone from these three SIP accounts.

The screenshot shows a web-based configuration interface for a VoIP ATA. The breadcrumb trail at the top reads "VoIP > SIP > SIP Settings > Edit". The main content area is divided into two sections: "SIP 1 Setting" and "Authentication".

SIP 1 Setting

- Active SIP Account
- Account Name: 6000
- Number: 6000
- SIP Display Name: (empty)
- SIP Server Address: server.sip.com
- Backup Sip Proxy Server
- SIP Server Port: 5060 (1-65535)
- SIP Service Domain: (empty)
- Register Expire (sec): 60
- Outbound Proxy Server: Enable
- Outbound Proxy Address: (empty)
- Outbound Proxy Port: 5060 (1-65535)

Authentication

- User Name: 6000
- Password: (masked with dots)

At the bottom of the form, there are four buttons: "Back", "Apply", "Reset", and "Advanced".

- Account Name: you can input the name you want to display.
 - Number: you need to input the User Name get from your ISP.
 - SIP Display Name: you can input the name you want to display.
 - SIP Server Addr: Enable / Disable Register Proxy server and input the Proxy Addr get from your ISP.
 - SIP Server Port: you need to input the Proxy Port get from your ISP.
 - SIP Server Domain: you need to input the SIP Domain get from your ISP.
 - Reg Expire (sec): SIP registration expired time.
 - Outbound Proxy Server: you need to input the Outbound Proxy get from your ISP. If your ISP does not provide the information, then you can skip this item.
 - Outbound Proxy Address: Enable / Disable Register Outbound Proxy server and input the Outbound Proxy Address get from your ISP.
- You can see the Register Status in the Status item. If the item shows "Registered", then your VoIP Phone is registered to the ISP, you can make a phone call directly.
- If you have more than one SIP account, you can following the steps to register to the other ISP.
- When you finished the setting, please click the Apply button.

- User Name: you need to input the Register Name get from your ISP.
- Password: you need to input the Register Password get from your ISP.

STUN Traversal

STUN {Simple Traversal of UDP through NATs (Network Address Translation)} is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

STUN enables a device to find out its public IP address and the type of NAT service its sitting behind.

When you enable the STUN function, you must input the STUN server address.

NAT Traversal	
STUN	<input checked="" type="checkbox"/> Enable
STUN Server Address	<input type="text"/>
STUN Server Port	<input type="text" value="3478"/>

SIP Advance

SIP : 1	
SIP Advanced	
SIP Port	<input type="text" value="5060"/>
Media Port	<input type="text" value="9000"/>
Packetization	<input type="text" value="20 ms"/>
DTMF Relay	<input type="text" value="PCM"/>
RFC2833 Payload Type	<input type="text" value="101"/>
SIP INFO Duration (ms)	<input type="text" value="250"/>
Call wait time	<input type="text" value="0"/> 0~128 seconds
Call Waiting	<input checked="" type="checkbox"/> Enable
DNS SRV	<input checked="" type="checkbox"/> Enable
Prohibit coming calls from other SIP server	<input checked="" type="checkbox"/> Enable

- SIP Port Number - Assign the SIP port number of IPG-110/IPG-200., default setting is 5060.
- Media Port Start - The starting range of port for RTP . Port number for initial of sending RTP packet., default setting is 9000.
- Packetization: Select the voice codec packetization interval in milliseconds. The default is 20 ms. This is used to minimize loss that happens during transmission of voice data over the network.
- DTMF Setting - you can setup the RFC2833 Out-Band DTMF, Inband DTMF and Send DTMF SIP Info in this page. To change this setting, please follow your ISP information. When you finished the setting, please click the Submit button.
- RFC2833 Payload Type - Sending the DTMF tone as a RTP payload signal. The RFC2833 signaling
- SIP INFO Payload Type - Sending the DTMF tone as a RTP payload signal. The SIP INFO signaling
- PCM Type - Sending the DTMF tone as a RTP payload signal. The Inband DTMF signaling
- SIP INFO Duration (ms) - Modify SIPINFO duration time.
- Call Waiting - Call Waiting Setting function: If user doesn't want to be inform there is a new incoming call, user can set the function off.
- DNS Server: Select Enable to have the IPG-110/IPG-200 Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server exercise difficulties, making it hard for you to make SIP calls.

Forward Setting	
Immediate Forward to	<input checked="" type="radio"/> Off <input type="radio"/> Enable
Immediate Number	<input type="text"/>
Busy Forward to	<input checked="" type="radio"/> Off <input type="radio"/> Enable
Busy Number	<input type="text"/>
No Answer Forward to	<input checked="" type="radio"/> Off <input type="radio"/> Enable
No Answer Number	<input type="text"/>
No Answer Time (sec)	<input type="text" value="5"/>

Forwarding Mode

You can setup the phone number you want to forward in this page. There are three type of Forward mode. You can setup Immediate Forward, Busy Forward, and No Answer Forward by click the icon.

Immediate Forward: All incoming call will forward to the number you entered. You can input the phone number. If you select this function, then all the incoming call will direct forward to the speed dial number you entered.

Busy Forward: If you are on the phone, the new incoming call will forward to the number you entered.

No Answer Forward: If no one picks up the phone, the incoming call will forward to the number you entered.

When you finished the setting, please click the Submit button.

Fax Option	
<input checked="" type="radio"/> G.711 Fax Passthrough	<input type="radio"/> T.38 Fax Relay
P-Asserted-Identity	
P-Asserted-Identity	<input type="checkbox"/> Enable
Dial Termination Key	
Dial Termination Key	<input checked="" type="checkbox"/> Enable
Session Timer	
<input type="checkbox"/> Enable	
Minimum Expiration Time	<input type="text" value="90"/> (Min 90, Max 65536, Default 90) sec
Maximum Expiration Time	<input type="text" value="1800"/> (Min 90, Max 65536, Default 1800) sec
MWI (Message Waiting Indication)	
<input type="checkbox"/> Active	
Expiration Time	<input type="text" value="1800"/> (1-65535) sec

FAX Option

G.711 Fax Pass through: Select this if the IPG-110/IPG-200 should use G.711 to send fax messages. The peer devices must also use G.711.

T.38 Fax Relay: Select this if the IPG-110/IPG-200 should send fax messages as UDP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38

Session Timer

Enable: Select Enable if you want to define how long the IPG-110/IPG-200 waits to receive a session-alive packet for a voice session from the SIP server.

Minimum Expiration Time: Enter the minimum time the IPG-110/IPG-200 waits for a session-alive packet (90-65536 seconds). If a session-alive packet is not received during this time, the voice session is terminated.

Maximum Expiration Time: Enter the maximum time the IPG-110/IPG-200 waits for a session-alive packet (90-65536 seconds). If a session-alive packet is not received during this time, the voice session is terminated.

MWI (Message Waiting Indications)

Active: Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your SIP service provider must support this feature.

Expiration Time : Keep the default value, unless your SIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the IPG-110/IPG-200 subscribes to the service. Before this time passes, the IPG-110/IPG-200 automatically subscribes again.

DND (Do Not Disturb)	
DND Mode	<input type="radio"/> Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
From	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)
To	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)
Block Anonymous Call	
Block Anonymous Call	<input type="checkbox"/> Enable

DND Setting

DND Setting: you can setup the DND setting to keep the device silence. You can choose Always or Enable or Disable.

DND Always: All incoming call will be blocked until disable this feature.

DND Enable: Select Enable and the IPG-200/IPG-110 will be blocked during the time period. If the "From" time is large than the "To" time, the Block time will from 00:00 to 23:59

When you finished the setting, please click the Submit button.

If there is nothing need to change, please click the Save Change Item in the left side, then click the Save button. The change you made will save into the system and the system will Reboot automatically.

Block Anonymous Call

Select to enable the option

Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k ▾
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
G726-32k	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>						
G726-40k	<input type="checkbox"/>	<input checked="" type="checkbox"/>							

Codec

A CODEC is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 9 kinds of codec, G.711/Ulaw, G.711/Alaw, G.729, G.723(5.3k / 6.3k bps), G.726(16K bps), G.726(24K bps), G.726(32K bps), G.726(40K bps)

QoS

The QoS (Quality Of Service) is to guarantee that the SIP and RTP should be transmitting at the same time and Data couldn't influence the Voice quality.

The QoS (Quality Of Service) is to guarantee that the Voice and Data should be transmitting at the same time and Data couldn't influence the Voice quality. When TOS bits is enabled, it will guarantee the Voice have the first priority pass through the TOS enable devices.

VoIP > SIP > QoS

SIP Settings **QoS**

TOS

SIP TOS Priority Setting (0~255)

RTP TOS Priority Setting (0~255)

VLAN Tagging

Use VOICE VLAN Tags Enable

Voice VLAN ID (0~4090) Priority (0~7)

Use DATA VLAN Tags Enable

Data VLAN ID (0~4090) Priority (0~7)

VLAN Tagging

VLAN Setting: You can set the VLAN setting in this page. There are two parts in this page. First one is to set the packets related to the IPG-110, and the second one is if you use the VLAN setting in the NAT Mode.

There are two kind of destination packets will come from the IPG-110's WAN port, one kind of packets will go to the IPG-110, the other will go through the LAN port to the PC.

VLAN Packets: if you enable the first VLAN Packets and set the VID, User Priority, then all the incoming packets will be check with the IP Address and the VID.

Voice Vlan ID: You can follow your service provider to set your Voice Vlan ID.

Data Vlan ID: You can follow your service provider to set your Data Vlan ID.

User Priority: Defines user priority, giving eight (2^3) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits. Usually this will be defined by your service provider.

When you enable the first VLAN Packets and set the VID, User Priority, then all the incoming packets with the TA's IP address and the same VID will be accept by the TA. If the incoming packets with the TA's IP address but the different VID then the packets will be discard by the IPG-110. The Other incoming packets with different IP address will go through the LAN port to the PC.

4.2 Phone

Analog Phone

Select Phone 1 or Phone 2 first, then, click the Advance Setup button.

The screenshot shows the configuration page for an Analog Phone. The breadcrumb navigation at the top reads "VoIP > Phone > Analog Phone". Below this, there are three tabs: "Analog Phone" (selected), "Common", and "Region".

The "Analog Phone" section contains the following settings:

- Port Setting :** A dropdown menu currently set to "Phone 1".
- Outgoing Call Use:** Two radio buttons, "SIP1" (selected) and "SIP2".
- Incoming Call apply to:** Two checkboxes, "SIP1" (checked) and "SIP2" (unchecked).

At the bottom of the configuration area, there are three buttons: "Apply", "Reset", and "Advanced Setup".

Advanced Setup:

VoIP > Phone > Analog Phone > Advanced

Phone Port : 1

Jitter Buffer Size

Min delay (ms): 60

Max delay (ms): 200

Voice Activity Detection

VAD Enable

Jitter Buffer Control

In IPG-110/IPG-200 VoIP device, The jitter buffer control is a shared data area where voice packets can be stored, collected, and sent to the voice shared Buffer in evenly spaced intervals. modify in packets arrival time, called jitter, can occur because of network congestion, timing drift, or route changes.

- Min delay (ms): Select min delay buffer time.(40ms – 100 ms)
- Max delay (ms): Select Max delay Buffer time.(130ms – 300ms)
- Optimization factor: Controls quickly the length of the Jitter Buffer is increased when Voice RTP on the network. .Default is 7
- Voice Active Detector - It is used in speech encoding software to determine if the voice being encoded is human speech or background noise

Voice Activity Detection

If this function is enabled, when silence is occurred for a period of time, no data will be sent across the network during this period in order to save bandwidth.

(If you use Asterisk, please disable Silence Compression, it maybe make you call disconnect.)

G.168 Echo cancelation

LEC Tail Length (ms) 2

Voice Volume Control

Listening Volume -3 (-32~31 ,Mute:-32)

Speaking Volume -3 (-32~31 ,Mute:-32)

G.168 Echo cancelation

Select the tail lengths of 1ms, 2ms, 4ms, 8ms, 16ms, 32ms

Voice Volume control

- (Phone In)Speaker Voice Gain (db)- Sets a specific sound intensity for receiving sound. Select a level from -32 to 31,
- (Phone out)MIC Voice Gain (db)- Sets a specific sound intensity for transmitting sound. Select a level

from -32 to 31,

Loop Current	
Loop Current	22 mA ▼
Polarity Reversal	
Polarity Reversal	<input type="checkbox"/> Enable

Loop Current

Select the loop current.

Polarity Reversal

As Callee Answer - Check this box to generate line polarity reversal while the remote user picks up the phone call. As Callee On-Hook - Check this box to generate line polarity reversal while the remote user hangs off the phone call.

Caller ID setting	
Caller ID Mode	DTMF ▼
FSK Date & Time Sync	<input type="checkbox"/> Enable
Short Ring before Caller ID	<input type="checkbox"/> Enable
Dual Tone before Caller ID	<input type="checkbox"/> Enable
Caller ID Prior First Ring	<input checked="" type="checkbox"/> Enable
Caller ID DTMF Start Digit	DTMF_A ▼
Caller ID DTMF End Digit	DTMF_C ▼
Private Caller ID	<input type="checkbox"/> Enable
Hook-Flash Timing	
Minimum on-hook time	80 (Minimum:30 ms)
Maximum on-hook time	500 (Maximum:2000 ms)
Hot Line	
Use Hot Line	<input type="checkbox"/> Enable
Hot Line Timer	3 (0~30 seconds)
Hot Line Number	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Caller ID Mode:

- FSK Date & Time Sync: Send FSK Date & Time to display device.
- Reverse Polarity before Caller ID: Send Reverse Polarity before Caller ID
- Short Ring before Caller ID: Send short ring before caller ID.
- Dual Tone before Caller ID: Send Dual Tone before Caller ID.
- Caller ID prior First Ring: Send Caller ID before first ring.
- Caller ID DTMF Start Digit: Set Caller ID DTMF start digit.
- Caller ID DTMF END Digit: Set Caller ID DTMF start digit.

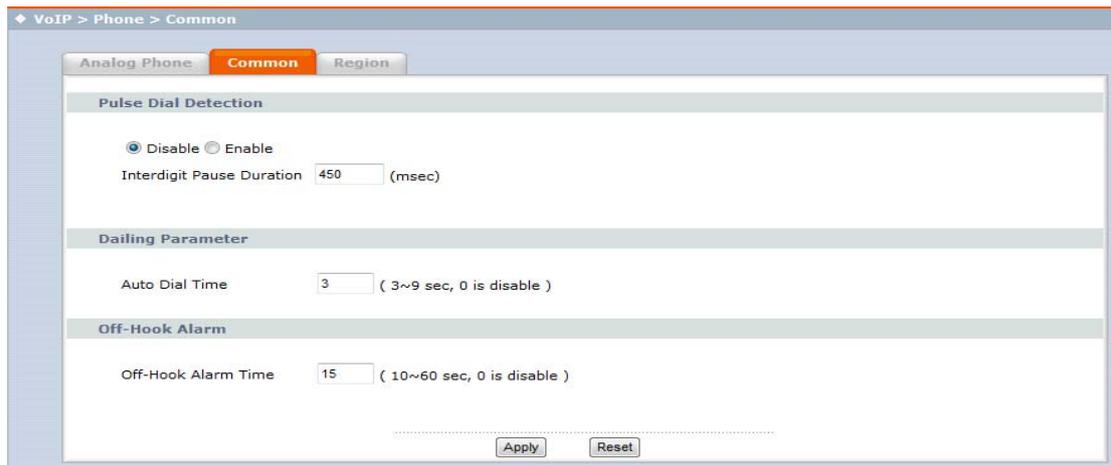
Hook-Flash Timing

- Minimum on-hook time default =30 ms
- Maximum on-hook time default =2000 ms

Hot Line

This service allows you to make a call to a pre-programmed number by only lifting the handset.

Common



Dialing Parameter

□Auto Dial Time- If no other number is being dialed within this interval, the IPG-110 will terminate this call. Assign the time interval from 1 to 9 seconds.

Off-Hook Alarm

□Off-Hook Alarm Time - Set has been off-hook, after this time, user will hear alarm. .

Region

Region Setting - Adjust the tone frequency according to each country. Select a country from the pull-down menu.

4.3 Phone Book

Speed Dial

Speed Dial lets you define a button or a set of buttons to link to a specific number defined in Speed Dial list.

Position	Name	Phone Number	Select
#01			<input type="checkbox"/>
#02			<input type="checkbox"/>
#03			<input type="checkbox"/>
#04			<input type="checkbox"/>
#05			<input type="checkbox"/>
#06			<input type="checkbox"/>
#07			<input type="checkbox"/>
#08			<input type="checkbox"/>
#09			<input type="checkbox"/>
#10			<input type="checkbox"/>

- Position - Select the speed dial shortcut to use from 0 to 9.
- Name—Phone number note.
- Phone Number - Enter the international number to dial.

Dial Plan With URL

The “Dialing plan with URL” need to set when the user use the method of Peer-to-Peer SIP VoIP call or SIP Proxy Server Mode. The SIP Dialing Plan has two kinds of directions: Outgoing (call out).

Dial Plan with URL							
Priority	Applied Target rule		Applied Operation				
	Lead Number	Min-Max Digits	Strip Digits Length	Prefix Number	Destination IP / URI	Destination SIP Port	Select (Enable)
1	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- “Lead Number” is the leading digits of the call out dialing number.
- “Min-Max Digits” has two text fields need filled: “Min Length” and “Max Length” are the min/max allowed length you can dial.
- “Strip Digits Length” is the number of digits that will be stripped from beginning of the dialed number.
- “Prefix Number” is the digits that will be added to the beginning of the dialed number.
- “Destination IP/ URI” is the IP address / Domain Name of the destination IPG-200/IPG-110 that owns this phone number.
- “Destination SIP Port” is port of the destination IPG-200/IPG-110 use.(Default is 5060)
- Call By PSTN: Priority to dial from PSTN

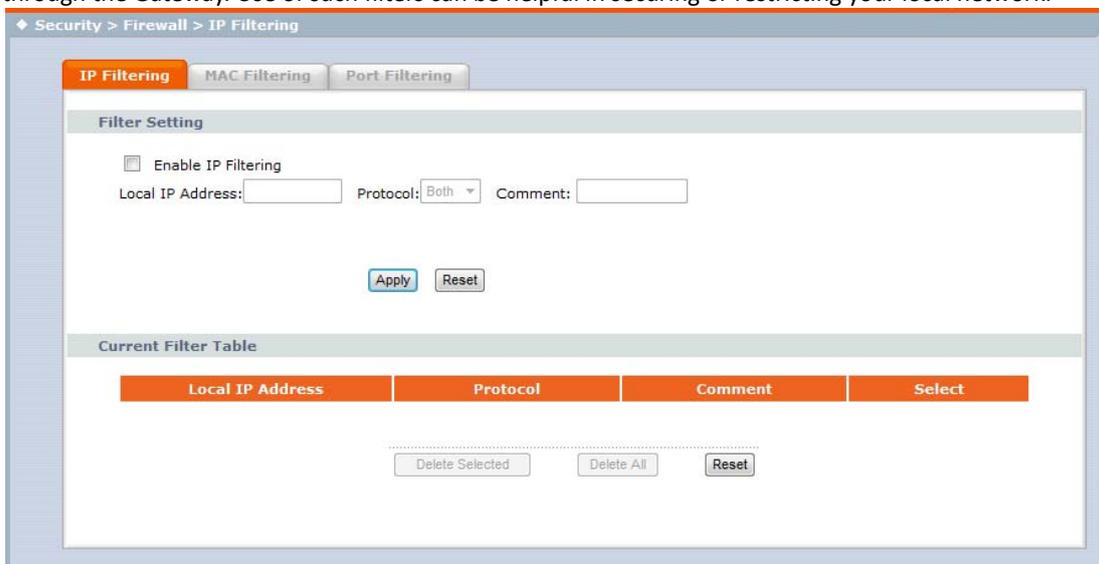
Security

5.1 Firewall

-  IP Filtering
-  Mac Filtering
-  Port Filtering
-  Content Filtering

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



Security > Firewall > IP Filtering

IP Filtering | MAC Filtering | Port Filtering

Filter Setting

Enable IP Filtering

Local IP Address: Protocol: Both Comment:

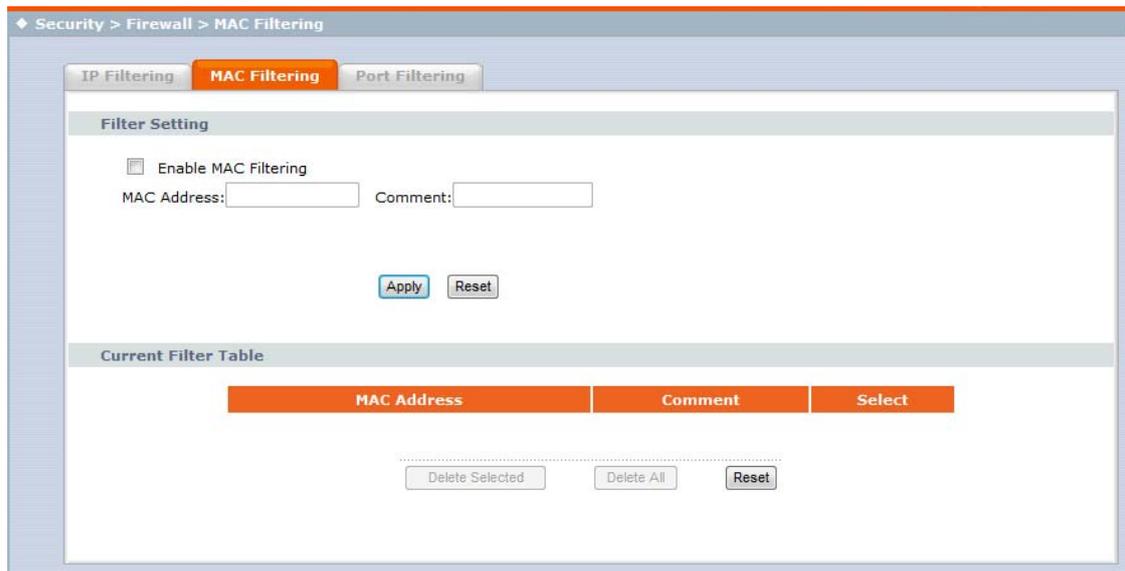
Current Filter Table

Local IP Address	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

- Enable/Disable IP Filtering - The IP address filter function ,control a network IP address from your local network to Internet through the Gateway ,default setting is disable.

Mac Filtering

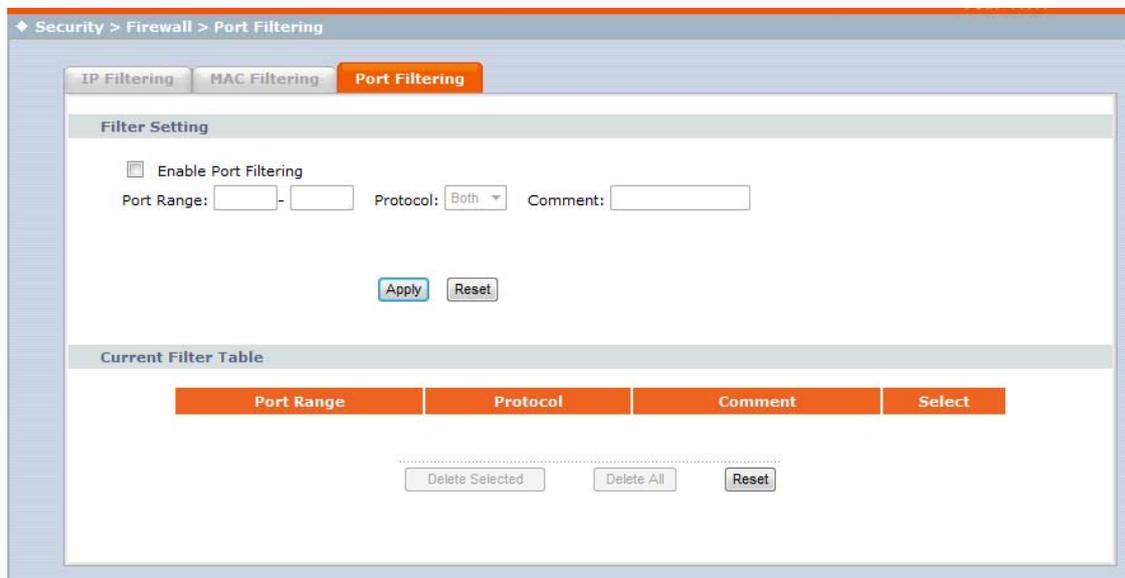
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



□MAC Enable/Disable –from your local network to Internet through the Gateway MAC filter function, default setting is disable.

Port Filtering

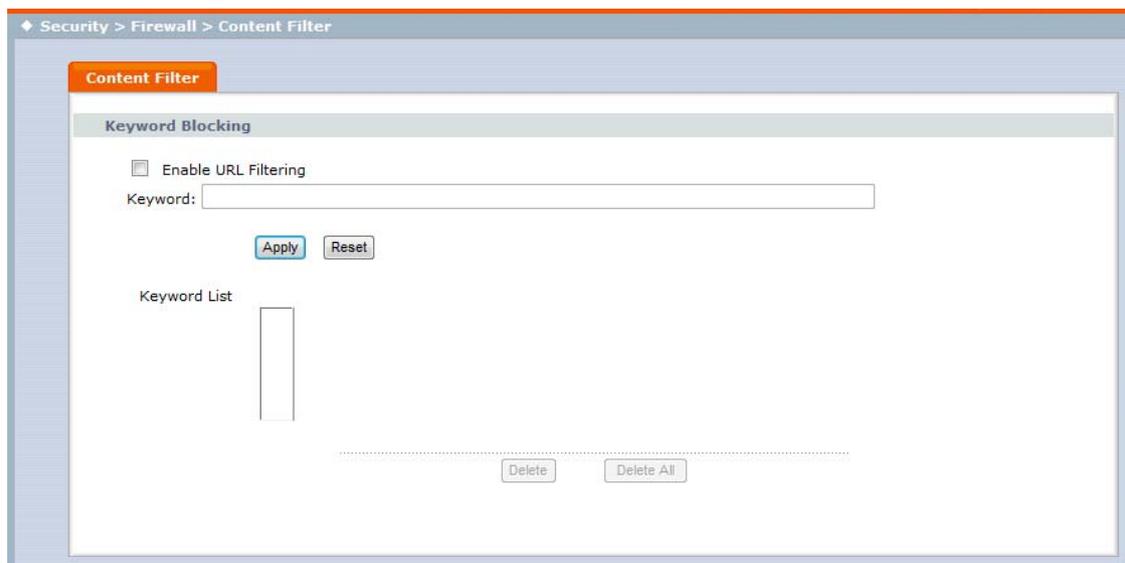
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network



Content Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

URL filter allows you to block sites based on a black list and white list. Sites matching the black list but not matching the white list will be automatically blocked and closed.



- Enable - Enable/Disable the URL filter function, default setting is Disable.
- Client IP - This is the Client IP is LAN address.
- URL Filter String - This is the filter URL.
Example: "http://www.yahoo.com/"

Maintenance

System

- Account setting
- Time Zone
- Auto Provision
- DDNS

Tool

- Configuration
- Upgrade Firmware
- Ping Test
- Restart

Log

- System Log

6.1 System

General

This page is used to set the Router or Bridge mode. And the account to access the web server of Access Point. Empty user name and password will disable the protection.

Note: If select Bridge mode, the system will disable the firewall and NAT automatically.

If select Bridge mode, please set the Management IP Address

The screenshot shows a web interface for system configuration. The breadcrumb path is "Maintenance > System > General". There are four tabs: "General" (selected), "Time Setting", "Auto Provision", and "Dynamic DNS".

System Setup

Mode: Router Bridge

Administrator Inactivity Timer : (minutes, 0 means no timeout)

Manager IP Address:

Note:

- 1.If change to Bridge mode, the system will automatic to disable firewall and NAT .
- 2.If change to Bridge mode, Please set Management IP Address

Administrator Account

User Name:

User Password:

User Account

User Name:

User Password:

Buttons:

Time Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

The screenshot shows the 'Time Setting' configuration page. At the top, there are tabs for 'General', 'Time Setting' (selected), 'Auto Provision', and 'Dynamic DNS'. Below the tabs is a 'General Setup' section with the following fields and options:

- Current Time : Year 2012, Month 2, Day 20, Hour 11, Minute 48, Second 59
- Time Zone Select : (GMT+01:00)Sarajevo, Skopje, Sofija, Warsaw, Zagreb
- Enable NTP client update
- Automatically Adjust Daylight Saving
- NTP server : 192.5.41.41 - North America (selected), (Manual IP Setting)

At the bottom of the form are three buttons: 'Apply', 'Reset', and 'Refresh'.

Auto Provision

Enable or disable the auto-provisioning feature. If enabled, the phone will try to download the two configuration files from the provisioning server via FTP/TFTP / HTTP on system startup; Default is disabled.

The screenshot shows the 'Auto Provision' configuration page. At the top, there are tabs for 'General', 'Time Setting', 'Auto Provision' (selected), and 'Dynamic DNS'. Below the tabs is an 'Auto Provision' section with the following fields and options:

- Protocol : Disable
- File Path : Exp. auto
- Expiration Time : 10800 seconds

At the bottom of the form are two buttons: 'Apply' and 'Reset'.

DDNS

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly ever changing) IP-address.

The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet.

Without DDNS, the users should use the WAN IP to reach internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported, you apply a DNS name (e.g., www.TA-201.com) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.ata.com regardless of the WAN IP.

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, you can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname.

Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.

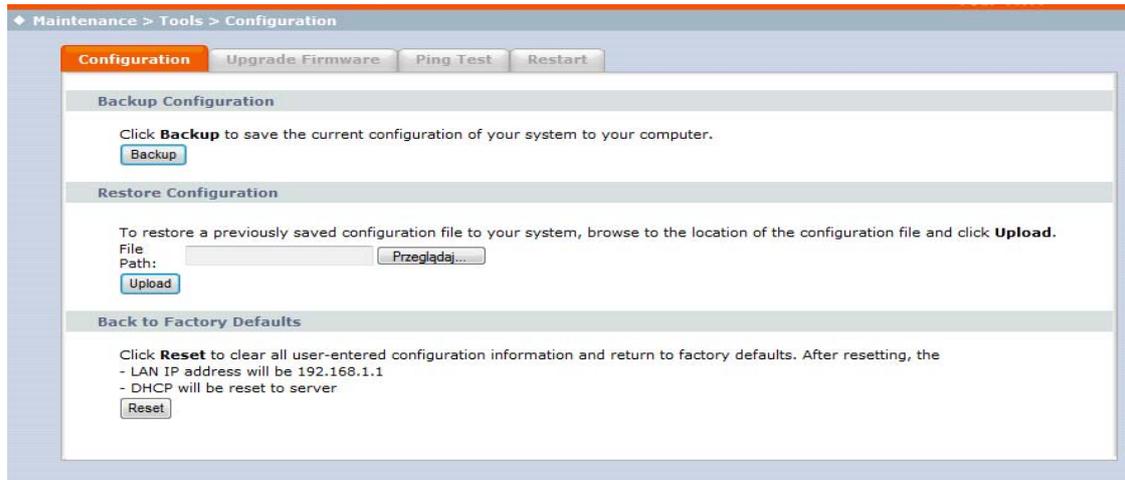
DDNS is a method of keeping a domain name linked to a changing (dynamic) IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the TA-201, you can setup your DDNS service and the ATA will automatically update your DDNS server every time it receives a different IP address.

- Enable - Enable/Disable the DDNS service, default setting is Disable.
- DDNS Server Type - The IPG-110 support two types of DDNS, DynDns.org or TZO.net
- Domain Name - The hostname which you register in DynDns.org or TZO.net website.
- DDNS Username - The username which you register in DynDns.org or TZO.net website.
- DDNS Password - The password which you register in DynDns.org or TZO.net website.

6.2 Tools

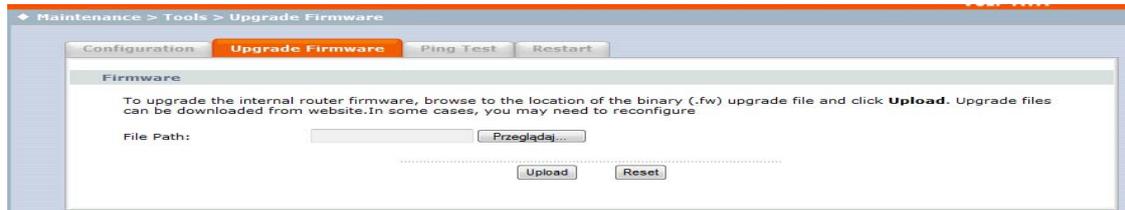
Configuration

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.



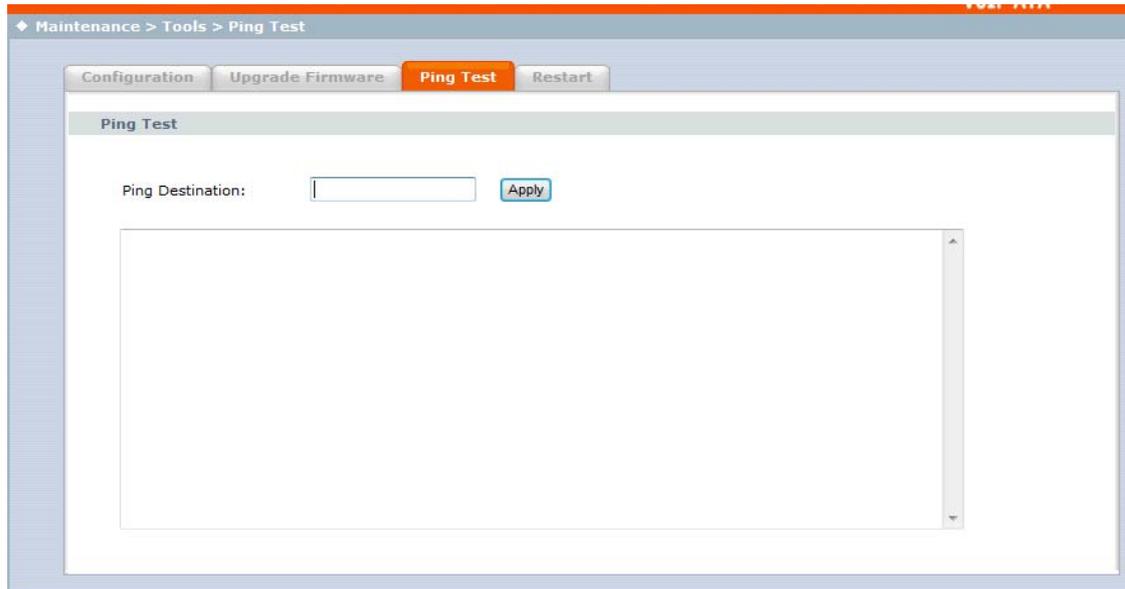
Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.



Ping Test

Ping function you can Ping IP or Domain.



EX:

Ping 168.95.1.1 and response as follow:

```

PING 168.95.1.1 (168.95.1.1): 56 data bytes
64 bytes from 168.95.1.1: icmp_seq=0 ttl=247 time=80.0 ms
64 bytes from 168.95.1.1: icmp_seq=1 ttl=247 time=100.0 ms
64 bytes from 168.95.1.1: icmp_seq=2 ttl=247 time=240.0 ms
64 bytes from 168.95.1.1: icmp_seq=3 ttl=247 time=30.0 ms
--- 168.95.1.1 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 30.0/112.5/240.0 ms
    
```

Restart

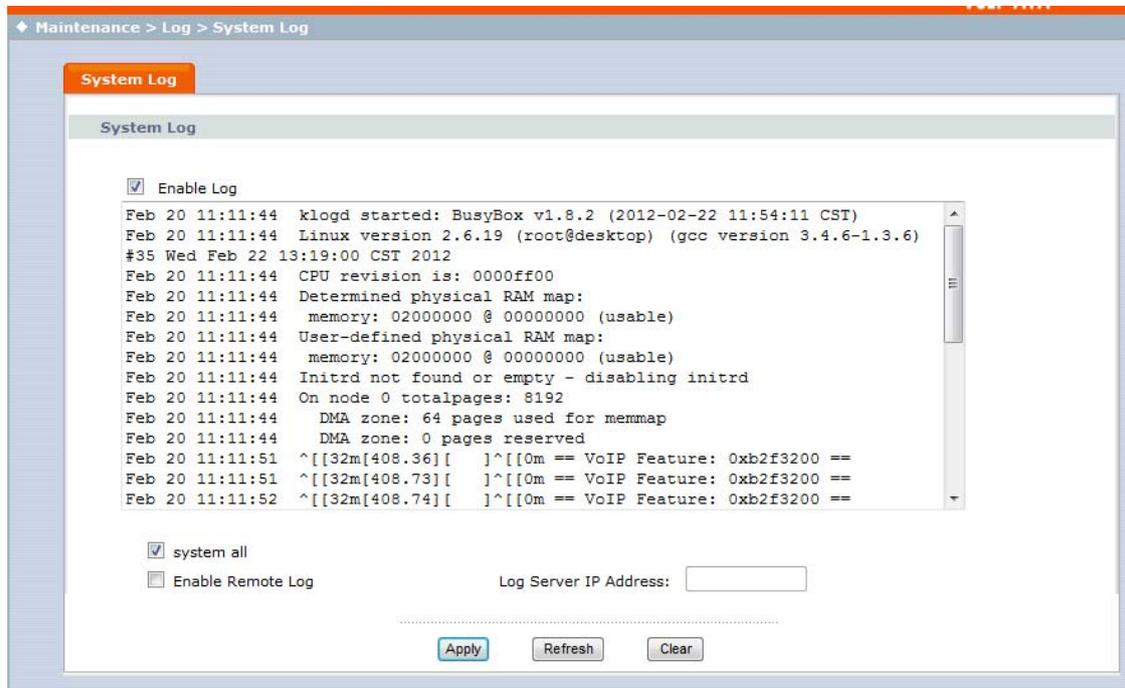
Restart function you can restart the IPG-200/IPG-110 device. If you want to restart the IPG-200/IPG-110, you can just click the Reboot button, than the VoIP Phone will automatically.

If for any reason the device is not responding correctly, you may want to restart the IPG-200/IPG-110 system



6.3 Log

If you want to Log the IPG-110/IPG-200 system log , you can enable log and enable system all ,
The system will record system log .



The screenshot shows a web interface for configuring the system log. The breadcrumb navigation is "Maintenance > Log > System Log". The page title is "System Log". There is a checkbox labeled "Enable Log" which is checked. Below this is a scrollable text area containing the following log output:

```
Feb 20 11:11:44 klogd started: BusyBox v1.8.2 (2012-02-22 11:54:11 CST)
Feb 20 11:11:44 Linux version 2.6.19 (root@desktop) (gcc version 3.4.6-1.3.6)
#35 Wed Feb 22 13:19:00 CST 2012
Feb 20 11:11:44 CPU revision is: 0000ff00
Feb 20 11:11:44 Determined physical RAM map:
Feb 20 11:11:44   memory: 02000000 @ 00000000 (usable)
Feb 20 11:11:44 User-defined physical RAM map:
Feb 20 11:11:44   memory: 02000000 @ 00000000 (usable)
Feb 20 11:11:44 Initrd not found or empty - disabling initrd
Feb 20 11:11:44 On node 0 totalpages: 8192
Feb 20 11:11:44   DMA zone: 64 pages used for memmap
Feb 20 11:11:44   DMA zone: 0 pages reserved
Feb 20 11:11:51 ^[[32m[408.36][ ]^[[0m == VoIP Feature: 0xb2f3200 ==
Feb 20 11:11:51 ^[[32m[408.73][ ]^[[0m == VoIP Feature: 0xb2f3200 ==
Feb 20 11:11:52 ^[[32m[408.74][ ]^[[0m == VoIP Feature: 0xb2f3200 ==
```

Below the log output, there are two checkboxes: "system all" (checked) and "Enable Remote Log" (unchecked). To the right of "Enable Remote Log" is a text input field labeled "Log Server IP Address:". At the bottom of the page are three buttons: "Apply", "Refresh", and "Clear".

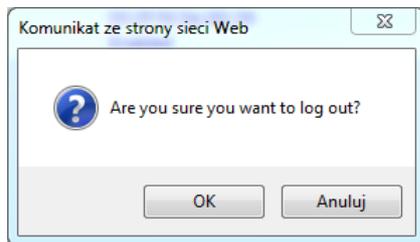
Logout

If you need to logout administrator right for web-access, please click the Logout link. The web system management interface will auto-logout with 1800 sec default value.

The screenshot shows the 8level VoIP ATA web interface. The top navigation bar includes the 8level logo and a 'Logout' link. A left sidebar contains menu items: Status, Network, VoIP, Security, and Maintenance. The main content area is titled 'Status' and contains several sections:

- Device Information:** Model Type: (2FXS 1WAN 1LAN), Firmware Version: sunnyline_tab_106.
- WAN Information:** WAN Access Type: Static IP, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, MAC Address: 00:0f:fd:Se:00:28.
- LAN Information:** IP Address: 192.168.1.1, IP Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, MAC Address: 00:0f:fd:Se:00:29, DHCP Server: Enabled.
- System Status:** System Uptime: 0day:0h:41m:48s, Current Date/Time: Mon Feb 20 11:53:03 2012, System Resource: CPU Usage: 0%, Memory Usage: 36%.
- Interface Status:** A table showing WAN (Down) and LAN (Up) with a rate of 100M.
- Summary Status:** Links for DHCP Table and Packet Statistics.
- VoIP Status:** A table with columns for SIP Account, Registration, REG Status, and URI.

SIP Account	Registration	REG Status	URI
Phone 1	UnRegister	503 Service Unavailable	6000@serwer.sip.com
Phone 2	UnRegister	503 Service Unavailable	6001@serwer.sip.com



Information

System Information

System Status

This page shows the current status and some basic settings of the device.

Click System Information to display system status, The Device Information has WAN type, and LAN type, Phone Status, more Status...etc.

The screenshot displays the 8level VoIP ATA web interface. The top navigation bar includes the 8level logo, a 'Status' dropdown menu, and a 'VoIP ATA' label. The main content area is divided into several sections:

- Device Information:** Shows model type (2FXS 1WAN 1LAN), firmware version (sunnyline_tab_106), WAN information (Static IP, 0.0.0.0), and LAN information (192.168.1.1).
- System Status:** Displays system uptime (0day:0h:41m:48s), current date/time (Mon Feb 20 11:53:03 2012), system resource usage (CPU: 0%, Memory: 36%), and interface status (WAN: Down, LAN: Up).
- VoIP Status:** A table showing SIP account registration details for two phones.

SIP Account	Registration	REG Status	URI
Phone 1	<input type="button" value="UnRegister"/>	503 Service Unavailable	6000@server.sip.com
Phone 2	<input type="button" value="UnRegister"/>	503 Service Unavailable	6001@server.sip.com

This page displays the current information for the device. It will display the LAN \ WAN and system firmware information. This page will display different information for you, according your WAN setting (Static IP, DHCP, PPPoE, PPTP).

If your WAN connection is set up for Dynamic IP address, there will be a Release button and Renew button. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your WAN connection is set up for PPPoE, there will be a Connect button and **Disconnect button**. Use **"Disconnect"** to drop the PPPoE connection and use "Connect" to establish the PPPoE connection

IVR Command

Can use the fxs port keypad to operator IPG-200/IPG-110, follow the instruction to listen IPG-200/IPG-110 configuration.

Category	Command	Definition
Voice Network Settings	#120	Voice IP address
	#121	Voice IP type
	#123	Voice netmask
	#124	Voice gateway
	#125	Voice DNS
	#128	Voice firmware Version

Appendix

A - FAQ List

1. What is the default administrator password to login to the IPG-200/IPG-110? How to Login?

A: By default, default username is “admin”, default password is also “admin” to login to the router. For security, you should modify the password to protect your gateway against hacker attacks. Default Wan Port Access type is DHCP Client, LAN Port IP Address is “192.168.1.1”. Logging Web User Interface, open the Browser (IE/FireFox) and input IP address.

2. I forgot the administrator password. What should I do?

A: Press the **Reset** button on the rear panel for over 5 seconds to reset all settings to default factory values. Then you can use the default Username/Password to Login Web UI.

3. Why is it that I can ping to outside hosts, but not access Internet Web sites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router will assign the DNS settings to the DHCP-client-enabled PC.

4. What is the maximum number of IP addresses that the DHCP server of the gateway can assign to local PCs?

A: The built-in DHCP server can support 253 IP addresses for local network usage.

5. Why can I call out by IPG-200/IPG-110?

A: Please check your IPG-200/IPG-110 is registered SIP Proxy Server (ITSP), and check your Internet works fine. IPG-200/IPG-110 can't make a call without Internet or SIP Account that from ITSP supply. You must have a SIP account or know the other ATA/Gateway IP/Domain Name, then you can make a VoIP call.

6. I can't use web interface to setting IPG-200/IPG-110, How can I do?

A: Please check your PC connects the IPG-200/IPG-110 Lan port or PC and IPG-200/IPG-110 with the same Subnet. If your PC aren't at the same Subnet, you can't Login the IPG-110 Web interface. Else you let your IPG-200/IPG-110 on Public Internet (Public IP address).

7. Why does the one way talk happen?

A: Generally, one way talk happen when use the different codec between VoIP devices make call. Please check and setting the same codec, most one way talk will be solved.

8. Why can I call out when the IPG-200/IPG-110 under the NAT?

A: Most VoIP products have problem in NAT Pass through. By SIP, there are many NAT Pass through Function can solve 80% NAT Problem. You can choose STUN/Outbound Proxy/ Symmetric RTP to Pass through NAT, you don't set any other setting (DMZ/Virtual Server) by router side. If you use STUN/Outbound Proxy, you must have a STUN/Outbound Proxy Server to support. If they can't pass NAT, please open the DMZ/Virtual Server by Router/NAT/Firewall.

B - Scenario Application Samples

