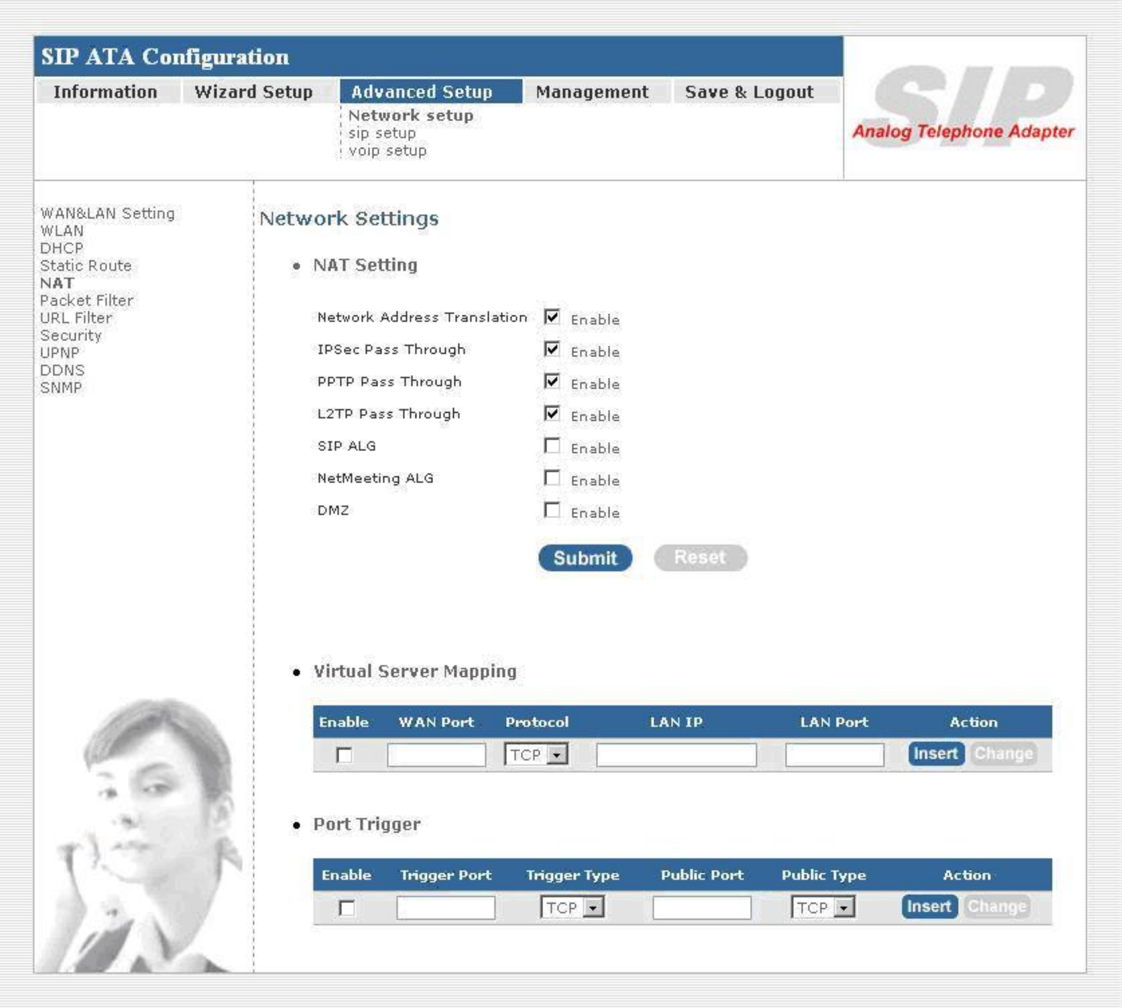


Network Settings

- NAT Setting

Network Address Translation	☑ Enable
IPSec Pass Through	☑ Enable
PPTP Pass Through	☑ Enable
L2TP Pass Through	☑ Enable
SIP ALG	□ Enable
NetMeeting ALG	□ Enable
DMZ	□ Enable

- Virtual Server Mapping

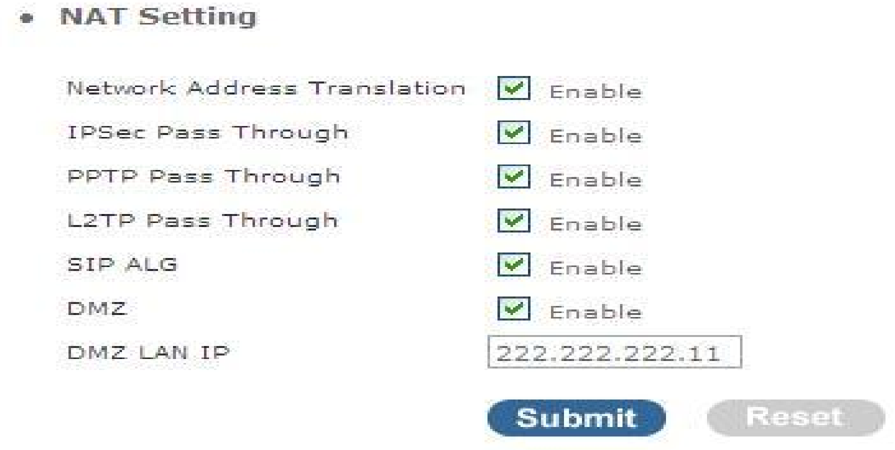
Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
□		TCP			Insert Change

- Port Trigger

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
□		TCP		TCP	Insert Change

NAT Setting

Network Address Translation - Enable/Disable NAT.
□IPSec Pass Through - IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Enable/Disable this framework verification.



- NAT Setting

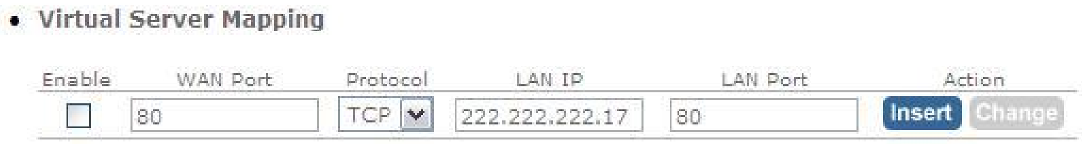
Network Address Translation	☑ Enable
IPSec Pass Through	☑ Enable
PPTP Pass Through	☑ Enable
L2TP Pass Through	☑ Enable
SIP ALG	☑ Enable
DMZ	☑ Enable
DMZ LAN IP	222.222.222.11

□PPTP Pass Through - PPTP (Point-to-Point Tunneling Protocol) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public

Internet. Enable/Disable this protocol verification.
□L2TP Pass Through - L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. Enable/Disable this function.
□SIP ALG - SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.
□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.

Virtual Server Setting (for AP mode)

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network. You will only need to input the LAN IP address of the computer running the service and enable it.
A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP.

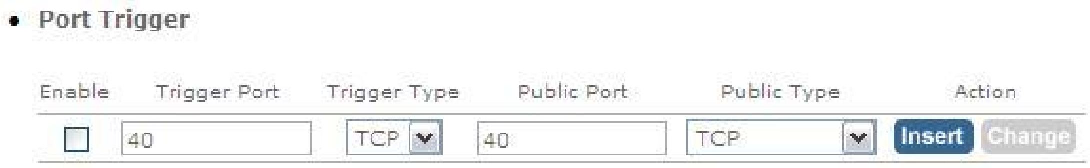

- Virtual Server Mapping

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
□	80	TCP	222.222.222.17	80	Insert Change

□Enable - Enable/Disable the virtual server mapping, default setting is Disable.
□WAN Port - The port number on the WAN side that will be used to access the virtual service. Enter the WAN Port number, e.g. enter 80 to represent the Web(http server), or enter 25 to represent SMTP (email server). Note: You can *specify maximum 32 WAN Ports.*
□Protocol - The protocol used for the virtual service. Select a protocol type is TCP or UDP.
□LAN IP - The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.
□LAN Port - The port number of the service used by the Private IP computer. Enter the LAN port number.
□Action - Insert a new WAN port or update a specified WAN port.

Port Trigger

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol), then enter the public ports associated with the trigger port to open them for inbound traffic.



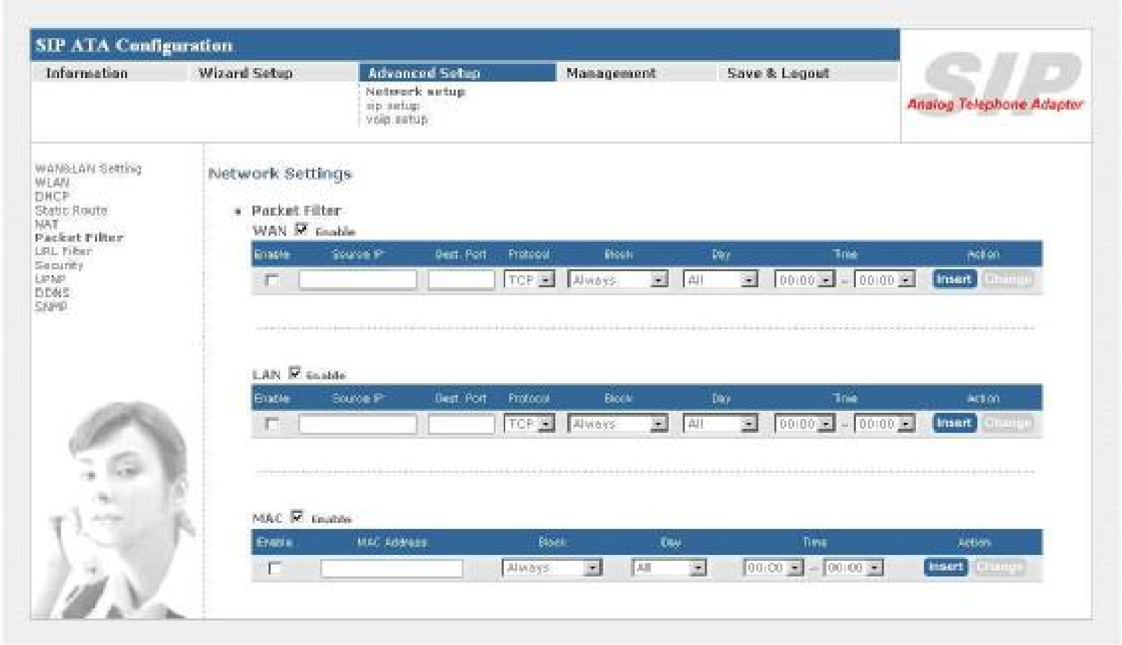
- Port Trigger

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
□	40	TCP	40	TCP	Insert Change

□Enable - Enable/Disable the port trigger, default setting is Disable.
□Trigger Port - This is the port used to trigger the application. It can be either a single port or a range of ports.
□Trigger Type - This is the protocol used to trigger the special application.
□Public Port - This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.
□Public Type - This is the protocol used for the special application.
□Action - Insert a new Port Trigger or update a specified Port Trigger.

3.6 PacKet Filter

Controlling access to a network by analyzing the incoming packets and letting them pass or halting them based on the IP addresses of the source.



Network Settings

- Packet Filter

WAN ☑ Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
□			TCP	Always	All	00:00 - 00:00	Insert Change

LAN ☑ Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
□			TCP	Always	All	00:00 - 00:00	Insert Change

MAC ☑ Enable

Enable	MAC Address	Block	Day	Time	Action
□		Always	All	00:00 - 00:00	Insert Change

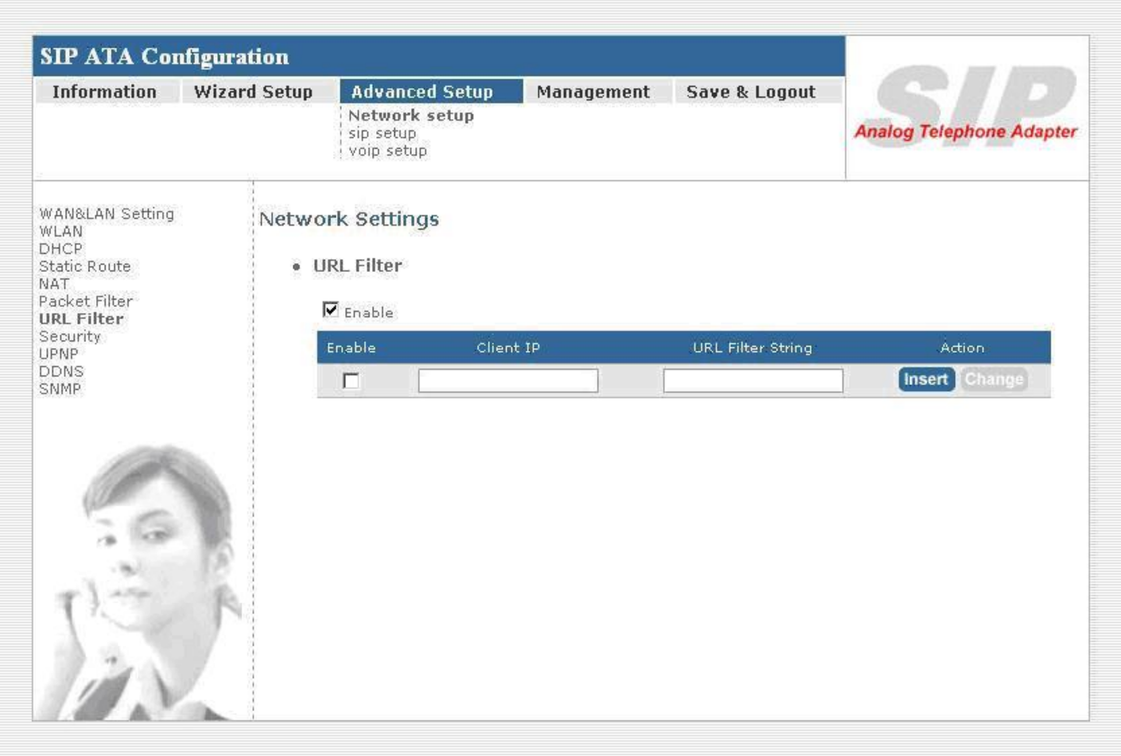
□WAN Enable/Disable - The WAN IP port packet filter function ,control a network IP port ,default setting is Enable.
□Enable - Enable/Disable the Internet to WAN IP source port rules, default setting is Disable.
□Source IP - This is the filter WAN IP address.
Example: 209.131.36.158
□Dest. Port - This is the port used for source IP service.
□Protocol - This Protocol Used for the source IP service. Select a protocol type is TCP or UDP.
□Black - Wan IP Port Black time. Select a Always or by schedule.
□Day - Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59.
□LAN Enable/Disable – Internet to LAN filter function ,default setting is Enable. A prohibitive rule set should only allow the necessary Internet/DMZ services to LAN (Local Area Network) clients.
□Enable - Enable/Disable the WAN IP source port rules, default setting is Disable.
□Source IP - This is the filter source IP address to LAN.
□Dest. Port - This is the port used for source IP.

□Protocol - This Protocol Used for the WAN Filter service. Select a protocol type is TCP or UDP
□Day - Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59

□MAC Enable/Disable –Form internet MAC filter function ,default setting is Enable.
□Black - Wan IP Port Black time. Select a Always or by schedule.
□Day – Select Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59

3.7 URL Filter

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.



Network Settings

- URL Filter

☑ Enable

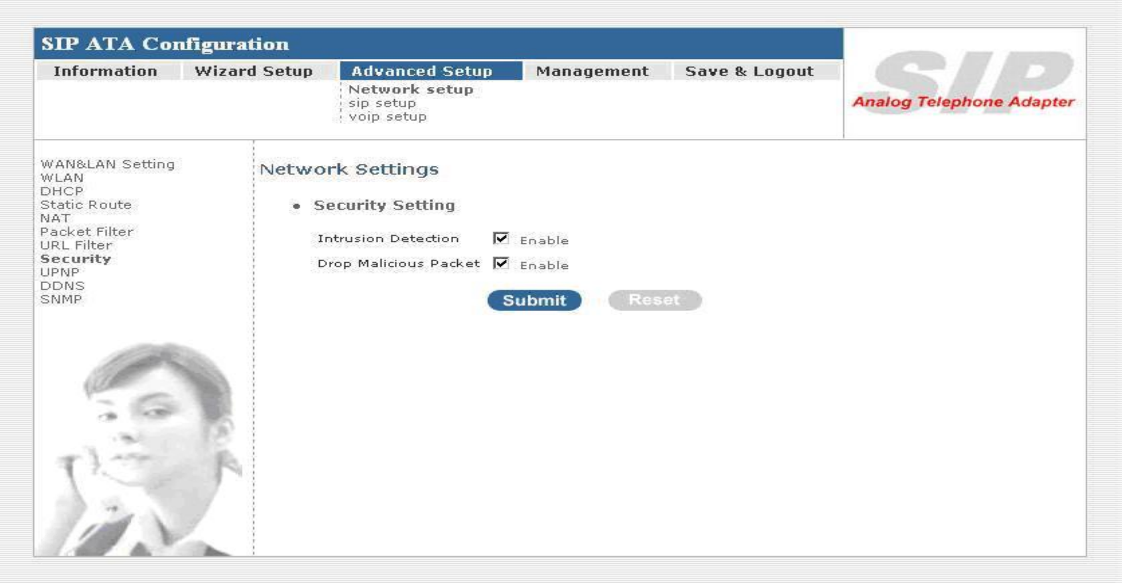
Enable	Client IP	URL Filter String	Action
□			Insert Change

□Enable - Enable/Disable the URL filter function, default setting is Disable.
□Enable - Enable/Disable Block URL to the Clinet IP, default setting is Disable
□Client IP - This is the Clinet IP is LAN address.
Example: 222.222.222.100
□URL Filter String - This is the filter URL.
Example: “http://www.yahoo.com/”

3.8 Security (For AP mode only)

Intrusion Detection has powerful management and analysis tools that let your IT administrator see what's going on in your network. Such as who's surfing the Web, and gives you the tools to block access to inappropriate Web sites.

Malicious code (also called vandals) is a new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone. In contrast to viruses that require a user to execute a program in order to cause damage, vandals are auto-executable applications.



Network Settings

- Security Setting

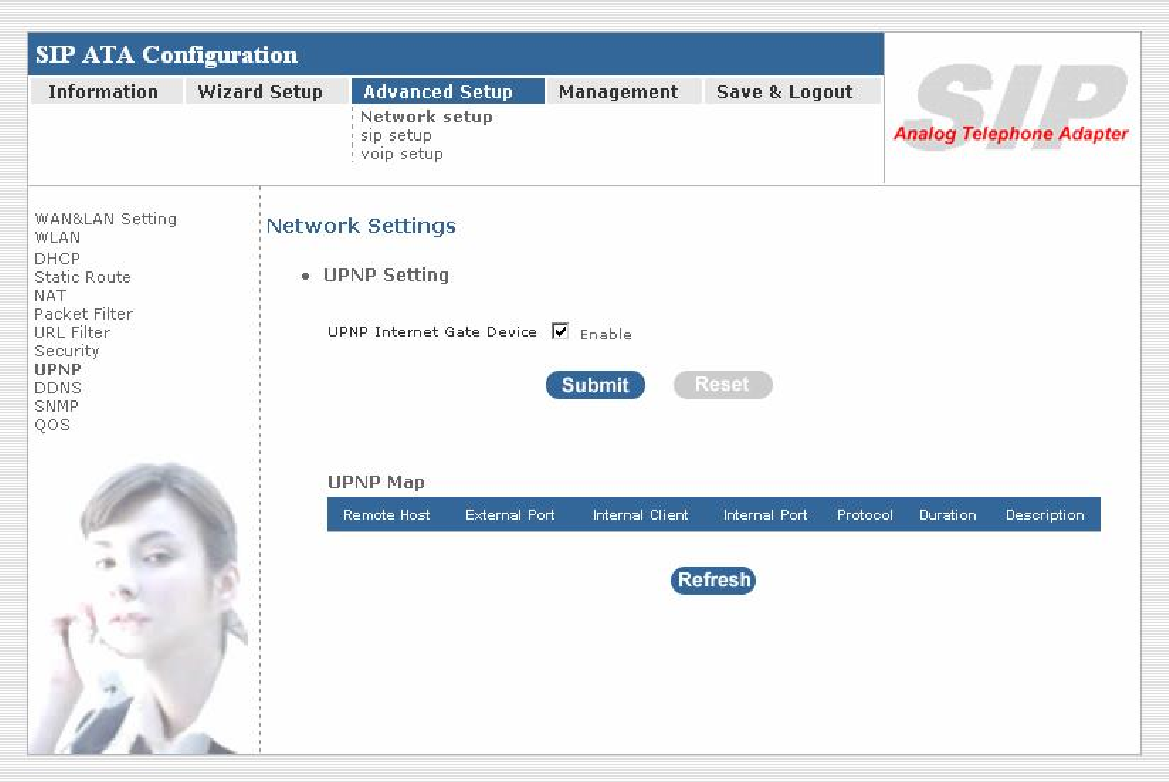
Intrusion Detection ☑ Enable

Drop Malicious Packet ☑ Enable

□Intrusion Detection - Enable / Disable , network / internet security protection.
□Drop Malicious Packet - Enable / Disable , Detect and drop malicious application layer traffic.

3.9 UPNP (For AP mode only)

UPnP provides support for communication between control points and devices. The network media, the TCP/IP protocol suite and HTTP provide basic network connectivity and addressing needed. On top of these open, standard, Internet based protocols, UPnP defines a set of HTTP servers to handle discovery, description, control, events, and presentation.



Network Settings

- UPNP Setting

UPNP Internet Gate Device ☑ Enable

UPNP Map

Remote Host	External Port	Internal Client	Internal Port	Protocol	Duration	Description

□ UPNP Internet Gate Device – Enable/Disable UPNP Service to working ,default setting is Disable.

3.10 DDNS (For AP mode only)

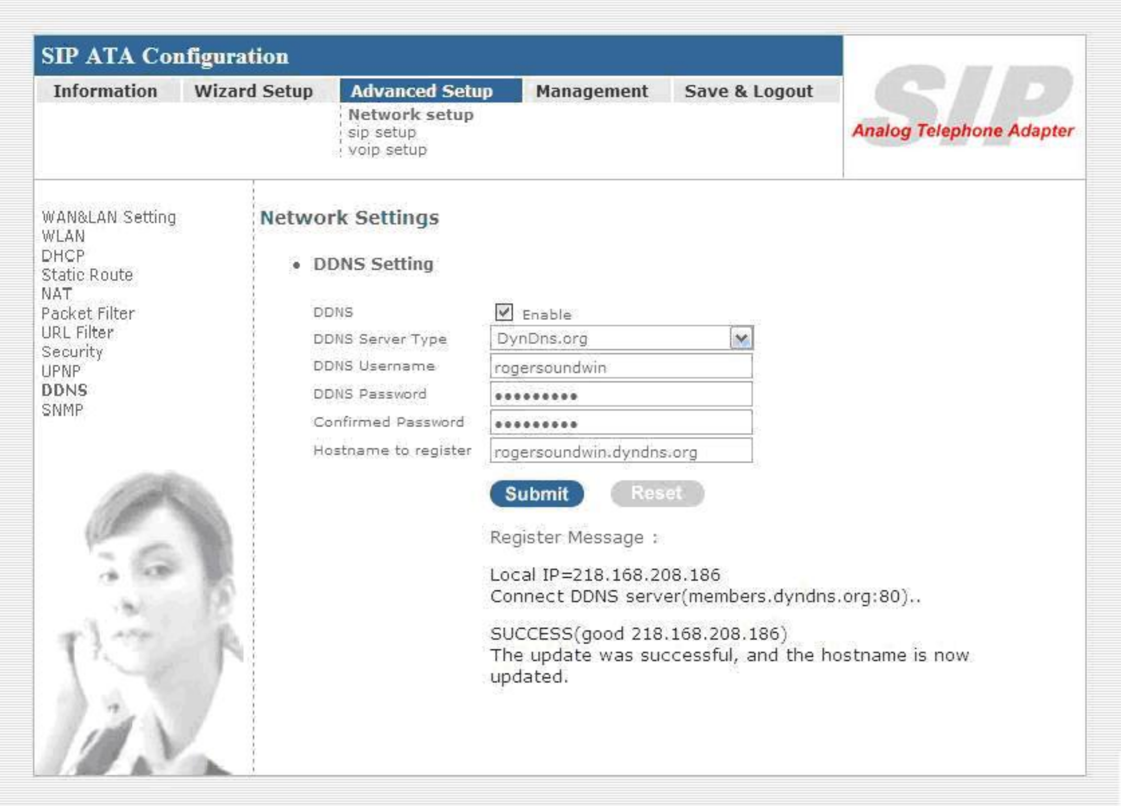
The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet.

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.ata.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 ATA, you can setup your DDNS service and the ATA will automatically update your DDNS server every time it receives a different IP address.



Network Settings

- DDNS Setting

DDNS	☑ Enable
DDNS Server Type	DynDns.org
DDNS Username	rogersoundwin
DDNS Password	●●●●●●●●●
Confirmed Password	●●●●●●●●●
Hostname to register	rogersoundwin.dyndns.org

Register Message :

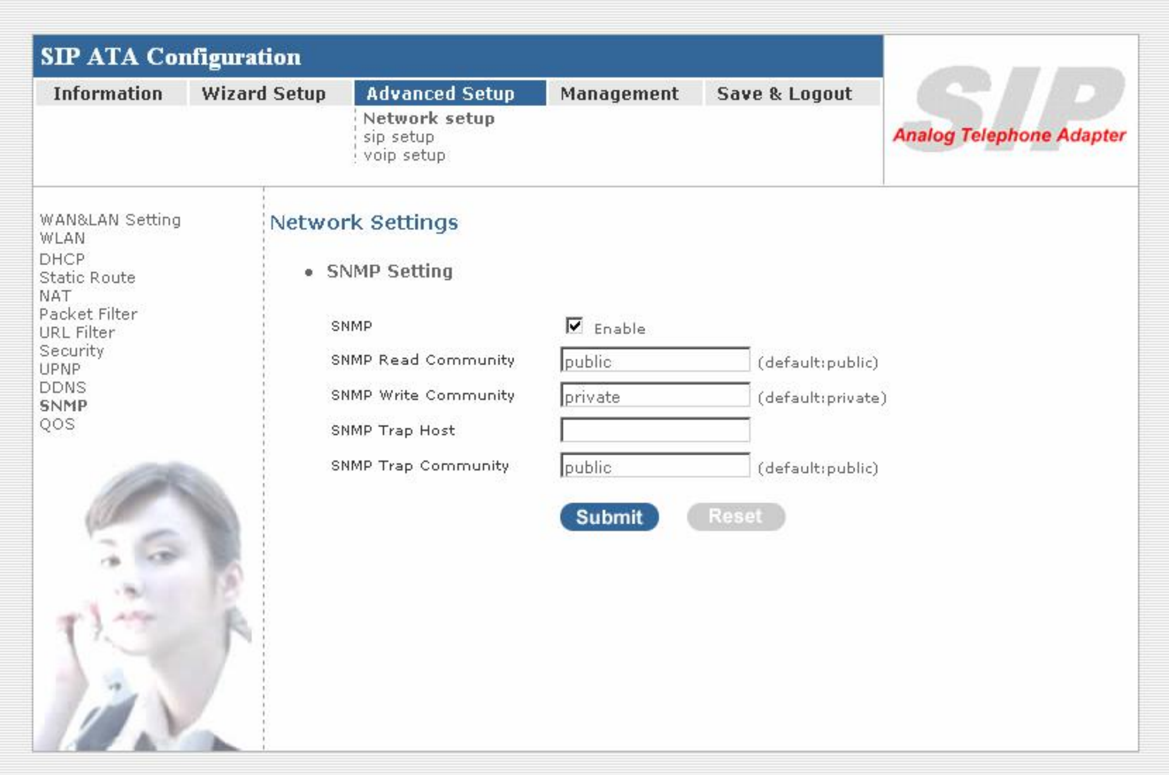
```
Local IP=218.168.208.186
Connect DDNS server(members.dyndns.org:80)..

SUCCESS(good 218.168.208.186)
The update was successful, and the hostname is now
updated.
```

□Enable - Enable/Disable the DDNS service, default setting is Disable.
□DDNS Server Type - The ATA support two types of DDNS, DynDns.org or No-IP.com
□DDNS Username - The username which you register in DynDns.org or No-IP.com website.
□DDNS Password - The password which you register in DynDns.org or No-IP.com website.
□Confirmed Password - Confirm the password which you typing.
□Hostname to register - The hostname which you register in DynDns.org or No-IP.com website.

3.11 SNMP (For AP mode only)

The simple network management protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.



Network Settings

- SNMP Setting

SNMP	☑ Enable	
SNMP Read Community	public	(default:public)
SNMP Write Community	private	(default:private)
SNMP Trap Host		
SNMP Trap Community	public	(default:public)

□Enable - Enable/Disable the SNMP service, default setting is Disable. (Support SNMP version 1 or SNMP version 2c).

□SNMP Read Community - SNMP Read Community string so that EPICenter can retrieve information.(default :public)

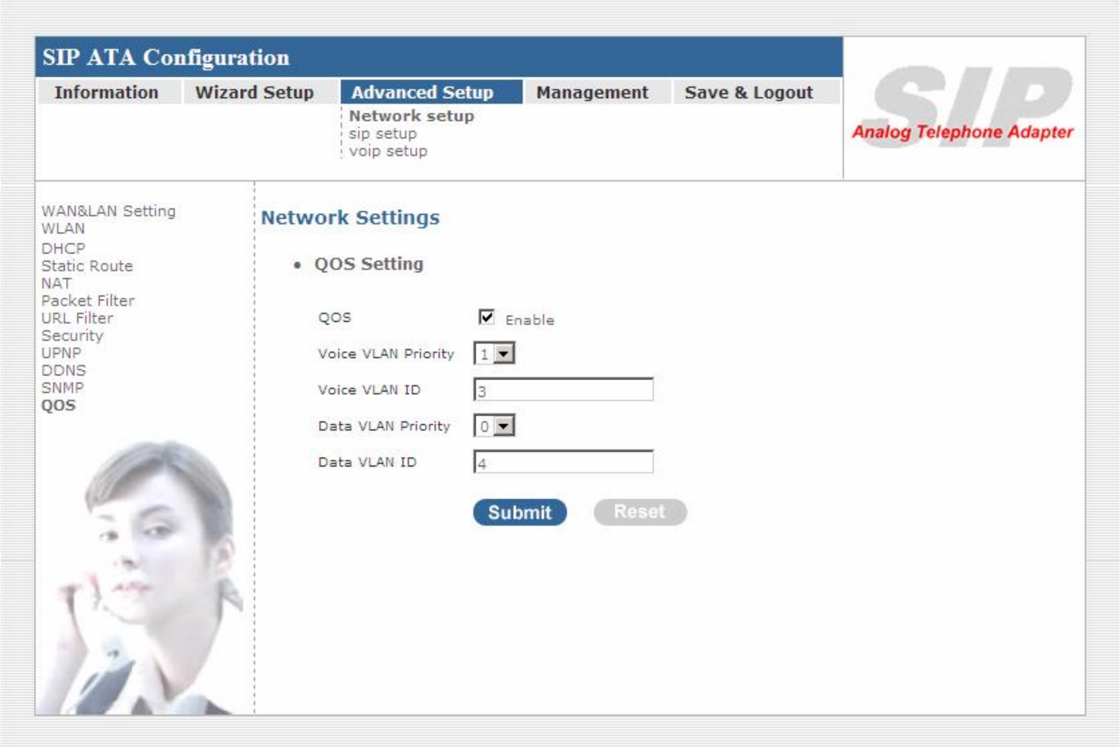
□SNMP Write Community - Specifies the name of the SNMP write community to which the printer device that this actual destination represents belongs.(Default:private)

□SNMP Trap Host - Defines an SNMP trap host to which AppCelera will send trap messages. (Default address is empty)

□SNMP Trap Community –The SNMP trap community name. The community name functions as a password for sending trap notifications to the target SNMP manager.(Default : public).

3.12 QOS (VLAN)

VLAN which stands for Virtual LAN is defined in the IEEE802.1q. It is a technology allowing a company or an individual to extend their LAN over the WAN interface, breaching the physical limitations of regular LANs.



Network Settings

- QOS Setting

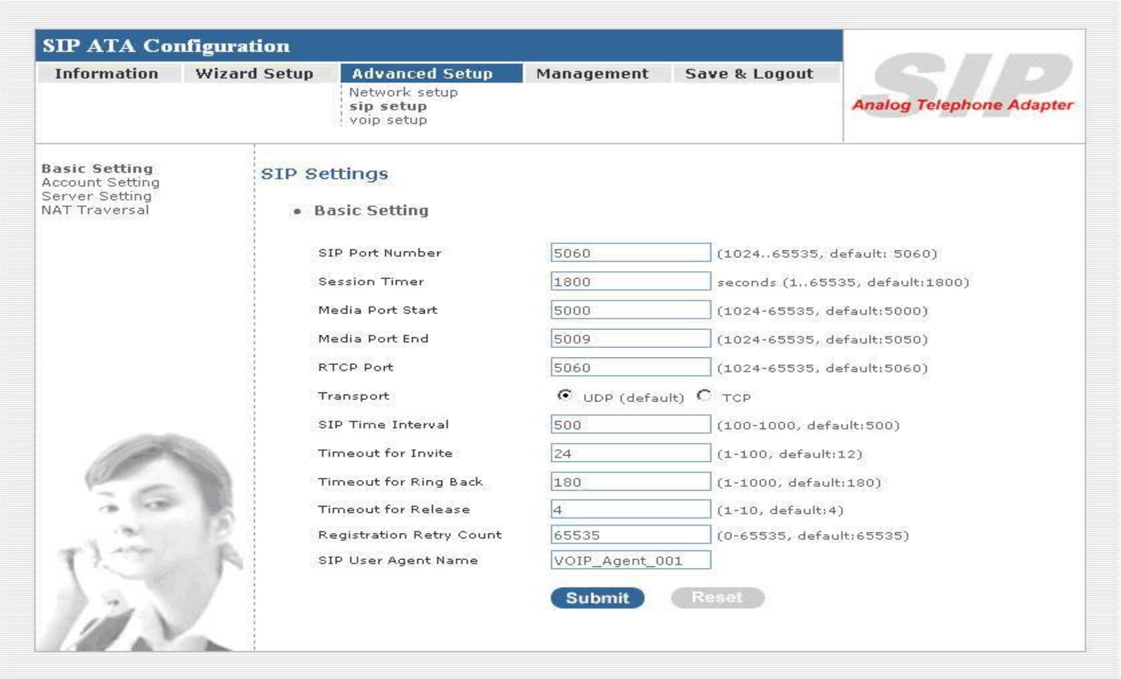
QOS	☑ Enable
Voice VLAN Priority	1
Voice VLAN ID	3
Data VLAN Priority	0
Data VLAN ID	4

□Enable - Enable/Disable the QOS service, default setting is Disable .
□Voice VLAN Priority – Set voice VLAN Priority 0 -7 ,Default is 1.
□Voice VLAN ID - Voice Vlan ID is entered as an integer , Default is 3 ,value between 0 and 4095 .
□Data VLAN Priority - Set Data VLAN Priority 0 -7 ,Default is 0.
□Data VLAN ID - Data VLAN ID is entered as an integer , Default is 4 ,value between 0 and 4095 .

4. SIP Setting

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.

- Basic Setting
- Account Setting
- Server Setting
- NAT Traversal

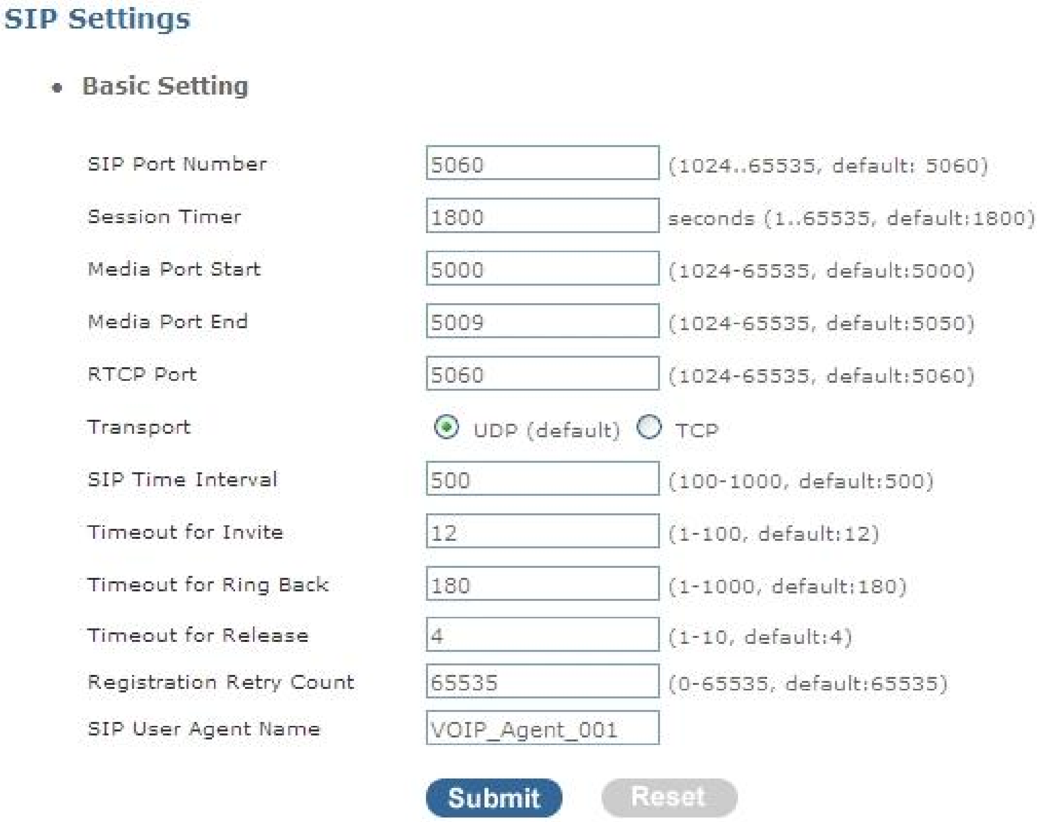


SIP Settings

- Basic Setting

SIP Port Number	5060	(1024..65535, default: 5060)
Session Timer	1800	seconds (1..65535, default:1800)
Media Port Start	5000	(1024-65535, default:5000)
Media Port End	5009	(1024-65535, default:5050)
RTCP Port	5060	(1024-65535, default:5060)
Transport	● UDP (default) ○ TCP	
SIP Time Interval	500	(100-1000, default:500)
Timeout for Invite	24	(1-100, default:12)
Timeout for Ring Back	180	(1-1000, default:180)
Timeout for Release	4	(1-10, default:4)
Registration Retry Count	65535	(0-65535, default:65535)
SIP User Agent Name	VOIP_Agent_001	

4.1 Basic Setting



SIP Settings

- Basic Setting

SIP Port Number	5060	(1024..65535, default: 5060)
Session Timer	1800	seconds (1..65535, default:1800)
Media Port Start	5000	(1024-65535, default:5000)
Media Port End	5009	(1024-65535, default:5050)
RTCP Port	5060	(1024-65535, default:5060)
Transport	● UDP (default) ○ TCP	
SIP Time Interval	500	(100-1000, default:500)
Timeout for Invite	12	(1-100, default:12)
Timeout for Ring Back	180	(1-1000, default:180)
Timeout for Release	4	(1-10, default:4)
Registration Retry Count	65535	(0-65535, default:65535)
SIP User Agent Name	VOIP_Agent_001	

□SIP Port Number - Assign the SIP port number of Telephone adapter. Its range is 1024 to 65535, default setting is 5060.

□Session Timer - SIP session refresh time interval. The time interval in which the phone periodically refresh SIP sessions by sending repeated INVITE or Update request, depending on session type. Its range is 1 to 65535, default setting is 1800 seconds.

□Media Port Start - The starting range of port for RTP. Port number for initial of sending RTP packet. Its range is 1024 to 65535, default setting is 5000.

□Media Port End - The ending range of port for RTP. Its range is 1024 to 65535, default setting is 5050.

□RTCP Port - The Real Time Transport Control Protocol (RTP control protocol or RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. The underlying protocol must provide multiplexing of the data and control packets, for example using separate port numbers with UDP. Assign the RTCP port number of Telephone adapter. Its range is 1024 to 65535, default setting is 5060.

□Transport - Assigns the default SIP transport protocol.

UDP - UDP (User Datagram Protocol) provides very few error recovery services, offering instead a direct way to send and receive datagram over an IP network. It's used primarily for broadcasting messages over a network. Here the UDP is a default setting.

TCP - TCP (Transmission Control Protocol) guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

□SIP Time Interval - SIP time interval in milliseconds. The default setting is 500 m-sec.

□Timeout for Invite - INVITE message timeout value. Assigns a value 1 to 100, default setting is 12 seconds. It denotes if an INVITE request was sent, and a response is not received from the remote site within the allotted time (the value of Invite Timeout). The present request will be dropped and a new connection request will be initiated.

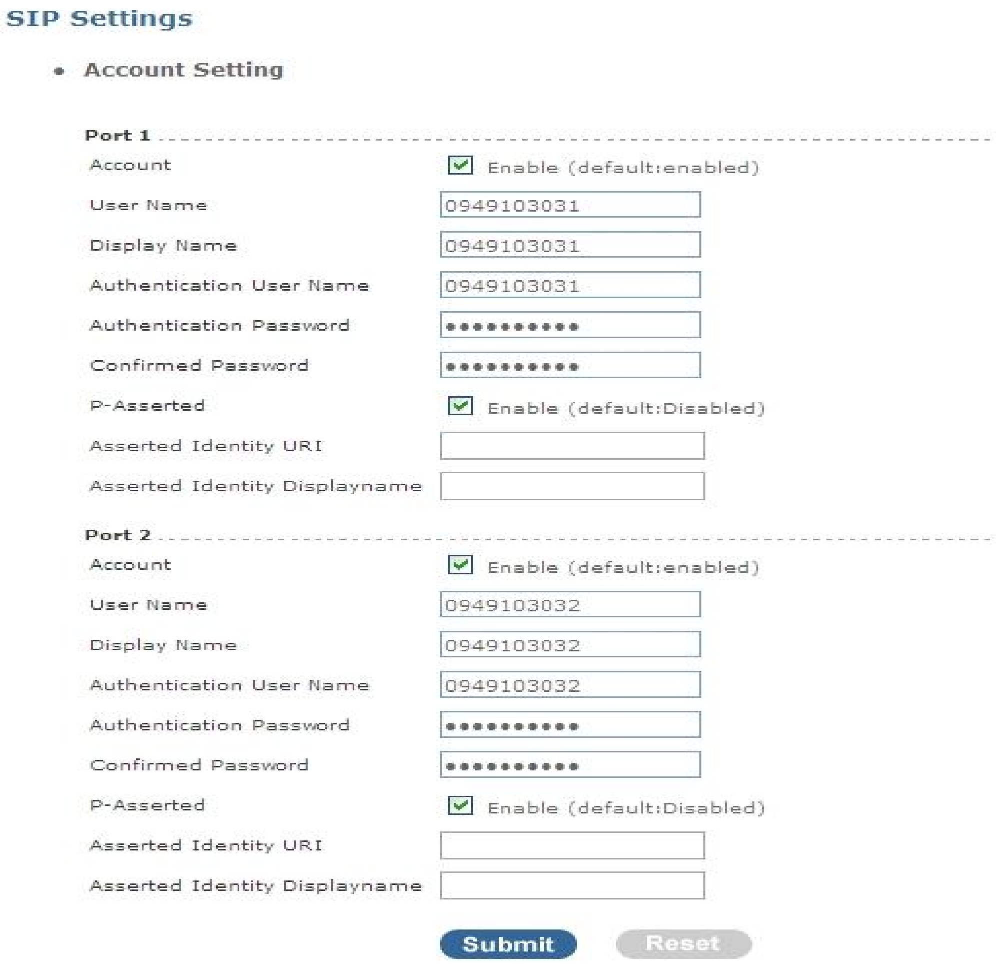
□Timeout for Ring Back - Timeout value for dropping a call after receiving 180 responses. Ring back is an intermittent audio tone that a caller in a telephone system hears after dialing a number, when the distant end of the circuit is receiving a ringing signal. It can be generated by the servicing switch of either the called party or the calling party. It is not generated by the called instrument. The default setting is 180 seconds.

□Timeout for Release - BYE message timeout value. Assigns a time interval 1 to 4, default setting is 4 seconds.

□Registration Retry count - Assigns a value 1 to 65535 ,To set the retry count for keepalive retransmission, use the retry keepalive command in SIP user agent configuration mode. To restore the retry count to the default value for keepalive retransmission, use the no form of this command.

□SIP User Agent name - if specfied, is the user-agent name to be used in a REGISTER request. If not specified, the value in”SIP User Agent Name” will be used for REGISTER request also. Default value is VOIP_Agent_001.

4.2 Account Setting



SIP Settings

- Account Setting

Port 1

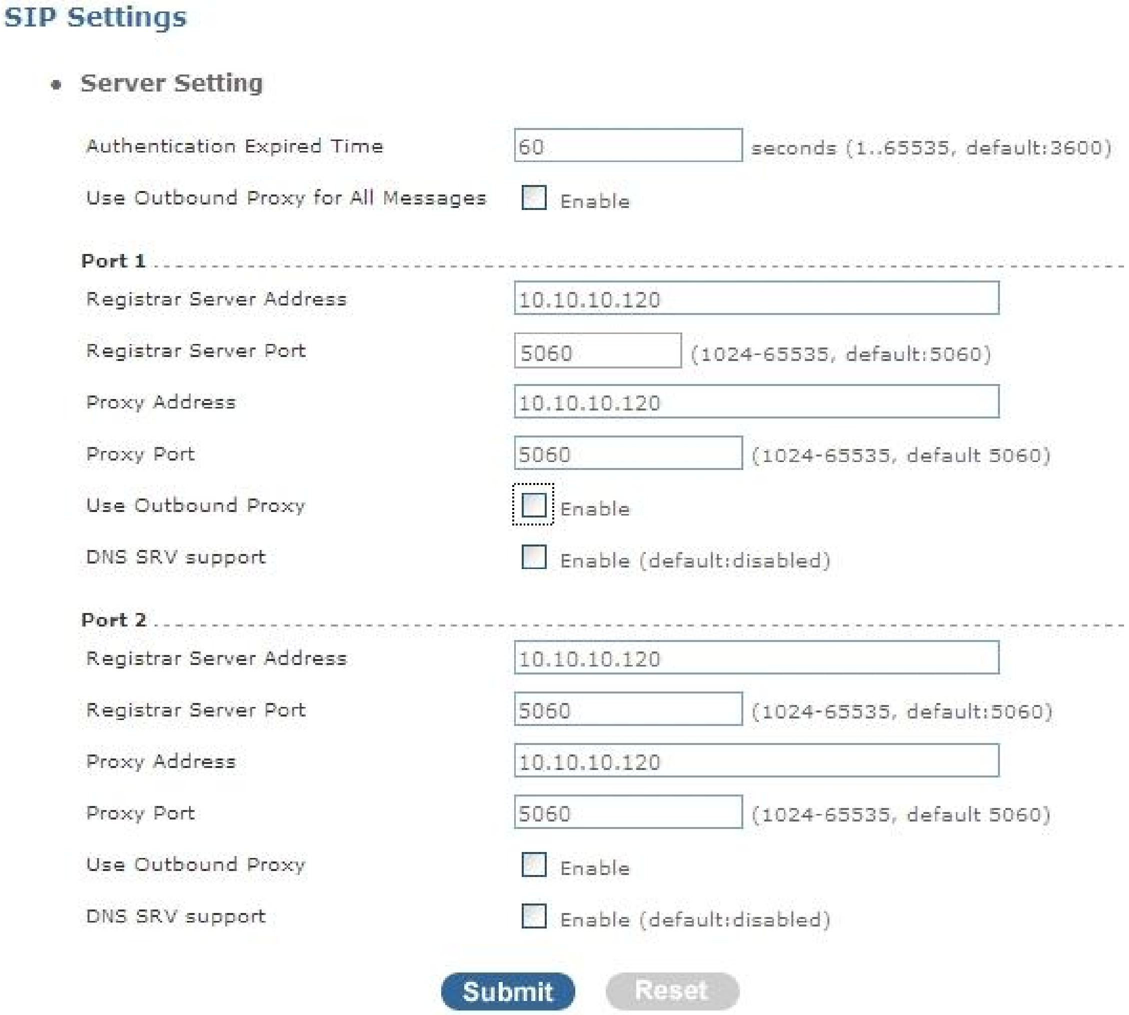
Account	☑ Enable (default:enabled)
User Name	0949103031
Display Name	0949103031
Authentication User Name	0949103031
Authentication Password	••••••••••
Confirmed Password	••••••••••
P-Asserted	☑ Enable (default:Disabled)
Asserted Identity URI	
Asserted Identity Displayname	

Port 2

Account	☑ Enable (default:enabled)
User Name	0949103032
Display Name	0949103032
Authentication User Name	0949103032
Authentication Password	••••••••••
Confirmed Password	••••••••••
P-Asserted	☑ Enable (default:Disabled)
Asserted Identity URI	
Asserted Identity Displayname	

There are two ports can be setup for SIP account.
□Phone Number - Assigns Phone number for the first port, maximum 15 digits. Do not contain any special characters or spaces. E.g. if you want to enter the number +886 2 2788-8118, then it should be 886227888118.
□Display Name - This text message will be sent between the callee and caller and will show on LCD panel for general using.
□Authentication User Name - User name for authentication. Maximum 36 characters.
□Authentication Password - User password for authentication. Maximum 24 characters.
Confirmed Password - Enter the password again, this is used to confirm user password for authentication. Maximum 24 characters.
□P-Asserted - Enable/Disable . Support for the Remote-Party-ID header and P-Asserted-Identity header—The present SIP implementation always derives the calling party number from the user name field of From header. But if P-Asserted-Identity header or Remote-Party-ID header is present in an incoming SIP INVITE message the user name should be derived from those headers.
□Asserted Identity URI – Enter your URI (Uniform Resource Identifier), Maximum 24 characters.
□Asserted Identity Displayname - Enter your Display name, Maximum 24 characters.

4.3 Server Setting



SIP Settings

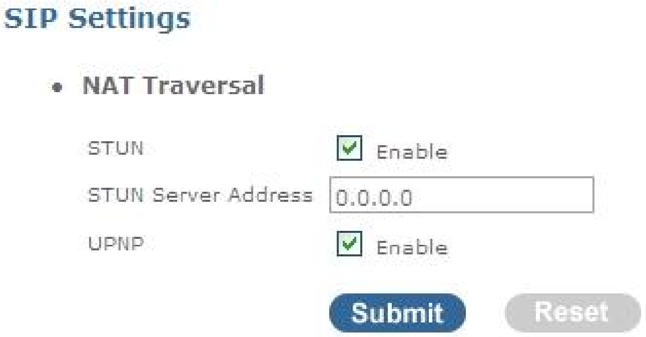
- Server Setting

Authentication Expired Time	60	seconds (1..65535, default:3600)
Use Outbound Proxy for All Messages	□ Enable	
Port 1		
Registrar Server Address	10.10.10.120	
Registrar Server Port	5060	(1024-65535, default:5060)
Proxy Address	10.10.10.120	
Proxy Port	5060	(1024-65535, default 5060)
Use Outbound Proxy	□ Enable	
DNS SRV support	□ Enable (default:disabled)	
Port 2		
Registrar Server Address	10.10.10.120	
Registrar Server Port	5060	(1024-65535, default:5060)
Proxy Address	10.10.10.120	
Proxy Port	5060	(1024-65535, default 5060)
Use Outbound Proxy	□ Enable	
DNS SRV support	□ Enable (default:disabled)	

□Authentication Expired Time - SIP registration expired time. Assigns the time interval from 1 - 65535, default setting is 3600 seconds.
□Use Outbound Proxy for All Messages - Enable/Disable this flag for out-bound (out-session and in-session) requests. Default setting is Disable.
□Registrar Server Address - Assigns the SIP Register Server's IP address.
□Registrar Server Port - Port number of SIP Register Server. Assigns a value from 1024 to 65535, default setting is 5060.
□Use Outbound Proxy for Session - Enable/Disable this flag for proxy-outbound, default setting is Disable.
□Outbound Proxy Address - Outbound Proxy server's IP address. Assigns the server's IP which is in charge of call-out service.
□Outbound Proxy Port - Port number of Outbound Proxy Server. Assigns a number from 1024 to 65535, default setting is 5060.
□DNS SRV support – Enable/Disable DNS SRV support function,You'll need DNS server if you want to use email server. To use it you should check Direct delivery on the addresses tab. DNS server is used to give a route to recipients' mailbox. You can use any DNS you know. But the best choice for the fastest sending is to use your ISP's DNS.

4.4 NAT 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.



SIP Settings

- NAT Traversal

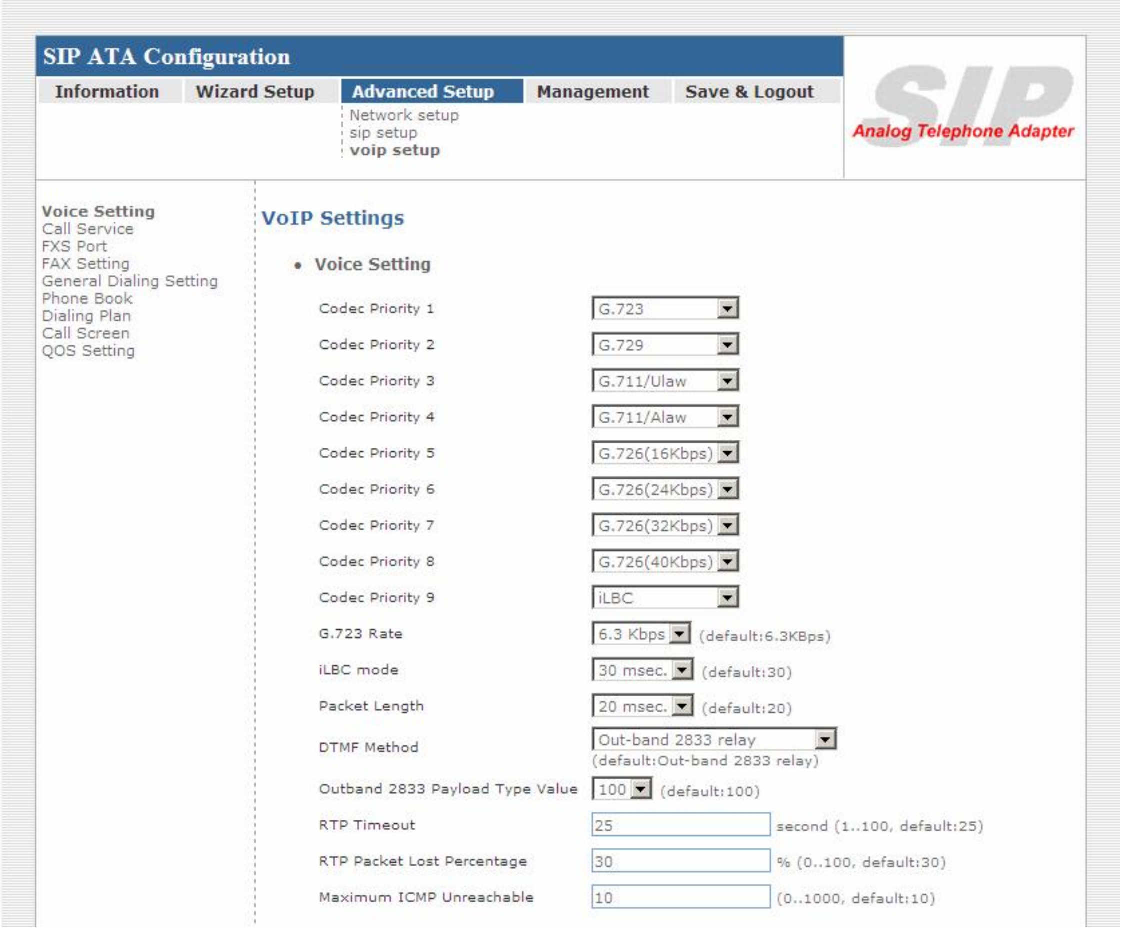
STUN ☑ Enable
STUN Server Address 0.0.0.0
UPNP ☑ Enable

□UPNP – Enable/Disable Universal Plug and Play , default setting is Disable.

5. VoIP Setting

- Voice Setting
- Call Service
- FXS Port
- FAX Setting
- General Dialing Setting
- URI Phone Book
- Call Screen
- QOS Setting

5.1 Voice Setting



SIP ATA Configuration

Information | Wizard Setup | Advanced Setup | Management | Save & Logout

Network setup
sip setup
voip setup

Voice Setting
Call Service
FXS Port
FAX Setting
General Dialing Setting
Phone Book
Dialing Plan
Call Screen
QOS Setting

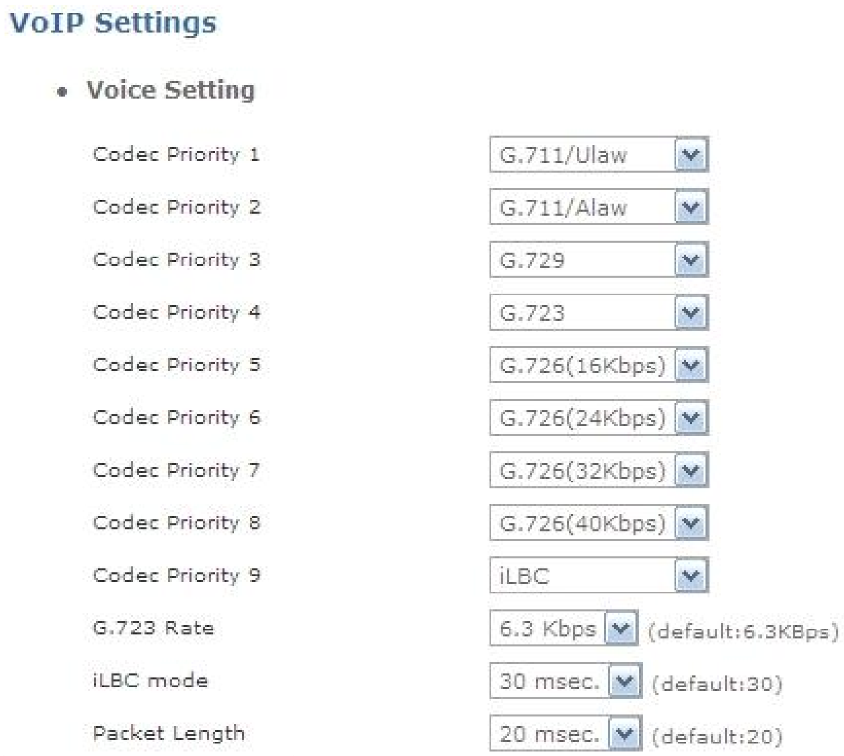
VoIP Settings

- Voice Setting

Codec Priority 1	G.723	
Codec Priority 2	G.729	
Codec Priority 3	G.711/Ulaw	
Codec Priority 4	G.711/Alaw	
Codec Priority 5	G.726(16Kbps)	
Codec Priority 6	G.726(24Kbps)	
Codec Priority 7	G.726(32Kbps)	
Codec Priority 8	G.726(40Kbps)	
Codec Priority 9	iLBC	
G.723 Rate	6.3 Kbps	(default:6.3KBps)
iLBC mode	30 msec.	(default:30)
Packet Length	20 msec.	(default:20)
DTMF Method	Out-band 2833 relay	(default:Out-band 2833 relay)
Outband 2833 Payload Type Value	100	(default:100)
RTP Timeout	25	second (1..100, default:25)
RTP Packet Lost Percentage	30	% (0..100, default:30)
Maximum ICMP Unreachable	10	(0..1000, default:10)

Codec

A CODEC (COmpressor/DECompressor) 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, G.726(16K bps), G.726(24K bps), G.726(32K bps), G.726(40K bps), and iLBC.



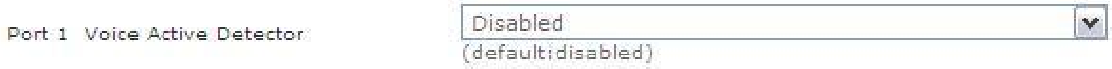
VoIP Settings

- Voice Setting

Codec Priority 1	G.711/Ulaw	
Codec Priority 2	G.711/Alaw	
Codec Priority 3	G.729	
Codec Priority 4	G.723	
Codec Priority 5	G.726(16Kbps)	
Codec Priority 6	G.726(24Kbps)	
Codec Priority 7	G.726(32Kbps)	
Codec Priority 8	G.726(40Kbps)	
Codec Priority 9	iLBC	
G.723 Rate	6.3 Kbps	(default:6.3KBps)
iLBC mode	30 msec.	(default:30)
Packet Length	20 msec.	(default:20)

□Codec Priority 1~9 - The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 9 kinds of codec. To determine the priority, selects one codec algorithm from the pull-down menus individually.
□G.723 Rate –This defines the encoding rate for G723 Codec(6.3Kbps/5.3Kbps), default is 6.3Kbps Rate.
□ILBC Mode - RTP Payload length. Select a length from the pull-down menu, default setting is 30 m-sec.
□Packet Length - RTP payload length. Selects a length from the pull-down menu, default setting is 20 m-sec.

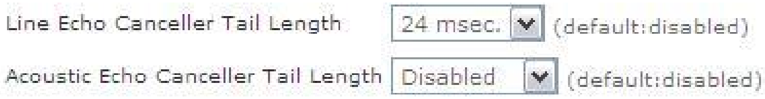
Voice Active Detector



Port 1 Voice Active Detector	Disabled (default:disabled)

□Voice Active Detector - It is used in speech encoding software to determine if the voice being encoded is human speech or background noise. There are three type of silence suppression: NO CNG, Only G.711 Annex II type, and Codec Specific CN.

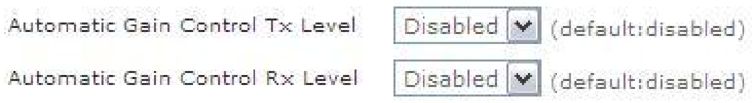
Echo Canceller



Line Echo Canceller Tail Length	24 msec.	(default:disabled)
Acoustic Echo Canceller Tail Length	Disabled	(default:disabled)

The echo canceller literally removes your voice from the returning audio stream without removing the audio coming from your caller.
□Line Echo Canceller Tail Length - Tail length for line echo cancellation. Default setting is in Disable mode.
□Acoustic Echo Canceller Tail Length - Tail length for acoustic echo cancellation. Default setting is in Disable mode.

Gain Control Level



Automatic Gain Control Tx Level Disabled (default:disabled)

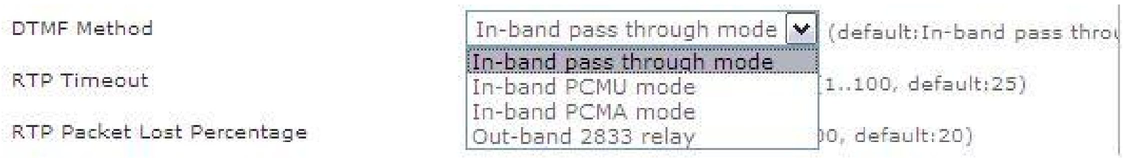
Automatic Gain Control Rx Level Disabled (default:disabled)

You can adjust the FXO Tx/Rx Gain Control level, range from 0db to 30db. The “gain” means increase in the power of electrical signal, measures by decibel.

□Automatic Gain Control Tx Level - Automatic voice gain control for transmitting. Default setting is in Disable mode.

□Automatic Gain Control Rx Level - Automatic voice gain control for receiving. Default setting is in Disable mode.

DTMF Method



DTMF Method In-band pass through mode (default:In-band pass thro

RTP Timeout (1..100, default:25)

RTP Packet Lost Percentage 00, default:20)

After the VoIP call is connected, when you dial a digit, this digit is sent to the other side by DTMF tone. There are two methods of sending the DTMF tone, In-band and Out-band. Choose “I n-band” will send the DTMF tone in voice packet. Choose “Out-band” will send the DTMF tone as a RTP payload signal. Sending DTMF tone as a signal could tolerate more packet loss caused by the network. If this selection is enabled, the DTMF tone will be sent as a signal.

□DTMF Method - Select the DTMF relay method, default setting is In-band pass through mode.

◎In-band - For voice data. The In-band signaling is the sending of metadata and control information in the same channel used for data. There are three type of mode can be selected: In-band pass through mode, In-band PCMU mode, and In-band PCMA mode.

◎ Out-band - For RFC-2833, that is, sending the DTMF tone as a RTP payload signal. The Out-of-band signaling has the following meanings:

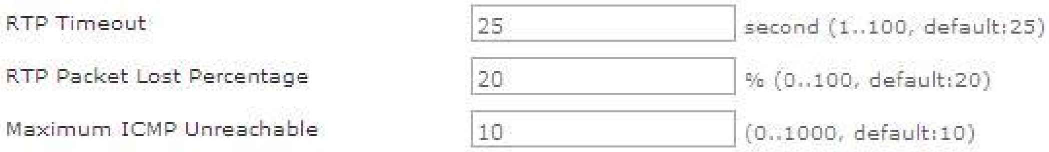
1. Signaling that uses a portion of the channel bandwidth provided by the transmission medium, e.g., the carrier channel, which portion is above the highest frequency used by, and is denied to, the speech or intelligence path by filters.

Note: Out-of-band signaling results in a lowered high-frequency cutoff of the effective available bandwidth.

2. Signaling via a different channel (either FDM or TDM) from that used for the primary information transfer.

RTP

RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.



RTP Timeout 25 second (1..100, default:25)

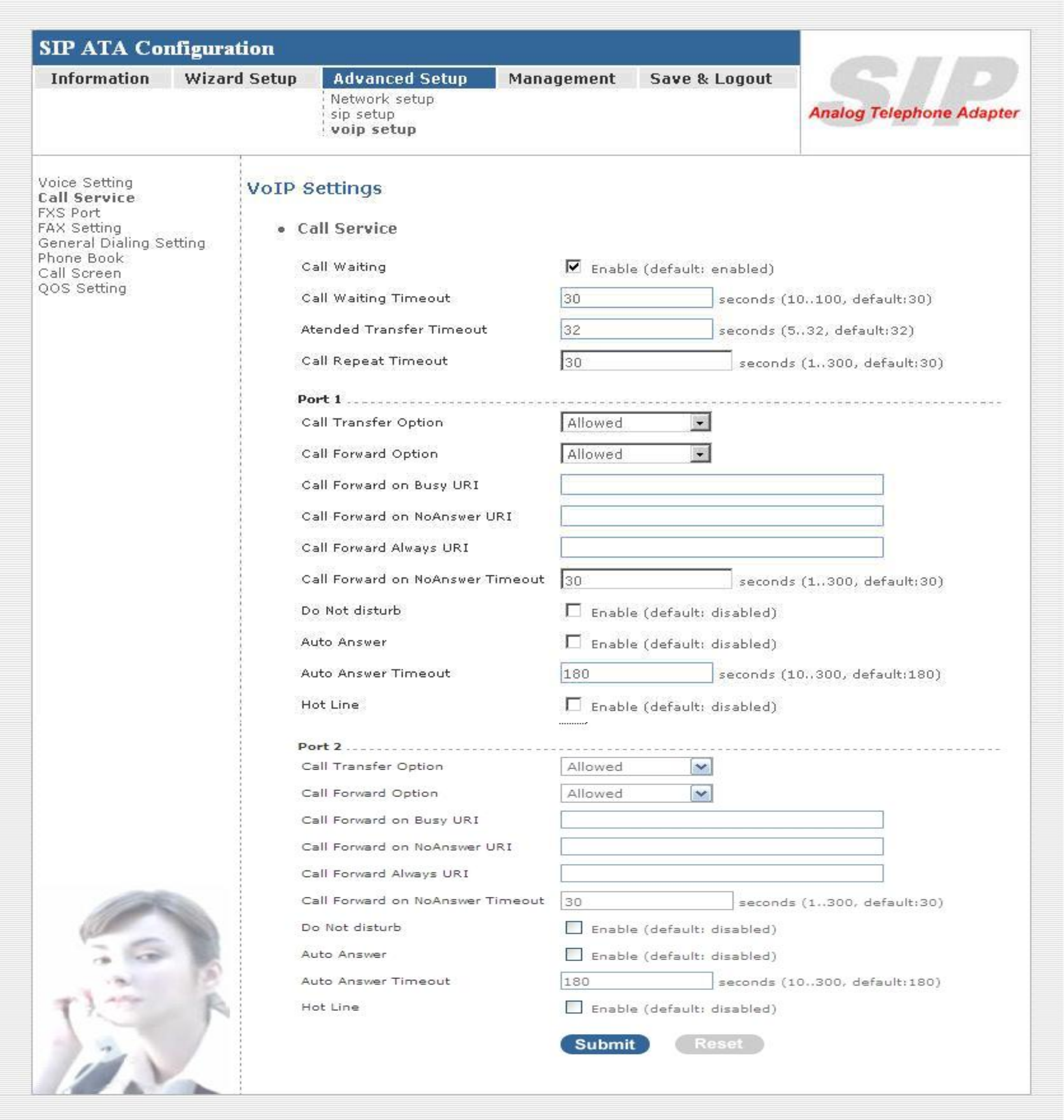
RTP Packet Lost Percentage 20 % (0..100, default:20)

Maximum ICMP Unreachable 10 (0..1000, default:10)

□RTP Timeout - Disconnect a call after not receiving RTP packet for this time value. Assigns the

time value from 1 to 100, default setting is 25 seconds.
□RTF Packet Lost Percentage - Allowable the maximum percentage of RTP packet loss. Assigns the percentage from 0 to 100, default setting is 20%
□Maximum ICMP Unreachable - Allowable the maximum number of consecutive ICMP destination unreachable responses. ICMP differs in purpose from TCP and UDP in that it is usually not used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host. Assigns a number from 10 to 100, default setting is 10.

5.2 Call Service



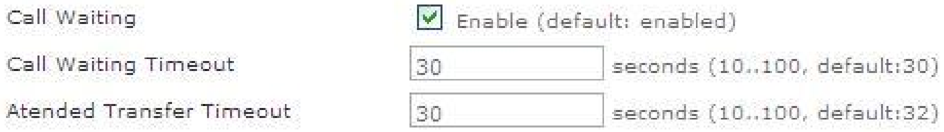
VoIP Settings

- Call Service

Call Waiting	☑ Enable (default: enabled)
Call Waiting Timeout	30 seconds (10..100, default:30)
Atended Transfer Timeout	32 seconds (5..32, default:32)
Call Repeat Timeout	30 seconds (1..300, default:30)
Port 1	
Call Transfer Option	Allowed
Call Forward Option	Allowed
Call Forward on Busy URI	
Call Forward on NoAnswer URI	
Call Forward Always URI	
Call Forward on NoAnswer Timeout	30 seconds (1..300, default:30)
Do Not disturb	□ Enable (default: disabled)
Auto Answer	□ Enable (default: disabled)
Auto Answer Timeout	180 seconds (10..300, default:180)
Hot Line	□ Enable (default: disabled)
Port 2	
Call Transfer Option	Allowed
Call Forward Option	Allowed
Call Forward on Busy URI	
Call Forward on NoAnswer URI	
Call Forward Always URI	
Call Forward on NoAnswer Timeout	30 seconds (1..300, default:30)
Do Not disturb	□ Enable (default: disabled)
Auto Answer	□ Enable (default: disabled)
Auto Answer Timeout	180 seconds (10..300, default:180)
Hot Line	□ Enable (default: disabled)

Call Waiting

It is a feature on telephone network. If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the called party is able to suspend the current telephone call and switch to the new incoming call, and can then negotiate with the new or the current caller an appropriate time to ring back if the message is important, or to quickly handle a separate incoming call.



Call Waiting	☑ Enable (default: enabled)
Call Waiting Timeout	30 seconds (10..100, default:30)
Atended Transfer Timeout	30 seconds (10..100, default:32)

□Call Waiting - The default setting is Enable mode.
□Call Waiting Timeout - Assigns the time interval from 10 to 100. Default setting is 30 seconds.
□Attended Transfer Timeout - Assigns the time interval from 10 to 100. Default setting is 30 seconds.

Call Transfer Option

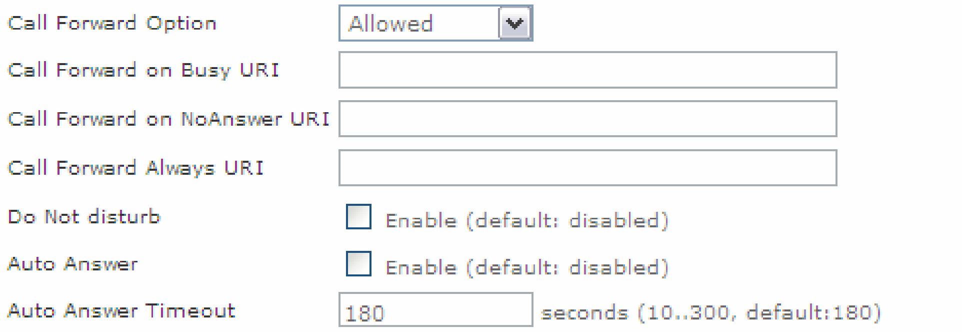
The Call Transfer Option feature which can enables a user to relocate an existing call to another telephone or attendants console by using the transfer button then dialing the required location. The transferred call is either announced or unannounced.

Call Transfer Option: Allowed

□Call Transfer Option - Indicates whether the remote end is allowed to transfer the call to a third party. There are three type, Restricted, Allowed, and User Invocation Required. The default setting is in Allowed mode.

Call Forward Option

The Call Forwarding Option is a feature on telephone network that allow an incoming call to a called party which would be otherwise unavailable to be redirected to a mobile telephone or other telephone number where the desired called party is situated.



Call Forward Option	Allowed
Call Forward on Busy URI	
Call Forward on NoAnswer URI	
Call Forward Always URI	
Do Not disturb	□ Enable (default: disabled)
Auto Answer	□ Enable (default: disabled)
Auto Answer Timeout	180 seconds (10..300, default:180)

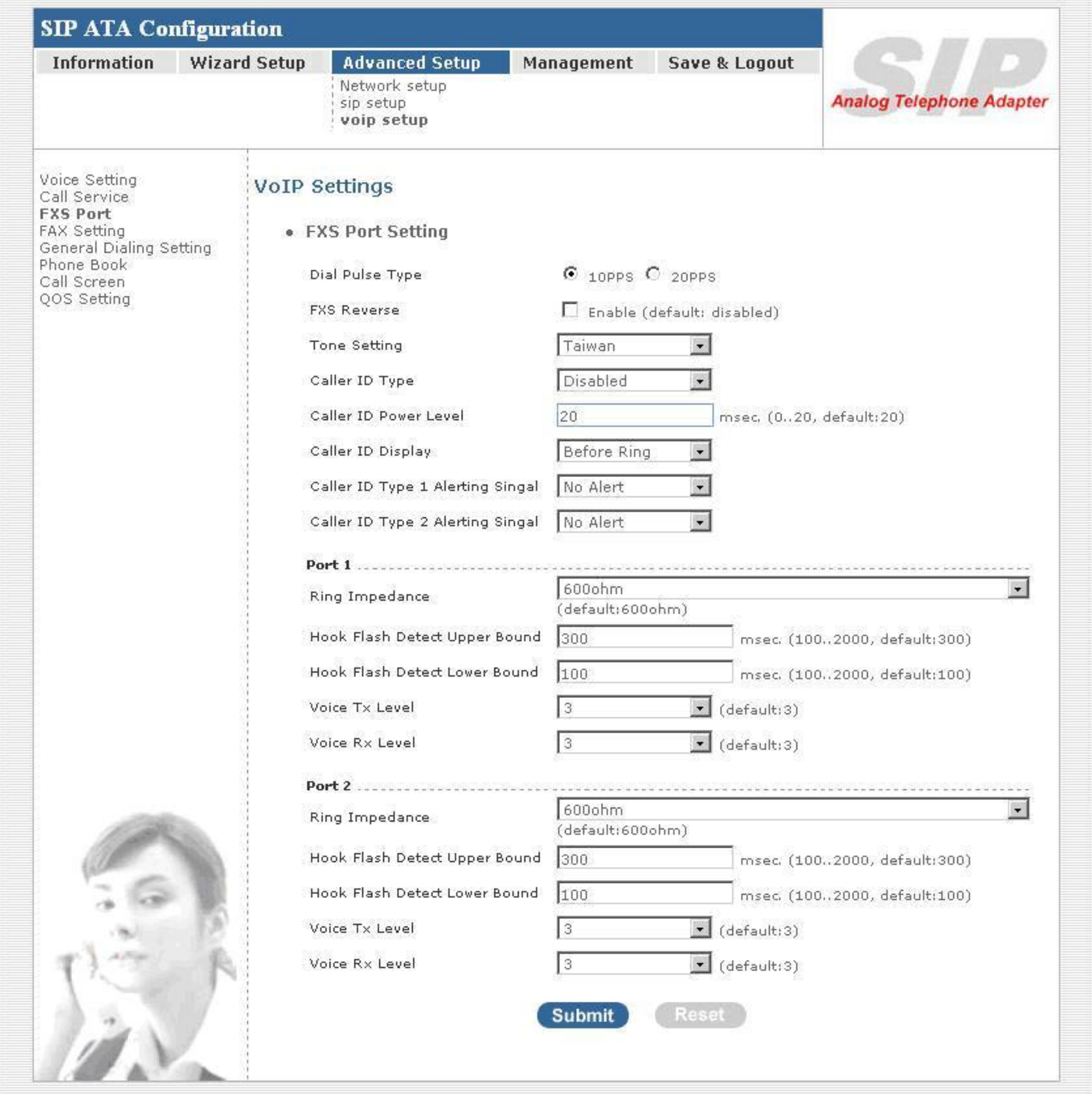
□Call Forward Option - Indicates whether the remote end is allowed to forward the call to a third party. There are three type, Restricted, Allowed, and User Invocation Required. The default setting is in Allowed mode.
□Call Forward on Busy URI - Assigns a phone number. When the port is busy, the incoming call will be redirected to the specified phone number.
□Call Forward on No Answer URI - Assigns a phone number. When the port is no answer, the incoming call will be redirected to the specified phone number.
□Call Forward Always URI - Assigns a phone number; if you want all incoming calls of the port always be redirected.
□Do Not disturb - Enable/Disable the do not disturb, default setting is disabled.
□Auto Answer - Enable/Disable the auto answer, default setting is disabled.
□Auto Answer Timeout - When the phone is ring a long time (180 seconds), the incoming call will timeout and redirected to the specified phone number which is fill in “Call Forward on No Answer URI”. Default setting is 180 seconds.

Hot Line □ Enable (default: disabled)

□Hot line - Enable/Disable , default setting is disable, This service allows you to make a call to a pre-programmed number by only lifting the handset.

5.3 FXS Port Setting

FXS (Foreign Exchange Station) is the interface on a VoIP device for connecting directly to telephones, fax MAChines, or similar device and supplies ring, voltage, and dial tone.



VoIP Settings

- FXS Port Setting

Dial Pulse Type	● 10PPS ○ 20PPS
FXS Reverse	□ Enable (default: disabled)
Tone Setting	Taiwan
Caller ID Type	Disabled
Caller ID Power Level	20 msec. (0..20, default:20)
Caller ID Display	Before Ring
Caller ID Type 1 Alerting Singal	No Alert
Caller ID Type 2 Alerting Singal	No Alert

Port 1

Ring Impedance	600ohm (default:600ohm)
Hook Flash Detect Upper Bound	300 msec. (100..2000, default:300)
Hook Flash Detect Lower Bound	100 msec. (100..2000, default:100)
Voice Tx Level	3 (default:3)
Voice Rx Level	3 (default:3)

Port 2

Ring Impedance	600ohm (default:600ohm)
Hook Flash Detect Upper Bound	300 msec. (100..2000, default:300)
Hook Flash Detect Lower Bound	100 msec. (100..2000, default:100)
Voice Tx Level	3 (default:3)
Voice Rx Level	3 (default:3)

□Dial Pulse Type - This field defines the number of pulse per second. There are 2 selections,

◎10 PPS - Represents as a series of audible clicks of 16.66 ms duration with silence duration of 33.33 ms.

◎20 PPS - Represents as a series of audible clicks of 33.33 ms duration with silence duration of 66.66 ms.

Note: These values apply to the Japanese Network for which the algorithm was developed.

These click sounds are digitized and subsequently analyzed to determine the digit that was dialed.

□FXS Reverse - A specific signal indicating the status of the conversation.

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

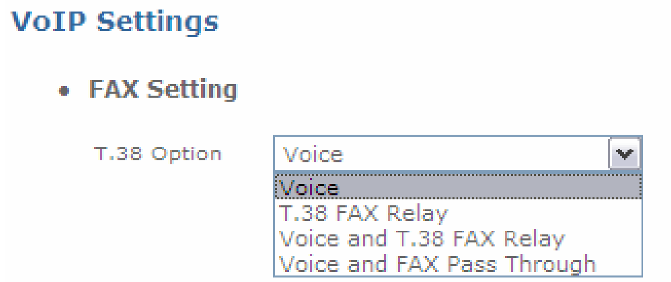
□Caller ID Type - The Caller ID normal display the number, system date, and time on system phone screen of the incoming call. The DTMF is the general type for using. Select a type from the pull-down menu. Default setting is Disabled.
□Caller ID Power Level - Assigns the Caller ID Power Lever from 0 to 100. Default setting is 20 m-secs.
□Caller ID Display - There are two types to display the caller information on the screen. Before Ring, the caller id information is displayed before first ring. After Ring, the caller id information is displayed between first ring and second ring. Default setting is Before Ring.
□Caller ID Type 1 Alerting Signal - Type 1 alerting signal is used to detect CID when □device is ON-HOOK. Default setting is No Alert.
□Caller ID Type 2 Alerting Signal - Type 2 alerting signal is used to detect CID when device is OFF-HOOK. Default setting is No Alert.
□Hook Flash Detect - Hook-flash indicates the condition when a request for voice conference and is recognized as a quick off-hook/on-hook/off-hook cycle. Assign a time interval for Hook-flash detection from 100 to 2000; default setting is 300 m-secs.
□Voice Tx Level - Sets a specific sound intensity for transmitting sound. Select a level from 1 to 8, default setting is 6. Table1 lists the receive/transmit voice gain value for reference. The "gain" means increase in the power of electrical signal, measures by decibel.
□Voice Rx Level - Sets a specific sound intensity for receiving sound. Select a level from 1 to 8, default setting is 6. Table 1 lists the receive/transmit voice gain value for reference. The "gain" means increase in the power of electrical signal, measures by decibel.

Table 1 Receive/Transmit Voice Gain Value

Level	Decibel
1	-24db
2	-18db
3	-12db
4	-6db
5	-2.5db
6	0db(default setting)
7	3.5db
8	6db

5.4 FAX Setting

The T.38 FAX procedure is used for the changeover from VoIP to fax mode during a call. The SIP will establish a normal VoIP call using INVITEs with SDP field to support T.38 detail.

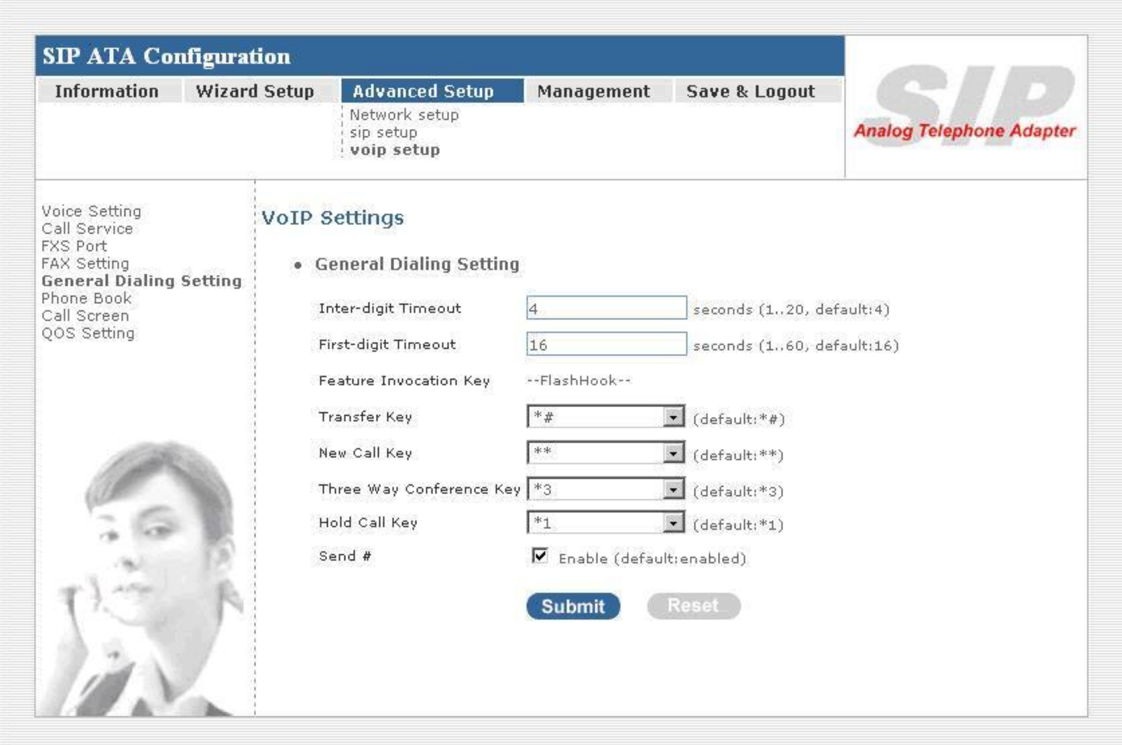

VoIP Settings

- FAX Setting

T.38 Option: Voice

□T.38 Option - Select an option from the pull-down menu. Default setting is Voice.

5.5 General Dialing Setting



VoIP Settings

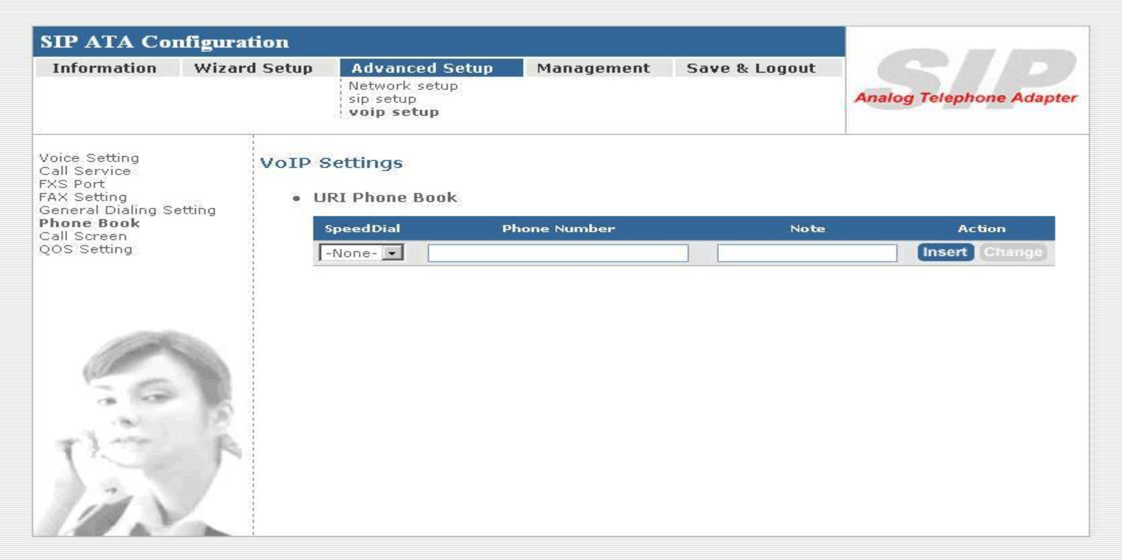
- General Dialing Setting

Inter-digit Timeout	4	seconds (1..20, default:4)
First-digit Timeout	16	seconds (1..60, default:16)
Feature Invocation Key	--FlashHook--	
Transfer Key	*#	(default:*#)
New Call Key	**	(default:**)
Three Way Conference Key	*3	(default:*3)
Hold Call Key	*1	(default:*1)
Send #	☑ Enable (default:enabled)	

□Inter-digit Timeout - If no other number is being dialed within this interval, the Telephony ATA will terminate this call. Assign the time interval from 1 to 20, default setting is 4 seconds.
□First-digit Timeout - If you pick up the phone without dialing any number within this period of time, the tone will be changed to busy tone. Assign the time interval from 1 to 60, default setting is 16 seconds.
□Feature Invocation Key - Key to invocate the other features. The setting is FlashHook key.
□Transfer Key - Keys to be pressed to initiate a call transfer. This is activated when
□HOLD/FLASH-HOOK is pressed on a call. The default setting is *#.
□New Call Key - Keys to be pressed to initiate a new call. The default setting is **.
□Three Way Conference Key - Keys to be pressed to initiate a 3-way conference call. The default setting is *3.
□Hold Call Key - Keys to be pressed will be holding a call. The default setting is *1.
□Send # - Enable/Disable , Default is Enable. speed dial ,after final dial don’t need wait inter-digit time.

5.6 Phone Book

URI (Uniform Resource Identifier) Phone Book lets you define a button or a set of buttons to link to a specific number defined in URI Phone Book.



SpeedDial	Phone Number	Note	Action
-None-			Insert Change

□SpeedDial - Select the speed dial shortcut to use from #1 to #9.
□Phone Number - Enter the international number to dial.
□Note – Phone munber note.

5.7 Dialing Plan (Outgoing Mode)

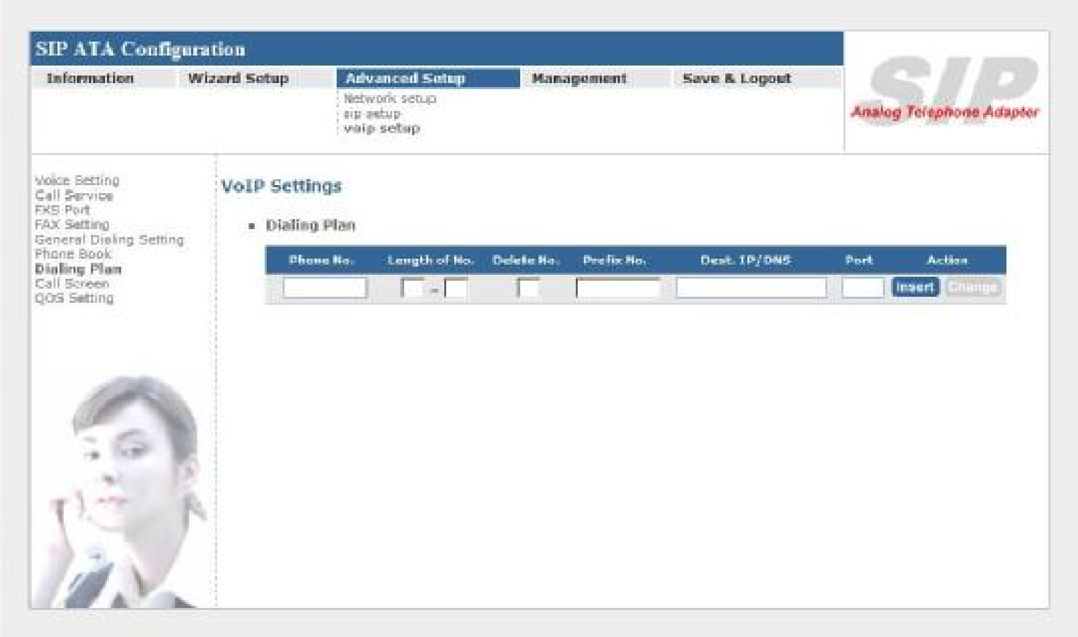
The “**Dialing plan**” need setting when the user use the method of Peer-to-Peer SIP VoIP call or SIP Proxy Server Mode. The SIP Dialing Plan has two kinds of directions: Outgoing (call out).

1. **Dial Plan (Outgoing):**

   Peer-to-Peer Call Mode: Effective

   Registering to SIP Proxy Server Mode: Effective

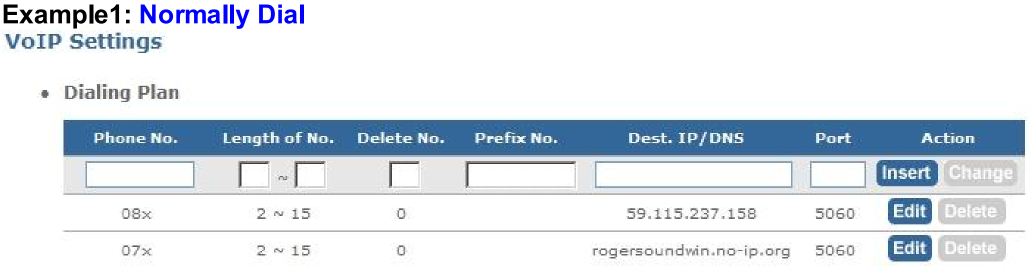
In the “Dial Plan Configurations (Outgoing)” settings: Maximum Entries : 30



Phone No.	Length of No.	Delete No.	Prefix No.	Dest. IP/DNS	Port	Action
	-					Insert Change

□“Outbound number” is the leading digits of the call out dialing number.
□“Length of Number” has two text fields need filled: “Min Length” and “Max Length” is the min/max allowed length you can dial.
□“Delete Length” is the number of digits that will be stripped from beginning of the dialed number.
□“Add Digit Number” is the digits that will be added to the beginning of the dialed number.
□“Destination IP Address / Domain Name” is the IP address / Domain Name of the destination ATA (Gateway) that owns this phone number.
□“Destination Port” is port of the destination ATA (Gateway) use.(Default is 5060)

Example1: Normally Dial



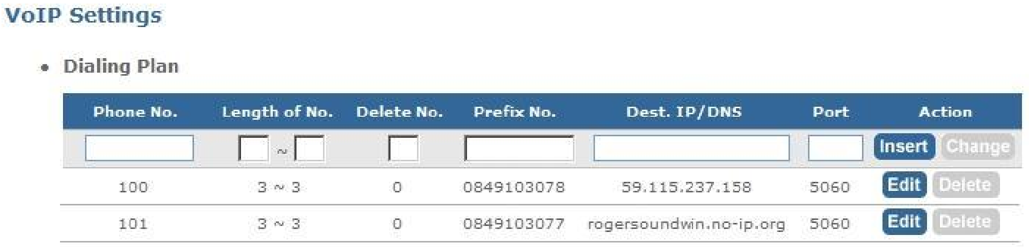
VoIP Settings

- Dialing Plan

Phone No.	Length of No.	Delete No.	Prefix No.	Dest. IP/DNS	Port	Action
	~					Insert Change
08x	2 ~ 15	0		59.115.237.158	5060	Edit Delete
07x	2 ~ 15	0		rogersoundwin.no-ip.org	5060	Edit Delete

1.08x leading call out, call to Destination IP address: 59.115.237.158
2.07x leading call out, call to Destination Domain Name: rogersoundwin.no-ip.org

Example2: Speed Dial



VoIP Settings

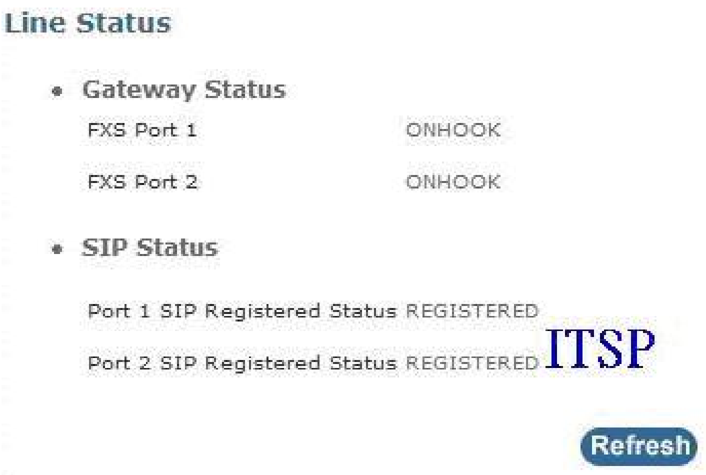
- Dialing Plan

Phone No.	Length of No.	Delete No.	Prefix No.	Dest. IP/DNS	Port	Action
	~					Insert Change
100	3 ~ 3	0	0849103078	59.115.237.158	5060	Edit Delete
101	3 ~ 3	0	0849103077	rogersoundwin.no-ip.org	5060	Edit Delete

1. If user dial “100”,
ATA automatically dial “0849103078” to Destination IP address 59.115.237.158
2. If user dial “101”,
ATA automatically dial “0849103077” to Destination IP address rogersoundwin.no-ip.org

Example3: Speed Dial Register server.

1. Registered ITSP SIP server (WWW.ITSP.COM)



Line Status

- Gateway Status

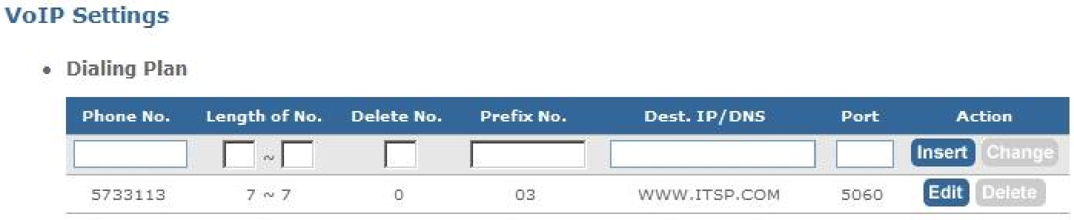
FXS Port 1 ONHOOK

FXS Port 2 ONHOOK

- SIP Status

Port 1 SIP Registered Status REGISTERED

Port 2 SIP Registered Status REGISTERED



VoIP Settings

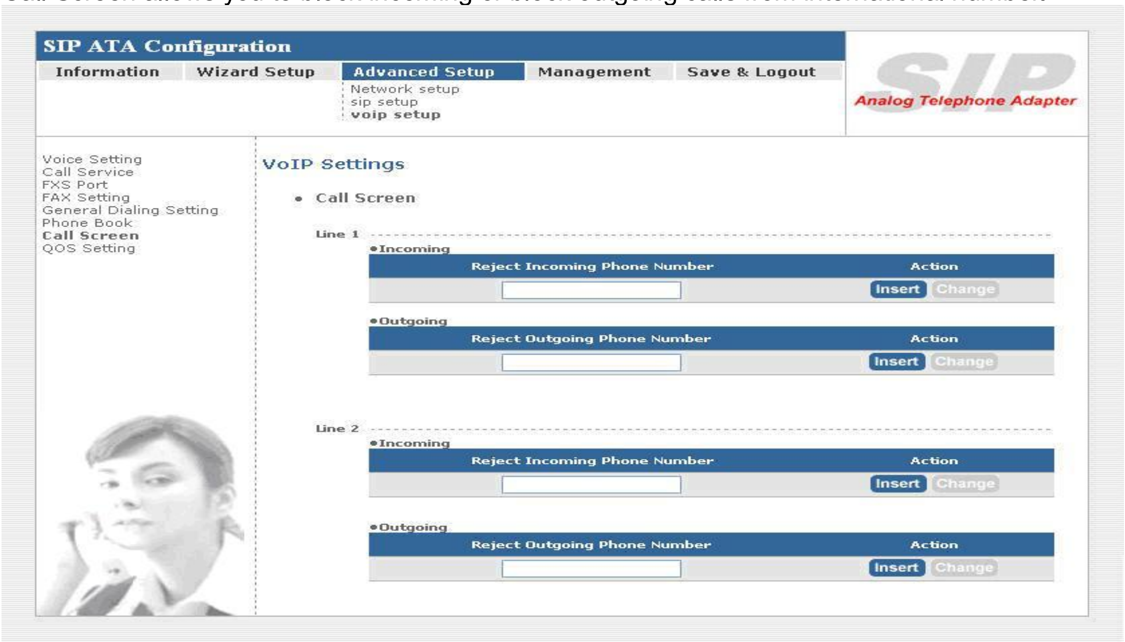
- Dialing Plan

Phone No.	Length of No.	Delete No.	Prefix No.	Dest. IP/DNS	Port	Action
	~					Insert Change
5733113	7 ~ 7	0	03	WWW.ITSP.COM	5060	Edit Delete

**1. If user dial “5733113”,
ATA automatically dial “035733113” to ITSP IP address WWW.ITSP.COM.**

5.8 Call Screen

Call Screen allows you to block incoming or block outgoing calls from international number.



VoIP Settings

- Call Screen

Line 1

●Incoming

Reject Incoming Phone Number	Action
	Insert Change

●Outgoing

Reject Outgoing Phone Number	Action
	Insert Change

Line 2

●Incoming

Reject Incoming Phone Number	Action
	Insert Change

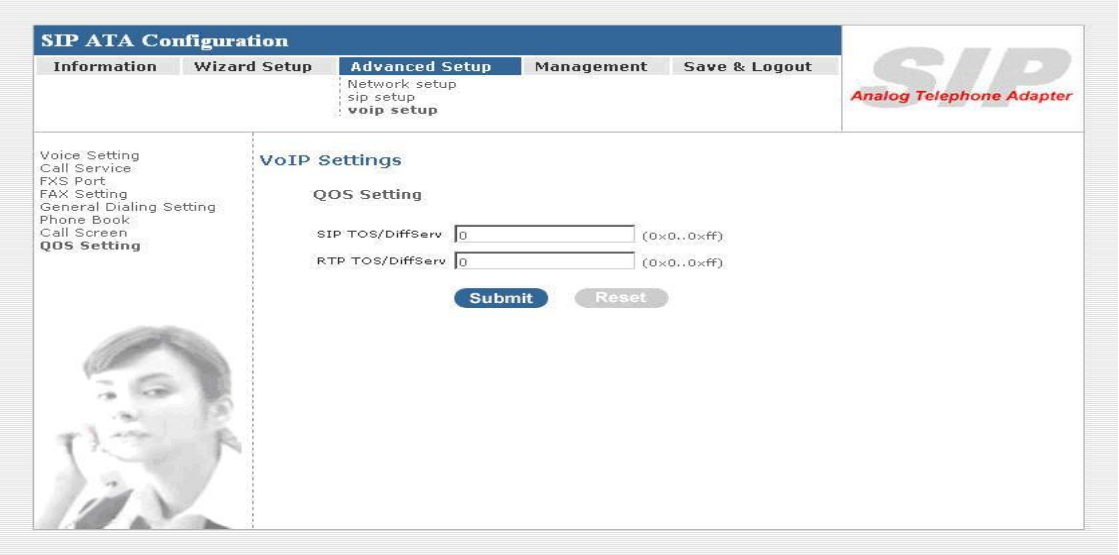
●Outgoing

Reject Outgoing Phone Number	Action
	Insert Change

□Reject Incoming Phone Number - . Create and maintain a list of numbers to be screened. Incoming calls from the "screened callers" list will be blocked.
□Reject Outgoing Phone Number - . Create and maintain a list of numbers to be screened. Reject Outgoing Phone number from local user dial number.

5.9 QOS Setting

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.



SIP TOS/DiffServ 0 (0x0..0xff)

RTP TOS/DiffServ 0 (0x0..0xff)

□SIP TOS/Diffserv – Set to value

□SIP TOS/Diffserv – Set to value

tos=0x10 low delay

tos=0x08 high throughput

tos=0x04 high reliability

tos=0x02 ECT bit set

tos=0x01 CE bit set

or set multiple bits, such as

```
tos=0x18
```

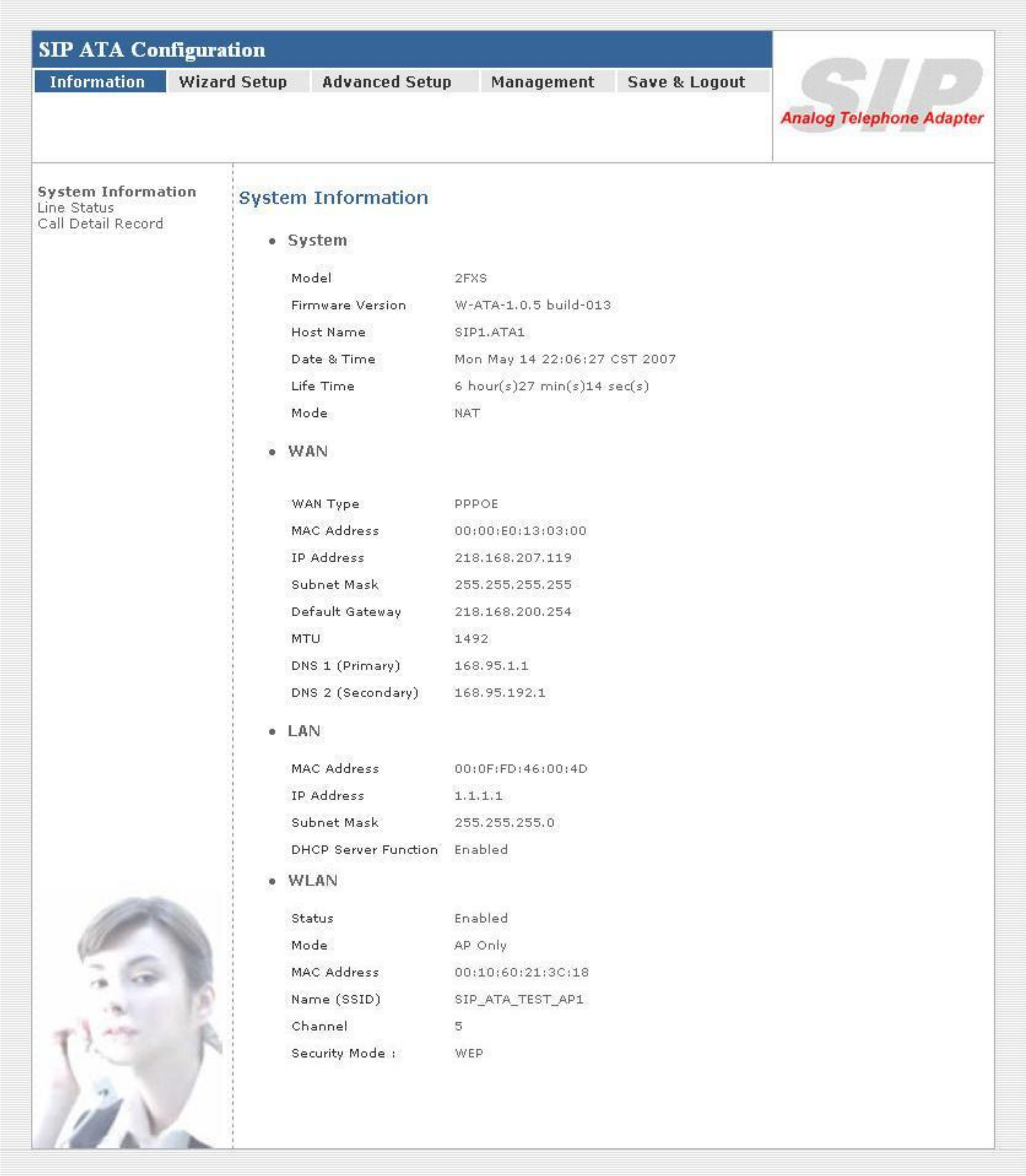
to set both low delay and high throughput.

6. Information

- System Information
- Line Status

6.1 System Information

Click System Information to display system status, WAN type, and LAN type. WLAN type.



System Information

- System

Model	2FXS
Firmware Version	W-ATA-1.0.5 build-013
Host Name	SIP1.ATA1
Date & Time	Mon May 14 22:06:27 CST 2007
Life Time	6 hour(s)27 min(s)14 sec(s)
Mode	NAT

- WAN

WAN Type	PPPOE
MAC Address	00:00:E0:13:03:00
IP Address	218.168.207.119
Subnet Mask	255.255.255.255
Default Gateway	218.168.200.254
MTU	1492
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

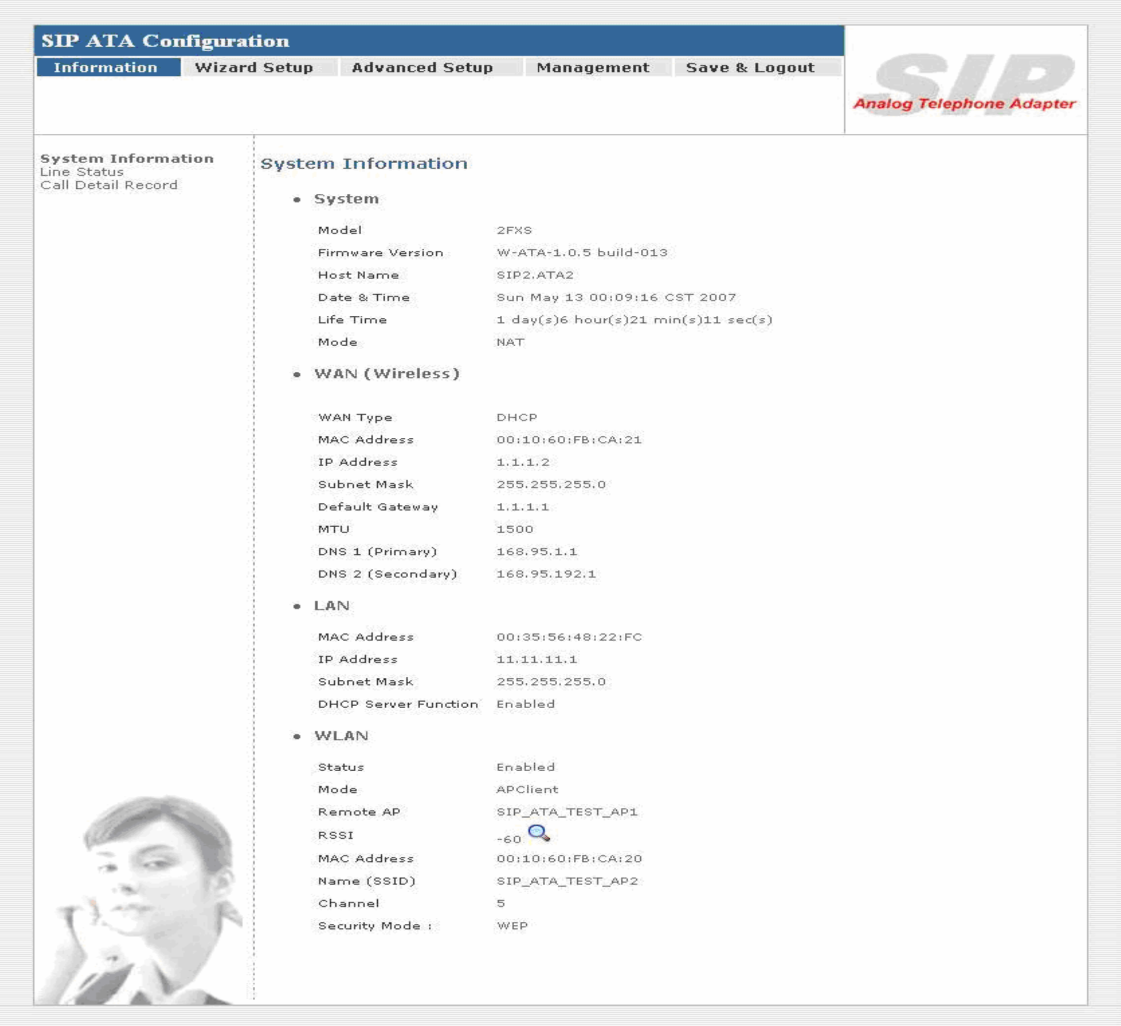
- LAN

MAC Address	00:0F:FD:46:00:4D
IP Address	1.1.1.1
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

- WLAN

Status	Enabled
Mode	AP Only
MAC Address	00:10:60:21:3C:18
Name (SSID)	SIP_ATA_TEST_AP1
Channel	5
Security Mode :	WEP

This system information page is “AP Mode”.



System Information

- System

Model	2FXS
Firmware Version	W-ATA-1.0.5 build-013
Host Name	SIP2.ATA2
Date & Time	Sun May 13 00:09:16 CST 2007
Life Time	1 day(s)6 hour(s)21 min(s)11 sec(s)
Mode	NAT

- WAN (Wireless)

WAN Type	DHCP
MAC Address	00:10:60:FB:CA:21
IP Address	1.1.1.2
Subnet Mask	255.255.255.0
Default Gateway	1.1.1.1
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

- LAN

MAC Address	00:35:56:48:22:FC
IP Address	11.11.11.1
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

- WLAN

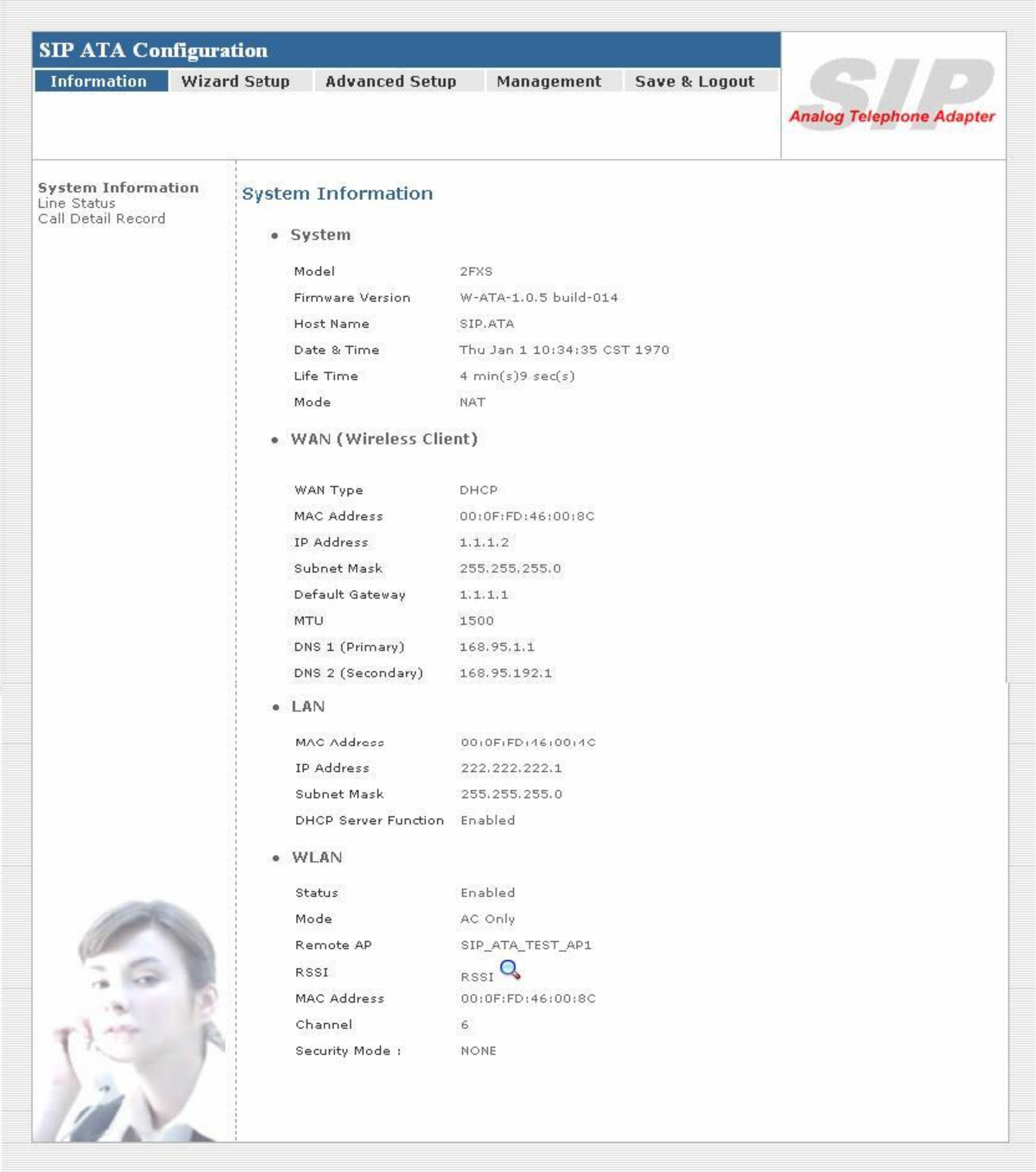
Status	Enabled
Mode	APClient
Remote AP	SIP_ATA_TEST_AP1
RSSI	-60
MAC Address	00:10:60:FB:CA:20
Name (SSID)	SIP_ATA_TEST_AP2
Channel	5
Security Mode :	WEP

This system information page is “AP & AC Client” Mode.

This page displays the current information for the device. It will display the LAN, WAN,WLAN (Status / Wireless Mode / Remote AP SSID / RSSI / MAC Address / Channel / Name (SSID) / Security Mode)and system firmware information. This page will display different information for you, according your WAN setting (Static IP, DHCP, or PPPoE).

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



System Information

- System

Model	2FXS
Firmware Version	W-ATA-1.0.5 build-014
Host Name	SIP.ATA
Date & Time	Thu Jan 1 10:34:35 CST 1970
Life Time	4 min(s)9 sec(s)
Mode	NAT

- WAN (Wireless Client)

WAN Type	DHCP
MAC Address	00:0F:FD:46:00:8C
IP Address	1.1.1.2
Subnet Mask	255.255.255.0
Default Gateway	1.1.1.1
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

- LAN

MAC Address	00:0F:FD:46:00:4C
IP Address	222.222.222.1
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

- WLAN

Status	Enabled
Mode	AC Only
Remote AP	SIP_ATA_TEST_AP1
RSSI	RSSI 🔍
MAC Address	00:0F:FD:46:00:8C
Channel	6
Security Mode :	NONE

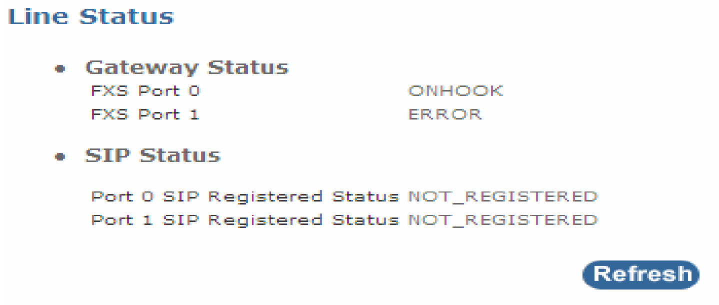
This system information page is “AC Client” Mode.

This page displays the current information for the device. It will display the LAN, WAN,WLAN (Status / Wireless Mode / Remote AP SSID / RSSI / MAC Address / Channel / Name (SSID) / Security Mode)and system firmware information. This page will display different information for you, according your WAN setting (Static IP, DHCP, or PPPoE).

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

6.2 Line Status


Line Status

- Gateway Status

FXS Port 0 ONHOOK
FXS Port 1 ERROR

- SIP Status

Port 0 SIP Registered Status NOT_REGISTERED
Port 1 SIP Registered Status NOT_REGISTERED

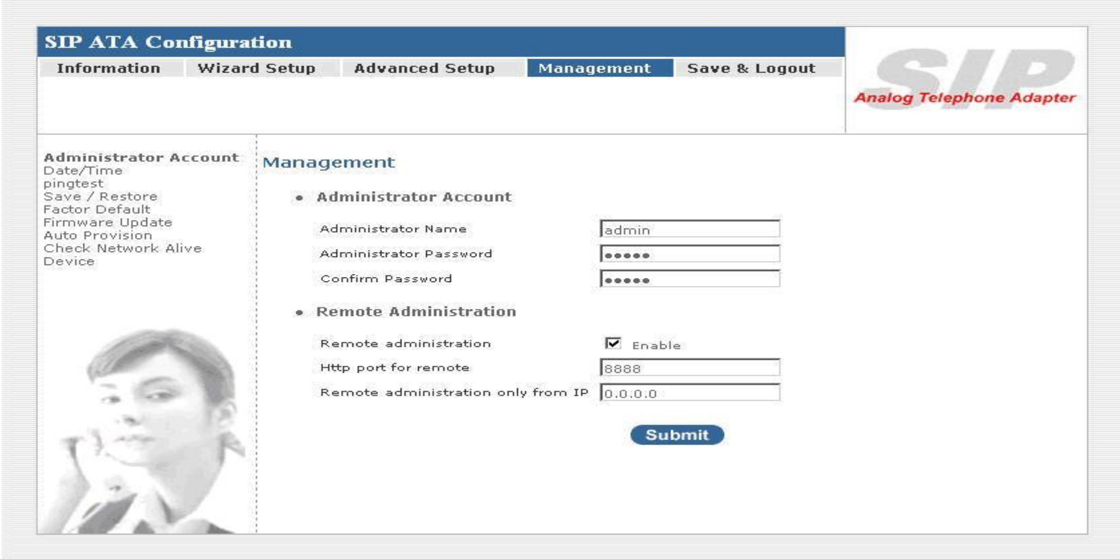
This window displays the FXS ports and SIP registered status. Click on Refresh button to retrieve the status.

7. Management

- Administrator Account
- Date/Time
- PING Test
- Save/Restore
- Factory Default
- Firmware Update
- Auto Provision
- Check Network Alive
- Device

7.1 Administrator Account

The administrator account can access the management interface through the web browser. Only the administrator account has the ability to change account password.



Management

- Administrator Account

Administrator Name admin
Administrator Password ●●●●●
Confirm Password ●●●●●

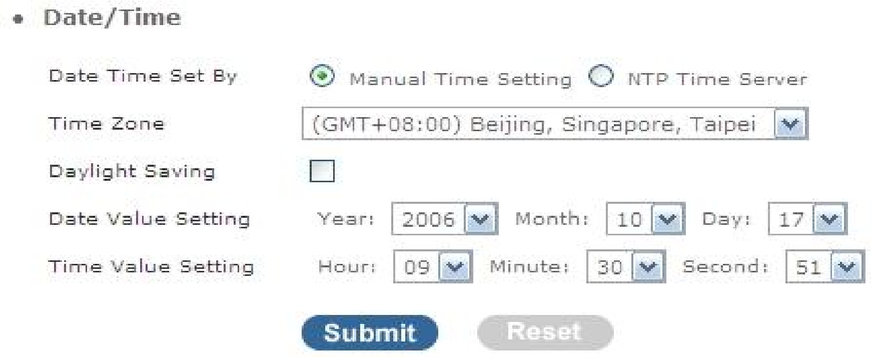
- Remote Administration

Remote administration ☑ Enable
Http port for remote 8888
Remote administration only from IP 0.0.0.0

□Administrator Name - Assign a name to represent the administrator account. Maximum 16 characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign¡ ”_”.
The administrator name is case-sensitive. Note: the “blank” character is an *illegal character*

□Administrator Password - Assign the administrator password. Maximum 16 characters and minimum 6 characters. Mix the characters with the digits. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign”_”. The password is case-sensitive.
Note: the “blank” character is an illegal character.
□Confirm Password - Enter the administrator password again. Remote Administrator allows the device to be configured through the WAN port from the Internet using a web browser. A username and password is still required to access the browser-based management interface.
□Remote Administration - Enable/Disable to access from remote site. Default setting is “Disable”.
□Http port for remote - If you allowed the access from the remote site, assign the http port used to access the ATA. Default port number is “8888”.
□Remote administration only from IP - Internet IP address of the computer that has access to the ATA. Assign the legal IP address.
Example:
http://x.x.x.x:8080 where as x.x.x.x is the WAN IP address and 8080 is the port used for the Web-Management interface.

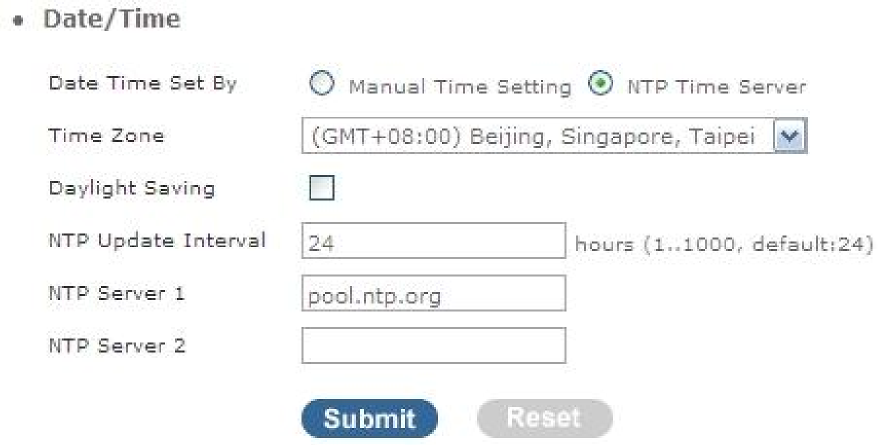
7.2 Date/Time



- Date/Time

Date Time Set By	● Manual Time Setting ○ NTP Time Server
Time Zone	(GMT+08:00) Beijing, Singapore, Taipei
Daylight Saving	□
Date Value Setting	Year: 2006 Month: 10 Day: 17
Time Value Setting	Hour: 09 Minute: 30 Second: 51

□Manual Time Setting - Set up the time manually.



- Date/Time

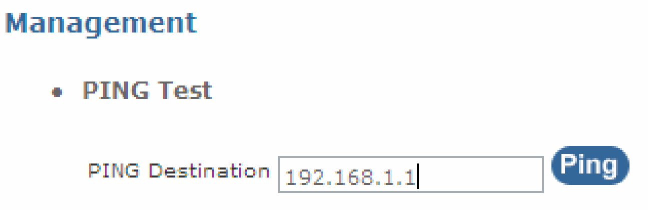
Date Time Set By	○ Manual Time Setting ● NTP Time Server
Time Zone	(GMT+08:00) Beijing, Singapore, Taipei
Daylight Saving	□
NTP Update Interval	24 hours (1..1000, default:24)
NTP Server 1	pool.ntp.org
NTP Server 2	

□NTP Time Server - Protocol used to help match your system clock with an accurate time source. For example atomic clock or a server.
□Time Zone – Choose your time zone , Default is (GMT+8:00)Beijing,Singapore,Taipei.
□Daylight Saving – Enable / Disable ,Default is Disable,time during which clocks are set one hour ahead of local standard time; widely adopted during summer to provide extra daylight in the evenings
□NTP Update Interval – Default is 24 hours , This is used to select the frequency of. NTP updates
□NTP Server 1 – Default is “pool.ntp.org”,NTP Server address.
□NTP Server 2 – Default is empty.

7.3 Ping Test

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping (Packet Internet Groper) and click Ping.

Example: www.yahoo.com or 216.115.108.245



Management

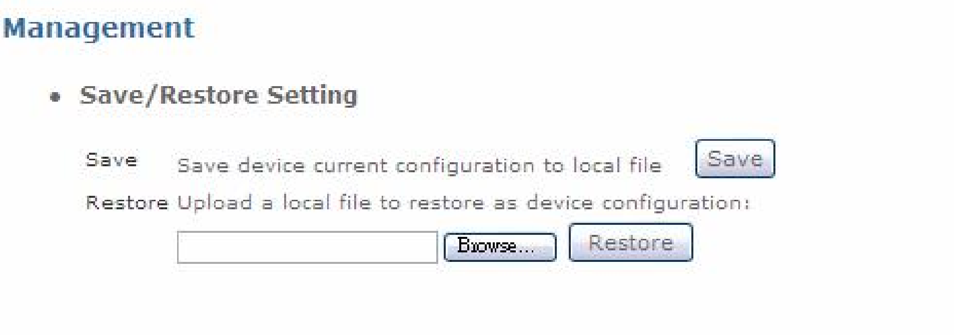
- PING Test

PING Destination: 192.168.1.1

□Ping Destination - Assign a legal IP address.

7.4 Save/Restore

All settings can be saving to a local file. Or, you can upload a local file to restore as the device configuration for the Telephony ATA.



Management

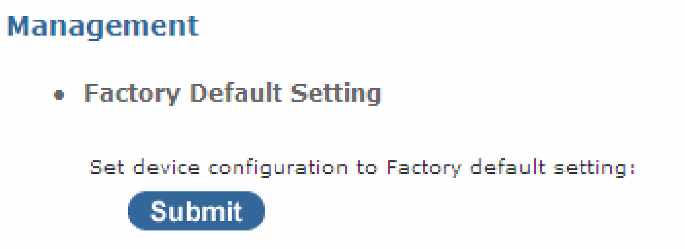
- Save/Restore Setting

Save: Save device current configuration to local file

Restore: Upload a local file to restore as device configuration:

7.5 Factory Default

This function is used to restore all the parameters back to factory default setting. You can use the Save/Restore Setting (please refer to the section of 7.3 "Save/Restore¡¨) to check the factory default configuration, after you click on the **Set** button.



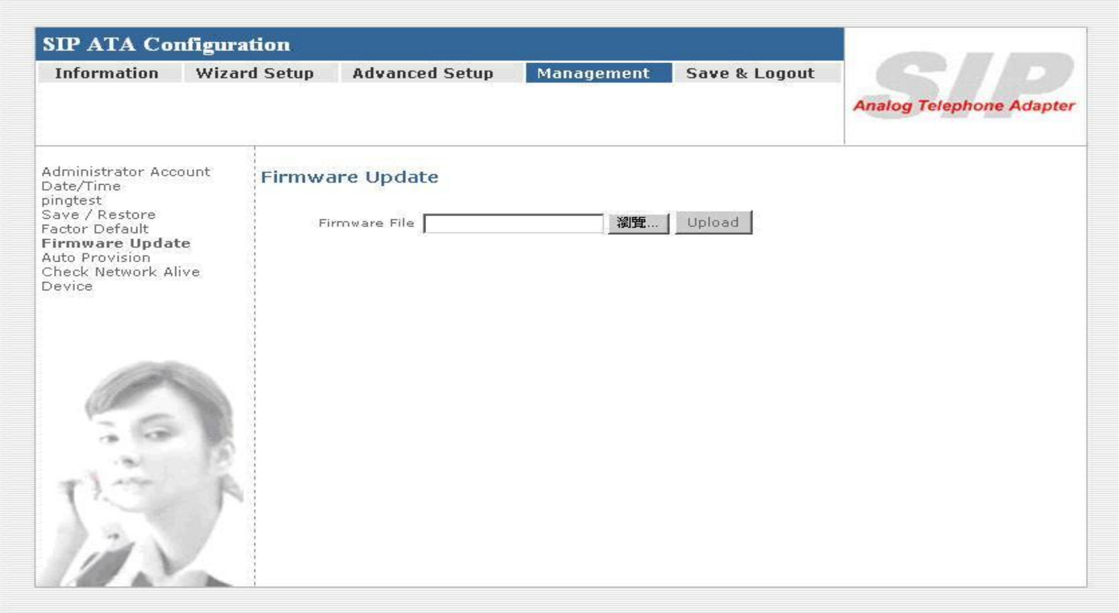
Management

- Factory Default Setting

Set device configuration to Factory default setting:

7.6 Firmware Update

You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on Browse to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.



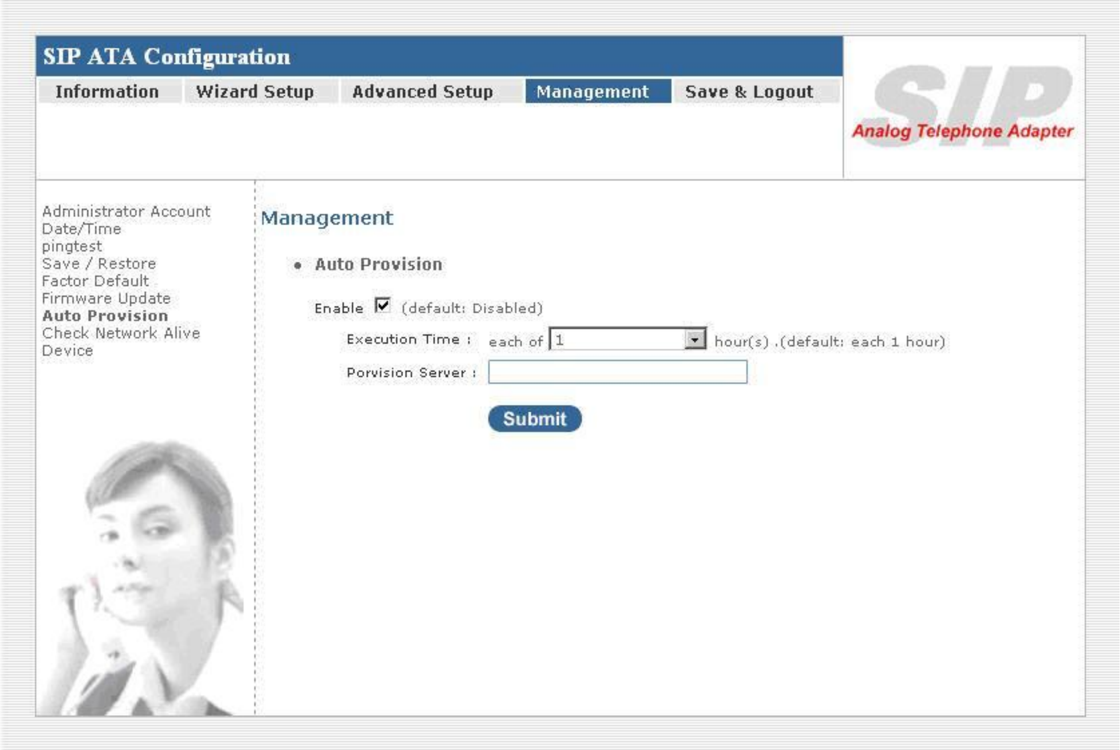
Firmware Update

Firmware File

Firmware Name: select that you want to upgrade Firmware version.

7.7 Auto Provision

Enable or disable the auto-provisioning feature. If enabled ATA will try to download the configuration files from the provisioning server.



Management

- Auto Provision

Enable ☑ (default: Disabled)

Execution Time : each of 1 hour(s) .(default: each 1 hour)

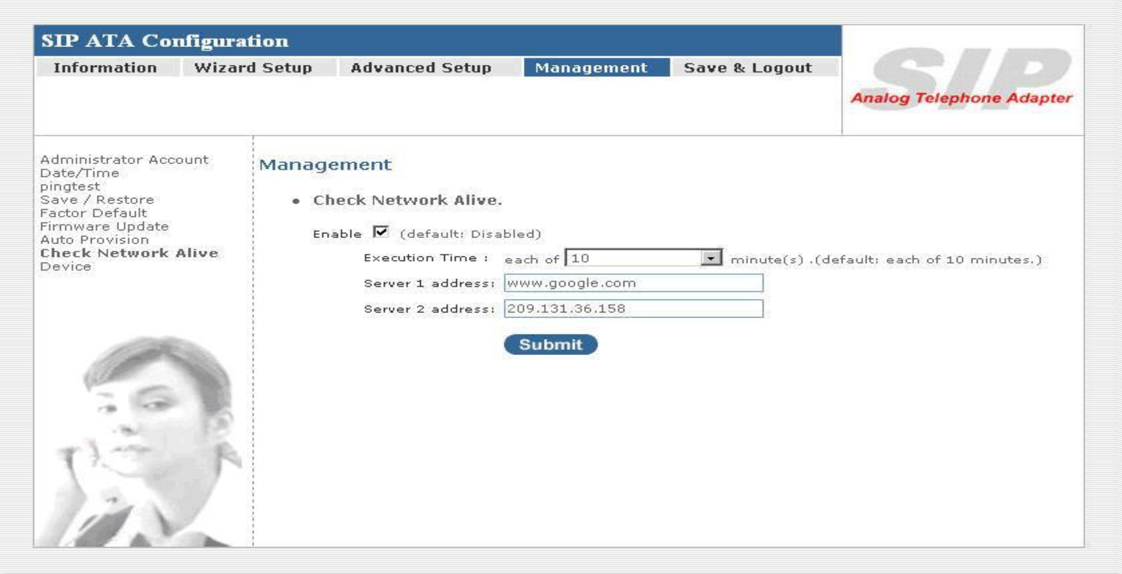
Porvision Server :

□Excution Time - Default 1 hour (1 to 10 hours) , ATA will try to download the configuration files from the provisioning server.

□Provision Server - Provision Server ,default is empty.

7.8 Check Network Alive

Use the Check network alive Net valid node checking security feature to allow or deny access to server processes from network clients with specified IP addresses.



Management

- Check Network Alive.

Enable ☑ (default: Disabled)

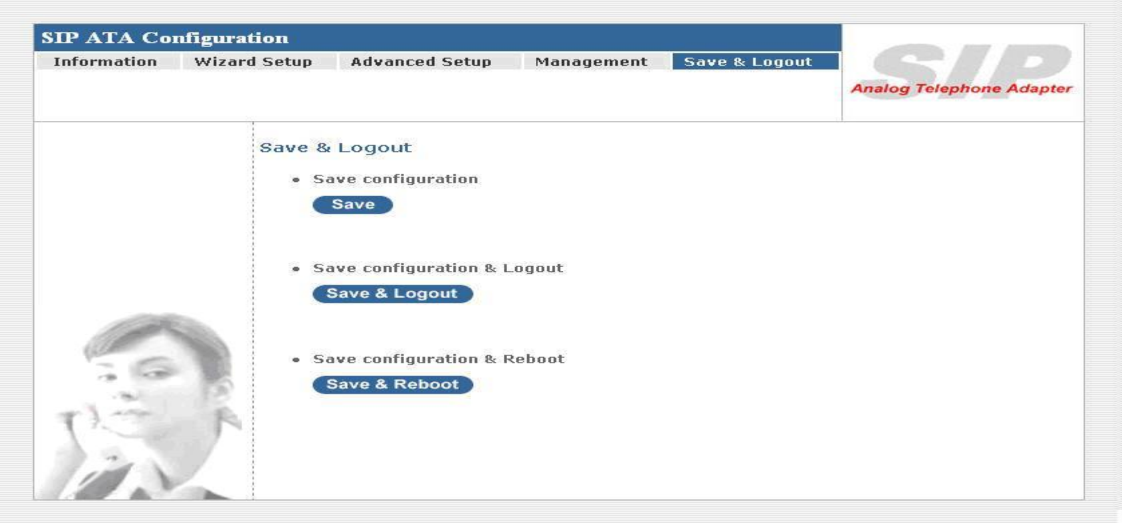
Execution Time : each of 10 minute(s) .(default: each of 10 minutes.)

Server 1 address: www.google.com

Server 2 address: 209.131.36.158

□Execution Time - 5 ~ 55 min,default 10min
□Server 1 address - www.google.com
□Server 2 address - 209.131.36.158

Save & Logout

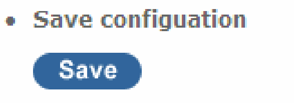


Save & Logout

- Save configuration
- Save configuration & Logout
- Save configuration & Reboot

8.1 Save

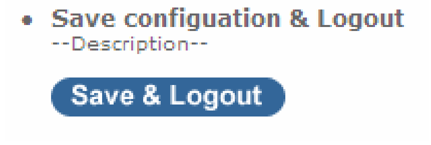
Save your ATA Setting after you setting finish.



- Save configuation

8.2 Save & 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.



8.3 Save & Reboot

If for any reason the device is not responding correctly, you may want to reboot the ATA system

Appendix

A - FAQ List

1. What is the default administrator password to login to the ATA? 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 IP Address is "192.168.1.1", Lan Port IP Address is "222.222.222.1".Loging Web User Interface, open the Bowser(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 ATA?
A: Please chick your ATA is registered SIP Proxy Server(ITSP), and chink your Internet works fine. ATA 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.

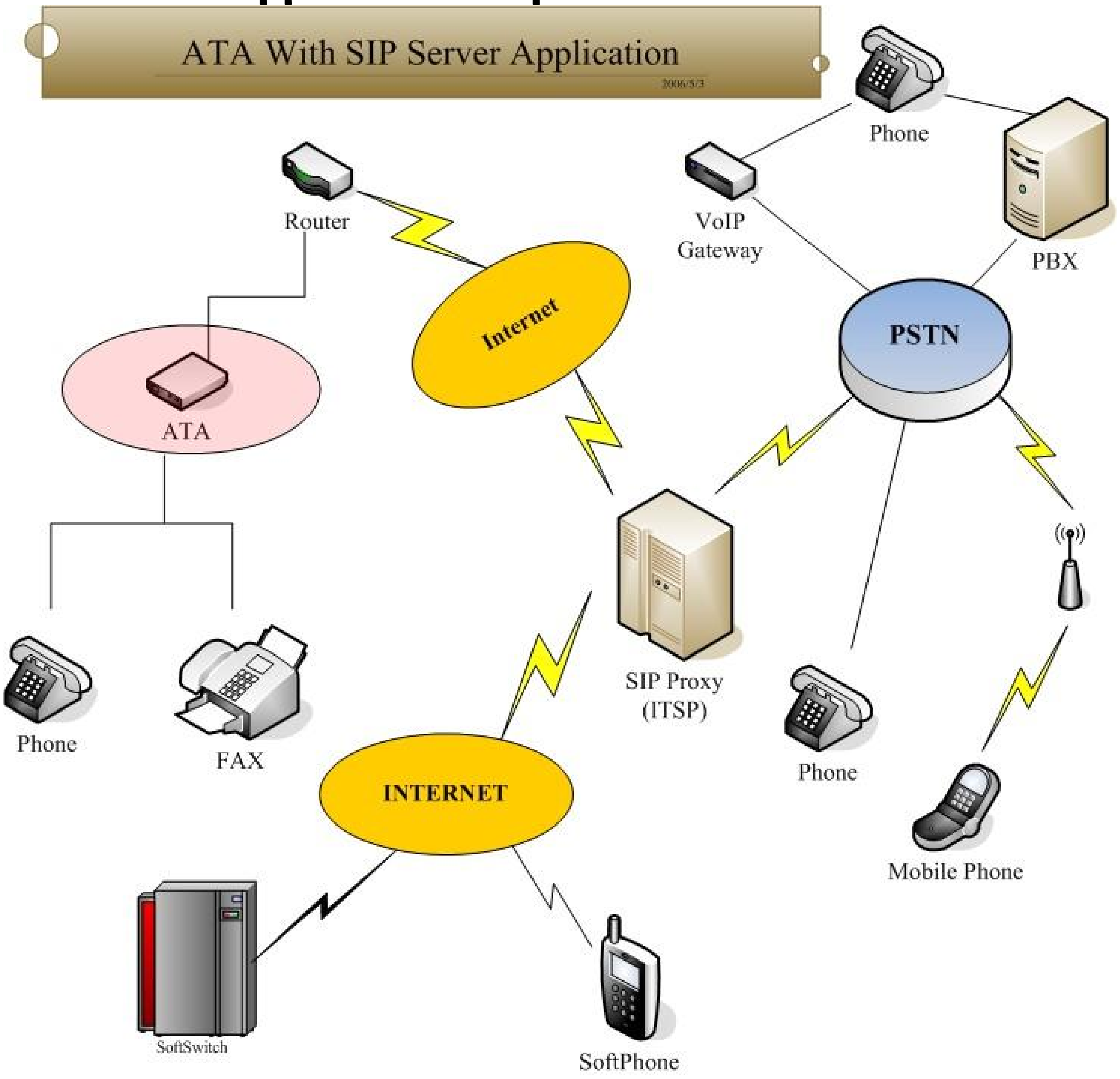
6. I can't use web Interface to setting ATA, How can I do?
A: Please check you PC connect the ATA Lan port or PC and ATA with the same Subnet. If you PC aren't at the same Subnet, you can't Login the ATA Web interface. Else you let your ATA on Public Internet(Public IP address).

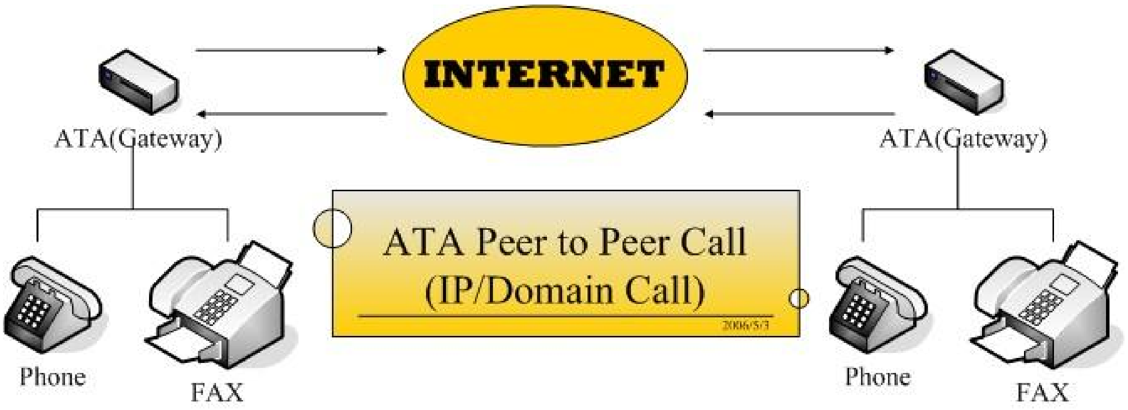
7. Why does the one way talk happen?
A: Generally, one way talk happen when use the different codec between VoIP device make call.

Please check and setting the same codec, most one way talk will be solved.

8. Why can I call out when the ATA under the NAT?
A: VoIP product almost have NAT Pass through problem. 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




INTERNET
ATA(Gateway)
ATA(Gateway)
Phone
FAX
Phone
FAX
ATA Peer to Peer Call
(IP/Domain Call)
2006/5/3

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses

and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1 This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority

to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed

and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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