Wireless Analog Telephone Adapter

VIP-161W / VIP161SW

User’s manual

Version 1.0.0

Copyright

The products and programs described in this User’s Manual are licensed products of PLANET Technology, This User’s Manual contains proprietary information protected by copyright, and this User’s Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User’s Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User’s Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User’s Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User’s Manual. PLANET makes no commitment to update or keep current the information in this User’s Manual, and reserves the right to make improvements to this User’s Manual and/or to the products described in this User’s Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

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

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks.

Revision

User’s Manual for PLANET Wireless Analog Telephone Adapter:

Model: WATA

Rev: 1.0.0 (2007, August)

Part No. EM-VIP_WATAV1

TABLE OF CONTENTS

Chapter 1

Introduction

Overview

Combining the cutting edge of Internet telephony and ATA manufacturing experience, PLANET now introduces the latest member of PLANET Wireless ATA family: the VIP-161W/VIP-161SW.

To bring the most satisfaction to customers, the WATA not only provides the high quality of voice communications and wired Internet sharing capabilities but also offers Access Point (AP) function for daily wireless communication. With advanced router and VoIP DSP processor technology, the WATA is able to make calls via SIP proxy voice communications plus the IP sharing and the QoS mechanism.

The WATA is the ideal choice for Voice over IP communication and integrates Internet sharing for the daily tasks. To give most flexibility to users, the Wireless ATA provides direct analog interface for fax machine and analog telephones. Users can not only make the daily VoIP communication but also enjoy the convenience brought by FoIP communications.

With the WATA, home users and companies are able to save the cost of installation and extend their previous investments in telephones, conferences and speakerphones. The WATA equipped with two telephony interfaces, so users may register to different SIP proxy servers and establish up to 2 concurrent VoIP calls for more flexibility in the voice communications. The WATA can be the bridge between traditional analog telephones and IP network with an extremely affordable investment.

The WATA includes two Ethernet interface for Internet (PPPoE, DHCP or Fixed IP) or office LAN connection. The dual Ethernet design brings the greatest convenience when deploying VoIP network. With a built-in IEEE 802.11b/g wireless AP/CPE, the Wi-Fi ATA offers wireless connectivity via 54Mbps data transmissions.

Product Features

- IEEE 802.11b/g compliant
- Multi-mode: AP, AP-Client Mode
- Smart QoS mechanism to ensure the voice quality
- Auto-config feature for flexible, ease-of use system integration
- NAT Router, Static Routing, Virtual Server, DMZ
- Smart QoS mechanism to ensure the voice quality
- IP ToS (IP Precedence) / DiffServ

VoIP Featires

- SIP 2.0 (RFC3261) compliant
- Up to 2 concurrent VoIP calls
- Voice codec support: G.711, G.729 AB, G.723, G.276
- T.38 FAX transmission over IP network (G.711 Fax pass-through)
- In-band and out-of-band DTMF Relay (RFC 2833)
- Three-way conference calls
- Call Waiting / Forward / Transfer / Hold / Resume / Screen
- Caller ID Detection/Generation: DTMF, Bellcore, ETSI, NTT
- Voice processing: VAD, CNG, Dynamic Jitter Buffer, G.168~2000 echo cancellation

Package Content

The contents of your product should contain the following items：

1. Wireless Analog Telephone Adapter
2. Power adapter
3. Dipole Antenna
4. Quick Installation Guide
5. User’s Manual CD
6. RJ-45 cable

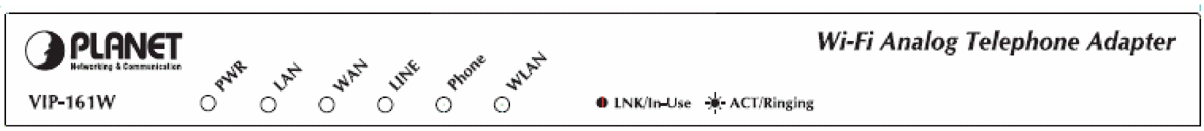
Physical Details

The following figure illustrates the front/rear panel of WATA.

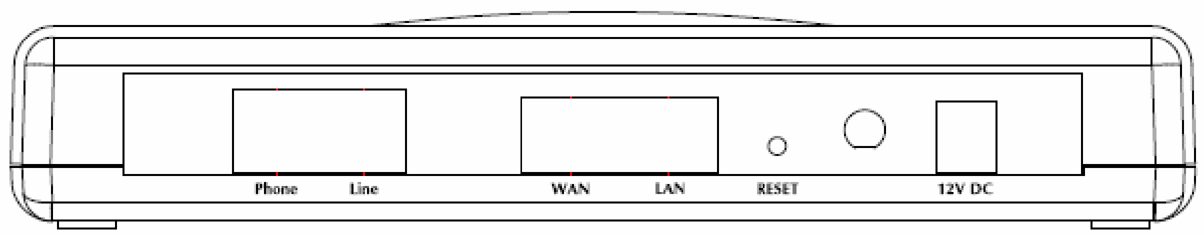
Respective model/descriptions are shown below:

VIP-161W: 1 FXS / 1 PTSN Wireless Analog Telephone Adapter.

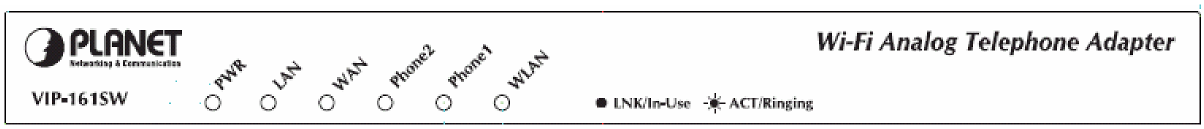
VIP-161SW: 2 FXS Wireless Analog Telephone Adapter



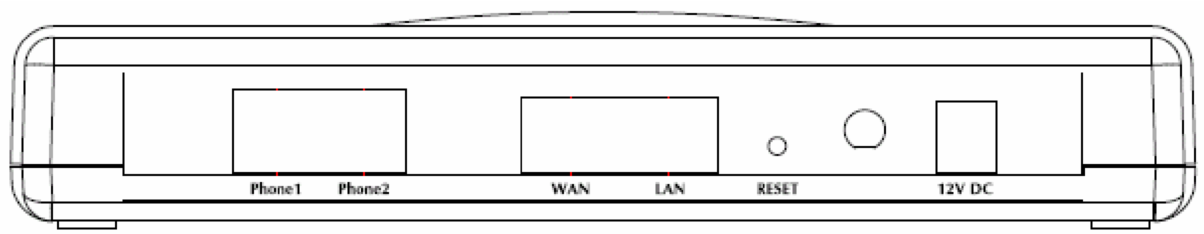
Front Panel of VIP-161W



Back Panel of VIP-161W



Front Panel of VIP-161SW



Back Panel of VIP-161SW

LED Display

LED display of VIP-161W / VIP-161SW

LED Indicators	Descriptions
PWR	**On:** WATA is power ON **Off:** WATA is power Off
WAN	**On:** WATA network connection established **Flashing:** Data traffic on cable network **Off:** Waiting for network connection
LAN	**On:** LAN is connected successfully **Flashing:** Data is transmitting **Off:** Ethernet not connected to PC
Phone 1 （FXS1） **Phone 2 （FXS2）** **Line (VIP-161W only)**	**Off:** Telephone Set is On-Hook **Flashing:** Ring Indication **On:** Telephone Set is Off-Hook
WLAN	**OFF**: Wireless network connection established. **Flashing:** Data traffic on cable network **ON:** Waiting for network connection

Note

Press RESET button on rear panel over 5 seconds will reset the WATA to factory default value

Chapter 2 2

Preparations & Installation

Physical Installation Requirement

This chapter illustrates basic installation of Wireless Analog Telephone Adapter ("WATA" in the following term)

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ-45 connectors.
- TCP/IP protocol must be installed on all PCs.

For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem

Hardware Installation

Port Description

1	**WAN**	Connect to the network with an Ethernet cable. This port allows your WATA 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.
2	**LAN**	Connect to PC with Ethernet cable. 1 port allows your PC or Switch/Hub to be connected to the WATA through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
3	**Phone**	FXS port can be connected to analog telephone sets or Trunk Line of PBX.
4	**Line**	Line port can be connected to RJ11 PSTN line (VIP-161W only)
5	**Reset**	Push this button until 3 seconds, and WATA will be set to factory default configuration.
6	**External Antenna Area.**	Used to Wirelessly Connect to 802.11b/g networks 802.11b: 11/5.5/2 Mbps 802.11g: 54/48/36/24/19/12/6Mbps
7	**12V DC**	12V DC Power input outlet

Installation

1 Connect the 12V DC IN to the power outlet with power adaptor.

2 Connect Line to PSTN.

3 Connect Phone 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.

Administration Interface

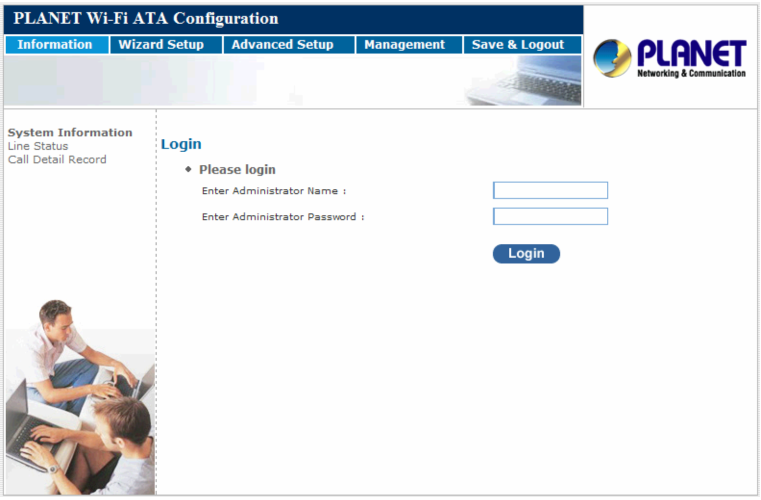
PLANET WATA provides GUI (Web based, Graphical User Interface) for machine management and administration.

Web configuration access

To start WATA web configuration, you must have one of these web browsers installed on computer for management

- Microsoft Internet Explorer 6.0 or higher with Java support

Default LAN interface IP address of WATA is 192.168.0.1. You may now open your web browser, and insert http://192.168.0.1 in the address bar of web browser to logon WATA web configuration page.



Login

- Please login

Enter Administrator Name :

Enter Administrator Password :

WATA will prompt for logon username/password, please enter: **root / null (no password)** to continue machine administration.

Note

In order to connect machine for administration, please locate your PC in the same network segment (192.168.0.x) of VIP-161W/VIP-161SW. If you're not familiar with TCP/IP, please refer to related chapter on user's manual CD or consult your network administrator for proper network configurations.

Wizard Setup

Wizard for Quick Setup of the WATA, after finishing the authentication, the Main menu will display 4 parts of configuration, please click "**Wizard Setup**" to enter quick start:

STEP1: Operation Mode

a. AP Mode

b. AP-Client Mode

c . WISP & AP Mode

STEP2: Internet Setting

a. AP Only Mode

b. AP-Client Only Mode

c. WISP & AP Mode

STEP3: NAT Settings

a. Phone Number

b. SIP Proxy Server IP

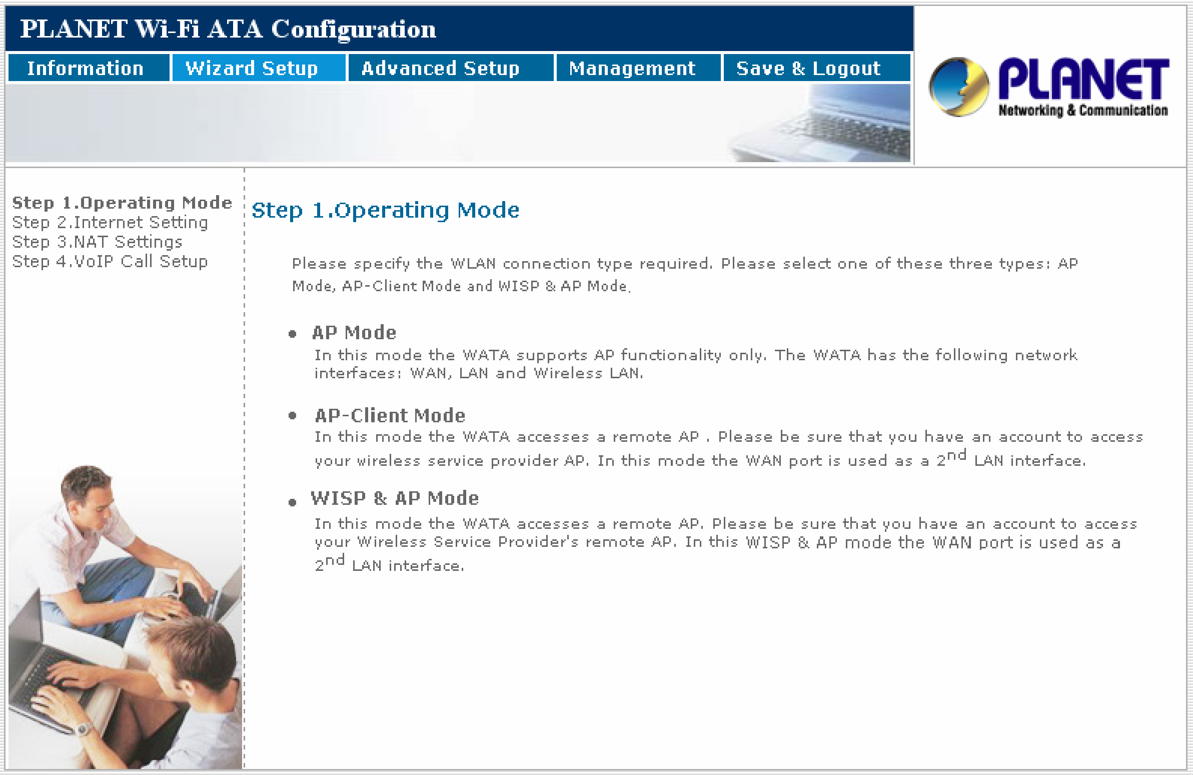
STEP4: VOIP Call Setup

a . Phone Number

b . SIP Proxy Server IP

Operation Mode

For most users, Internet access is the primary application. The WATA supports the WAN or WLAN interface for Internet access and remote access. When you click "**Operation Mode**" from within the Wizard Setup, the following setup page will be show.



Step 1.Operating Mode

Please specify the WLAN connection type required. Please select one of these three types: AP Mode, AP-Client Mode and WISP & AP Mode.

- AP Mode
  In this mode the WATA supports AP functionality only. The WATA has the following network interfaces: WAN, LAN and Wireless LAN.
- AP-Client Mode
  In this mode the WATA accesses a remote AP . Please be sure that you have an account to access your wireless service provider AP. In this mode the WAN port is used as a 2nd LAN interface.
- WISP & AP Mode
  In this mode the WATA accesses a remote AP. Please be sure that you have an account to access your Wireless Service Provider's remote AP. In this WISP & AP mode the WAN port is used as a 2nd LAN interface.

Three WLAN modes of operation are available for Internet Access:

AP Mode:

In this mode the WATA supports AP functionality only. The WATA has the following network interfaces: WAN, LAN and Wireless LAN.

AP-Client Mode:

In this mode the WATA accesses a remote AP. Please be sure that you have an account to access your wireless service provider AP. In this mode the WAN port is used as a 2nd LAN interface.

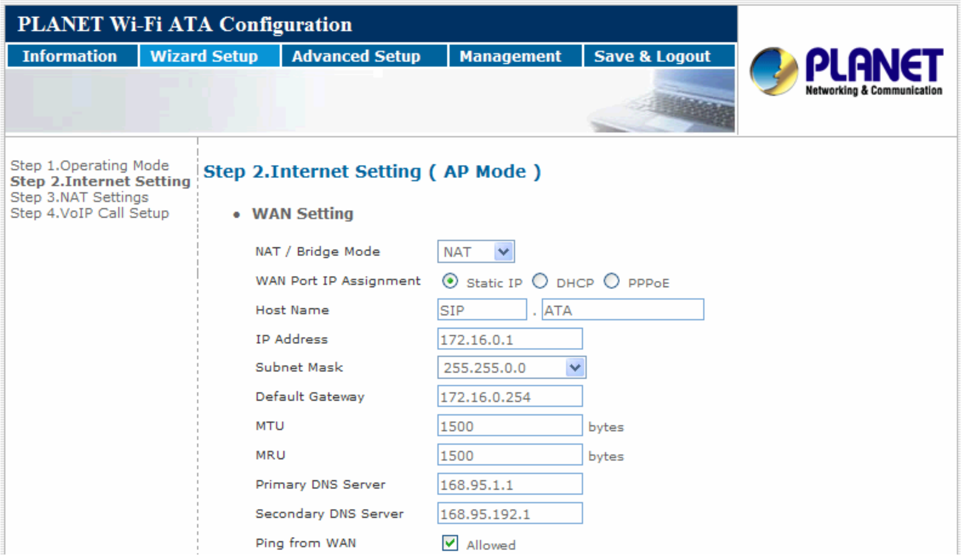
WISP & AP Mode：

In this mode the WATA accesses a remote AP. Please be sure that you have an account to access your Wireless Service Provider's remote AP. In this WISP & AP mode the WAN port is used as a 2nd LAN interface.

Internet Setting Setup

WAN Setting

NAT Mode	Network Address Translation (NAT) serves connecting multiple computers to the Internet using one IP address.
Bridge Mode	Bridge mode serves to connect a local area network (LAN / Wireless) to another local area network that uses the same protocol.
WAN Port IP Assignment	Three methods are available for Internet Access. Static IP / DHCP / PPPoE type for your select .you should refer to section 3.1 “WAN Setting” in user menu.



Step 2.Internet Setting (AP Mode)

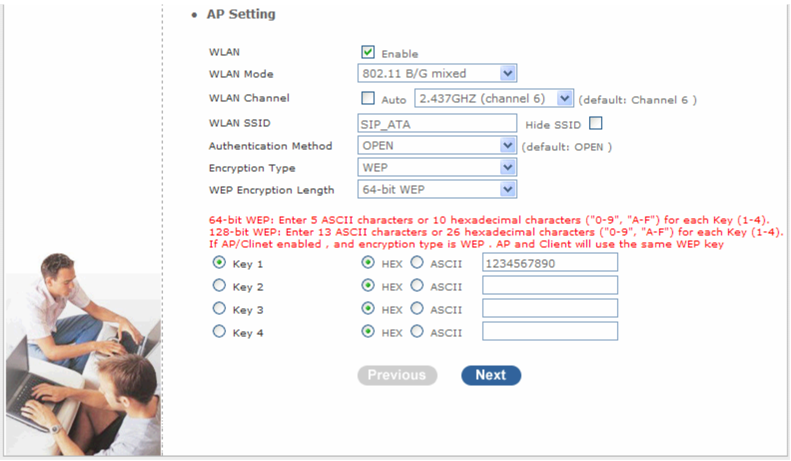
- WAN Setting

NAT / Bridge Mode	NAT
WAN Port IP Assignment	● Static IP ○ DHCP ○ PPPoE
Host Name	SIP . ATA
IP Address	172.16.0.1
Subnet Mask	255.255.0.0
Default Gateway	172.16.0.254
MTU	1500 bytes
MRU	1500 bytes
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
Ping from WAN	☑ Allowed

AP Setting

For configuring correctly the WLAN port in client mode. the below instructions will provide a quick start. It is advised if possible to use the simplest network settings for first try.

For making sure the WATA is connecting to your wireless router (AP). You need to set up the following: SSID, Frequency Channel, Authentication method and Encryption parameters (Type/Encryption length/Keys.)



- AP Setting

WLAN	☑ Enable
WLAN Mode	802.11 B/G mixed
WLAN Channel	□ Auto 2.437GHZ (channel 6) (default: Channel 6)
WLAN SSID	SIP_ATA Hide SSID □
Authentication Method	OPEN (default: OPEN)
Encryption Type	WEP
WEP Encryption Length	64-bit WEP

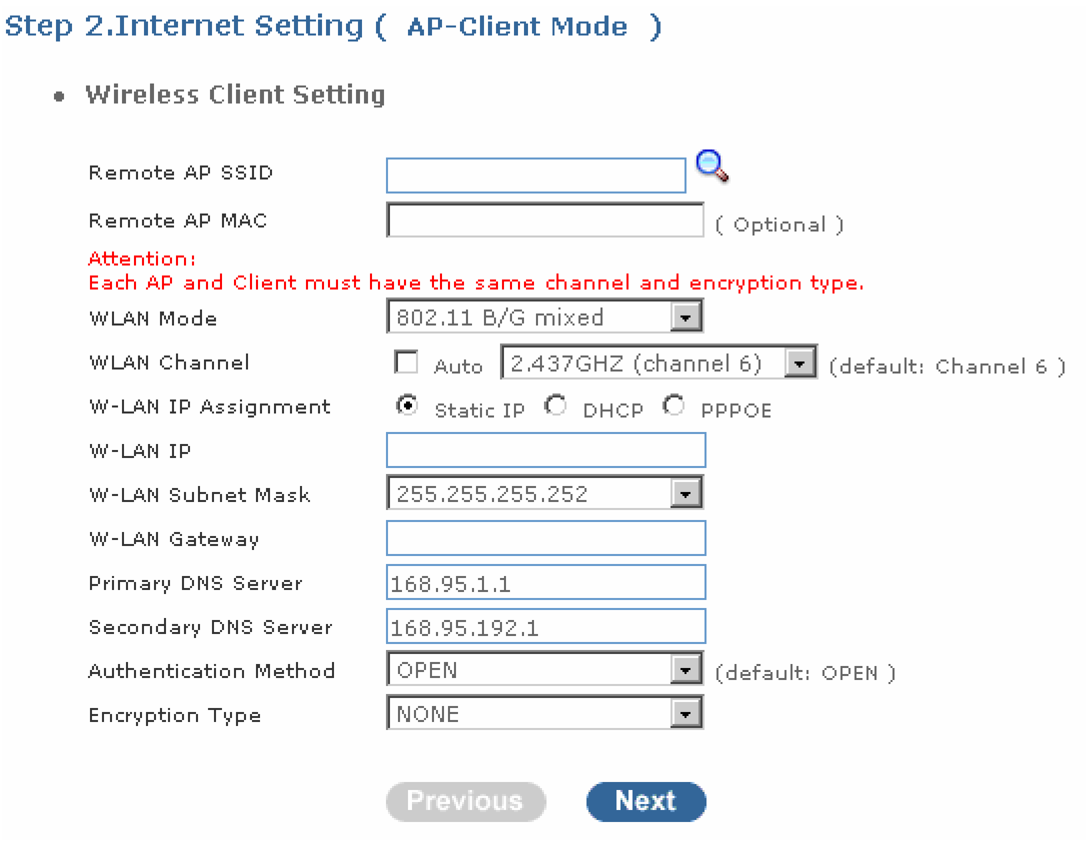
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
If AP/Clinet enabled , and encryption type is WEP . AP and Client will use the same WEP key

● Key 1	● HEX ○ ASCII	1234567890
○ Key 2	● HEX ○ ASCII	
○ Key 3	● HEX ○ ASCII	
○ Key 4	● HEX ○ ASCII	

AP-Client Mode

This paragraph defines the required parameters to set up the WLAN interface as a Client on your wireless access network. You need to define the following parameters:

Default WLAN mode / Remote SSID / Authorization key / IP / Gateway.



Step 2.Internet Setting (AP-Client Mode)

- Wireless Client Setting

Remote AP SSID	
Remote AP MAC	(Optional)

Attention:
Each AP and Client must have the same channel and encryption type.

WLAN Mode	802.11 B/G mixed
WLAN Channel	□ Auto 2.437GHZ (channel 6) (default: Channel 6)
W-LAN IP Assignment	● Static IP ○ DHCP ○ PPPOE
W-LAN IP	
W-LAN Subnet Mask	255.255.255.252
W-LAN Gateway	
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
Authentication Method	OPEN (default: OPEN)
Encryption Type	NONE

WISP & AP Mode

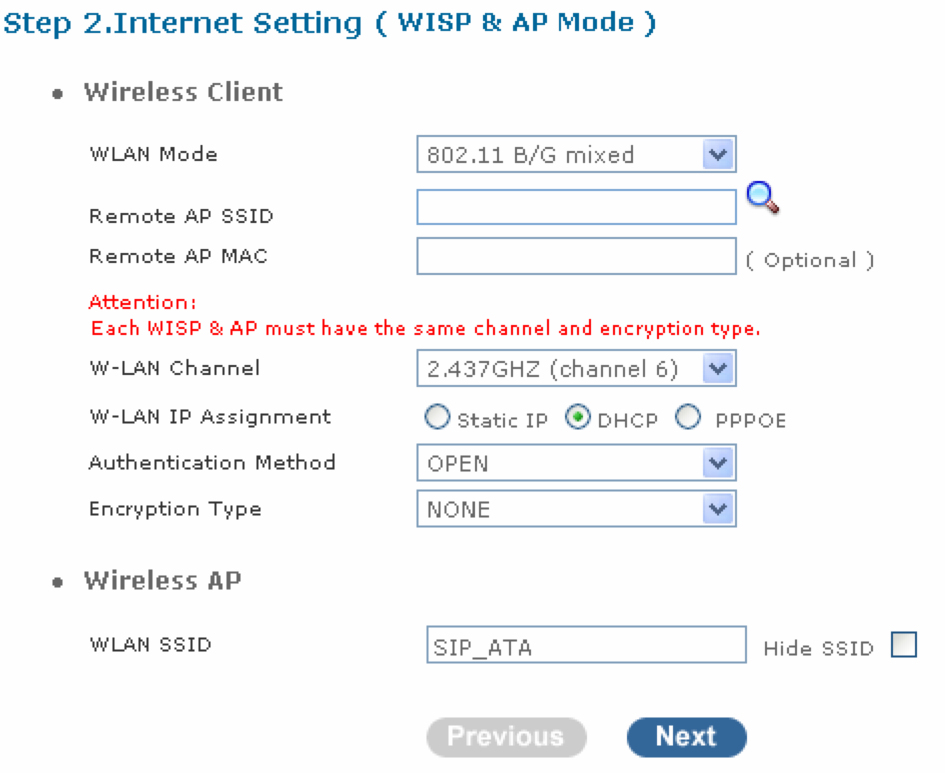
This paragraph defines the required parameters to set up the WLAN interface as a Client on your wireless access network. You need to define the following parameters:

Wireless Client

Default WLAN mode / Remote SSID / Encryption parameters / IP / Gateway

Wireless AP

Local SSID.



Step 2.Internet Setting (WISP & AP Mode)

- Wireless Client

WLAN Mode: 802.11 B/G mixed

Remote AP SSID:

Remote AP MAC: (Optional)

Attention:
Each WISP & AP must have the same channel and encryption type.

W-LAN Channel: 2.437GHZ (channel 6)

W-LAN IP Assignment: ○ Static IP ● DHCP ○ PPPOE

Authentication Method: OPEN

Encryption Type: NONE

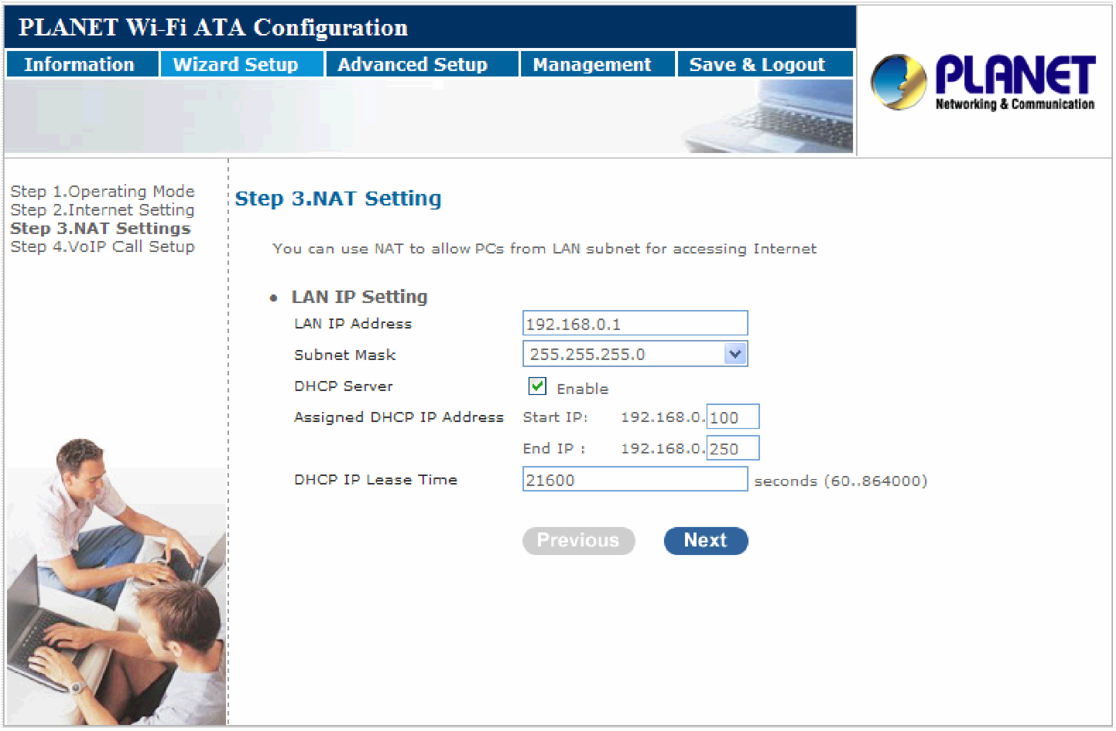
- Wireless AP

WLAN SSID: SIP_ATA Hide SSID □

NAT setting

LAN IP Setting

LAN IP Address	Private IP address for connecting to a local private network. (Default: 192.168.0.1)
Subnet Mask	Subnet mask for the local private network (Default: 255.255.255.0)
DHCP Server	Enable to open LAN port DHCP server
Assigned DHCP IP Address	DHCP server range from start IP to end IP
DHCP IP Lease Time	Client to ask DHCP server refresh time, range from 60 to 86400 seconds



Step 1.Operating Mode
Step 2.Internet Setting
Step 3.NAT Settings
Step 4.VoIP Call Setup

Step 3.NAT Setting

You can use NAT to allow PCs from LAN subnet for accessing Internet

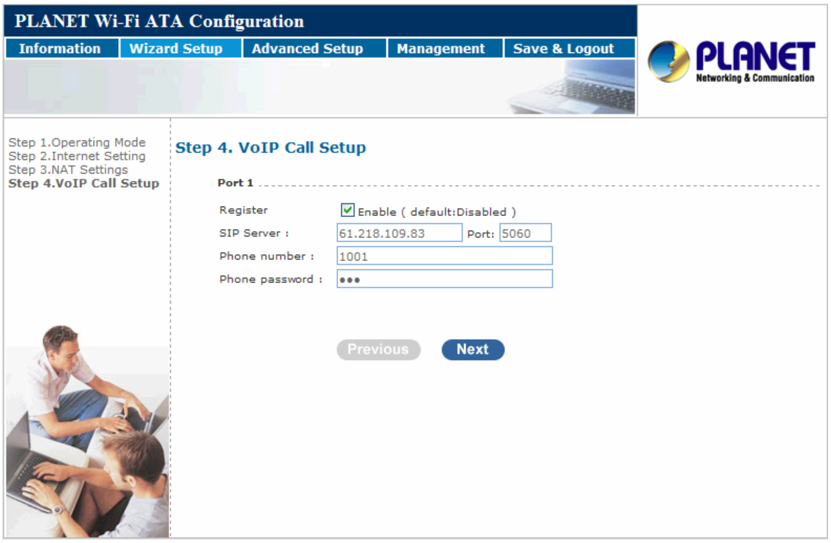
- **LAN IP Setting**

LAN IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP Server: ☑ Enable
Assigned DHCP IP Address: Start IP: 192.168.0.100
End IP : 192.168.0.250
DHCP IP Lease Time: 21600 seconds (60..864000)

VoIP Call Setup

Configure the numbering with phone/line ports

SIP Proxy Server IP addresses	There is a SIP Proxy Server address and port fields. Check with your ITSP provider.
Phone number / password	Pleae check with your ISP provider.



Step 1.Operating Mode
Step 2.Internet Setting
Step 3.NAT Settings
Step 4.VoIP Call Setup

Step 4. VoIP Call Setup

Port 1

Register: ☑ Enable (default:Disabled)
SIP Server : 61.218.109.83 Port: 5060
Phone number : 1001
Phone password : •••

Finishing the Wizard Setup

After completing the Wizard Setup, please click “Finish” bottom. The WATA will save the configuration and rebooting WATA automatically. After 30 Seconds, you could re-login the WATA.

Chapter 3

Network Service Configurations

Configuring Netowrk setting for your Wi-Fi ATA

The WATA integrates a web-based graphical user interface that can cover most configurations and machine status monitoring. Via standard web browser, you can configure and check machine status from anywhere around the world.

- **WAN Setting / LAN Setting**
- **WLAN**
- **DHCP Setting**
- **Static Route (Default Router)**
- **NAT**
- **Packet Filter**
- **URL Filter**
- **Security**
- **UPNP**
- **DDNS**
- **SNMP**
- **QOS (VLAN)**

WAN Setting / LAN Setting

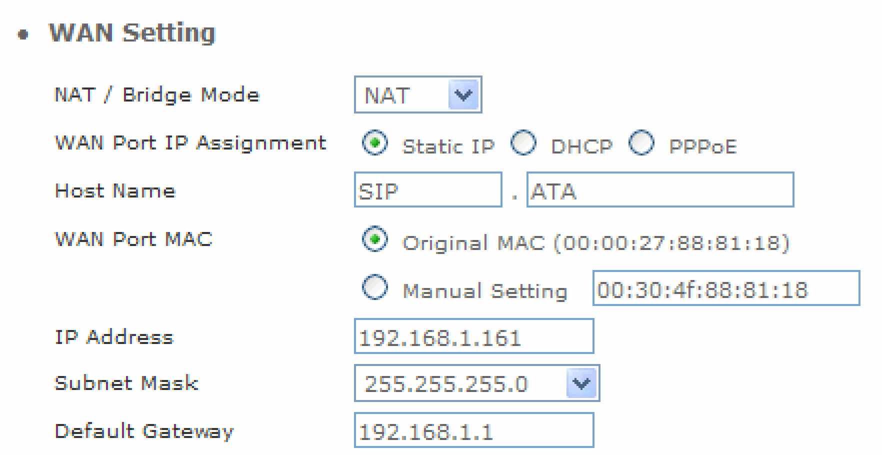
WAN (Wide Area Network) is a network connection connecting one or more LANs together over some distance. For example, the means of connecting two office buildings separated by several kilometers would be referred to as a WAN connection. The size of a WAN and the number of distinct LANs connected to a 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. WATA 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

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.

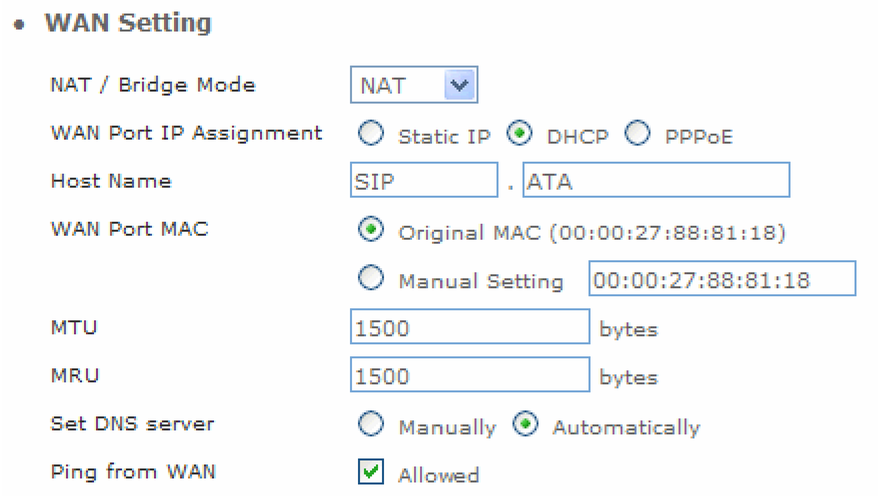


- **WAN Setting**

NAT / Bridge Mode	NAT
WAN Port IP Assignment	● Static IP ○ DHCP ○ PPPoE
Host Name	SIP . ATA
WAN Port MAC	● Original MAC (00:00:27:88:81:18) ○ Manual Setting 00:30:4f:88:81:18
IP Address	192.168.1.161
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

DHCP (Dynamic Host Configuration Protocol)

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.

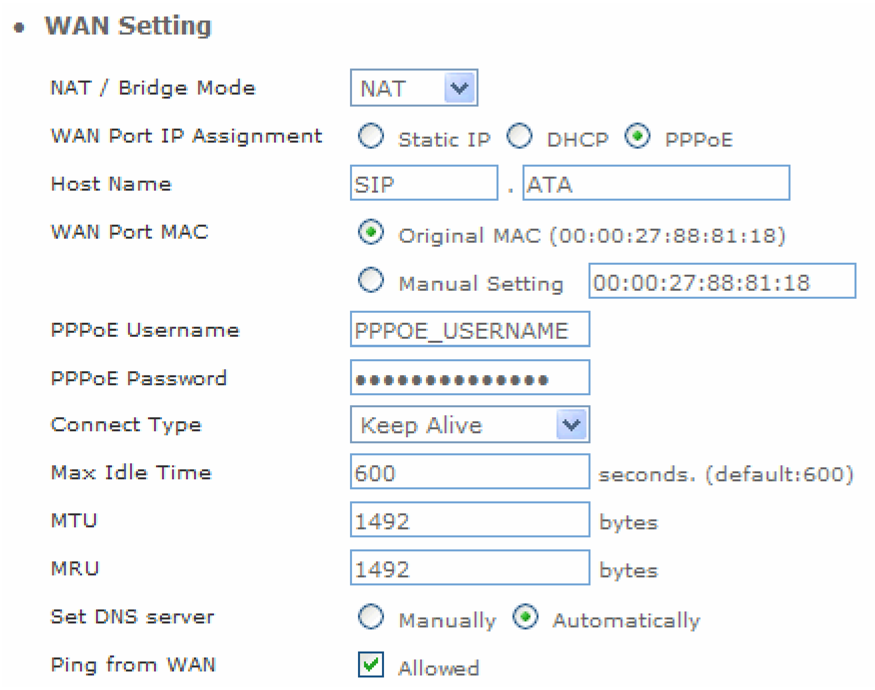


- **WAN Setting**

NAT / Bridge Mode	NAT
WAN Port IP Assignment	○ Static IP ● DHCP ○ PPPoE
Host Name	SIP . ATA
WAN Port MAC	● Original MAC (00:00:27:88:81:18) ○ Manual Setting 00:00:27:88:81:18
MTU	1500 bytes
MRU	1500 bytes
Set DNS server	○ Manually ● Automatically
Ping from WAN	☑ Allowed

PPPoE (Point-to-Point Protocol over Ethernet)

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.

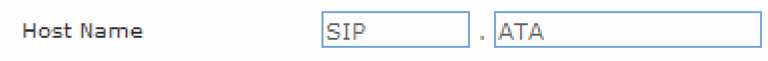


- WAN Setting

NAT / Bridge Mode	NAT
WAN Port IP Assignment	○ Static IP ○ DHCP ● PPPoE
Host Name	SIP . ATA
WAN Port MAC	● Original MAC (00:00:27:88:81:18) ○ Manual Setting 00:00:27:88:81:18
PPPoE Username	PPPOE_USERNAME
PPPoE Password	••••••••••••••
Connect Type	Keep Alive
Max Idle Time	600 seconds. (default:600)
MTU	1492 bytes
MRU	1492 bytes
Set DNS server	○ Manually ● Automatically
Ping from WAN	☑ Allowed

Host Name

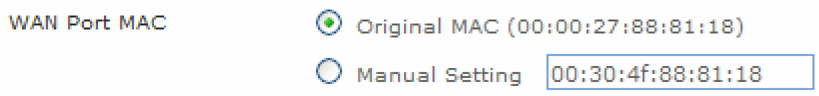
The Host Name field is optional but may be required by some Internet Service Providers. The default host name is the model number of the device. I



Host Name	SIP . ATA

WAN Port MAC

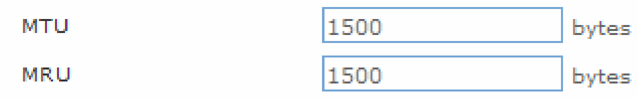
The MAC (Media Access Control) Address field is required by some Internet Service Providers (ISP). The default MAC address is set to the MAC address of the WAN interface in the device. It is only necessary to fill the field if required by your ISP.



WAN Port MAC	● Original MAC (00:00:27:88:81:18) ○ Manual Setting 00:30:4f:88:81:18

MTU and MRU

MTU stands for Maximum Transmission Unit, the largest physical packet size, measured in bytes that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

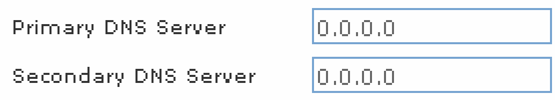


MTU	1500 bytes
MRU	1500 bytes

DNS Server

DNS stands for Domain Name System. Every Internet host must have a unique IP address; also they may have a user-friendly, easy to remember name such as www.wata.com The DNS server converts the user-friendly name into its equivalent IP address.

The original DNS specifications require that each domain name is served by at least 2 DNS servers for redundancy.



Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Ping From WAN

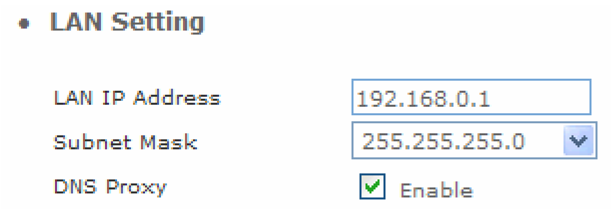
Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating.

Ping from WAN ☑ Allowed

LAN Setting

These are the IP settings of the LAN 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 192.168.0.1 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.



- LAN Setting

LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DNS Proxy	☑ Enable

DNS Proxy

A proxy server is a computer network service that allows clients to make indirect network connections to other network services. The default setting is Enable the DNS proxy server.

DNS Proxy ☑ Enable

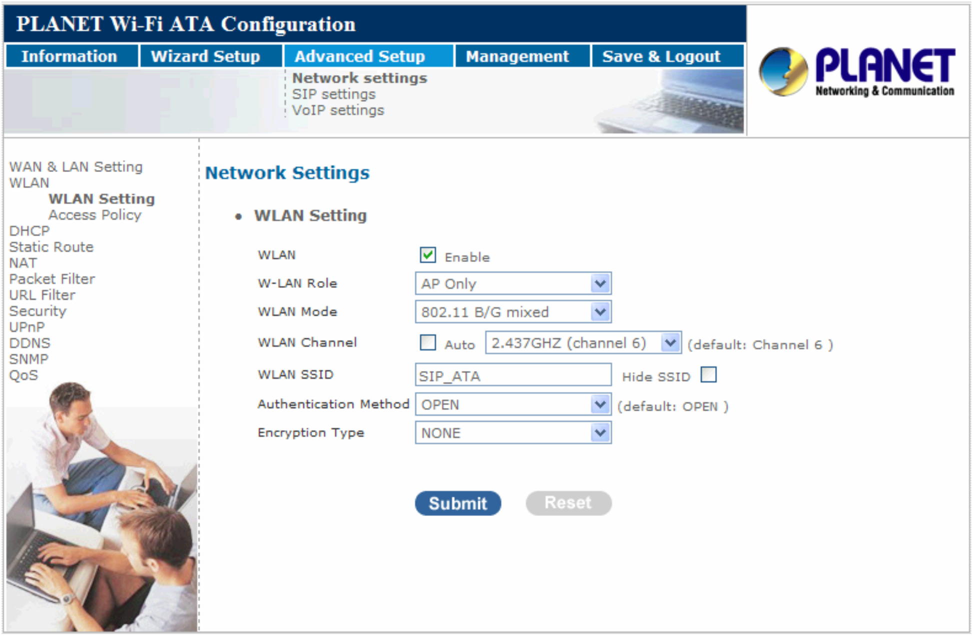
WLAN Setting

A WLAN is a data communication system that reduces the need for a wired connection, thereby adding new flexibility and convenience to your network. Using electromagnetic waves, WLAN's transmits and receives data over the air, minimizing the need for wired connections and combines data connectivity with user mobility.

WLAN Settings

AP Mode

Access Point only Mode, The AP functions as a wireless hub to which wireless clients can connect. The clients must make sure that they are configured to match the AP’s wireless settings. The AP must be connected to switch or other LAN segment patch cable.



Network Settings

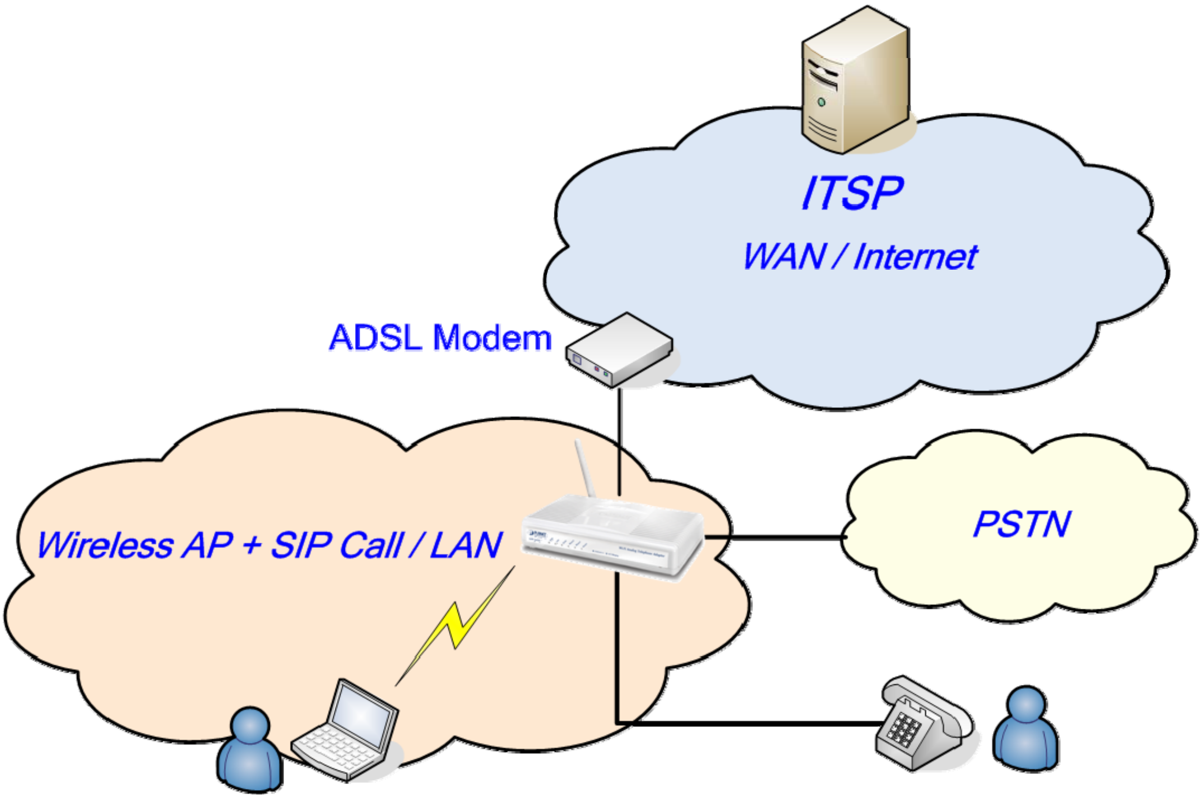
- WLAN Setting

WLAN	☑ Enable
W-LAN Role	AP Only
WLAN Mode	802.11 B/G mixed
WLAN Channel	□ Auto 2.437GHZ (channel 6) (default: Channel 6)
WLAN SSID	SIP_ATA Hide SSID □
Authentication Method	OPEN (default: OPEN)
Encryption Type	NONE

WLAN	Enable / Disable WLAN Function
WLAN Mode	For wireless connected type 802.11 B/G mixed / 802.11b only / 802.11G only
WLAN SSID	Wireless stations associating to the access point must have the same SSID. Enter a descriptive name for the wireless LAN.(support 20 ACSII characters)
Hide SSID	Hide SSID prevents outside users from joining the network without knowing the wireless Network's ID, default is check SSID.
WLAN Frequency	The range of radio frequencies used by IEEE 802.11b/g wireless

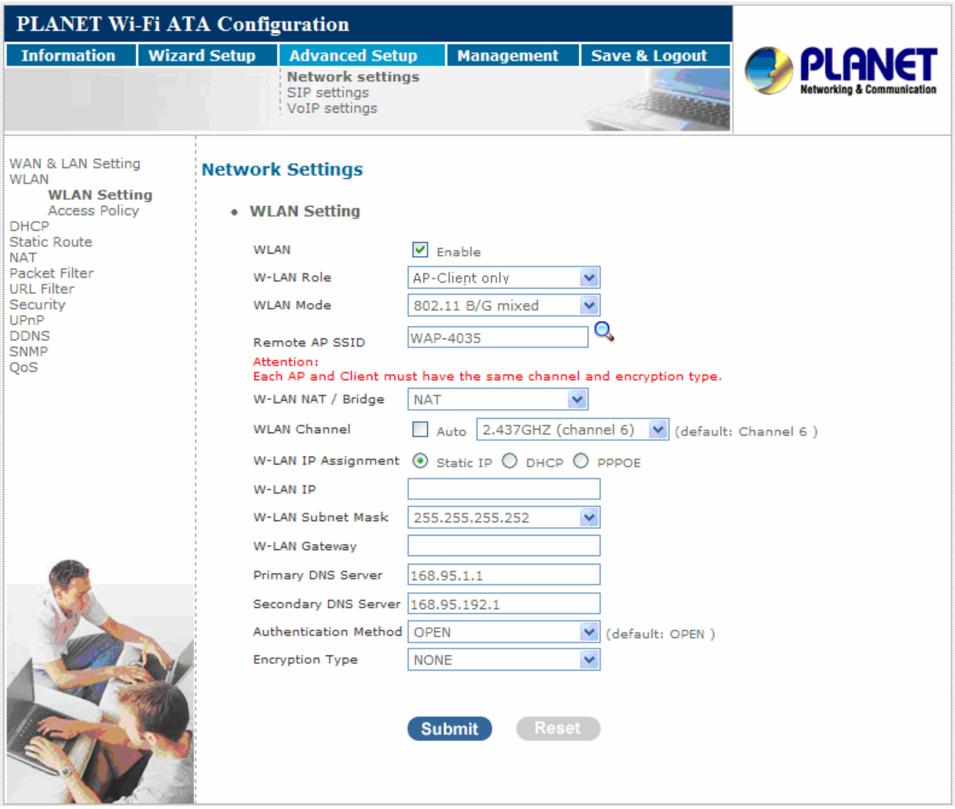
	devices is called a Selection channel. Select a channel ID that is not already in use by a neighboring device.
WLAN Frequency Auto	When the users select this option, the WIFI-ATA automatically finds the channel with the least interference and uses that channel for wireless ATA transmission.
Authentication Method	Select OPEN, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 mix mode, WPA-PSK/WPA2-PSK mix mode .Default is OPEN mode.

Example:



AP-Client Only Mode

In this mode the WATA is used to access the Wireless Service Provider network by connecting wirelessly to the remote (Outdoor AP). The user can access the PSTN network by connecting to the FXS ports or accessing the internet by connecting the PCs to the 2 Ethernet ports.



PLANET Wi-Fi ATA Configuration

Network Settings

- WLAN Setting

WLAN	☑ Enable
W-LAN Role	AP-Client only
WLAN Mode	802.11 B/G mixed
Remote AP SSID	WAP-4035

Attention:
Each AP and Client must have the same channel and encryption type.

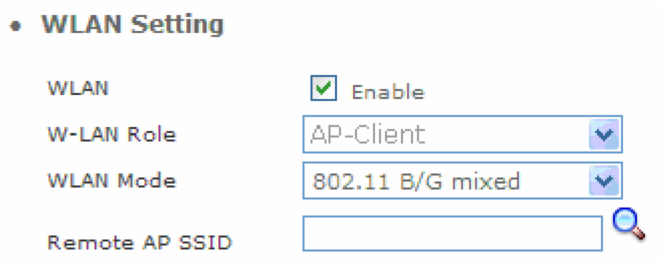
W-LAN NAT / Bridge	NAT
WLAN Channel	□ Auto 2.437GHZ (channel 6) (default: Channel 6)
W-LAN IP Assignment	● Static IP ○ DHCP ○ PPPOE
W-LAN IP	
W-LAN Subnet Mask	255.255.255.252
W-LAN Gateway	
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
Authentication Method	OPEN (default: OPEN)
Encryption Type	NONE

Note

```
When WATA operate in AP-Client Mode, the WAN and LAN RJ-45
interface will be configured as a 2 port switch for connecting
with 2 PCs for access wireless network
```

WLAN Mode	For wireless connected type 802.11 B/G mixed/ 802.11b only / 802.11G only
Remote AP SSID	Define the same as your Wireless Router uses.
Remote AP KEY	Enter the remote AP Authorization Key (WPA-PSK / WPA2-PSK / WPAPSK ,WPA2PSK Mix Mode to Show)
W-LAN Channel	Define the same as your Wireless Router uses.
W-LAN IP Assignment	1. DHCP client 2. Static IP Address

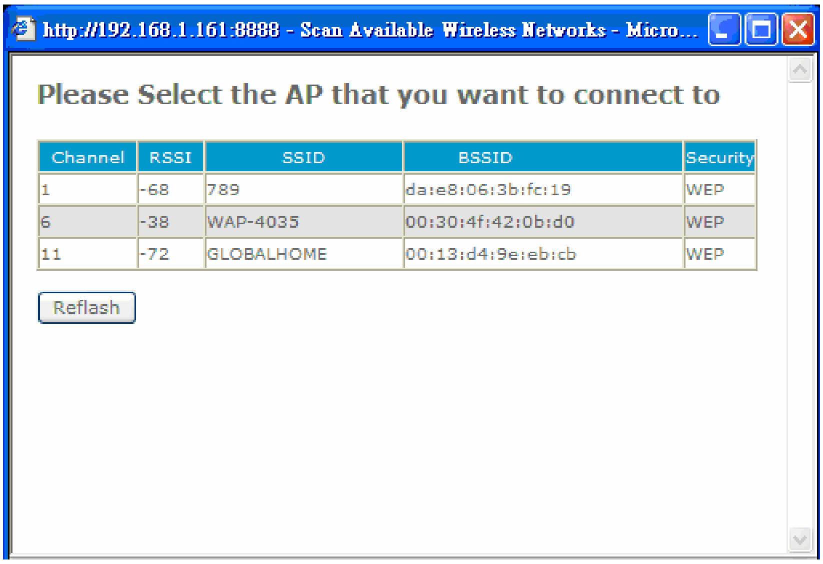
Static IP	Key in the W-LAN IP address, W-LAN Subnet mask and W-LAN Gateway from AP of WISP
DHCP Client	When the DHCP Client is enabled, the WIFI ATA will get the IP Address from Outdoor AP of WISP.
PPPoE Client	Enter User Name / Password provided by your ISP, the WATA will get the IP Address from Outdoor AP of WISP
Remote AP SSID	Define the same as your Wireless Router uses
Authentication Method	Define the same as your Wireless Router uses.(OPEN / SHARED Mode)
Encryption Type	Define the same as your Wireless Router uses. (OPEN / SHARED Mode)



- WLAN Setting

WLAN	☑ Enable
W-LAN Role	AP-Client
WLAN Mode	802.11 B/G mixed
Remote AP SSID	

Scan usable network：Select list to remote AP SSID (magnifying glass)



http://192.168.1.161:8888 - Scan Available Wireless Networks - Micro...

Please Select the AP that you want to connect to

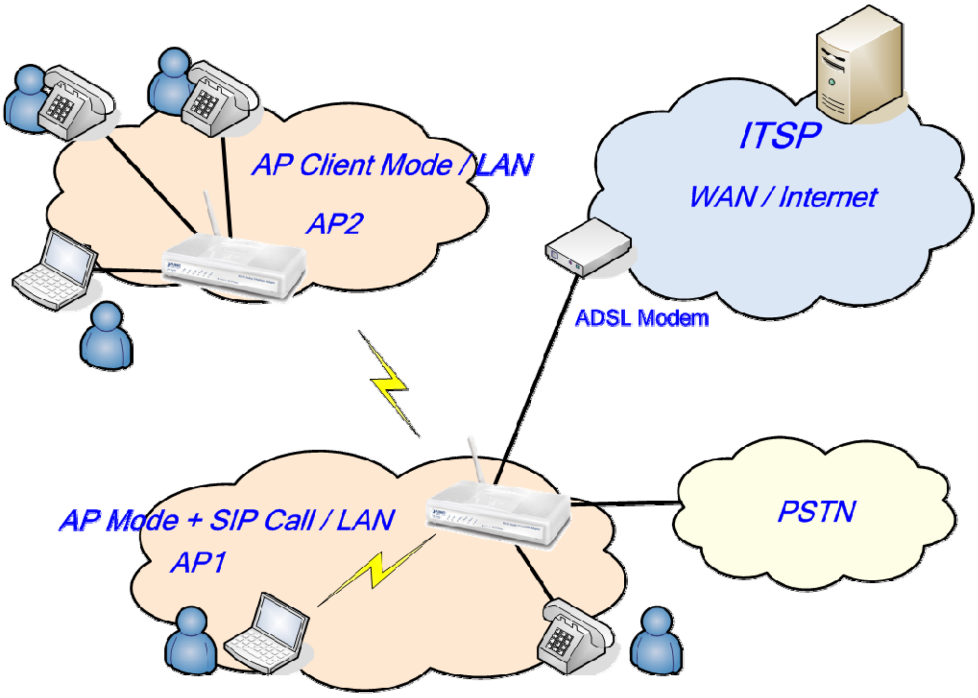
Channel	RSSI	SSID	BSSID	Security
1	-68	789	da:e8:06:3b:fc:19	WEP
6	-38	WAP-4035	00:30:4f:42:0b:d0	WEP
11	-72	GLOBALHOME	00:13:d4:9e:eb:cb	WEP

Search remote AP list page.

Note

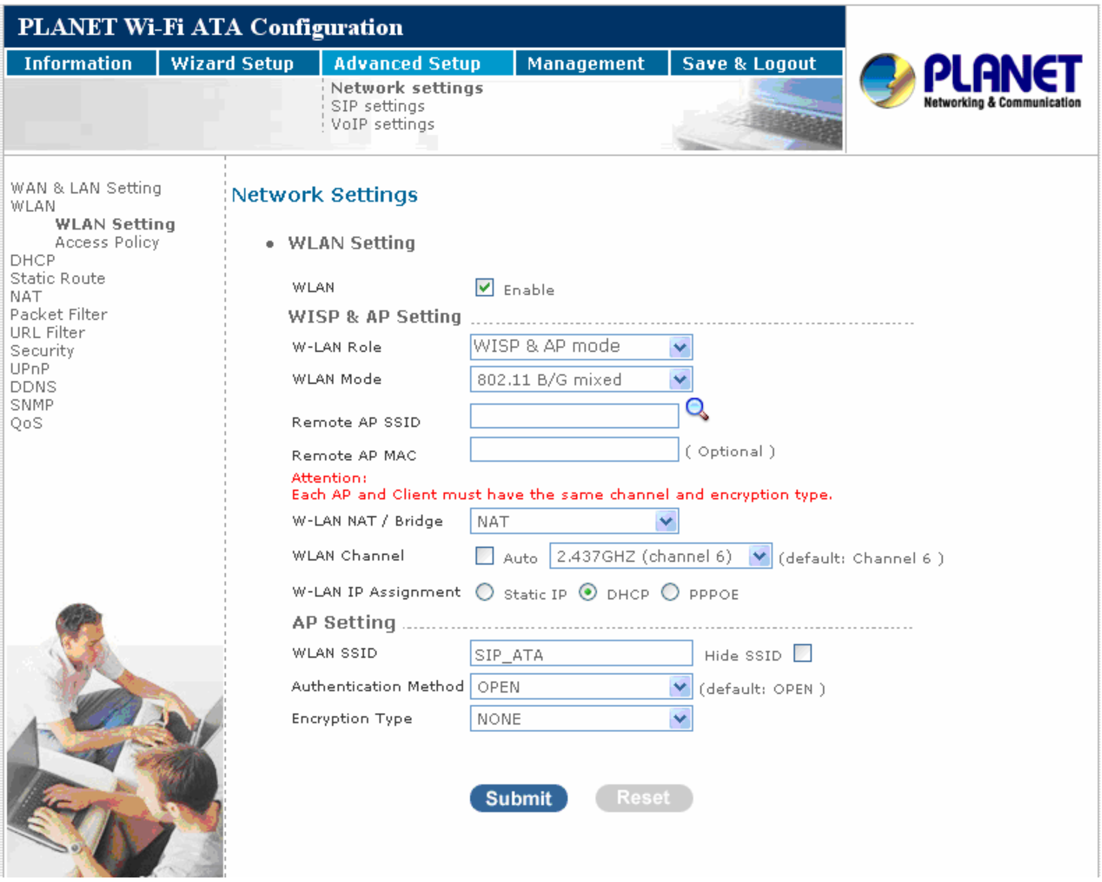
After scan and select the Outdoor AP, the channel and encryption method should be set the identical with the remote AP.

Example:



WISP & AP Mode

The WIFI ATA can operate in AP-Client and access to another (Outdoor) AP. The wireless client needs to have the same SSID, Channel, Encryption settings as the main AP. The user may need to change the default IP to avoid IP conflicts.



Network Settings

- WLAN Setting

WLAN ☑ Enable

WISP & AP Setting

W-LAN Role: WISP & AP mode

WLAN Mode: 802.11 B/G mixed

Remote AP SSID:

Remote AP MAC: (Optional)

Attention:
Each AP and Client must have the same channel and encryption type.

W-LAN NAT / Bridge: NAT

WLAN Channel: □ Auto 2.437GHZ (channel 6) (default: Channel 6)

W-LAN IP Assignment: ○ Static IP ● DHCP ○ PPPOE

AP Setting

WLAN SSID: SIP_ATA Hide SSID □

Authentication Method: OPEN (default: OPEN)

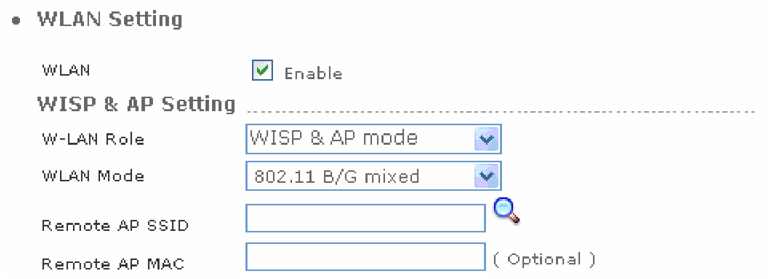
Encryption Type: NONE

Submit Reset

Note

```
When WATA operates in AP-Client (or WISP & AP) Mode, the WAN
and LAN RJ-45 interface will be configured as a 2 port switch
for connecting with 2 PCs for access wireless network.
```

WLAN Mode	For wireless connected type 802.11 B/G mixed/ 802.11b only / 802.11G only
Remote AP SSID	Define the same as your Wireless Router uses
Remote AP MAC	Define the same as your Wireless Router uses
Remote AP Key	Enter the remote AP Authorization Key (WPA-PSK / WPA2-PSK / WPAPSK ,WPA2PSK Mix Mode to Show)
W-LAN Channel	Define the same as your Wireless Router uses
W-LAN IP Assignment	1.DHCP client 2.Static IP Address
Static IP	Key in the W-LAN IP address, W-LAN Subnet mask and W-LAN Gateway from WISP
DHCP Client	When the DHCP Client is enabled, the WATA will get the IP Address from Outdoor AP of WISP
WLAN SSID	The service set identifier assigned to the wireless network (WLAN). Default SSID is SIP_ATA
Hide SSID	Hide SSID prevents outside users from joining the network without knowing the wireless Network's ID, default is check SSID
Authentication Method	Define the same as your Wireless Router uses. (OPEN / SHARED Mode)
Encryption Type	Define the same as your Wireless Router uses. (OPEN / SHARED Mode



- WLAN Setting

WLAN ☑ Enable

WISP & AP Setting

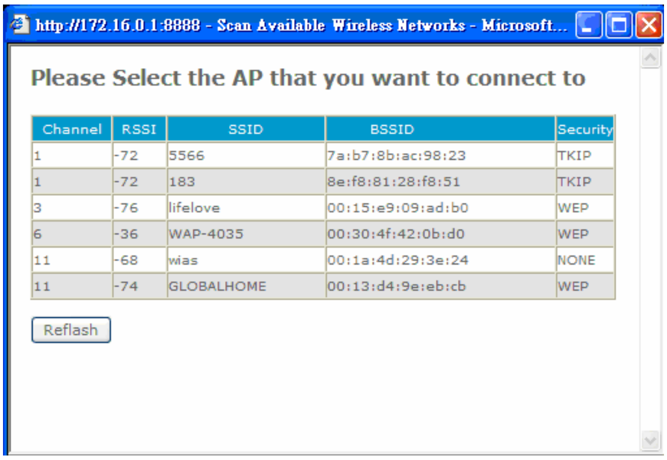
W-LAN Role: WISP & AP mode

WLAN Mode: 802.11 B/G mixed

Remote AP SSID:

Remote AP MAC: (Optional)

Scan usable network：Select list to remote AP SSID (magnifying glass)



http://172.16.0.1:8888 - Scan Available Wireless Networks - Microsoft...

Please Select the AP that you want to connect to

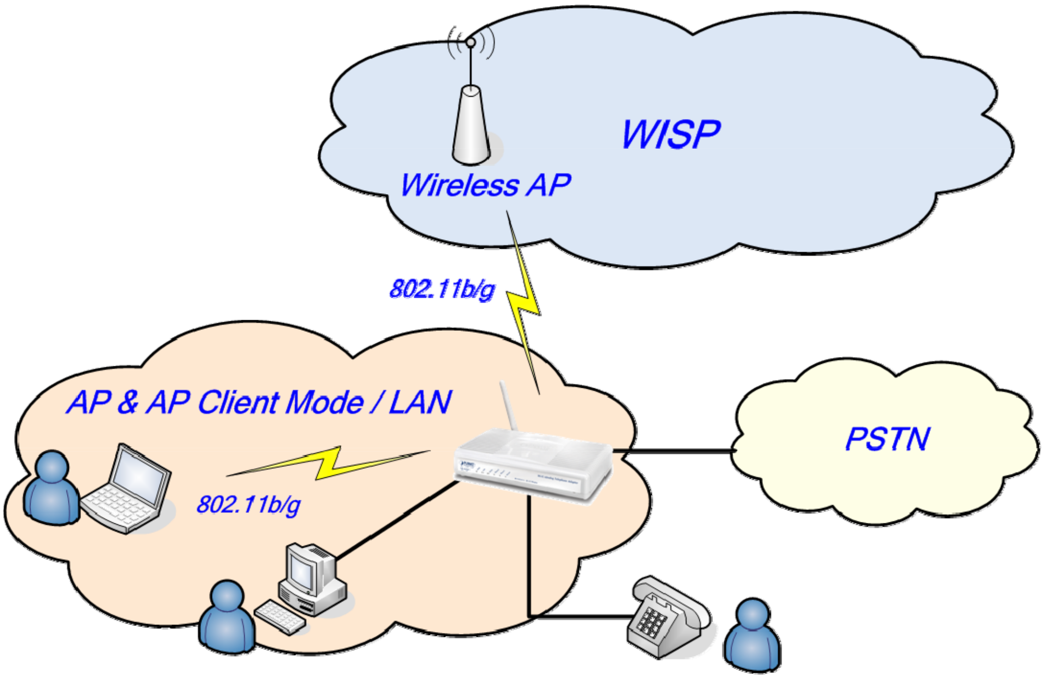
Channel	RSSI	SSID	BSSID	Security
1	-72	5566	7a:b7:8b:ac:98:23	TKIP
1	-72	183	8e:f8:81:28:f8:51	TKIP
3	-76	lifelove	00:15:e9:09:ad:b0	WEP
6	-36	WAP-4035	00:30:4f:42:0b:d0	WEP
11	-68	wias	00:1a:4d:29:3e:24	NONE
11	-74	GLOBALHOME	00:13:d4:9e:eb:cb	WEP

Search remote AP list page

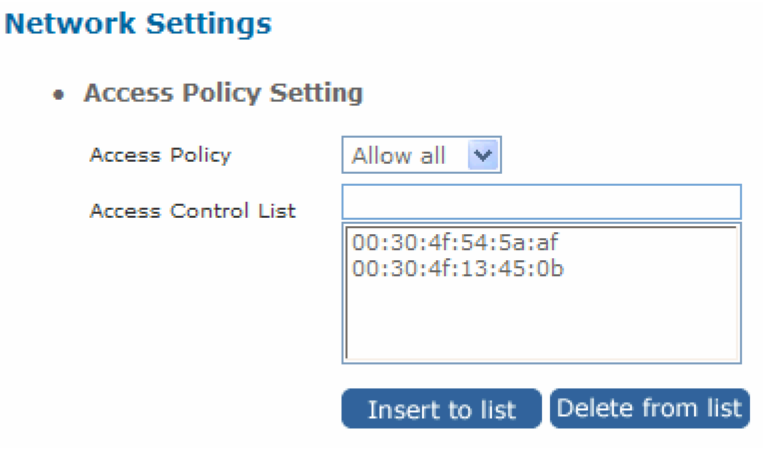
Note

```
After scan and select the Outdoor AP, the channel and
encryption method should be identical with the remote AP
```

Example:



Access Policy (For AP and AP& AP-Client mode only)

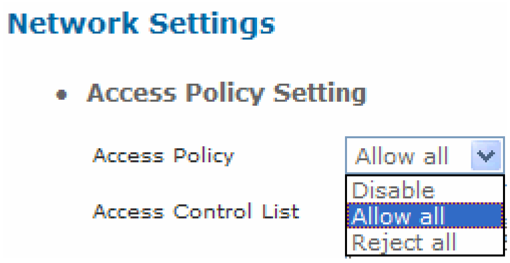


Network Settings

- Access Policy Setting

Access Policy: Allow all

Access Control List:
00:30:4f:54:5a:af
00:30:4f:13:45:0b



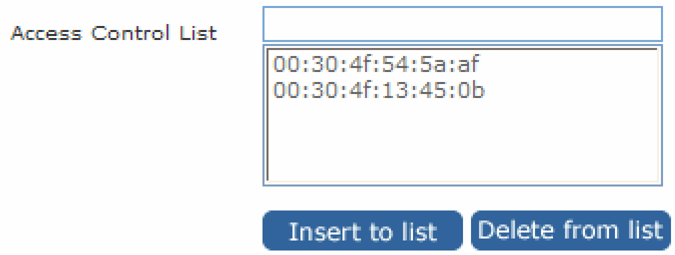
Network Settings

- Access Policy Setting

Access Policy: Allow all

Access Control List

Access Policy: in WATA security, an access control list is a list of “allow all / Reject all" to an MAC.



Access Control List:
00:30:4f:54:5a:af
00:30:4f:13:45:0b

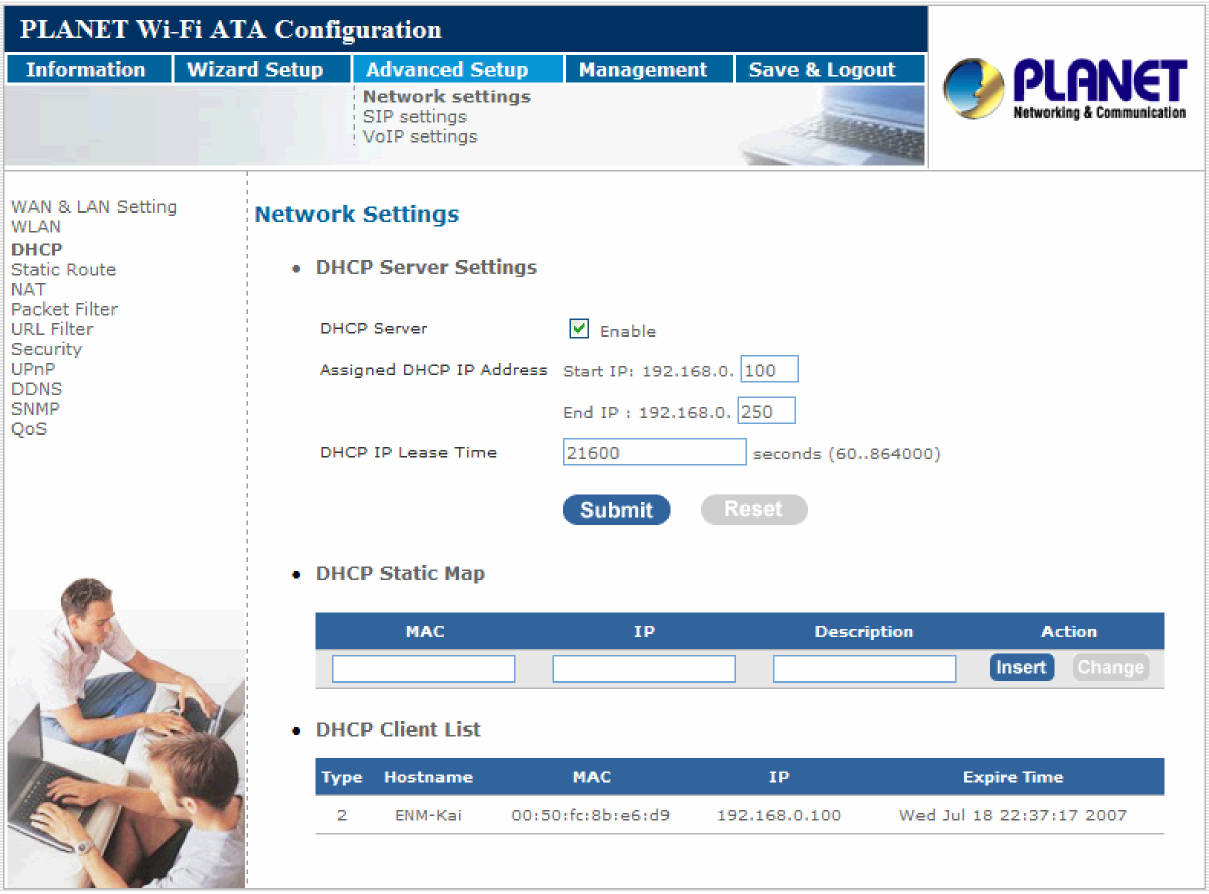
Access Control List：MAX MAC List：64.

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.

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:



Network Settings

- DHCP Server Settings

DHCP Server ☑ Enable

Assigned DHCP IP Address Start IP: 192.168.0. 100

End IP : 192.168.0. 250

DHCP IP Lease Time 21600 seconds (60..864000)

- DHCP Static Map

MAC	IP	Description	Action
			Insert Change

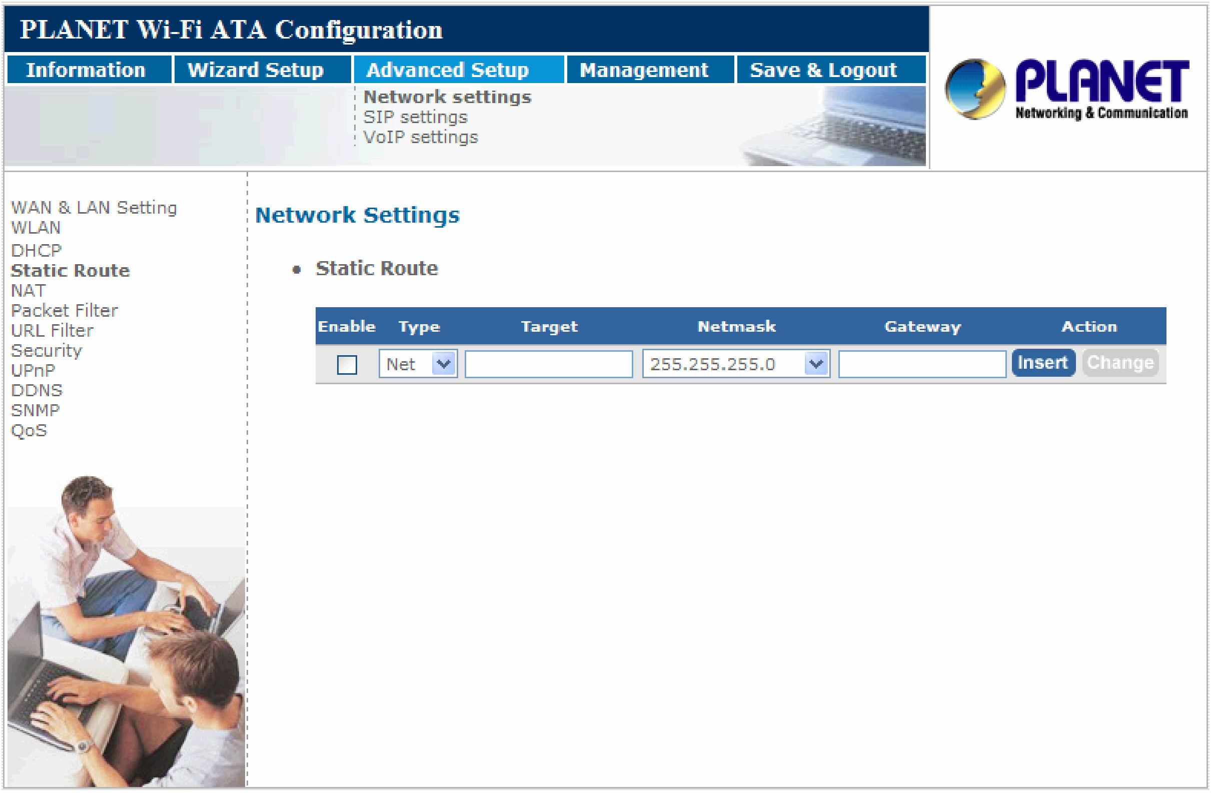
- DHCP Client List

Type	Hostname	MAC	IP	Expire Time
2	ENM-Kai	00:50:fc:8b:e6:d9	192.168.0.100	Wed Jul 18 22:37:17 2007

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.

Static Router

For use when managing local networks. Static routes are special routes that the network administrator manually enters into the router configuration. You could build an entire network based on static routes. The problem with doing this is that when a network failure occurs, the static route will not change without you performing the change. This could be fatal if the failure occurs when the administrator is not available. The route table allows the user to configure and define all the static routes supported by the router.



Network Settings

- Static Route

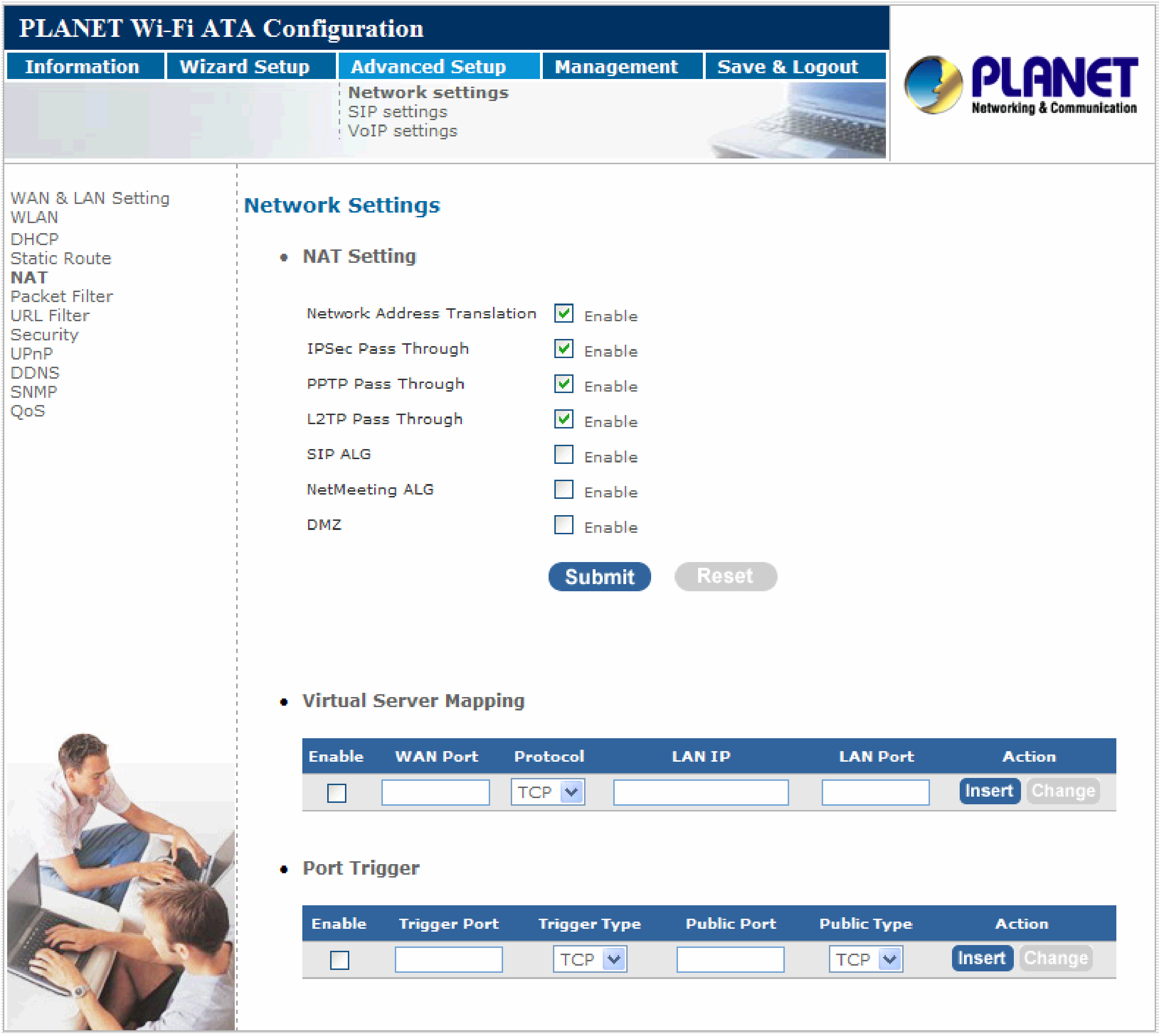
Enable	Type	Target	Netmask	Gateway	Action
□	Net		255.255.255.0		Insert Change

Enable	Enable/Disable the static route
Type	Indicates the type of route as follows, Host for local connection and Net for network connection
Target	Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route
NetMask	The subnet mask that will be AND'd with the destination IP address and then compared with the Target to see if this is the target route.
Gateway	The IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP address of the router
Action	Insert a new Static Router entry or update a specified entry

NAT (for AP / AP-Client / WISP & AP mode)

NAT (Network Address Translation) serves three purposes:

- Provides security by hiding internal IP addresses. Acts like firewall.
- Enables a company to access internal IP addresses. Internal IP addresses that are only available within the company will not conflict with public IP.
- Allows a company to combine multiple ISDN connections into a single internet connection.



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

Submit Reset

- 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.

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.

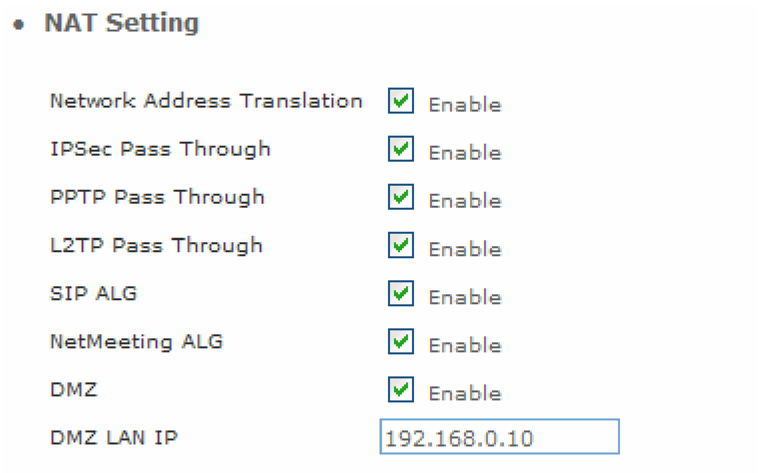
L2TP Pass Through：L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task

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.

DMZ LAN IP：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.



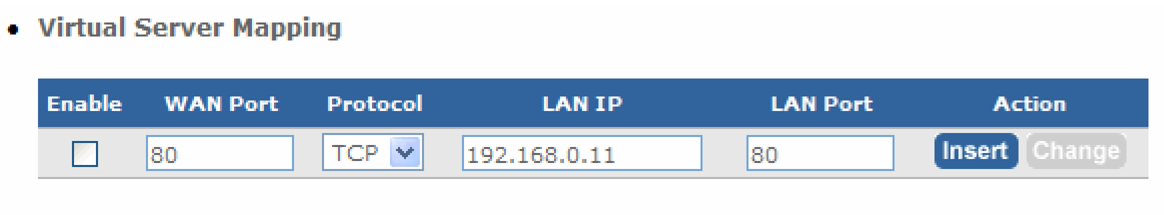
- NAT Setting

Network Address Translation	☑ Enable
IPSec Pass Through	☑ Enable
PPTP Pass Through	☑ Enable
L2TP Pass Through	☑ Enable
SIP ALG	☑ Enable
NetMeeting ALG	☑ Enable
DMZ	☑ Enable
DMZ LAN IP	192.168.0.10

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.



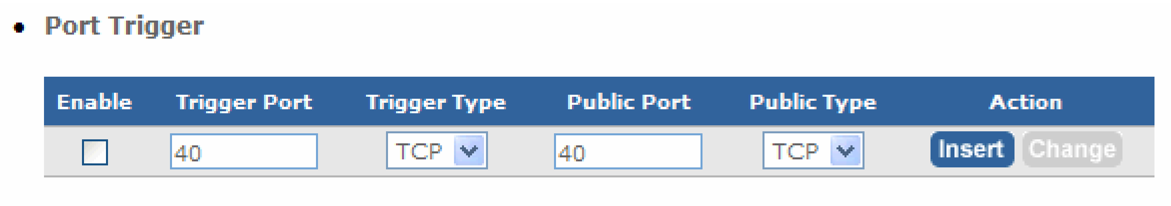
- Virtual Server Mapping

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
□	80	TCP	192.168.0.11	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

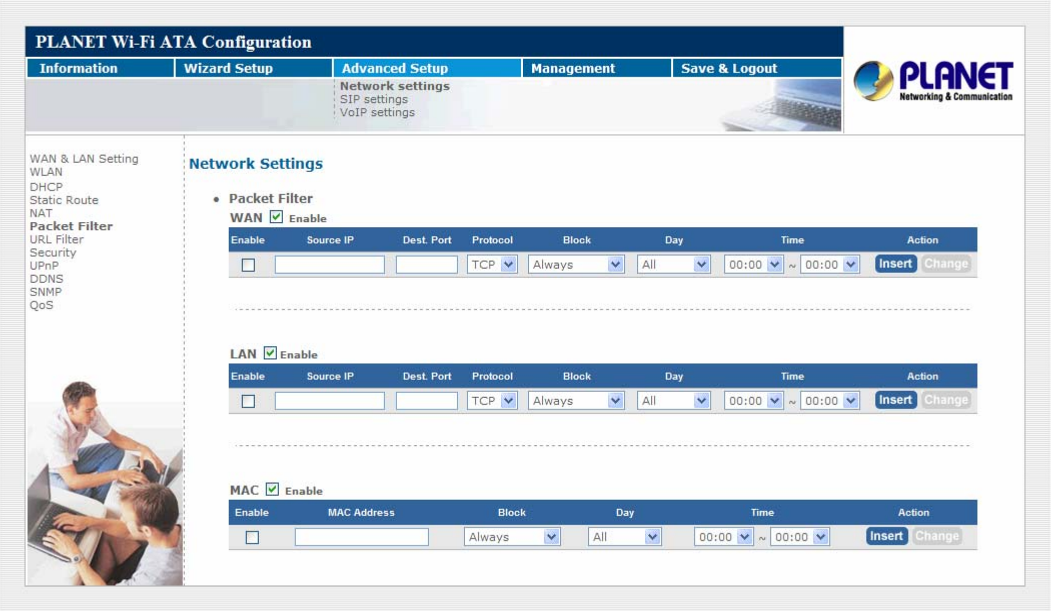
Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
□	40	TCP	40	TCP	Insert Change

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.

Packet Filter

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

(Can be useful for residential screening as well – for parental screening or other)



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

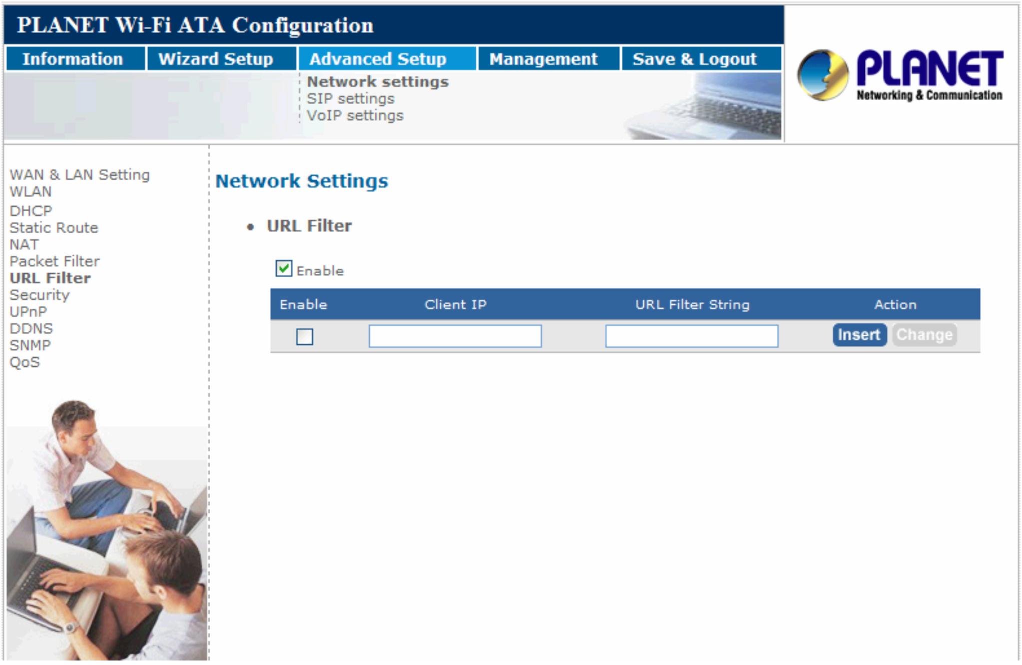
MAC ☑ Enable

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

WAN / LAN 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 Disabling
Source IP	This is the filter WAN IP address
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

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.



☑ Enable

Enable	Client IP	URL Filter String	Action
□			Insert Change

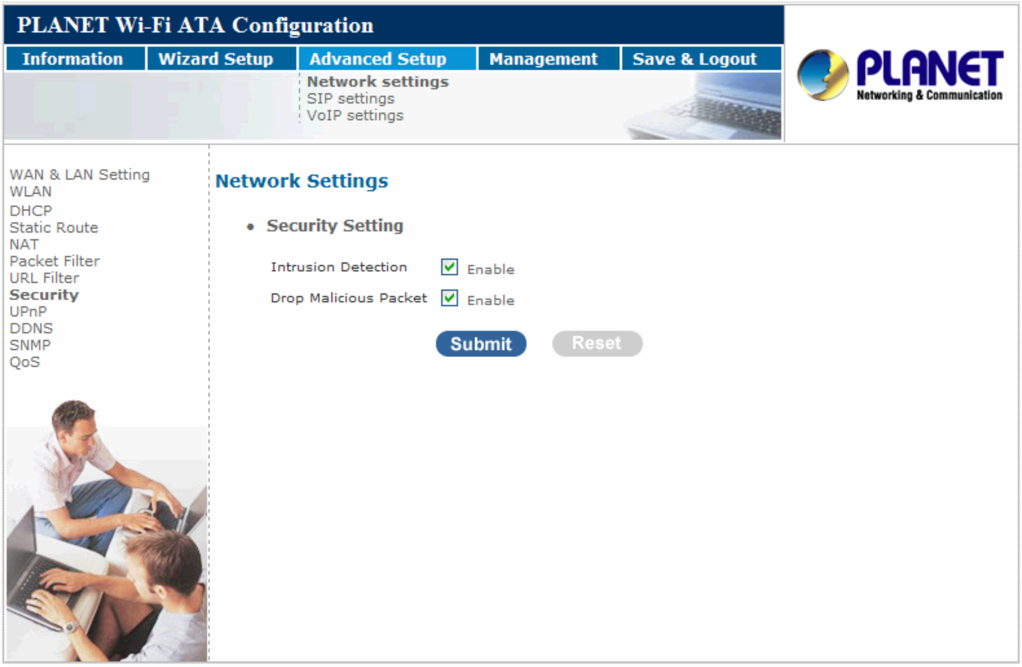
Enable	Enable/Disable the URL filter function, default setting is Disable
Enable	Enable/Disable Block URL to the client IP, default setting is Disable
Client IP	This is the client IP is LAN address.
URL Filter String	This is the filter URL.

Security (For AP / WISP & AP mode)

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.

Intrusion Detection：Enable / Disable the network / Internet security protection.

Drop Malicious Packet：Enable / Disable, Detect and drop malicious application layer traffic.



Network Settings

- Security Setting

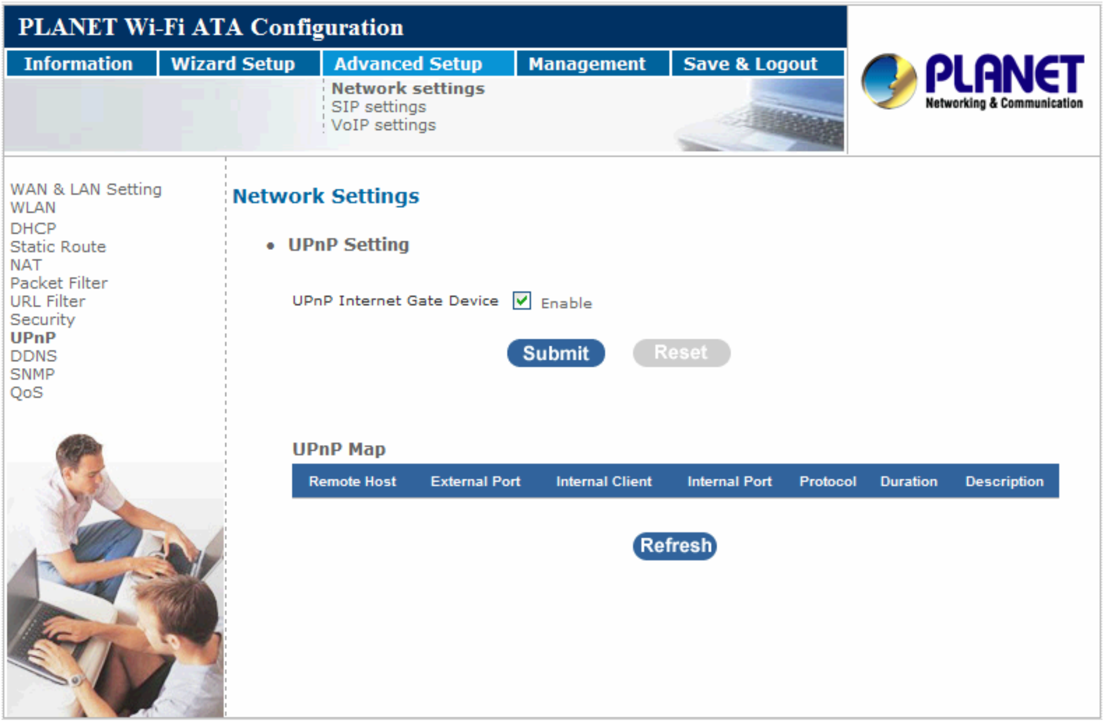
Intrusion Detection ☑ Enable

Drop Malicious Packet ☑ Enable

UPNP (For AP / WISP & AP mode)

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.

UPNP Internet Gate Device: Enable/Disable UPnP Service to working, default setting is Disable.



Network Settings

- UPnP Setting

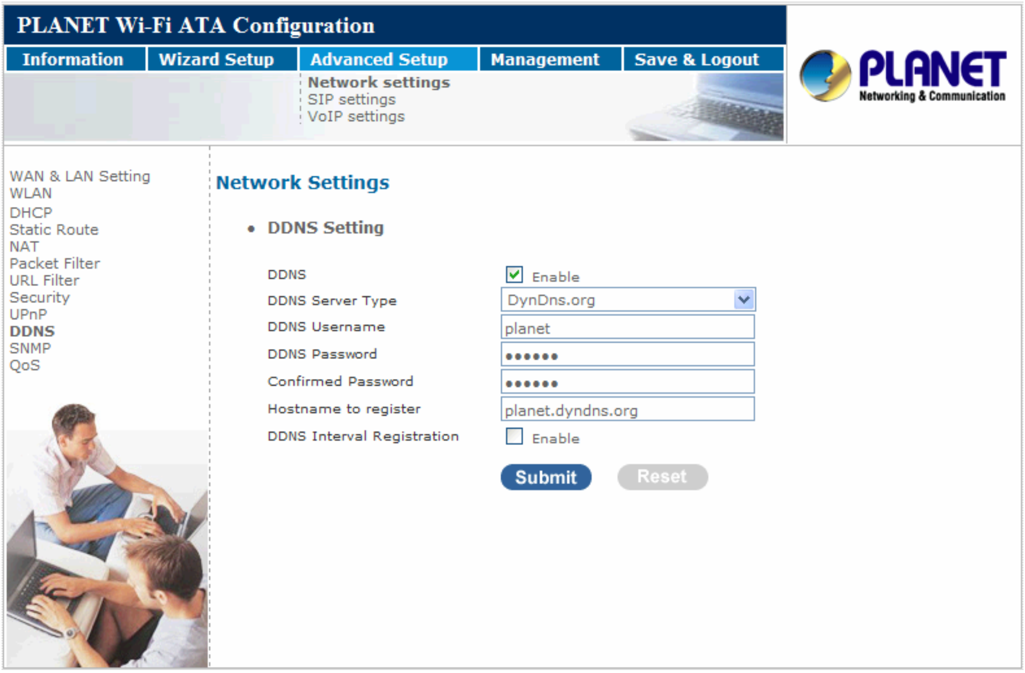
UPnP Internet Gate Device ☑ Enable

UPnP Map

Remote Host	External Port	Internal Client	Internal Port	Protocol	Duration	Description

DDNS (For AP / WISP & AP mode)

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. 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 net workers, who typically receive dynamic, frequently-changing IP addresses from their service provider.



Network Settings

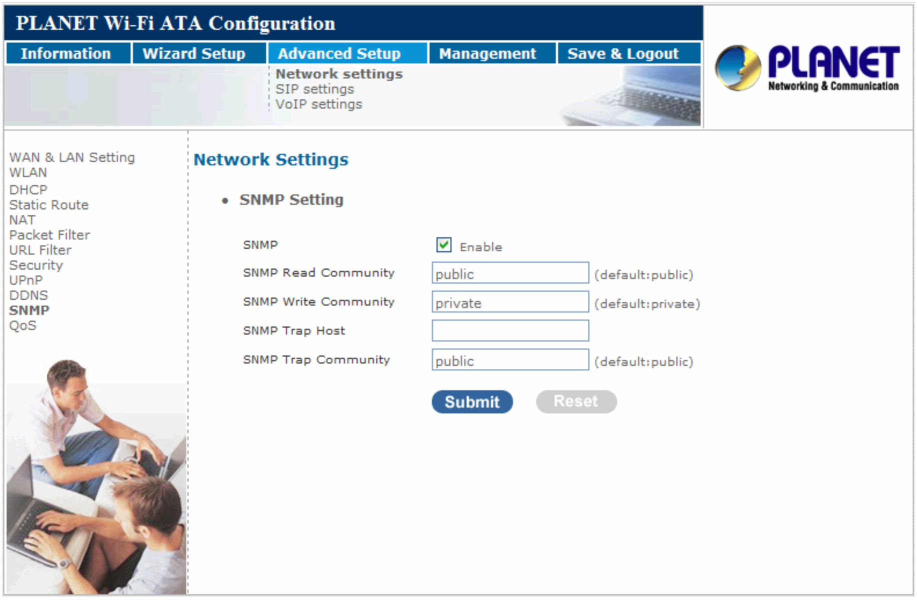
- DDNS Setting

DDNS	☑ Enable
DDNS Server Type	DynDns.org
DDNS Username	planet
DDNS Password	••••••
Confirmed Password	••••••
Hostname to register	planet.dyndns.org
DDNS Interval Registration	□ Enable

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

SNMP (For AP / WISP & AP mode)

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

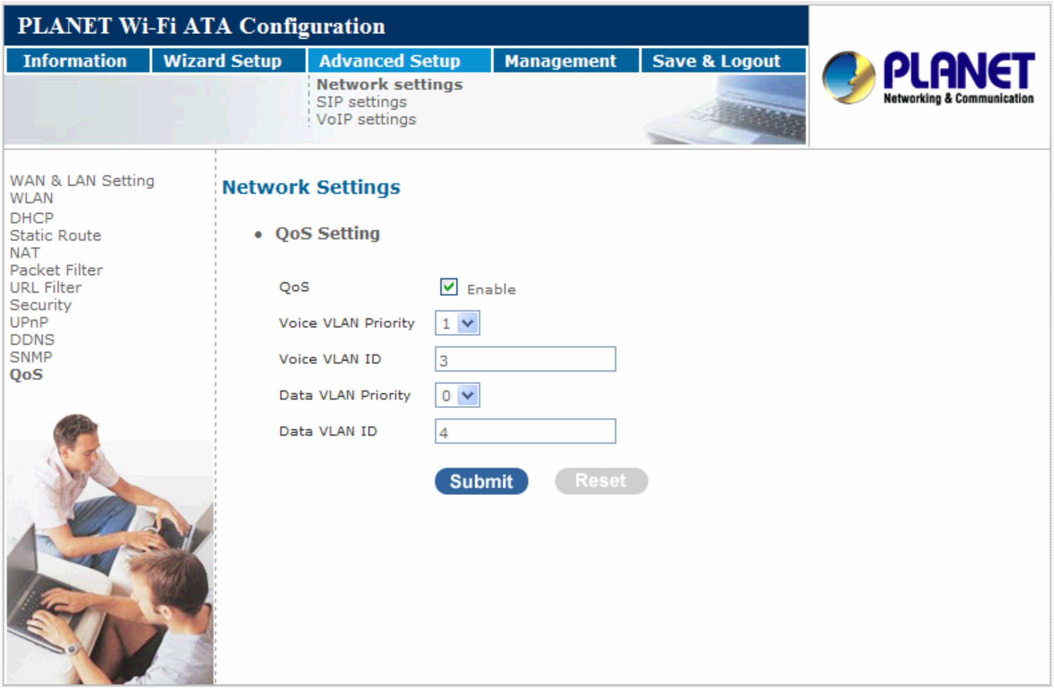
- SNMP Setting

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)

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

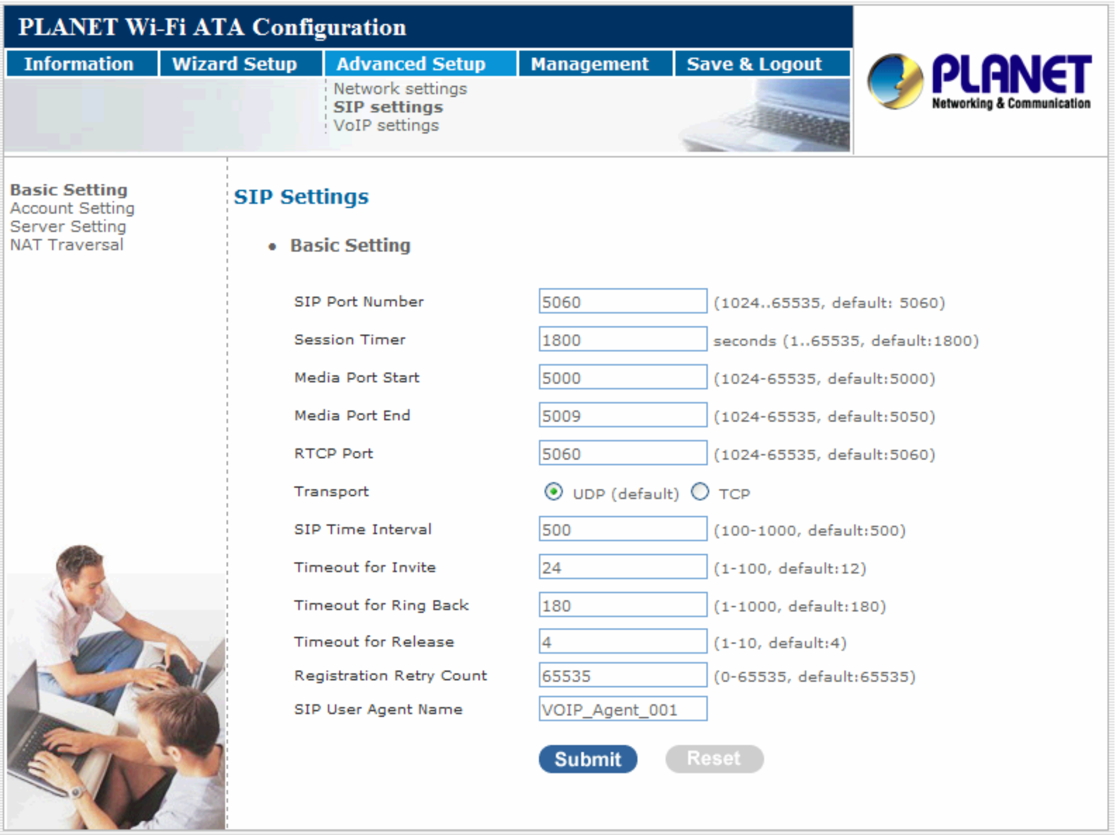
Chapter 4

Wireless Telephone Adapter Configurations

SIP Configuration

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**



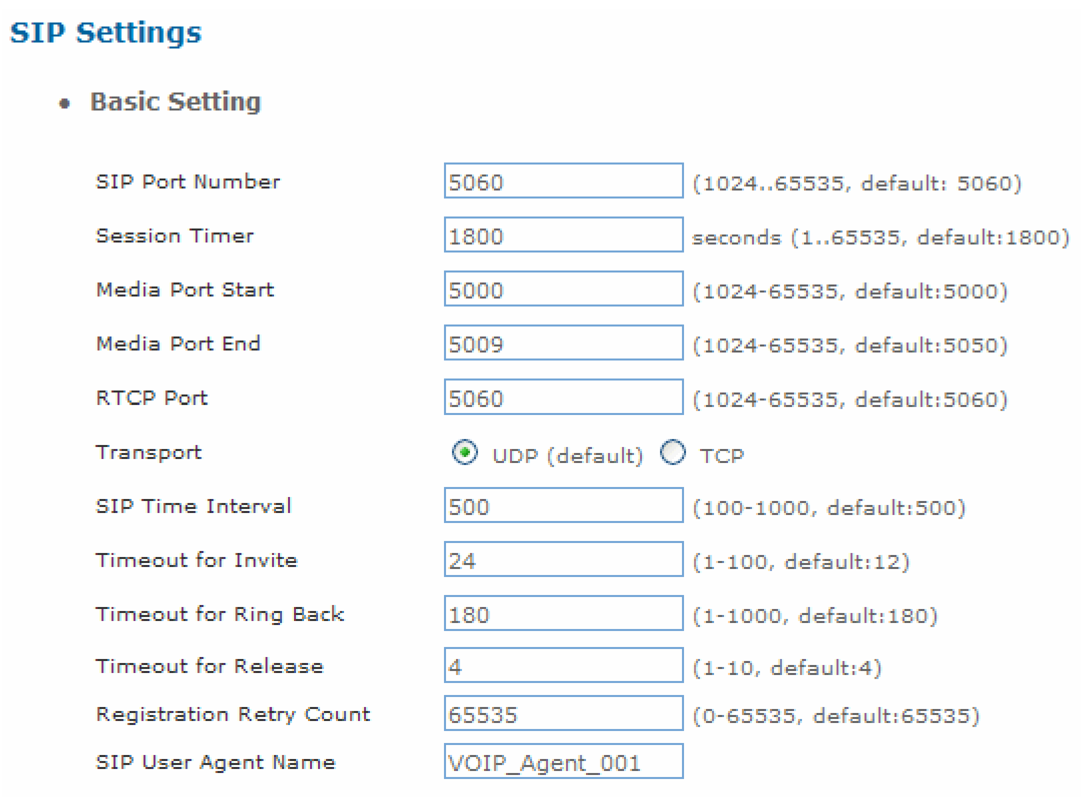
SIP Settings

- 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	

Basic Setting

This page defines the SIP and RTP port number in this page. Each ISP provider will have different SIP/RTPport setting, please refer to the ISP to setup the port number correctly. When you finished the setting, please click the Submit button.



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	

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 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. Its range is 1024 to 65535, default setting is 5060
Transport	Assigns the default SIP transport protocol
UDP	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

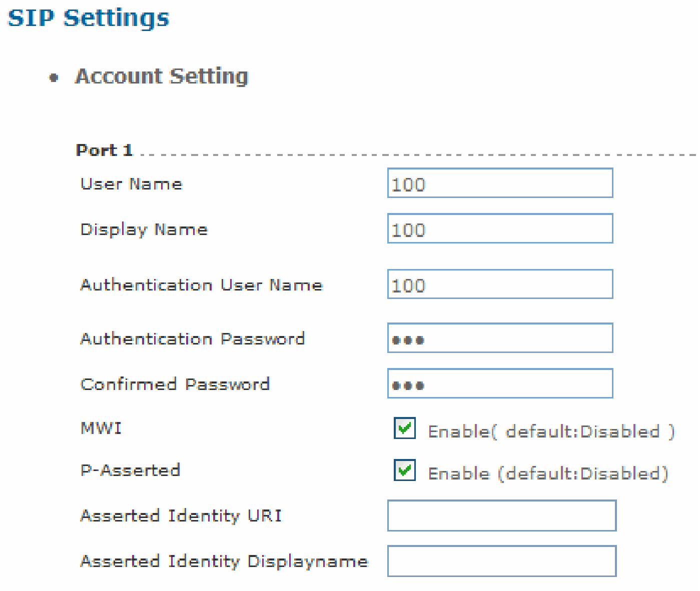
TCP	TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent
SIP Time Interval	SIP time interval in milliseconds. The default setting is 500 m-sec
Timeout for Invite	INVITE message timeout value. Assigns a value 1 to 100, default setting 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 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 specified, 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

Account Setting

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 1234-5678, then it should be 886212345678
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 Display name	Enter your Display name, Maximum 24 characters



SIP Settings

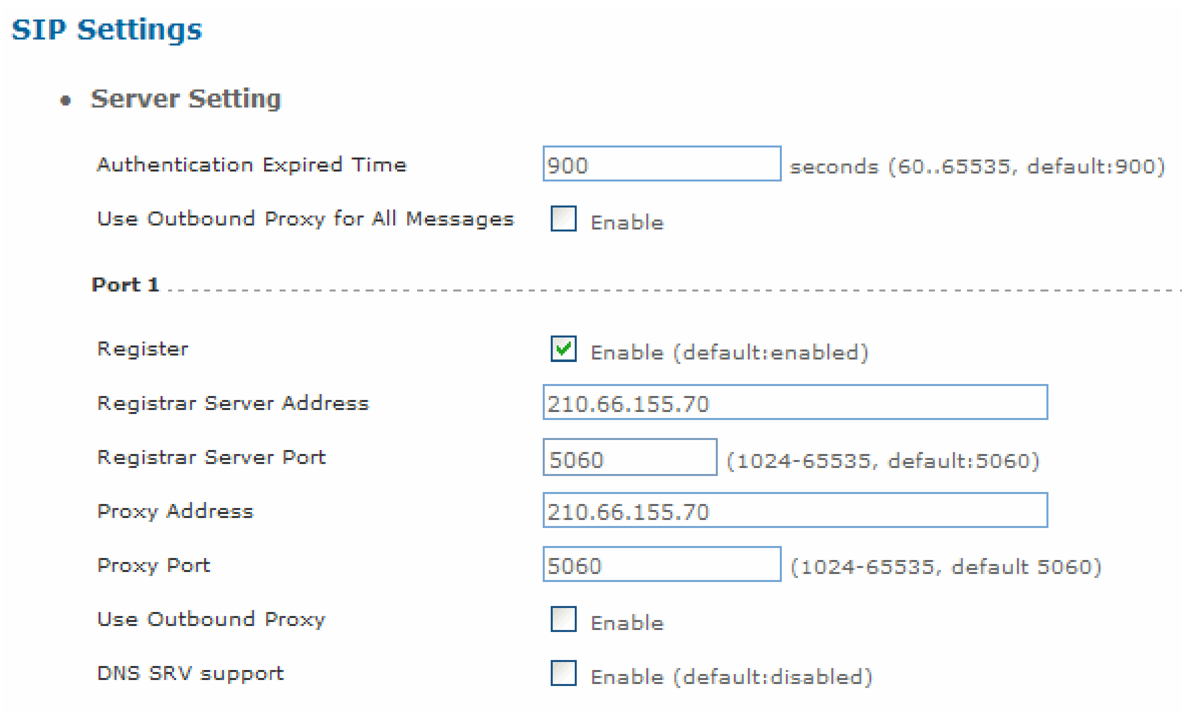
- Account Setting

Port 1

User Name	100
Display Name	100
Authentication User Name	100
Authentication Password	●●●
Confirmed Password	●●●
MWI	☑ Enable(default:Disabled)
P-Asserted	☑ Enable (default:Disabled)
Asserted Identity URI	
Asserted Identity Displayname	

Server Setting

In Server Setting you need to input the SIP Server related informations in this page, please refer to your ISP provider.



SIP Settings

- Server Setting

Authentication Expired Time	900 seconds (60..65535, default:900)
Use Outbound Proxy for All Messages	□ Enable

Port 1

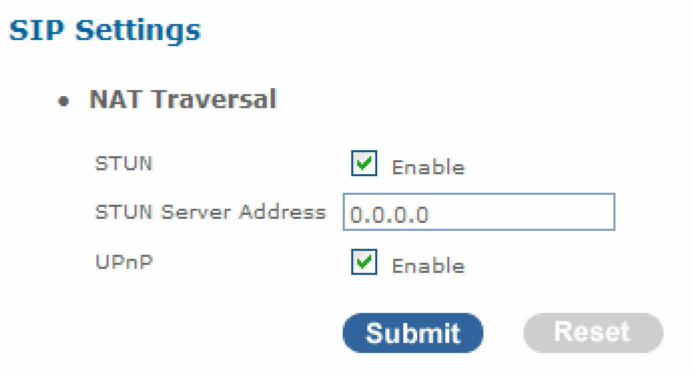
Register	☑ Enable (default:enabled)
Registrar Server Address	210.66.155.70
Registrar Server Port	5060 (1024-65535, default:5060)
Proxy Address	210.66.155.70
Proxy Port	5060 (1024-65535, default 5060)
Use Outbound Proxy	□ Enable
DNS SRV support	□ Enable (default:disabled)

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

NAT Traversal

STUN 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.

UPnP: Enable/Disable Universal Plug and Play, default setting is Disable.



SIP Settings

- NAT Traversal

STUN	☑ Enable
STUN Server Address	0.0.0.0
UPnP	☑ Enable

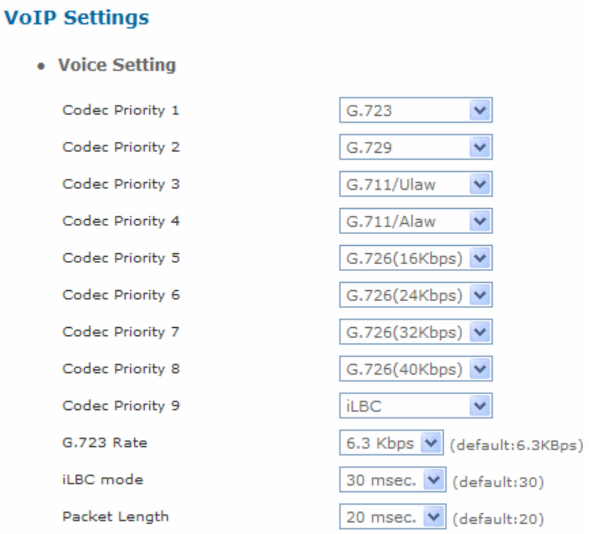
VoIP Setting

This page defines the Voice, Call service, FXS / FAX, General Dialing, URI Phone Book, Call Screen, QoS Setting. You need to follow the ISP suggestion to setup these items. When you finished the setting, please click the Submit button.

Voice Setting

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, G.726 (16K bps), G.726 (24K bps), G.726 (32K bps), G.726 (40K bps), and iLBC.



VoIP Settings

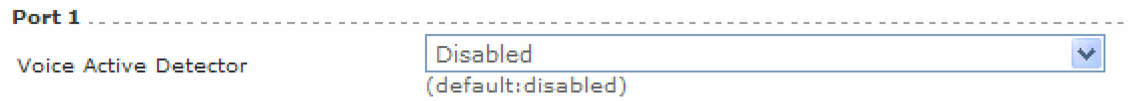
- Voice Setting

Codec Priority 1	G.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)

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, 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

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.

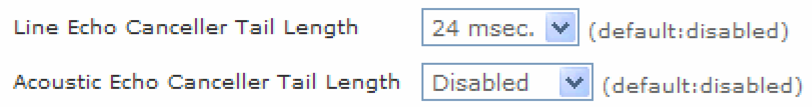


Port 1

Voice Active Detector: Disabled (default:disabled)

Echo Canceller

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: 24 msec. (default:disabled)

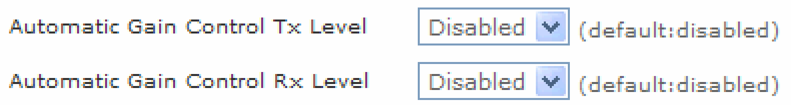
Acoustic Echo Canceller Tail Length: Disabled (default:disabled)

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

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 / Rx Level：Automatic voice gain control for transmitting. Default setting is in Disable mode.

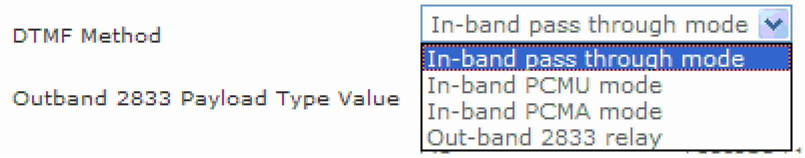


Automatic Gain Control Tx Level: Disabled (default:disabled)

Automatic Gain Control Rx Level: Disabled (default:disabled)

DTMF Method

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 "In-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: In-band pass through mode

Outband 2833 Payload Type Value

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

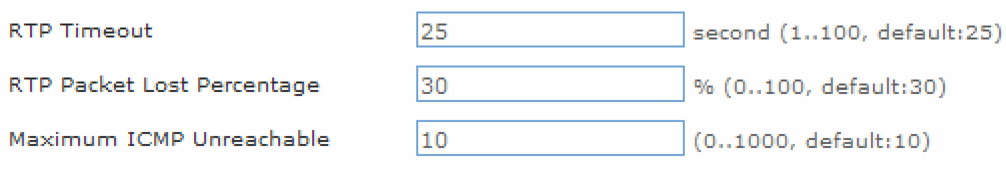
In-band	For voice data. The In-band signaling is the sending of metadata and control information in the same channel used for data. There are three type of mode can be selected: In-band pass through mode, In-band PCMU mode, and In-band PCMA mode
Out-band	For RFC-2833, that is, sending the DTMF tone as 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 2. Signaling via a different channel (either FDM or TDM) from that used for the primary information transfer

Note

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

RTP (Real-time Transport Protocol)

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 30 % (0..100, default:30)

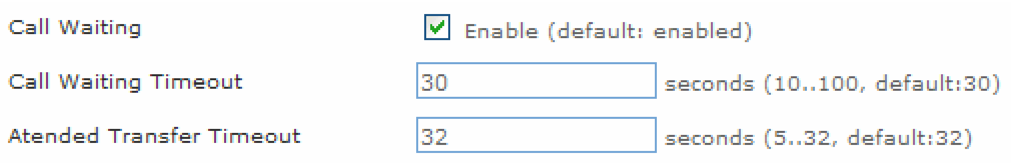
Maximum ICMP Unreachable 10 (0..1000, default:10)

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 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

Call Service

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 32 seconds (5..32, 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.

Port 1

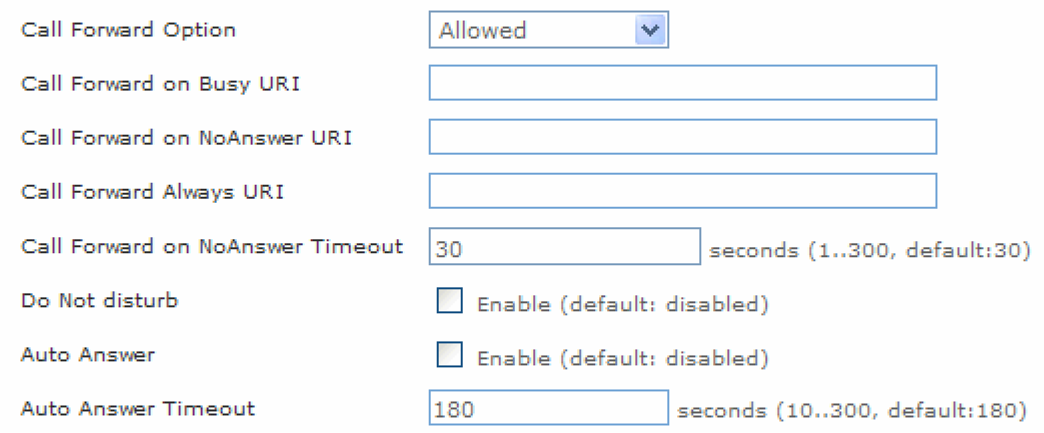
Call Transfer Option: Allowed

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	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



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

Hot Line	□ Enable (default: disabled)

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.

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

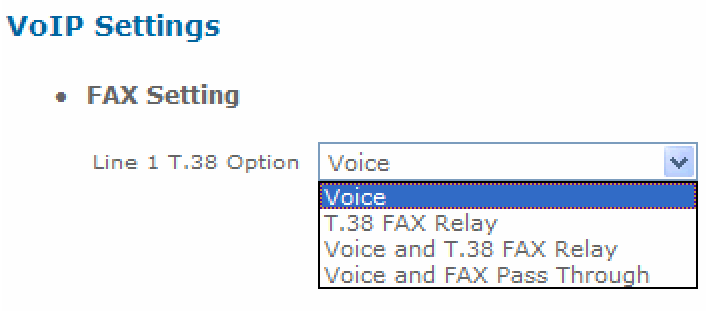
Caller ID Display	There are two types to display the caller information on the screen. Before Ring, the caller id information is displayed before first ring. After Ring, the caller id information is displayed between first ring and second ring. Default setting is Before Ring
Caller ID Type 1 Alerting 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

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

Line 1 T.38 Option: Voice

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

General Dialing Setting

Inter-digit Timeout: If no other number is being dialed within this interval, the Telephony WATA 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**.

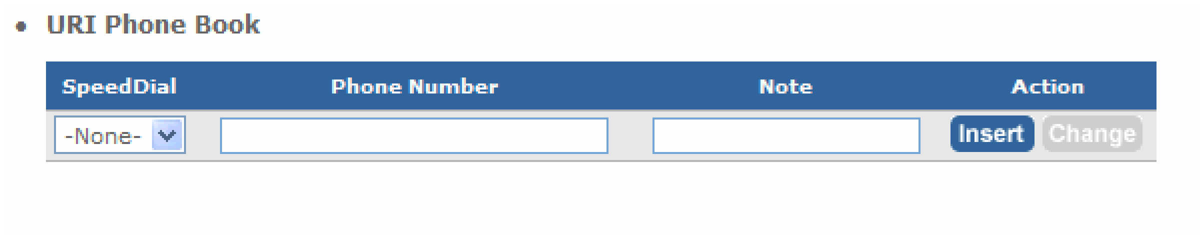
Hold Call Key: Keys to be pressed will be holding a call. The default setting is ***1**.

Send #：Enable/Disable, Default is Enable. Speed dial, after final dial don’t need wait inter-digit time.

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.

Speed Dial: Select the speed dial shortcut to use from #1 to #9.
Phone Number: Enter the international number to dial.
Note: Note descriptions for the Phone member.



- URI Phone Book

SpeedDial	Phone Number	Note	Action
-None-			Insert Change

Dialing Plan (Outgoing Mode)

The "**Dialing plan**" needs setting when the users 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 (Outgoing):

Peer-to-Peer Call Mode

Registering to SIP Proxy Server Mode

Note

Press RESET in the "Dial Plan Configurations (Outgoing)" setting
Maximum Entries: 30

Outbound number：is the leading digits of the call out dialing number.

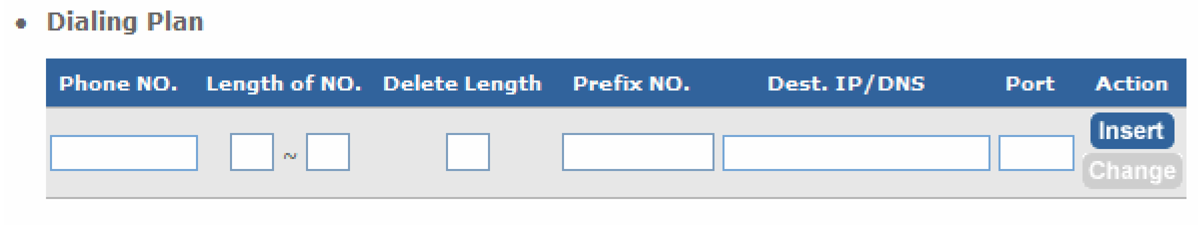
Length of Number：has two text fields need filled: "Min Length" and "Max Length" is the min/max allowed length you can dial.

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 WATA (Gateway) that owns this phone number.

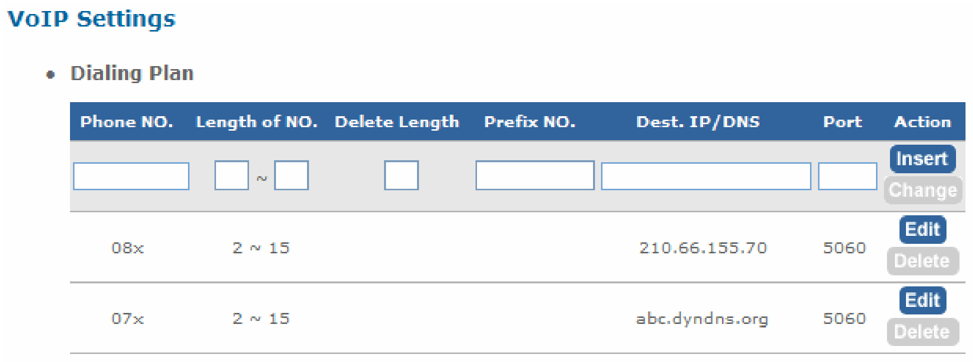
Destination Port：is port of the destination WATA (Gateway) use.(Default is 5060)



- Dialing Plan

Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change

Example_1



VoIP Settings

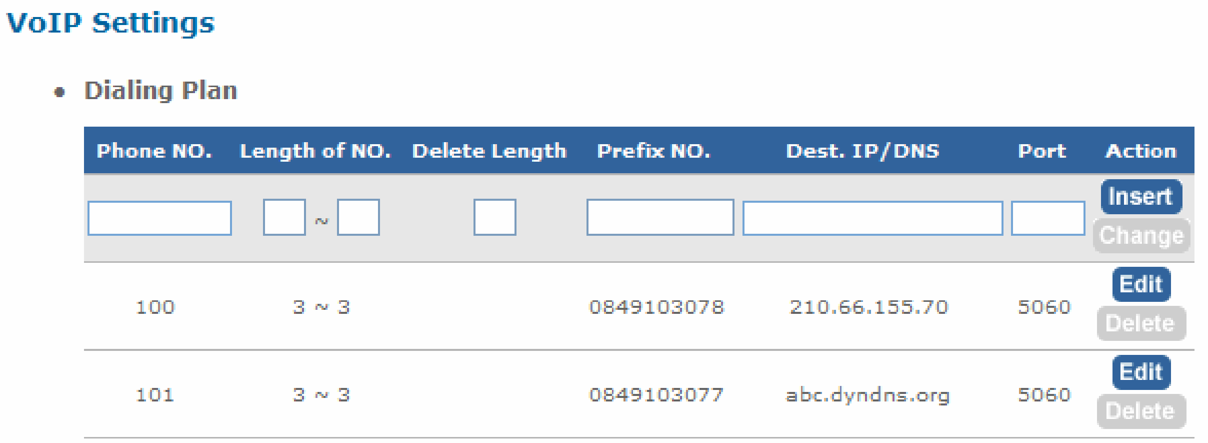
- Dialing Plan

Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change
08x	2 ~ 15			210.66.155.70	5060	Edit Delete
07x	2 ~ 15			abc.dyndns.org	5060	Edit Delete

1.08x leading call out, call to Destination IP address: 210.66.155.70

2.07x leading call out, call to Destination Domain Name: abc.dyndns.org

Example_2



VoIP Settings

- Dialing Plan

Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change
100	3 ~ 3		0849103078	210.66.155.70	5060	Edit Delete
101	3 ~ 3		0849103077	abc.dyndns.org	5060	Edit Delete

1. If user dial “100”,

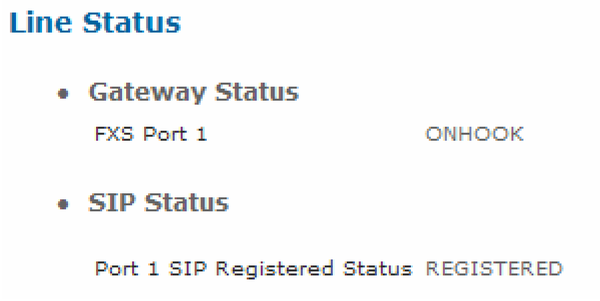
ATA automatically dial “0849103078” to Destination IP address 210.66.155.70

2. If user dial “101”,

ATA automatically dial “0849103077” to Destination IP address abc.dyndns.org

Example_3

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



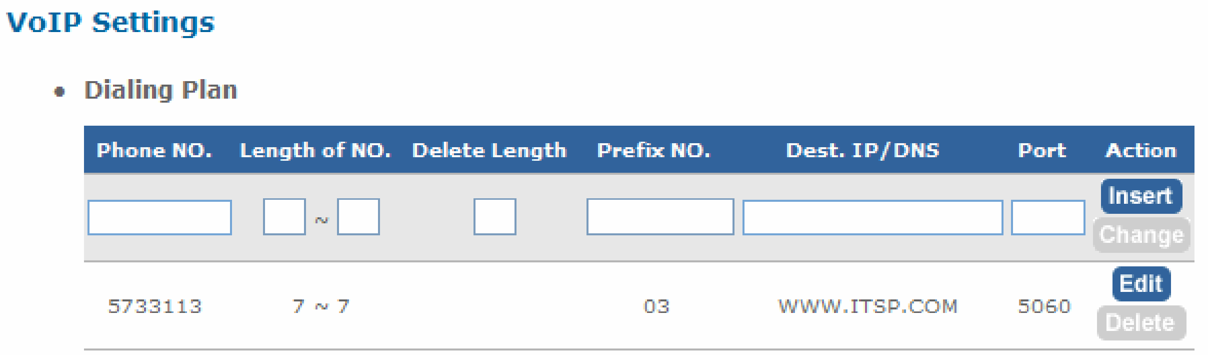
Line Status

- Gateway Status

FXS Port 1 ONHOOK

- SIP Status

Port 1 SIP Registered Status REGISTERED



VoIP Settings

- Dialing Plan

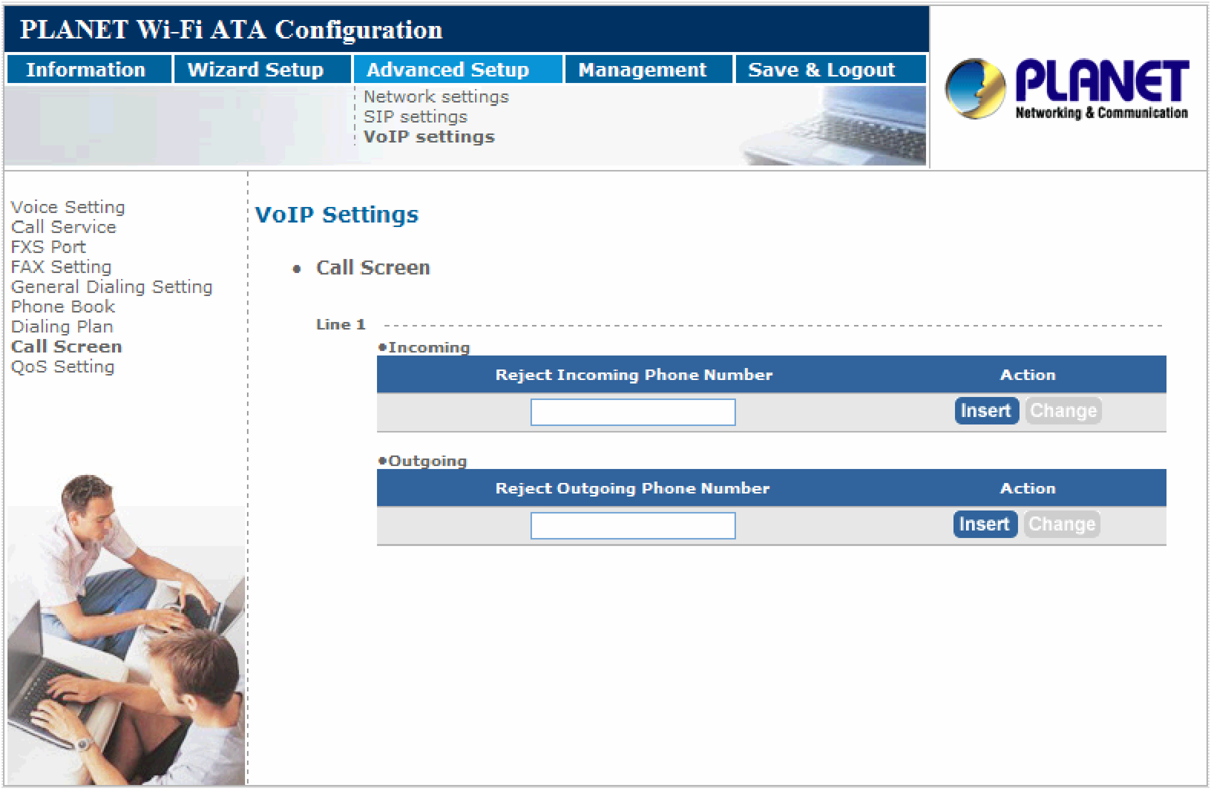
Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change
5733113	7 ~ 7		03	WWW.ITSP.COM	5060	Edit Delete

1. If user dial “5733113”,

ATA automatically dial “035733113” to ITSP IP address WWW.ITSP.COM.

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

Reject Incoming Phone Number：. Create and maintain a list of numbers to be screened.

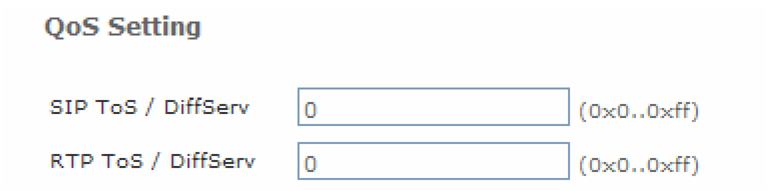
Incoming calls from the "screened callers" list will be blocked.

Reject Outgoing Phone Number：. Create and maintain a list of numbers to be screened.

Reject Outgoing Phone number from local user dial number.

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.



QoS Setting

SIP ToS / DiffServ: 0 (0x0..0xff)

RTP ToS / DiffServ: 0 (0x0..0xff)

SIP ToS/Diffserv：Set to value

RTP 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.

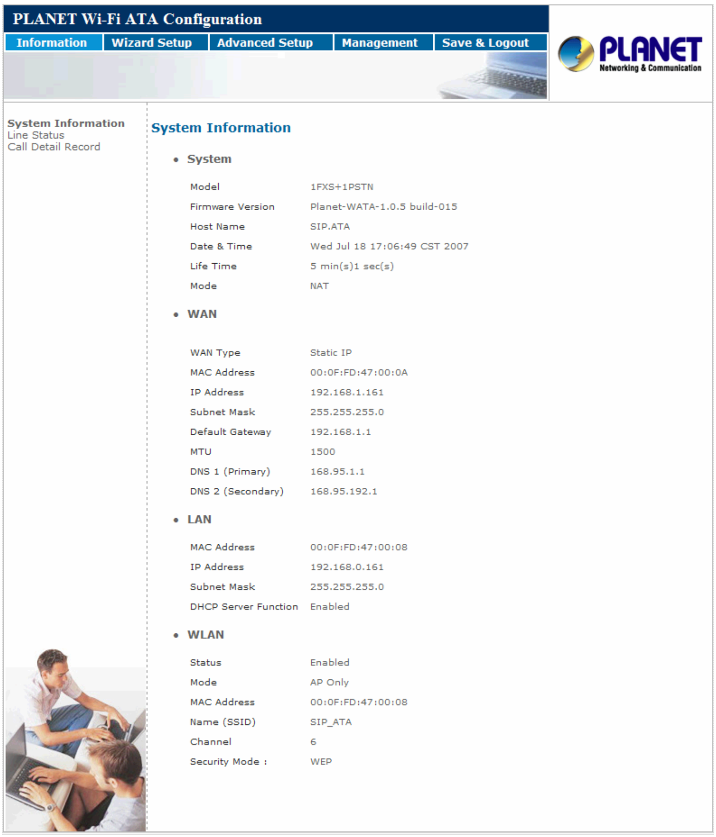
Information

- **System Information**
- **Line Status**

System Information

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

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).



System Information

- System

Model	1FXS+1PSTN
Firmware Version	Planet-WATA-1.0.5 build-015
Host Name	SIP.ATA
Date & Time	Wed Jul 18 17:06:49 CST 2007
Life Time	5 min(s)1 sec(s)
Mode	NAT

- WAN

WAN Type	Static IP
MAC Address	00:0F:FD:47:00:0A
IP Address	192.168.1.161
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

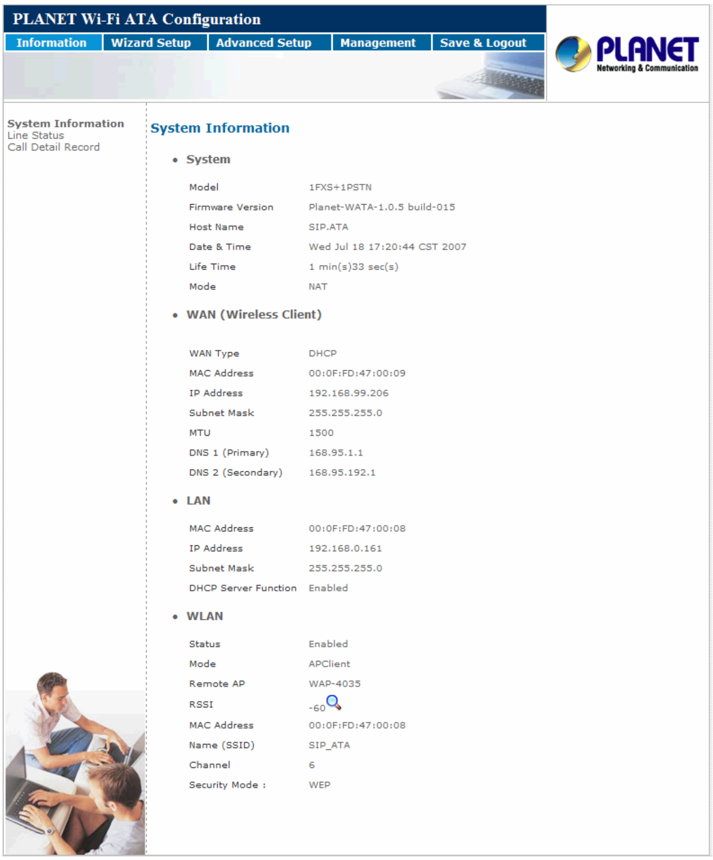
- LAN

MAC Address	00:0F:FD:47:00:08
IP Address	192.168.0.161
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

- WLAN

Status	Enabled
Mode	AP Only
MAC Address	00:0F:FD:47:00:08
Name (SSID)	SIP_ATA
Channel	6
Security Mode :	WEP

This system information page is “AP Mode”.



System Information

- System

Model	1FXS+1PSTN
Firmware Version	Planet-WATA-1.0.5 build-015
Host Name	SIP.ATA
Date & Time	Wed Jul 18 17:20:44 CST 2007
Life Time	1 min(s)33 sec(s)
Mode	NAT

- WAN (Wireless Client)

WAN Type	DHCP
MAC Address	00:0F:FD:47:00:09
IP Address	192.168.99.206
Subnet Mask	255.255.255.0
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

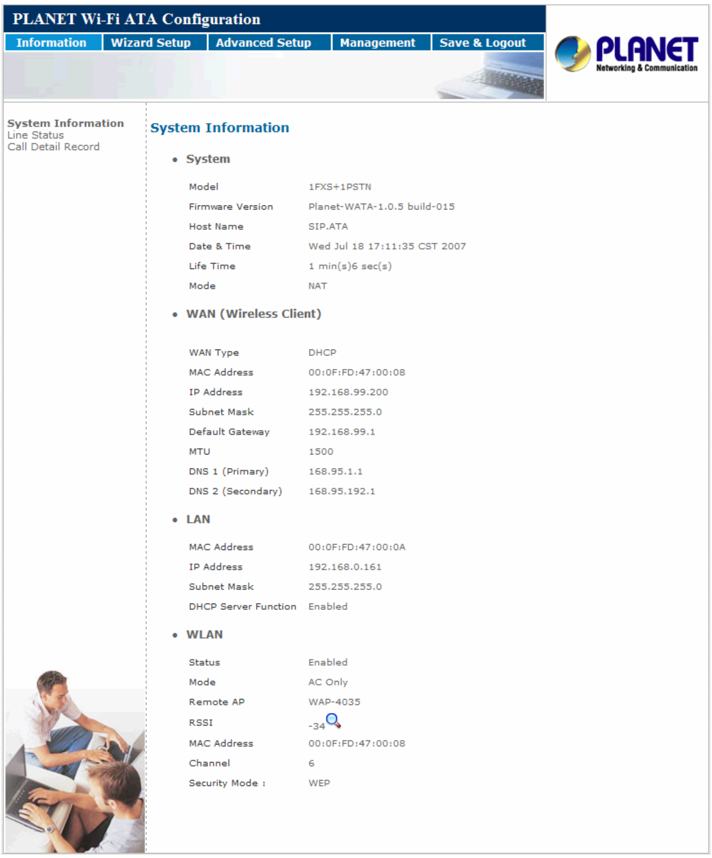
- LAN

MAC Address	00:0F:FD:47:00:08
IP Address	192.168.0.161
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

- WLAN

Status	Enabled
Mode	APClient
Remote AP	WAP-4035
RSSI	-60
MAC Address	00:0F:FD:47:00:08
Name (SSID)	SIP_ATA
Channel	6
Security Mode :	WEP

This system information page is “WISP & AP” Mode



System Information

- System

Model	1FXS+1PSTN
Firmware Version	Planet-WATA-1.0.5 build-015
Host Name	SIP.ATA
Date & Time	Wed Jul 18 17:11:35 CST 2007
Life Time	1 min(s)6 sec(s)
Mode	NAT

- WAN (Wireless Client)

WAN Type	DHCP
MAC Address	00:0F:FD:47:00:08
IP Address	192.168.99.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.99.1
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1

- LAN

MAC Address	00:0F:FD:47:00:0A
IP Address	192.168.0.161
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled

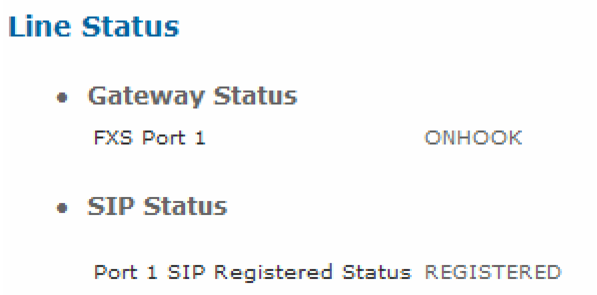
- WLAN

Status	Enabled
Mode	AC Only
Remote AP	WAP-4035
RSSI	-34
MAC Address	00:0F:FD:47:00:08
Channel	6
Security Mode :	WEP

This system information page is “AP-Client” Mode.

Line Status

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



Line Status

- Gateway Status

FXS Port 1 ONHOOK

- SIP Status

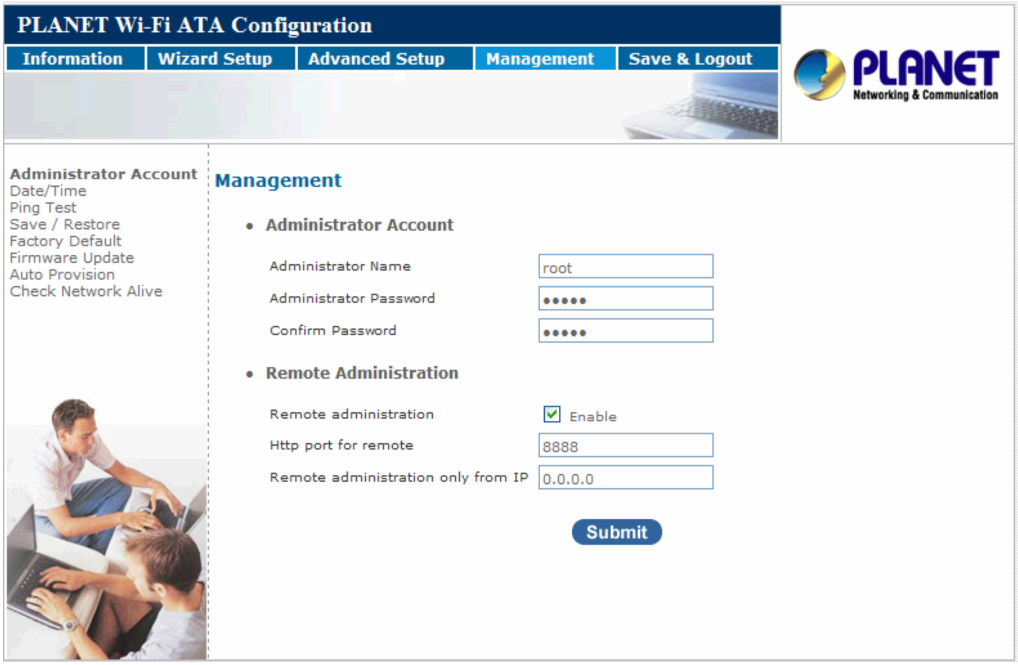
Port 1 SIP Registered Status REGISTERED

Management

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

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: root

Administrator Password: •••••

Confirm Password: •••••

- Remote Administration

Remote administration: ☑ Enable

Http port for remote: 8888

Remote administration only from IP: 0.0.0.0

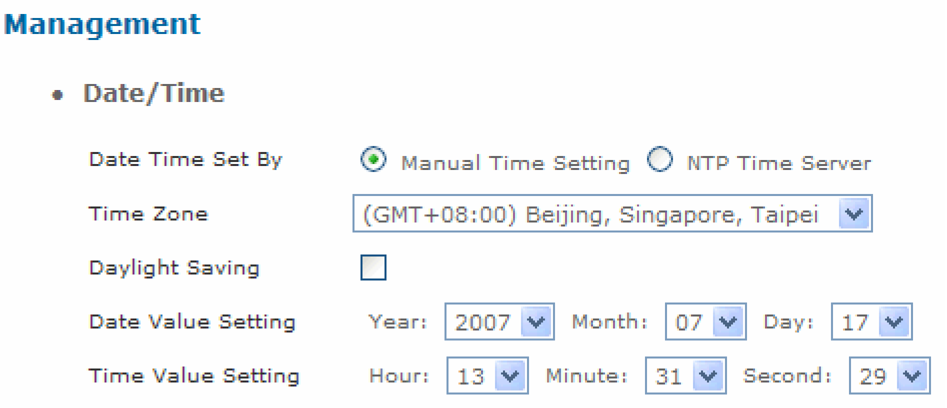
Administrator Name	Assign a name to represent the administrator account. Maximum 16 characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign¡ ”_”. The administrator name is case-sensitive. Note: the “blank” character is an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

Date/Time

Manual Time Setting：Set up the time manually.



Management

- Date/Time

Date Time Set By ● Manual Time Setting ○ NTP Time Server

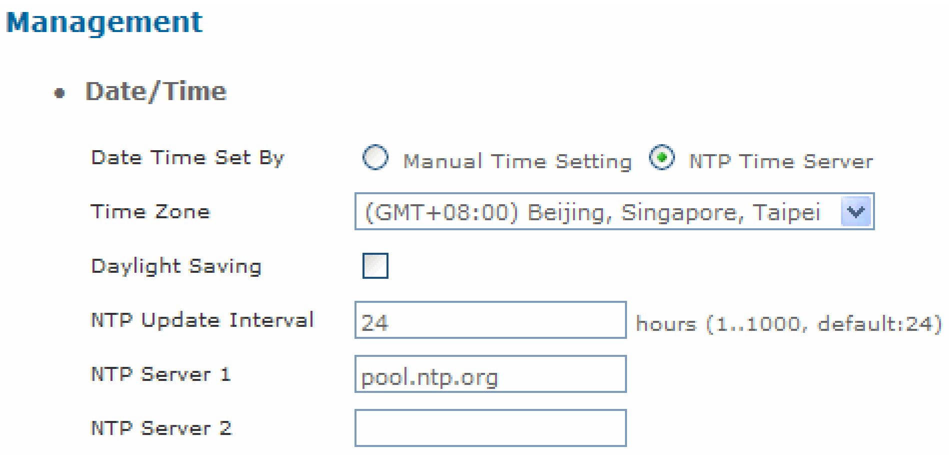
Time Zone: (GMT+08:00) Beijing, Singapore, Taipei

Daylight Saving: □

Date Value Setting: Year: 2007 Month: 07 Day: 17

Time Value Setting: Hour: 13 Minute: 31 Second: 29

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



Management

- Date/Time

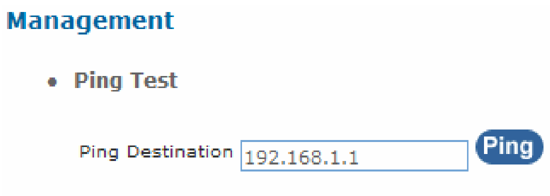
Date Time Set By	○ Manual Time Setting ● NTP Time Server
Time Zone	(GMT+08:00) Beijing, Singapore, Taipei
Daylight Saving	□
NTP Update Interval	24 hours (1..1000, default:24)
NTP Server 1	pool.ntp.org
NTP Server 2	

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.

Ping Destination：Assign a legal IP address.

Example: www.yahoo.com or 216.115.108.245



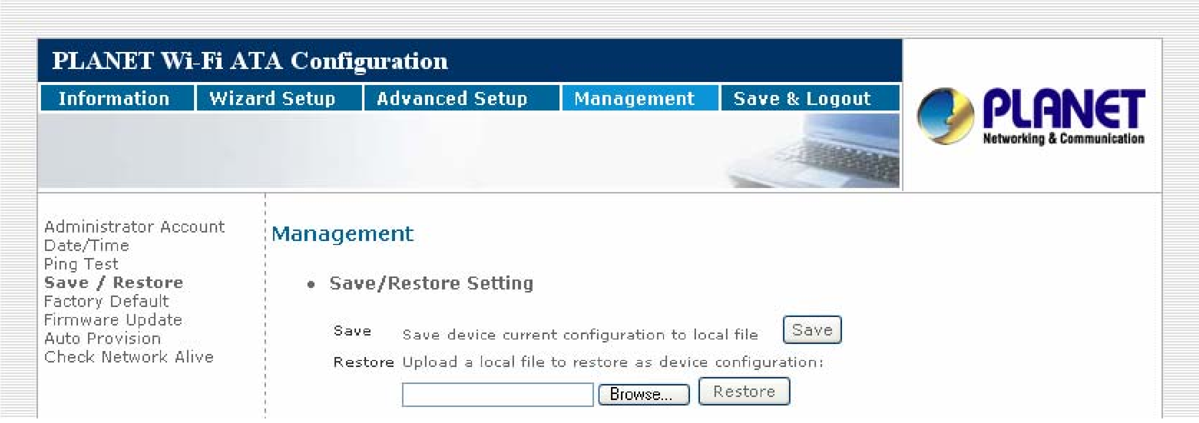
Management

- Ping Test

Ping Destination 192.168.1.1

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 WATA.



Management

- Save/Restore Setting

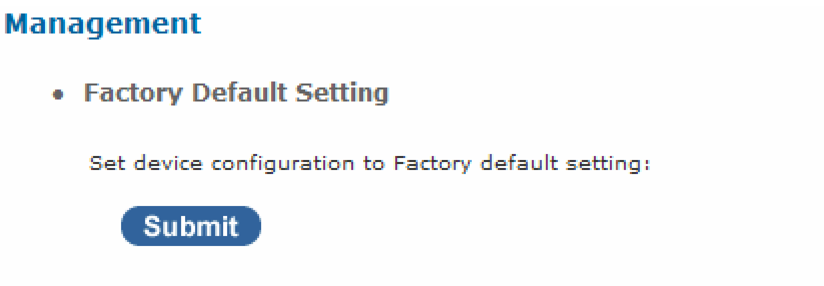
Save Save device current configuration to local file [Save]

Restore Upload a local file to restore as device configuration:

[Browse...] [Restore]

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 "Save / Restore") to check the factory default configuration, after you click on the **Set** button.



Management

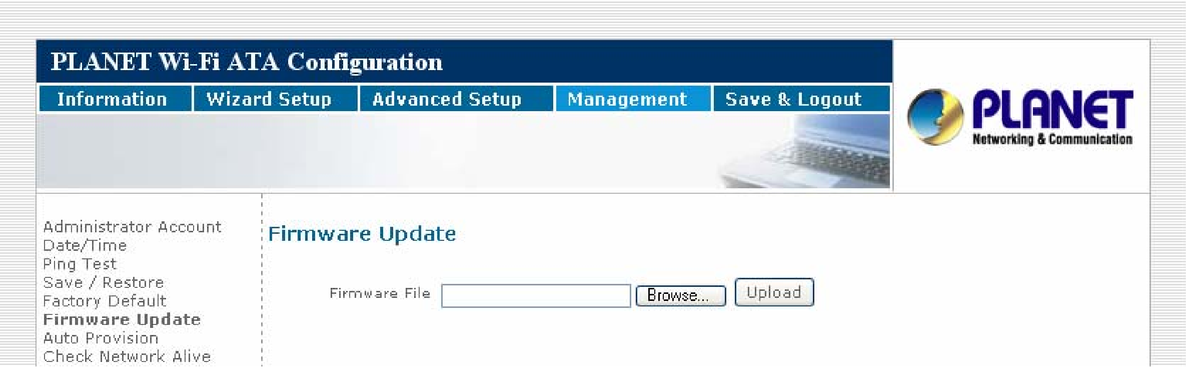
- Factory Default Setting

Set device configuration to Factory default setting:

[Submit]

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 your 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 [Browse...] [Upload]

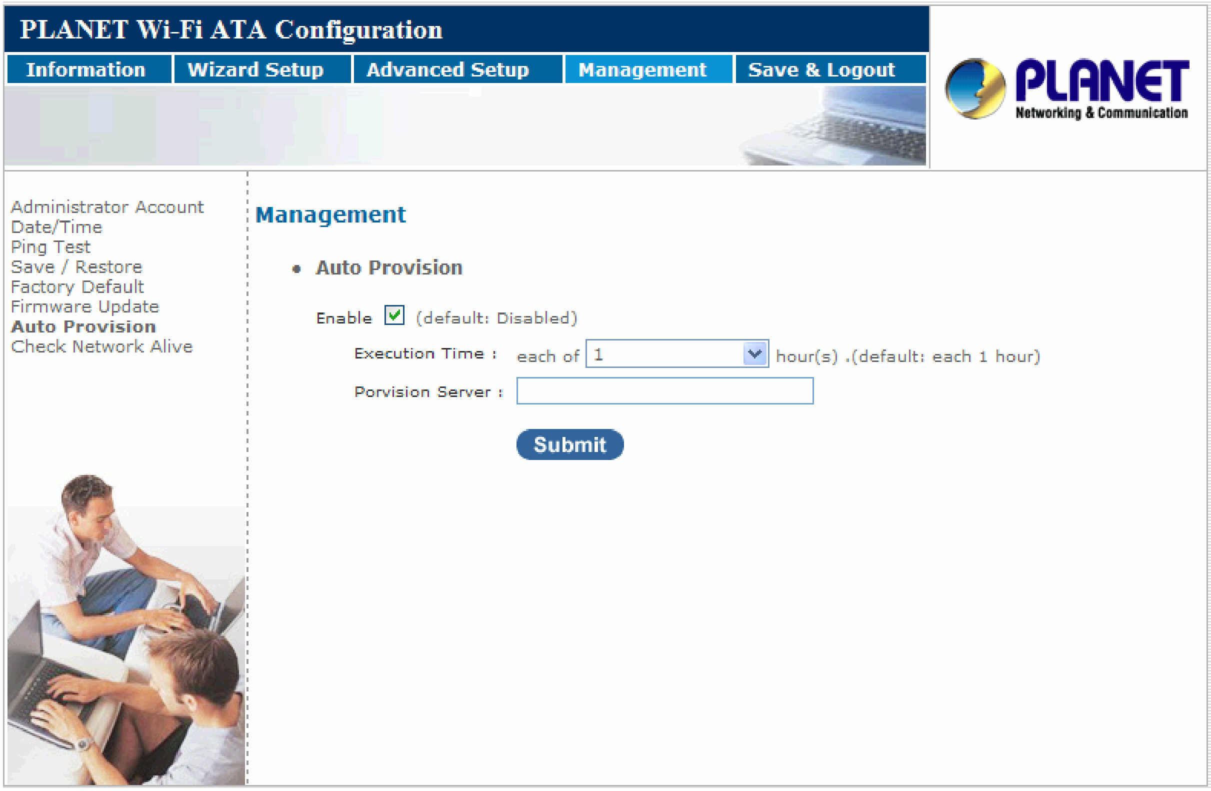
Firmware Name：Select that you want to upgrade Firmware version.

Auto Provision

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

Execution Time：Default 1 hour (1 to 10 hours), WATA will try to download the configuration files from the provisioning server.

Provision Server：Provision Server, default is empty.



Management

- Auto Provision

Enable ☑ (default: Disabled)

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

Porvision Server :

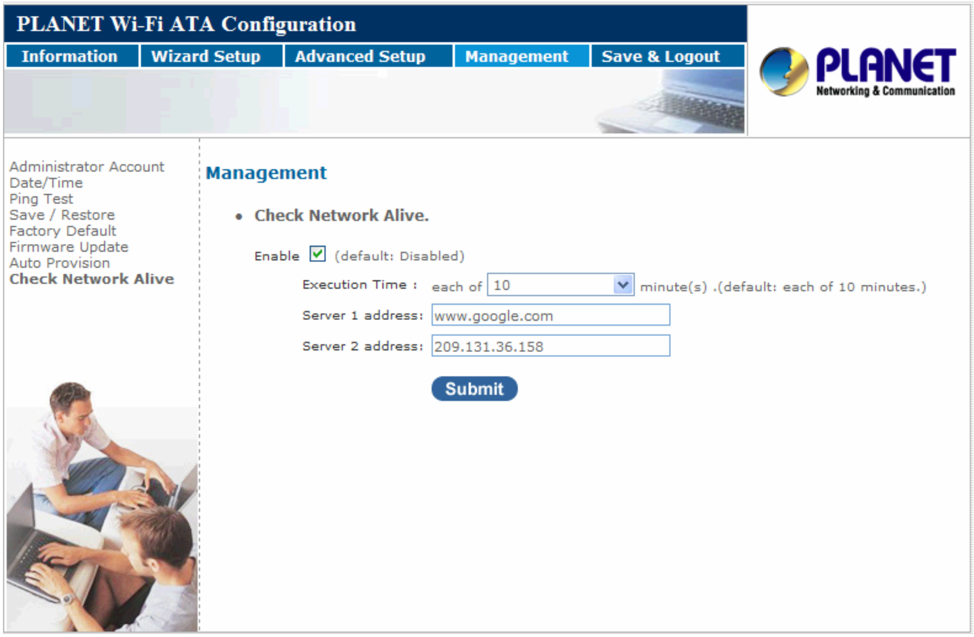
Check Network Alive

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.

Execution Time：5 ~ 55 min, default 10min

Server 1 address：www.google.com

Server 2 address：209.131.36.158



Management

- Check Network Alive.

Enable ☑ (default: Disabled)

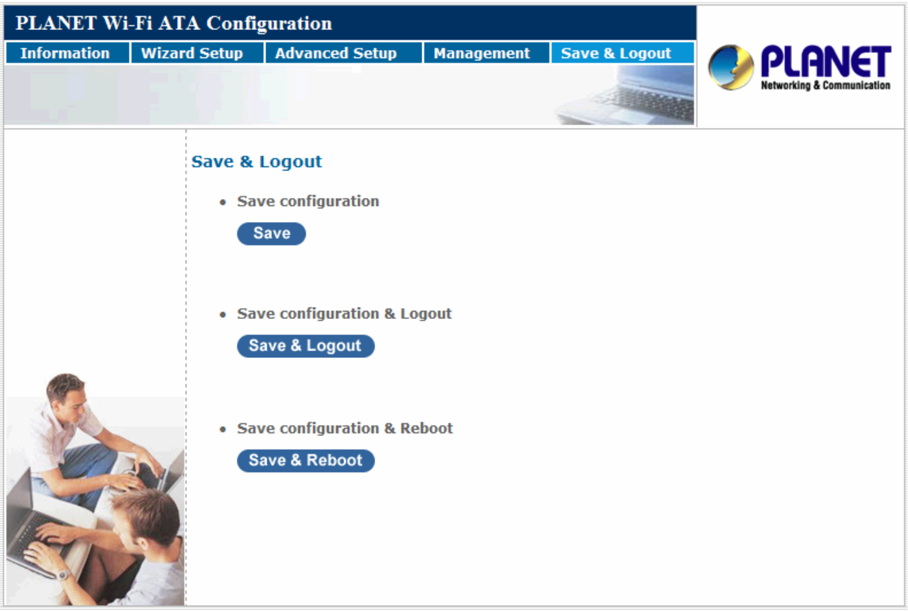
Execution Time : each of 10 minute(s) .(default: each of 10 minutes.)

Server 1 address: www.google.com

Server 2 address: 209.131.36.158

Save & Logout

In Save & Logout you can save the changes you have done. If you want to use new setting in the WATA, You have to click the Save button. After you click the Save button, the Phone Adapter will automatically restart and the new setting will effect.

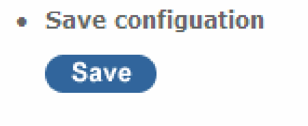


Save & Logout

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

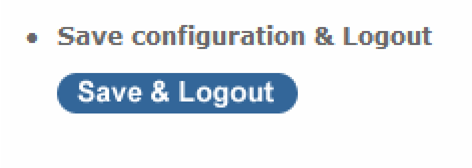
Save Configurations

Save your WATA Setting after you setting finish.



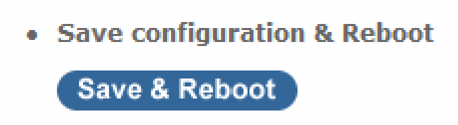
Save Configuration & Logout

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.



Save Configuration & Reboot

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



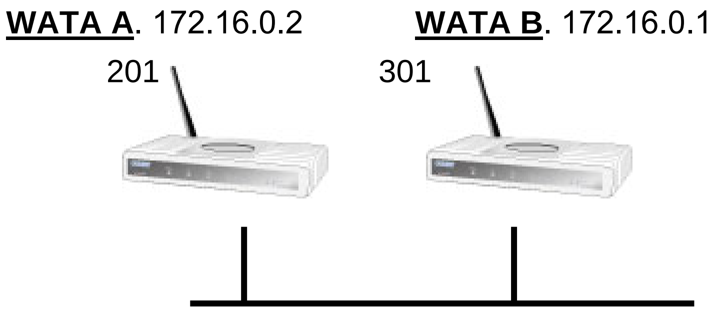
Appendix A Voice Communication Samples

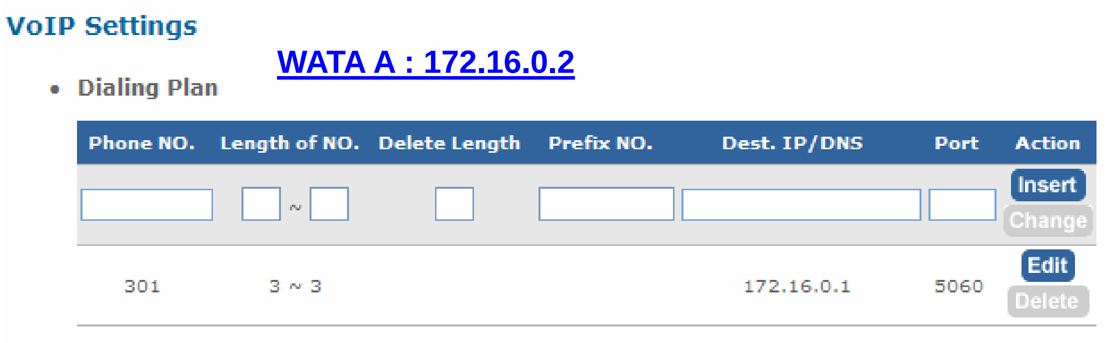
There are several ways to make calls to desired destination in WATA. In this section, we'll lead you step by step to establish your first voice communication via web browsers operations.

- **WATA to WATA connection via IP address (Peer-to-Peer mode)**

Assume there are two WATAs in the network the IP address are 172.16.0.1, 172.16.0.2

Analog telephone sets are connected to the phone (RJ-11) port of WATAs respectively



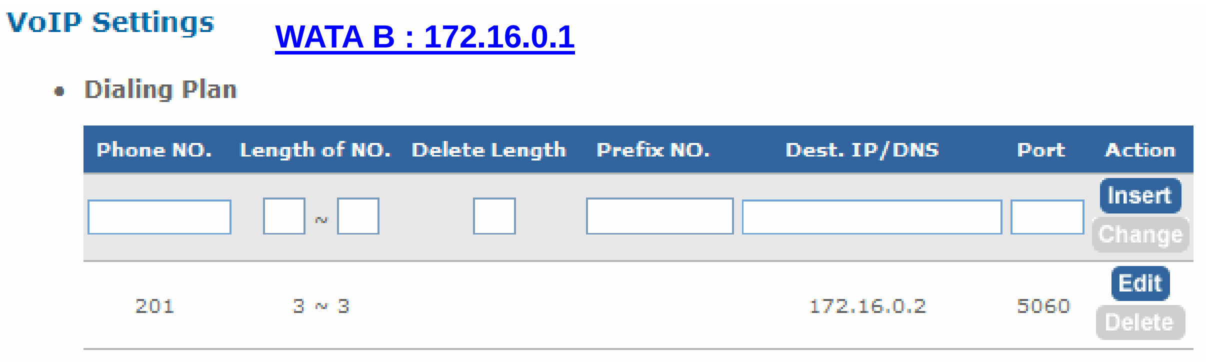


VoIP Settings

WATA A : 172.16.0.2

- Dialing Plan

Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change
301	3 ~ 3			172.16.0.1	5060	Edit Delete



VoIP Settings

WATA B : 172.16.0.1

- Dialing Plan

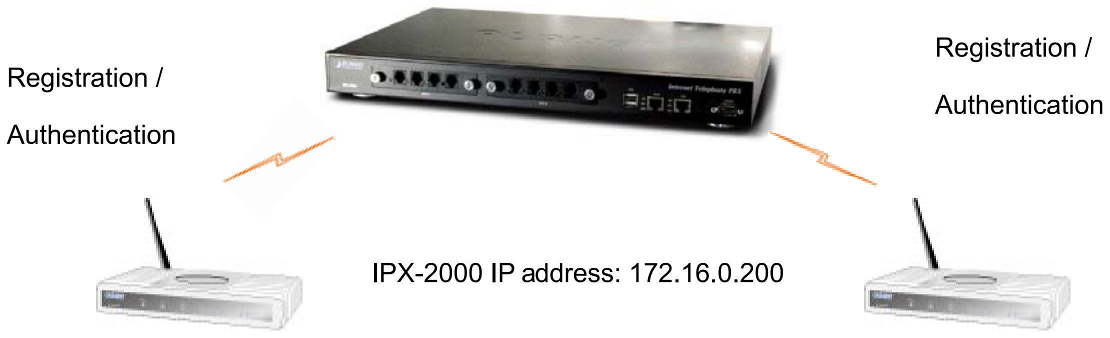
Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
	~					Insert Change
201	3 ~ 3			172.16.0.2	5060	Edit Delete

Operation steps:

Pick up the telephone on **WATA A**.

Press the keypad **301** shall be able to connect to the **WATA B**.

- **Voice communication via IP PBX system (IPX-2000)**



WATA AVIP-161W WAN IP address: 172.168.0.1
Line number: 1001

WATA B WAN IP address: 172.16.0.2
Line number: 2002

Device configurations on the WATA:

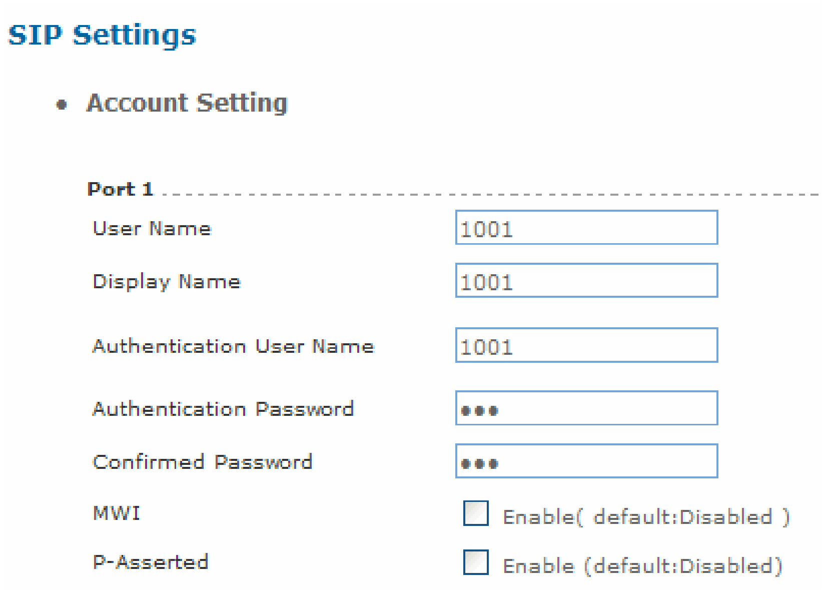
STEP 1:

Log in IPX-2000 and create two testing accounts/password: **1001**/**123** (for WATA A), and **2002**/**123** (for WATA B) for the voice calls.

STEP 2:

Please login WATA via web browser, browse to the **SIP Settings** menu and select the **Account Setting** menu. In the setting page, please insert the account/password information obtained from your service provider (in this sample, we're using PLANET IPX-2000 as the IP PBX system for SIP account, call authentications), and then the sample configuration

Screen is shown below:



SIP Settings

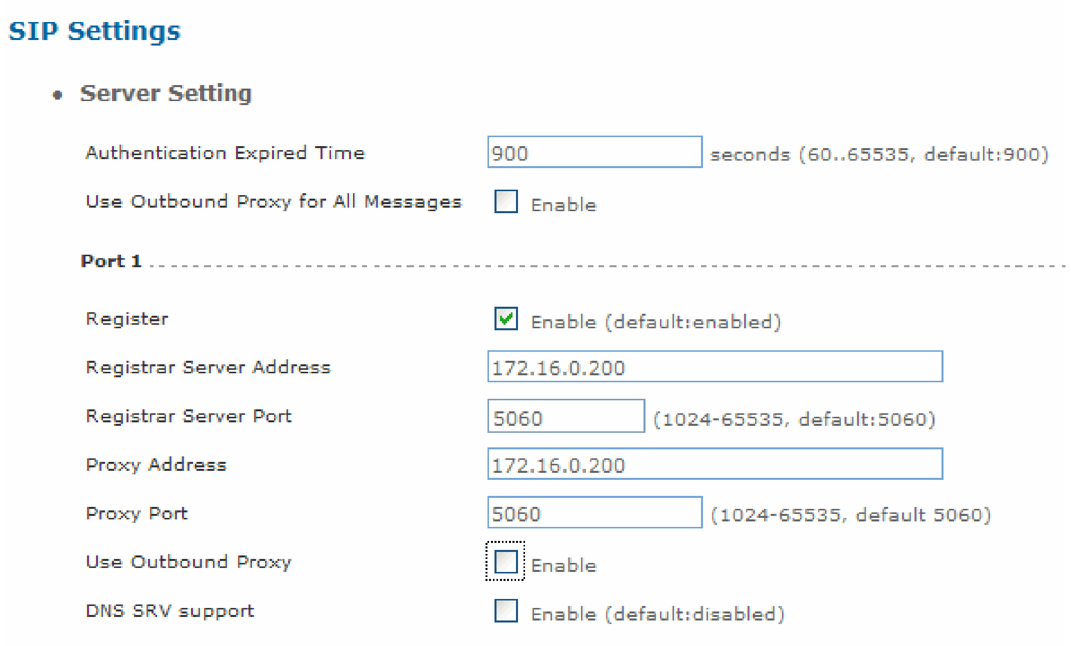
- Account Setting

Port 1

User Name	1001
Display Name	1001
Authentication User Name	1001
Authentication Password	●●●
Confirmed Password	●●●
MWI	☐ Enable(default:Disabled)
P-Asserted	☐ Enable (default:Disabled)

STEP 3:

Please browse **Server Setting** menu and insert the proxy server IP address (or domain name) information obtained from your service provider.



SIP Settings

- Server Setting

Authentication Expired Time	900	seconds (60..65535, default:900)
Use Outbound Proxy for All Messages	□ Enable	

Port 1

Register	☑ Enable (default:enabled)	
Registrar Server Address	172.16.0.200	
Registrar Server Port	5060	(1024-65535, default:5060)
Proxy Address	172.16.0.200	
Proxy Port	5060	(1024-65535, default 5060)
Use Outbound Proxy	□ Enable	
DNS SRV support	□ Enable (default:disabled)	

STEP 4:

Repeat the same configuration steps on WATA B, and check the machine registration status, make sure the registrations are completed.

Test the scenario:

To verify the VoIP communication, please

1) Pick up the telephone on **WATA A**
2) Press the keypad **2002** shall be able to connect to the **WATA B**
3) Then the telephone set in **WATA B** should ring.
4) Please repeat the same dialing steps on **WATA B** to establish the first voice communication from **WATA A**

Make a three - way conference call

1) Make a call to the first party.
2) "Flash hook" to hold the call.
3) Dial " ****** ", and then you will hear a dial tone.
4) Make the other call to the third party.
5) Dial " ***3** " to connect the two party calls for conferencing.

Note

If you want to make a PSTN phone call, press the “*” key to switch to PSTN mode.

Appendix B Frequently Asked Questions List

Q: What is the default administrator password to login to the WATA? How to Login?

A: By default, default username is “root” and no password 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 “172.16.0.1”, LAN port IP address is “192.168.0.1”. For modifying the default values please login into the Web User Interface, open the Bowser (IE/FireFox) and input IP address.

Q: 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.

Q: 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.

Q: What is the maximum number of IP addresses that the DHCP server of the WATA can assign to local PCs?

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

Q: Why can I call out by WATA?

A: Please look at the system information and line status pages check your WATA is registered to the SIP Proxy Server(ITSP), and check your Internet works fine. You must have a SIP account or know the other ATA/Gateway IP/Domain Name. Only then you can make a VoIP call.

Q: I can’t use web Interface to setting WATA.

A: Please check your PC is connected to the WATA LAN port and that your PC and the WATA are in the same Subnet. If you PC is not in the same Subnet, you can’t Login into the WATA Web interface. Else you let your WATA on Public Internet (Public IP address)

Q: Why does the one way talk happen?

A: Generally, one way talk happens when different codecs are used between the VoIP devices that are making the call. Please check the settings and make sure the same codec are used.

Q: Why can I call out when the WATA under the NAT?

A: Most VoIP products have NAT Pass through problems. With SIP, most of the NAT Pass through issues (about 80%) is solved. You can select STUN/Outbound Proxy/ Symmetric RTP to Pass through NAT, and then 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.

Appendix C VIP-161W/VIP-161SW Specifications

Product	Wireless Analog Telephone Adapter	
Model	VIP-161W	VIP-161SW
Hardware		
WLAN Standards	IEEE 802.11 b/g	
Wireless Frequency Range	2.4GHz ~ 2.4835 GHz	
Security	64/128 bit WEP data encryption, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 mix mode, WPAPSK/WPA2PSK mix mode.	
Operating Frequencies / Channel	USA/Canada: 2.412 GHz – 2.426 GHz (11 channels) Europe: 2.412 GHz – 2.472 GHz (13 channels) Japan: 2.412 GHz – 2.477 GHz (14 channels)	
Data Rate	802.11b: CCK (11Mbps,5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps)	
	802.11g: OFDM (54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps)	
Wireless Signal Range*	Indoors: Up to 230 ft (70 meters) Outdoors: Up to 1050 ft (320 meters)	
WAN	1 x 10/100 Base-TX RJ-45 port	
LAN	1 x 10/100 Base-TX RJ-45 port	
FXS (for telephone set connection)	1 x RJ-11 connection	2 x RJ-11 connection
Line	1 x RJ-11 connection	-
Protocols and Standard		
Standard	SIP 2.0 (RFC3261) SDP (RFC 2327) Symmetric RTP STUN (RFC 3489) ENUM (RFC 2916) RTP Payload for DTMF Digits (RFC2833) Outbound Proxy Support UPnP (UPnPTM)	
Voice codec	G.711(A-law /μ-law), G.729 AB, G.723 (6.3 Kbps / 5.3Kbps), G.276 (16,24,32,40 Kbps)	
Fax support**	T.38 (G.711 Fax pass-through)	
Voice Standard	VAD (Voice Activity Detection) CNG (Comfort Noise Generation) G.165~2000: LEC (Line Echo Canceller) Dynamic Jitter Buffer In-band and out-of-band DTMF Relay (RFC 2833) Caller ID Detection/Generation: DTMF, Bellcore, ETSI, NTT	
Protocols	SIP 2.0 (RFC-3261), TCP/IP, UDP/RTP/RTCP, HTTP, ICMP, ARP, DNS, DHCP, NTP/SNTP, PPP, PPPoE	
Internet features	NAT router, DHCP server, Static routing, Virtual server, Virtual DMZ, Smart QoS, IP ToS (IP Precedance) / DiffServ	
Network and Configuration		
Access Mode	Static IP, PPPoE, DHCP	
Management	Web-based graphical user interface	
Dimension (W x D x H)	180 mm x 110 mm x 25 mm	
Operating Environment	0~40 degree C, 10~90% humidity	
Power Requirement	12V DC	
EMC/EMI	CE, FCC Part 15 Class B	