



# Internet Telephony PBX System

## IPX-300 Series

### User's manual

Version 1.0.1

## Copyright

Copyright (C) 2008 PLANET Technology Corp. All rights reserved.

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 Internet Telephony PBX System:

Model: IPX-300/IPX-300W

Rev: 1.01 (February, 2008)

Part No. EM-IPX300 Series V1.01

**TABLE OF CONTENTS**

---

<b>Chapter 1 .....</b>	<b>6</b>
<b>Introduction.....</b>	<b>6</b>
<b>Overview.....</b>	<b>6</b>
<b>Package Content .....</b>	<b>8</b>
<b>Physical Details .....</b>	<b>8</b>
Front Panel Indicators.....	8
Rear Panel Indicators.....	9
<b>Chapter 2 Preparations &amp; Installation .....</b>	<b>10</b>
<b>Physical Installation Requirement .....</b>	<b>10</b>
Network Interface quick configurations .....	11
<b>Chapter 3 IP PBX Setup .....</b>	<b>16</b>
SIP Basic Setting .....	16
User Extensions Setup.....	18
Trunk Management – SIP Trunk .....	20
Trunk Management – Gateway Trunk.....	22
Trunk Management – Trunk Group.....	22
Trunk Management – Dialing Rules.....	24
Attendant Extension .....	26
Time Rules.....	27
Record Voice Menu .....	28
Call Parking .....	28
General Setting.....	29
Hunt Group Setting.....	31
<b>Chapter 4 Network Setup .....</b>	<b>35</b>
WAN & LAN Setup.....	35
DHCP .....	40
WLAN Setting (For IPX-300W) .....	42
Access Policy (For AP and WISP&AP mode) .....	49
Static Route.....	50
NAT .....	51
Packet Filter.....	54
URL Filter.....	56
Security.....	56
UPnP.....	57
Call Out Block List.....	57
SNTP .....	59
<b>Chapter 5 Management .....</b>	<b>60</b>

Admin Account.....	60
Date & Time .....	61
Ping Test .....	62
Save & Restore .....	62
Factory Default.....	63
Admin Account.....	63
<b>Chapter 6 Information .....</b>	<b>64</b>
System Information .....	64
PBX Extension Status.....	65
PBX Trunk Status .....	65
Call Detail Record .....	65
<b>Appendix A .....</b>	<b>67</b>
How to use Call Parking function .....	67
<b>Appendix B .....</b>	<b>68</b>
How to use Call Pick-up function.....	68
<b>Appendix C .....</b>	<b>69</b>
Record Voice Guide Process .....	69
<b>Appendix D .....</b>	<b>70</b>
<b>Voice Communication Samples .....</b>	<b>70</b>
IP Phone and Wi-Fi Phone register to IPX-300W .....	70
IP Phone and Wi-Fi Phone make off-Net calls via Gateway.....	74
IP Phone and Wi-Fi Phone make external SIP Proxy calls via SIP Trunk.....	79
<b>Appendix E .....</b>	<b>81</b>
<b>IPX-300 Series Specifications .....</b>	<b>81</b>

# Chapter 1

## Introduction



### Overview

PLANET IPX-300/IPX-300W IP PBX telephony systems ("IP PBX" in the following term) are designed and optimized for the small business in daily communications. It can support up to 100 user registrations and easy to install and manage a fully working system with the convenience and cost advantages. The future IP PBX telephony system offers all of the essential features of telephony which is required by small business users for their telecommunication/data needs.

The IP PBX series are the feature-rich SIP based IP PBX telephony system that integrates NAT functions to make it perfect for small business usage. The IP PBX integrates traditional PBX system functions and provides many advanced functions including voice mail to email, web management etc. Designed to run on a variety of VoIP applications, the IP PBX provide IP-based communications, voice conferencing, call detailed record (CDR), centralized Auto-Attendant (AA), and Interactive Voice Responses (IVR). The IP PBX utilizes standard PSTN / GSM lines via the interfaces of FXO / GSM gateway to become a feature-rich IP PBX telephony system that supports seamless communications among existing local calls, SIP-based endpoints including low cost of long distance service, telephone number portability and one network for both voice and data.

With a built-in IEEE 802.11b/g wireless AP / CPE, the Wi-Fi IP PBX (IPX-300W) offers wireless connectivity via 54Mbps data transmissions. Users may integrate PLANET IP Phone VIP-154T series, VIP-155PT/ 350PT/ 550PT, the VIP-156/ 157/ 158/ 161W of ATA (analog telephone adapter) series, the VIP-191/ 192 of Wi-Fi Phone, and Gateway series VIP-281/ 281GS/ 480 to build up the VoIP network deployment in minutes.

### IP PBX Features

- **PBX Features**
  - Automated Attendant (AA)
  - Interactive Voice Responses (IVR)
  - Voicemail support (VM)
  - Voicemail to E-Mail
  - Call Detailed Record (CDR)
  - User Management via Web Browser
  - Call/Pickup Group

- Display 100 Registered User's Status: Unregistered / Registered / On-Call

- **Call Features**

- Call Forward Immediate
- Call Forward on Busy
- Call Forward on No Answer
- Call Pickup / Call Park
- Caller ID
- Music on Hold / Music on Transfer
- Call Transfer / Call Hold / Call Waiting
- Three-way conference with feature phones (VIP-154T series, VIP-155PT/ 350PT/ 550PT and VIP-156/ 157/ 158/ 161W series)

- **Router/Firewall Features**

- DHCP Server for LAN Users
- Access Control / URL Filter
- Virtual Server / DMZ / Port Mapping
- Static Route
- Pass-through
- UPnP

- **Wireless Features (IPX-300W)**

- IEEE 802.11b/ 802.11g
- AP / AP-Client / WISP & AP Mode
- 64/128 bits WEP Data Encryption
- WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ Mix Mode
- WPAPSK/ WPS2PSK Mix Mode

## Package Content

The contents of your product should contain the following items:

Internet Telephony PBX system unit

Power Adapter

Quick Installation Guide

User's Manual CD

## Physical Details

The following figure illustrates the front/rear panel of IP PBX.

### Front Panel Indicators



Figure 1-1. Front Panel of IPX-300



Figure 1-2. Front Panel of IPX-300W

Front Panel LED	State	Descriptions
<b>PWR</b>	On	PBX Power ON
	Off	PBX Power OFF
<b>WAN Port</b>	On	PBX network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection
<b>LAN Port</b>	On	LAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC
<b>WLAN Port (IPX-300W only)</b>	On	WLAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC

Table1-1. Front Panel description of IP PBX



## Rear Panel Indicators

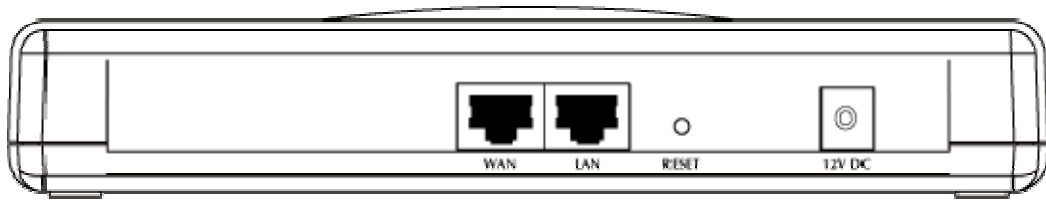


Figure 1-3. Rear Panel of IPX-300

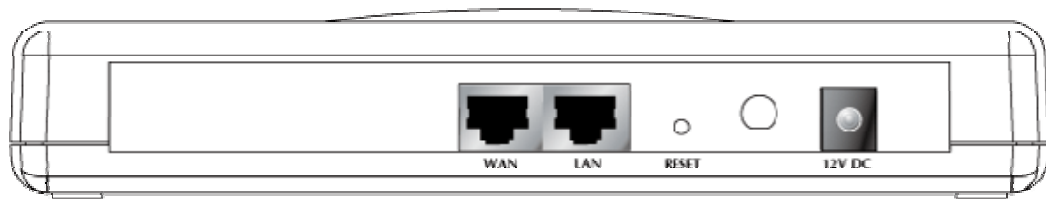


Figure 1-4. Rear Panel of IPX-300W

1	<b>12V DC</b>	12V DC Power input outlet
2	<b>Reset</b>	The reset button, when pressed, resets the IP PBX without the need to unplug the power cord.
3	<b>WAN</b>	The WAN port supports auto negotiating Fast Ethernet 10/100Base-T networks. This port allows your IP PBX to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet cable.
4	<b>LAN</b>	The LAN port allows your PC or Switch/Hub to be connected to the IP PBX through a CAT.5 twisted pair Ethernet cable.
5	<b>External Antenna 2db</b> <b>(IPX-300W only)</b>	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

Table 1-2. Rear Panel description of IP PBX

# Chapter 2

## Preparations & Installation

### Physical Installation Requirement

This chapter illustrates basic installation of IP PBX

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 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 (for WAN port usage)

### Administration Interface

---

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

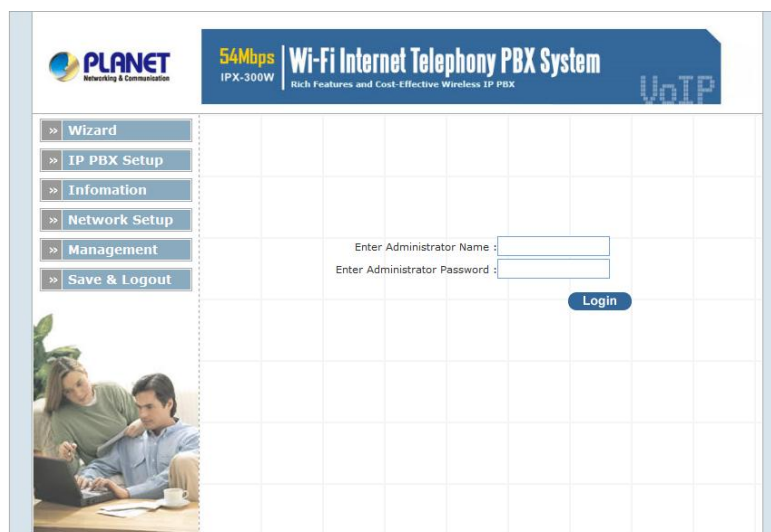
### Web configuration access:

To start IP PBX web configuration, you must have the web browsers installed on computer for management

- Microsoft Internet Explorer 6.0.0 or higher with Java support

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

IP PBX will prompt for logon username/password, please enter: **admin** / **123** to continue machine administration.



The screenshot displays the web configuration interface for the PLANET IP PBX system. The header includes the PLANET logo and the product name "54Mbps Wi-Fi Internet Telephony PBX System IPX-300W". A navigation menu on the left lists options: Wizard, IP PBX Setup, Information, Network Setup, Management, and Save & Logout. The main content area features a login form with two input fields: "Enter Administrator Name" and "Enter Administrator Password", followed by a "Login" button. A small image of two people working at a computer is visible in the bottom-left corner of the interface.

Figure 2-1. Input prompt

**Note**

In order to connect machine for administration, please locate your PC in the same network segment (192.168.0.x) of IP PBX. 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.

## Network Interface quick configurations

Wizard for Quick Setup of the IP PBX, after finishing the authentication, please click "Wizard" to enter quick start:

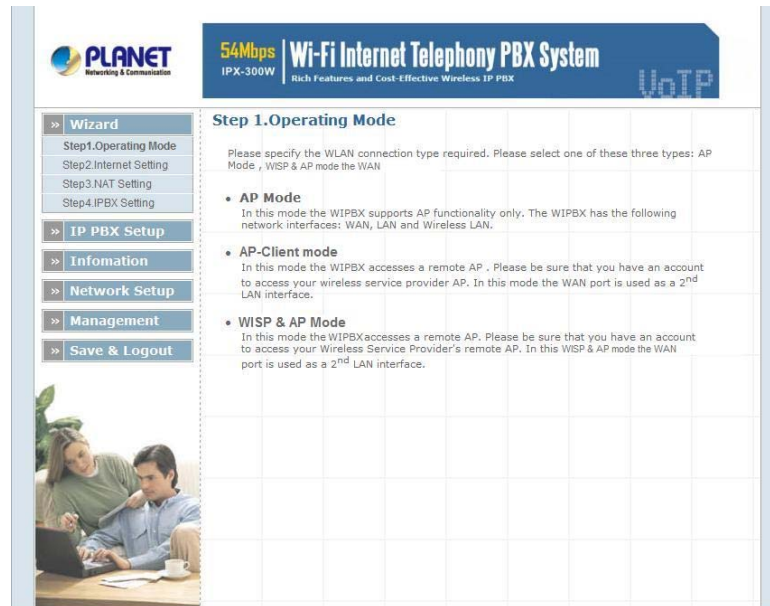


Figure 2-2. Wizard-Operating Mode settings

➤ **Step1. Operation Mode (For IPX-300W)**

For most users, Internet access is the primary application. The IP PBX supports the WAN, LAN and 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.

Three WLAN modes of operation are available for Internet Access:

**AP Mode:**

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

**AP-Client Mode:**

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

**WISP & AP Mode :**

The IP PBX must access remote AP .Please be sure that have account to access from remote AP. In this WISP & AP mode the network interface will change from WAN port to LAN port and all of network access will through by remote AP.

➤ **Step2. Internet Setting (AP Mode)**

**WAN Setting**

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

Table 2-1. WAN description of IP PBX

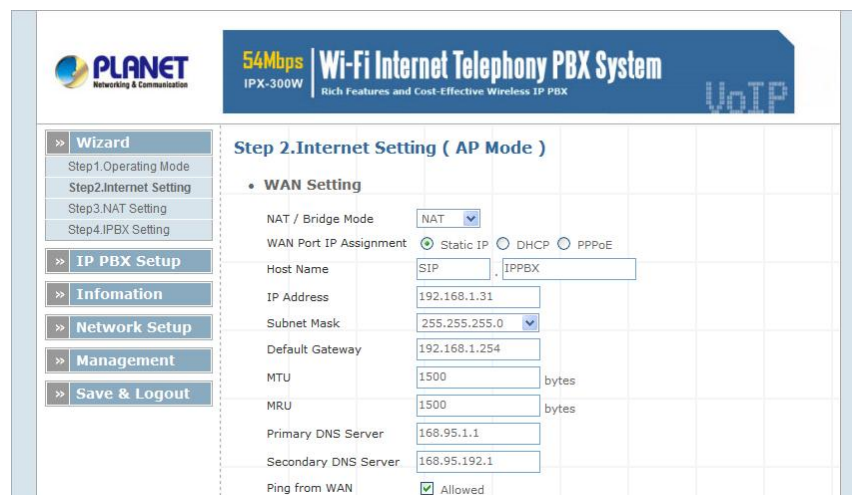


Figure 2-3. Wizard-Internet settings

**AP Setting (For IPX-300W)**

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 IP PBX 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.)

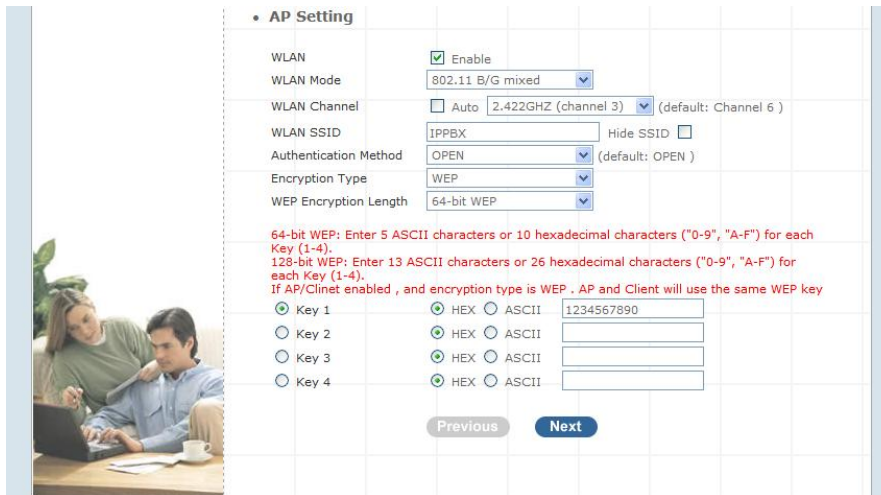


Figure 2-4. Wizard-AP settings

➤ Step3. NAT Setting

LAN IP Setting

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

Table 2-2. LAN IP description of IP PBX

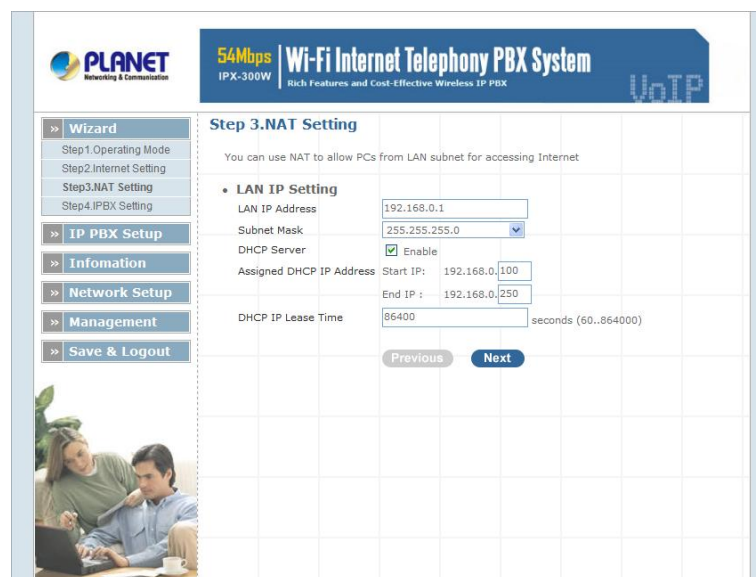


Figure 2-5. Wizard-NAT settings

## ➤ Step4. IPPBX Setup

The IP PBX allows multiple ITSP providers / User Extensions registration by simply fill-in the required information in the provided table.

Figure 2-6. Wizard-IP PBX settings

### *Service Provider:*

<b>Caller ID</b>	Service provider name
<b>Username</b>	Input Provider name
<b>Password</b>	Input Provider password
<b>Host</b>	Input Providers server address
<b>Port</b>	Providers server port

Table 2-3. Service provider description

### *User Extensions:*

<b>User Extension</b>	Input Extension number
<b>Password</b>	Input Extension password
<b>Caller Id</b>	Input Extension caller id

Table 2-4. User extension description

After completing the wizard setup, click "**Submit**" button, The IP PBX will save configuration and reboot IP PBX automatically, after 50 seconds, you can re-load setting page again.

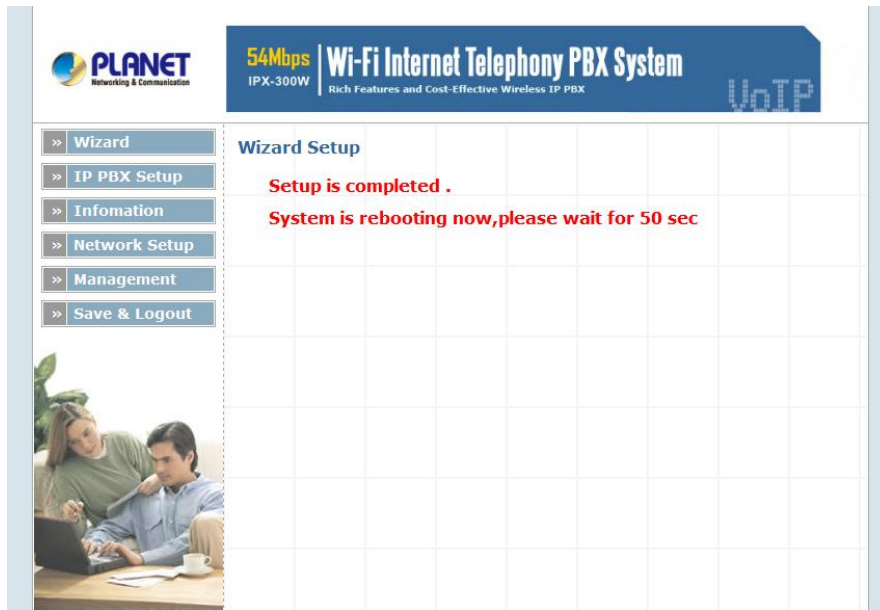


Figure 2-7. Wizard-Rebooting

**Note**

---

Please consult your ISP personnel to obtain proper PPPoE/IP address related information, and input carefully. If Internet connection cannot be established, please check the physical connection or contact the ISP service staff for support information.

---

# Chapter 3

## IP PBX Setup

3

### SIP Basic Setting

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

#### ➤ SIP Configuration

IP PBX Setup	
• SIP Configuration	
UDP Port to bind to	5060
Domain	
Allow guest calls	<input checked="" type="checkbox"/>
Allow Transfers	<input checked="" type="checkbox"/>
Overlap dialing support	<input checked="" type="checkbox"/>
Enable DNS SRV lookups (on outbound calls)	<input type="checkbox"/>
Min Registration/Subscription Time	900
Max Registration/Subscription Time	3600
Default Incoming/Outgoing Registration Time	360
Min Roundtrip Time (T1 Time)	200
Language	English
Enable Relaxed DTMF	<input type="checkbox"/>
Server UserAgent	PBX
DTMF Mode	rfc2833

Figure 3-1. SIP configuration settings

<b>UDP Port to bind to</b>	This is SIP Local Port 5060, if you have any specific reason for change this port.
<b>Domain</b>	IP PBX Server's IP address.
<b>Allow guest calls</b>	Enable/Disable guest calls. Default is <i>Enable</i> . Default is all IP.
<b>Overlap dialing support</b>	Enable/Disable overlaps dialing support. Default is <i>Enable</i> .
<b>Allow Transfers</b>	Enable Call Transfers.
<b>Enable DNS SRV lookups (on outbound calls)</b>	Enable DNS SRV lookups on calls



<b>Max Registration Time</b>	Maximum duration of incoming registration/subscriptions we allow. Default 3600 seconds.
<b>Min Registration Time</b>	Minimum duration of registrations/subscriptions. Default 60 seconds
<b>Default Incoming/Outgoing Registration Time</b>	Default duration (in seconds) of incoming / outgoing registration.
<b>Min RoundtripTime (T1 Time)</b>	Minimum roundtrip time for messages to monitored hosts, Defaults to 200 ms
<b>Language</b>	Set default language for all users.
<b>Enable Relaxed DTMF</b>	Use relaxed DTMF detection. Default is <i>Disable</i> .
<b>Server UserAgent</b>	Enable you to change the trunk User agent string, Default is <i>PBX</i> .
<b>DTMF Mode</b>	Set default DTMF mode for sending DTMF. Default: <i>rfc2833</i> .

Table 3-1. SIP configuration description

### ➤ SIP Codecs

The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 7 kinds of codec. To determine the priority, selects one codec algorithm from the pull-down menus individually.

• SIP Codecs	
Codec Priority 1	ulaw
Codec Priority 2	alaw
Codec Priority 3	gsm
Codec Priority 4	ilbc
Codec Priority 5	g726
Codec Priority 6	g729
Codec Priority 7	g723

Figure 3-2. SIP codecs settings

### ➤ Outbound SIP Registrations

• Outbound SIP Registrations	
Register TimeOut	30
Register Attempts	65535

Figure 3-3. Outbound SIP Registrations settings

<b>Register TimeOut</b>	Retry registration calls at every 'x' seconds (default 20).
<b>Register Attempts</b>	Number of registration attempts before we give up; 0 = continue forever.

Table 3-2. Outbound DIP registration description

### ➤ NAT Support

The *externip*, *externhost* and *localnet* settings are used if you use IP PBX behind a NAT device to communicate with services on the outside.



Figure 3-4. NAT support settings

<b>Extern IP</b>	Address that we're going to put in outbound SIP messages if we're behind a NAT.
<b>Extern Host</b>	Alternatively you can specify an external host, and <b>IP PBX</b> will perform DNS queries periodically. Not recommended for production environments! Use <i>externip</i> instead.
<b>Extern Refresh</b>	How often to refresh <i>externhost</i> if used. You may specify a local network in the field below.
<b>Local Network Address</b>	<p>localnet=192.168.0.0/255.255.0.0; All RFC 1918 addresses are local networks</p> <p>localnet=11.0.0.0/255.0.0.0 ; Also RFC1918</p> <p>localnet=171.16.0.0/12 ; Another RFC1918 with CIDR notation</p> <p>localnet=168.254.0.0/255.255.0.0; Zero conf local network</p>

Table 3-3. NAT support description

## User Extensions Setup

### ➤ Extension List

• **User Extensions Setting**

Add New User Extensions

**Extensions List** Extension Max is 100

User Extension	Password	Caller Id	Action
100	123	100	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
101	123	101	<input type="button" value="Advance"/> <input type="button" value="Delete"/>

Figure 3-5. User extension settings

<b>Advance</b>	Click <input type="button" value="Advance"/> to edit an extension other setting.
<b>Delete</b>	Click <input type="button" value="Delete"/> to delete an extension.

Table 3-4. User extension description

➤ **Advance Setup**

**User Extension Advance Setup**

User Extension

Password

Caller Id

• **Call group / Pickup group select**

Call Group  1  2  3  4  5  6  7  8  9  10

Pickup Group  1  2  3  4  5  6  7  8  9  10

• **Call forward option**

Call Forward Always

Call Forward on Busy

Call Forward on No Answer  IF Time out  Sec

• **Voice mail**

Voice mail  Enable

Figure 3-6. Extension advance settings

<b>User Extension</b>	Input Extension number
<b>Password</b>	Input Extension password
<b>Caller Id</b>	Input Extension caller id

Table 3-5. Extension advance description

- **Call group / Pickup group select :**

<b>Call Group</b>	An Extension can set single/multiple call group(s) 1-10 id
<b>Pickup Group</b>	An Extension can set single/multiple Pickup group(s) 1-10 id

Table 3-6. Call / Pickup group description

- **Call forward option :**

<b>Call forward always</b>	Input forward always number
<b>Call forward on busy</b>	Input forward on busy number
<b>Call forward no answer</b>	Input forward no answer number
<b>If time out "XXX" sec</b>	This is the maximum number allowed no answer time out used

Table 3-7. Call forward description

- **Voice mail :**

<b>Voice mail select</b>	Enable / Disable voice mail function
<b>Voice mail name</b>	Input voice mail name
<b>E-Mail address</b>	Input E-mail address
<b>Send voice to mail</b>	Enable / Disable send voice to mail
<b>Delete voice mail after send</b>	Save / Delete voice mail after send

Table 3-8. Voice mail description

## Trunk Management – SIP Trunk

**Services Providers Setting** allows IP PBX register to different SIP systems and ITSP Services (SIP Trunk).

On the "**Providers List**", you can press "**Add**" to add a new service provider or press "**Advance**" to edit the information of specific Service Provider or press "**Delete**" to delete the specified service provider information.



Figure 3-7. Server Providers Setting

➤ **Add New Service Providers**

Step 1. Press "**Add**" button to add an new service provider information.

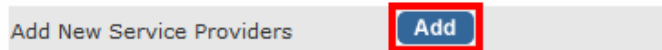


Figure 3-8. Add new service providers

Step 2. Fill in the required information in Service Provider Advance Setup page.

### Service Provider Advance Setup

Caller id

User name

Password

Register server address

Port

Outbound server address

Port

- **On duty / Off duty voice select**
  - Enable
- **Incoming call attendant**

- Dial\_300\_Ring\_Sales\_team
  - Dial\_400\_Ring\_RD\_Team
  - Dial\_500\_Ring\_Group\_1\_RR
  - Dial\_600\_Ring\_Group\_2\_Randon
  - Dial\_9\_to\_Ring\_Operator

Figure 3-9. Service provider advance setup

<b>Caller id</b>	The caller ID will be sent between the callee and caller and will be displayed on SIP device LCD panel for identification.
<b>User name</b>	User name for authentication
<b>Password</b>	User password for authentication
<b>Registrar Server Address</b>	Assigns the SIP Register Server's IP address / Domain name
<b>Registrar Server Port</b>	Port number of SIP Register Server. Assigns a value from 1024 to 65535, the common default SIP port is 5060.
<b>Outbound Proxy Address</b>	Outbound Proxy server's IP address / Domain name. Assign a server's IP / Domain name which is in charge of call-out service.
<b>Outbound Proxy Port</b>	Port number of Outbound Proxy Server. Assign a number from 1024 to 65535, the common default SIP port setting is 5060.
<b>On duty / Off duty voice</b>	When the service provider registered to PBX, incoming calls

<b>select</b>	will hear On / Off duty voice, default settings is "Enable". (For how to record On/Off duty voice please refer " <a href="#">Record Voice Menu</a> ").
<b>Incoming call attendant</b>	<p>Choose a pre-set hunt groups, default is "blank". There are 3 types of combination setup.</p> <ol style="list-style-type: none"> <li>1. If On duty/ Off duty voice is "Enabled", after caller hear the voice menu one time, the call will be transferred to the pre-defined group for call attendant.</li> <li>2. If On duty/ Off duty voice is "Disabled", caller will not hear the voice menu, the call will be directly transferred to the pre-defined group for call attendant.</li> <li>3. If On duty/Off duty voice is "Enabled" and no group is pre-defined, voice menu will repeat itself until incoming caller respond to it.</li> </ol> <p>(For how to make hunt group please refer "<a href="#">Hunt Group Setting</a>")</p>

Table 3-9. Service provider advance setup description

## Trunk Management – Gateway Trunk

**Gateway Trunk Setting** allows IP PBX makes VoIP calls to external Gateway by peer-to-peer mode. If the FXO ports of external Gateway have connected with PSTN lines, the user can make outgoing PSTN calls via external Gateway by this function.



Figure 3-10. Gateway Trunk setting

<b>IP</b>	Destination IP Address is the IP address of the destination Gateway that owns this phone number.
<b>Port</b>	Port is port of the destination Gateway use. (Default is 5060)

Table 3-10. Gateway Trunk setting description

## Trunk Management – Trunk Group

**Trunk Group** is defines the leading digit of the call out dialing number through SIP Trunk or Gateway Trunk. The IP PBX will according to the leading digit to determine to use which SIP or Gateway Trunks

for outgoing route.

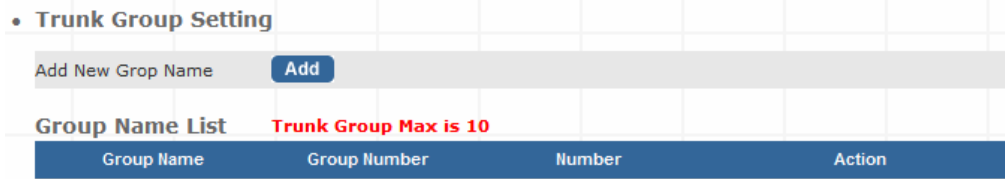


Figure 3-11. Trunk Group setting

➤ **Add New Trunk Group**

Step 1. Press “Add” button to add an new Group Name information.



Figure 3-12. Add an new Group Name

Step 2. Fill in the required information in Trunk Group Setup page.

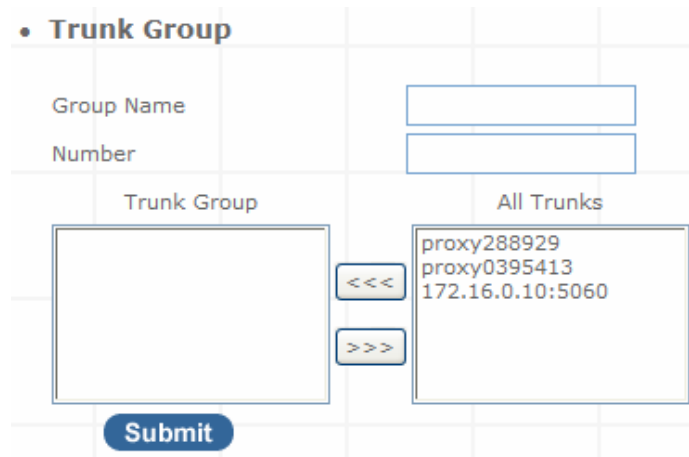


Figure 3-13. Trunk Group Setup


<b>Group Name</b>	The Trunk Group name
<b>Number</b>	If the leading digits are match with this number, IP PBX will delete this number and send out the following digits.
<b>All Trunk</b>	It will show all the available SIP Trunks and Gateway Trunks for selection.
<b>Trunk Group</b>	Choose the trunk at All Trunk box and press the  button to move the activated trunk to Trunk Group box.

Table 3-11. Trunk Group setting description

➤ **Scenario Sample**

IP PBX has created two different SIP trunks and one Gateway trunk for outgoing trunks.

Group Name List		Trunk Group Max is 10	
Group Name	Group Number	Number	Action
SIP_Trunk_1	81	proxy288929	<a href="#">Edit</a> <a href="#">Delete</a>
SIP_Trunk_2	82	proxy0395413	<a href="#">Edit</a> <a href="#">Delete</a>
FXO_Gateway	0	172.16.0.10:5060	<a href="#">Edit</a> <a href="#">Delete</a>

Figure 3-14. Trunk Group sample setting

**One-Stage Call:**

1. If user dials **81**123456, this call will hunt **SIP\_Trunk\_1** and send 123456 to call out.
2. If user dials **82**234567, this call will hunt **SIP\_Trunk\_2** and send 234567 to call out.
3. If user dials **0**345678, this call will hunt **FXO\_Gateway** and send 345678 to call out.

**Two-Stage Call:**

1. If user dials **81** and hear the dial tone, then dial 123456. This call will hunt **SIP\_Trunk\_1** and send 123456 to call out.
2. If user dials **82** and hear the dial tone, then dial 234567. This call will hunt **SIP\_Trunk\_2** and send 234567 to call out.
3. If user dials **0** and hear the dial tone, then dial 345678. This call will hunt **FXO\_Gateway** and send 345678 to call out.

**Trunk Management – Dialing Rules**

When want to make VoIP calls through the above SIP Trunk or Gateway Trunk, the user can use the “**Dialing Rules**” function to simplify the dialing number.

In the “Dialing Rules” settings: Maximum Entries: **100 records**

• **Dialing Rules**

Max Rule is 100			
Phone NO.	Delete Length	Prefix NO.	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<a href="#">Insert</a> <a href="#">Change</a>

Figure 3-15. Dialing Rules settings

Phone Number. is the leading digit of the call out dialing number.

Phone NO Pattern: “**N**” single digit from 2 to 9.

**Phone NO**

“**z**” single digit from 1 to 9.

“**X**” single digit from 0 to 9.

“.” unlimited length of digit.



<b>Delete Length</b>	Delete Length is the number of digits that will be stripped from beginning of the dialed number.
<b>Prefix NO</b>	Prefix NO is the digits that will be added to the beginning of the dialed number.

Table 3-12. Dialing Rules description

➤ **Scenario Sample**

IP PBX has created one SIP Trunk and three Dialing Rules records for making outgoing trunk calls.

**Group Name List** Trunk Group Max is 10

Group Name	Group Number	Number	Action
SIP_Trunk_1	81	proxy288929	<a href="#">Edit</a> <a href="#">Delete</a>

Figure 3-16. Trunk Group sample settings

• **Dialing Rules**

Max Rule is 100

Phone NO.	Delete Length	Prefix NO.	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<a href="#">Insert</a> <a href="#">Change</a>
01	2	77	<a href="#">Edit</a> <a href="#">Delete</a>
02N	2	88	<a href="#">Edit</a> <a href="#">Delete</a>
03z	2	99	<a href="#">Edit</a> <a href="#">Delete</a>
04X	2	11	<a href="#">Edit</a> <a href="#">Delete</a>
05.	2	22	<a href="#">Edit</a> <a href="#">Delete</a>
06	2	33	<a href="#">Edit</a> <a href="#">Delete</a>

Figure 3-17. Dialing Rules sample settings

**One-Stage Call:**

1. If user dials **8101**, this call will hunt SIP\_Trunk\_1 and send **77** to call out.
2. If user dials **81022**, this call will hunt SIP\_Trunk\_1 and send **882** to call out.
3. If user dials **81033**, this call will hunt SIP\_Trunk\_1 and send **993** to call out.
4. If user dials **81044**, this call will hunt SIP\_Trunk\_1 and send **114** to call out.
5. If user dials **810556789**, this call will hunt SIP\_Trunk\_1 and send **2256789** to call out.
6. If user dials **06**, this is an invalid call and user will get the busy prompt sound. (This call won't hunt SIP\_Trunk\_1)

 **Note**

The Dialing Rules function needs to arrange use with Trunk Group function, and it can not be used by itself.

**Two-Stage Call:**

1. If user dials **81** and hear the dial tone, then dial **01**. This call will hunt SIP\_Trunk\_1 and send

- 77 to call out.
2. If user dials 81 and hear the dial tone, then dial 022. This call will hunt SIP\_Trunk\_1 and send 882 to call out.
  3. If user dials 81 and hear the dial tone, then dial 033. This call will hunt SIP\_Trunk\_1 and send 993 to call out.
  4. If user dials 81 and hear the dial tone, then dial 044. This call will hunt SIP\_Trunk\_1 and send 114 to call out.
  5. If user dials 81 and hear the dial tone, then dial 0556789. This call will hunt SIP\_Trunk\_1 and send 2256789 to call out.
  6. If user dials 81 and hear the dial tone, then dial 06678. This call will hunt SIP\_Trunk\_1 and send 06678 to call out.

### Attendant Extension

Attendant Extension in IP PBX system helps you to configure internal dial plan for extension setup. It can allow more calls to be handled by IVR from Gateway's FXO, and FXS port. **Attendant Extension Provide 10 sets of IVR.**

• Attendant Extension

Attendant Extension Number 1	<input type="text"/>
Attendant Extension Number 2	<input type="text"/>
Attendant Extension Number 3	<input type="text"/>
Attendant Extension Number 4	<input type="text"/>
Attendant Extension Number 5	<input type="text"/>
Attendant Extension Number 6	<input type="text"/>
Attendant Extension Number 7	<input type="text"/>
Attendant Extension Number 8	<input type="text"/>
Attendant Extension Number 9	<input type="text"/>
Attendant Extension Number 10	<input type="text"/>

Submit Reset

Figure 3-18. Attendant extension settings

The IP PBX will handle incoming *Caller ID* and show to remote / local registered IP-Phone.

**Note**

If your Gateway can bypass Mobile/Analog Phone number, The IP PBX will handle incoming caller ID and show to remote / local registered IP-Phone.

➤ **Sample:**

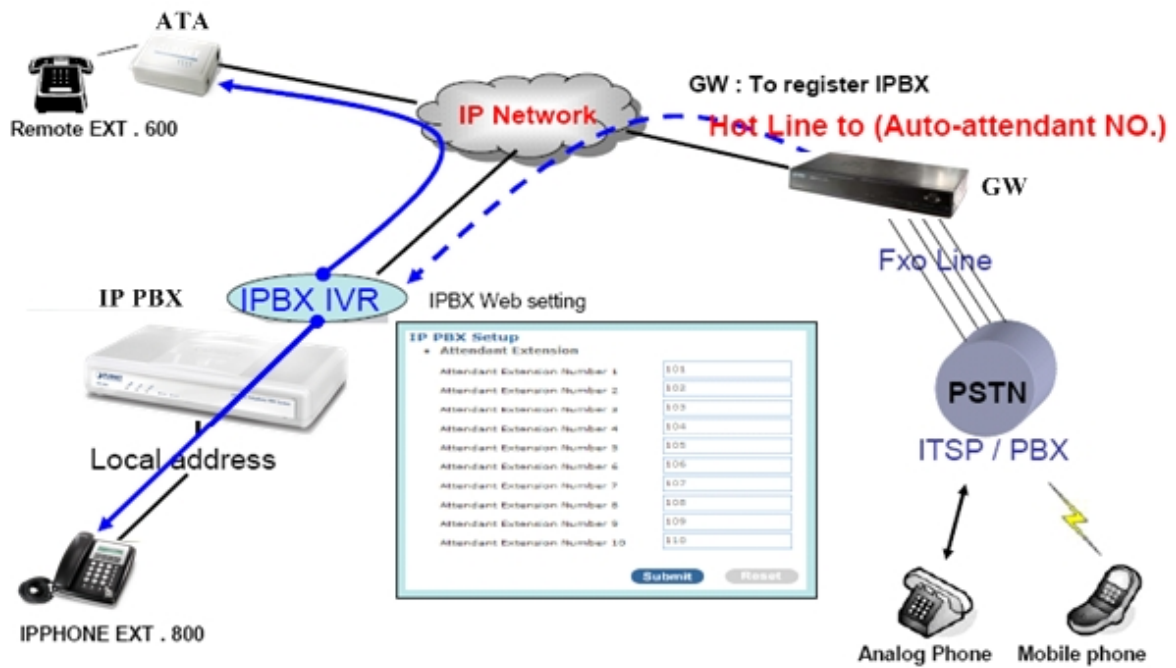


Figure 3-19. Auto-attendant sample

## Time Rules

Defined **Service providers** based on date and time voice rule.

• **Attendant Time**

Day Setting	Start Day	Mon	End Day	Fri
Time Setting	Start Time	08	:	30
	End Time	17	:	30
Month Setting	Start Month	Jan	End Month	Dec
Date Setting	Start Date	1	End Date	31
<b>Submit</b>				

Figure 3-20. Attendant time settings

<b>Day setting</b>	Defined Start day / end time
<b>Time setting</b>	Defined Start time / End time
<b>Month setting</b>	Defined Start Month / End Month
<b>Date setting</b>	Defined Start Date / End Date

Table 3-13. Attendant time description

## Record Voice Menu

Allow you to record On / Off duty voice menu over a register ip-phone.



• **Record Voice Menu**

Record voice  Ex:\*9

Play voice  Ex:\*10

Default voice  Ex:\*11

Password

**Submit**

---

Answer Extension

On - Off Duty

Figure 3-21. Record voice menu settings

Pick up your register IP-Phone handset and press “function key + password “ to enter into voice menu guide.

<b>Record voice</b>	Record your voice menu , Default is *9
<b>Play voice</b>	Play your record voice menu ,Default is *10
<b>Default voice</b>	To set default voice menu, Default is *11
<b>Password</b>	This is record / default voice password , Default is 1234

Table 3-14. Record voice menu description

Answer Extension enable you to record the customized voice menu remotely from a registered IP-Phone.

<b>Answer extension</b>	Call from registered IP-Phone to record the voice menu.
-------------------------	---

Table 3-15. Answer extension description

## Call Parking

Build a calling rule for IP Phone to park the calls during the phone conversation.

## IP PBX Setup

### • Call Parking

Extension to Dial for Parking Calls	<input type="text" value="700"/>	
What extension to park calls on	<input type="text" value="701-720"/>	Ex:100-150
Number of seconds a call can be parked for	<input type="text" value="30"/>	

Figure 3-22. Call parking settings

<b>Extension to Dial for Parking Calls</b>	Set an extension number to dial when need to park the call. Default number is 700.
<b>What extension to park calls on</b>	Set the Extension range for call parking retrieving. (Example: '701-720').
<b>Number of seconds a call can be parked for</b>	Set allowed parking time for the parking call. Default is 30/sec.
<b>Pickup Extension</b>	Set up a number for IP Phone to retrieve back the call. Default is *8.
<b>Timeout for answer on attended transfer</b>	Set a timeout value for answer the transferred call. Default is 30 Sec.

Table 3-16. Call parking description

## General Setting

IP Phone or sip device extension connected IP PBX, extension have call forward / transfer and pickup / voice key ...

### ➤ Call Forward Key

• Call Forward Key		
Call Forward Alway	Enable	<input type="text" value="*1"/> (default:*1)
	Disable	<input type="text" value="*2"/> (default:*2)
Call Forward Busy	Enable	<input type="text" value="*3"/> (default:*3)
	Disable	<input type="text" value="*4"/> (default:*4)
Call Forward No Answer	Enable	<input type="text" value="*5"/> (default:*5)
	Disable	<input type="text" value="*6"/> (default:*6)

Figure 3-23. Call forward key settings

<b>Call forward always</b>	<b>Enable:</b> Dial the “ *1 + number ” enable call forward always function <b>Disable:</b> Dial the “ * 2 ” disable call forward always function
<b>Call forward Busy</b>	<b>Enable:</b> Dial the “ *3 + number ” enable call forward busy function <b>Disable:</b> Dial the “ * 4 ” disable call forward busy function
<b>Call forward no answer</b>	<b>Enable:</b> Dial the “ *5 + number ” enable call forward no answer function <b>Disable:</b> Dial the “ * 6 ” disable call forward no answer function

Table 3-17. Call forward description

➤ **Transfer Feature**

• **Transfer Feature**

Attendant Transfer  (default:#1)

Blind Transfer  (default:#2)

Transfer Digit Timeout  (default:30)

Figure 3-24. Transfer feature settings

<b>Attendant Transfer</b>	When you attendant transfer fail, you can definition other transfer number
<b>Blind Transfer</b>	Blind Transfer , When Ex: Ext 100 call Ext 200, Ext 200 blind transfer to Ext 300 , Ignore the Ext.300 status, the Ext.200 will immediately on-hook
<b>Transfer Digit time out</b>	Set (Attendant/blind) transfer digit time out sec

Table 3-18. Transfer feature description

➤ **Pickup Key**

• **Pickup Key**

Pickup Extension  (default:\*8)

Figure 3-25. Pickup key settings

<b>Pickup Extension</b>	Set call pickup (Default is *8 )
-------------------------	----------------------------------

Table 3-19. Pickip description

➤ **Voice Mail**

• **Voice Mail**

Max Time of A Voice Mail	<input type="text" value="20"/> Seconds(5~20)
Max Number of Messages Per Folder	<input type="text" value="3"/> Seconds
Dial Voice Mail Number	<input type="text" value="*12"/> (default:*12)
Dial My Voice Mail Number	<input type="text" value="*13"/> (default:*13)

Figure 3-26. Voice mail settings

<b>Max time of a voice mail</b>	Set a voice mail max time
<b>Max number of messages per folder</b>	Max number of voice mail per folder
<b>Dial voice mail number</b>	Dial “ *12 “ into voice mail guide
<b>Dial my voice mail number</b>	Dial “ *13 + Ext number “ into voice mail guide

Table 3-20. Voice mail description

➤ **SMTP Setting**

SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified. Input the valid account number, the extension setting voice mail will be been in used.

• **SMTP Setting**

SMTP Server IP / Address	<input type="text"/>
SMTP Autheticated User Name	<input type="text"/>
SMTP Autheticated Password	<input type="text"/>

Figure 3-27. SMTP settings

<b>SMTP server IP / Address</b>	Input server IP / Address
<b>SMTP Authentication user name</b>	Input SMTP Authentication user name
<b>SMTP Authentication password</b>	Input SMTP Authentication password

Table 3-21. SMTP description

**Hunt Group Setting**

This setting will allow the caller to choose the specific extension group to answer the phone (e.g. Press 9 for Operator). Every incoming call (from Service Provider or Attendant Extension) will first hear the pre-recorded On / Off Duty Voice for call group options for caller to select.

Users can also setup multiple groups to manage the incoming calls.

• **Hunt Group Setting**

Add New Gropu Name

**Group Name List**

Group Name	Extension Number	Action
------------	------------------	--------

Figure 3-28. Hunt Group settings

- Press **“Add”** to add a new Hunt Group;
- Press **“Edit”** to the edit a specified hunt group;
- Press **“Delete”** to delete a specified hunt group;

➤ **Add New Hunt Group**

Step 1. Press **“Add”** button to add an new Group Name information.

Add New Gropu Name

Figure 3-29. Add an new Group Name

Step 2. Fill in the required information in Hunt Group Setup page.

• **Hunt Group**

Group Name

Hunt Mode

Incoming Call Dial Number

Ring (Group/Extension) Timeout  sec(default:30)

Ring Group

All Extension/Users

100
101
102
103
104
105
106

Figure 3-30. Hunt Group setup

<b>Group Name</b>	Input your group name
<b>Hunt Mode</b>	<p>There are 3 modes available: <b>Round Robin / Ring All / Random Mode.</b></p> <ol style="list-style-type: none"> <li>1. Round Robin: Take turns ringing each available Extension / Users</li> <li>2. Ring All: Ring all Extension/Users, until any one Extension / Users answer the call.</li> <li>3. Random: Ring random group inside Extension / Users</li> </ol>



<b>Incoming Call Dial Number</b>	Associate a dial number with a call group voice instruction to instruct incoming calls (e.g. If “20” is associated with Group A, when the caller dial “20”, all extensions under Group A will ring). Default incoming call dial number is <i>empty</i> .
<b>Ring (Group/Extension) Timeout</b>	Setup a timeframe to control the call group hunting timeout. Default setting is 30 sec.

Table 3-22. Hunt Group description

➤ **To add extension/users to Ring group**

Step 1. Select your extension

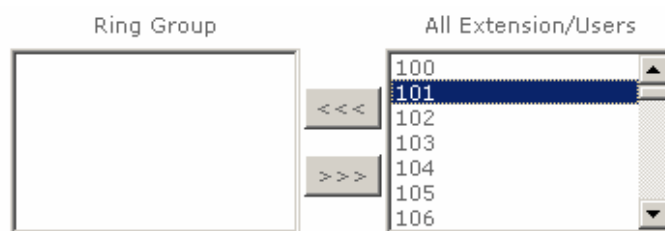



Figure 3-31. Add Extension/User

Step 2. Press  to add extension/users to ring group.

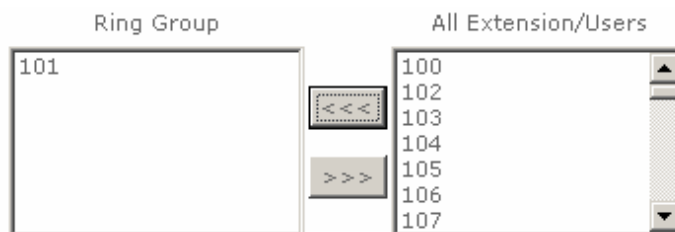


Figure 3-32. Add Extension/User

➤ **To delete Ring Group inside extension/users**

Step 1. Select the extensions

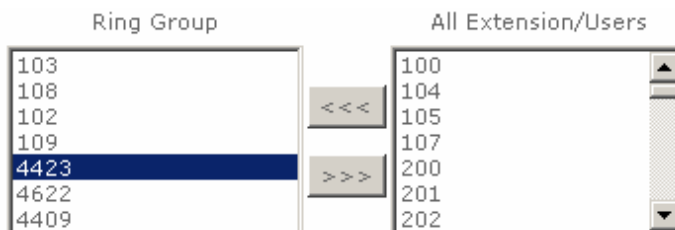



Figure 3-33. Delete Extension/User

Step 2. Press  to delete extension/users to ring group.

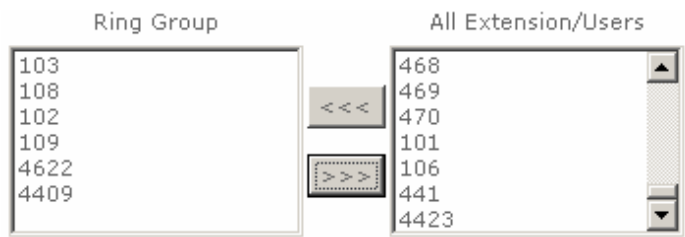


Figure 3-34. Delete Extension/User

# Chapter 4

## Network Setup



### WAN & LAN Setup

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. IP PBX 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 & LAN Setup**", the following setup page will be shown. Three methods are available for Internet Access.

**Network Settings**

- WAN Setting**
  - NAT / Bridge Mode: NAT
  - WAN Port IP Assignment:  Static IP  DHCP  PPPoE
  - Host Name: SIP . IPPBX
  - WAN Port MAC:  Original MAC (00:30:4F:FD:54:0F)  Manual Setting 00:30:4F:88:81:18
  - 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
- LAN Setting**
  - LAN IP Address: 192.168.0.1
  - Subnet Mask: 255.255.255.0
  - DNS Proxy:  Enable

**Submit** **Reset**

Figure 4-1. Network settings

➤ **Static IP**

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. *Example: 168.95.1.2*

The screenshot shows the 'Network Settings' page with the 'WAN Setting' section expanded. The 'NAT / Bridge Mode' is set to 'NAT'. Under 'WAN Port IP Assignment', 'Static IP' is selected with a radio button. The 'Host Name' is set to 'SIP' and 'IPPBX'. Under 'WAN Port MAC', 'Original MAC (00:30:4F:FD:54:0F)' is selected. The 'IP Address' is '172.16.0.1', 'Subnet Mask' is '255.255.0.0', and 'Default Gateway' is '172.16.0.254'.

Figure 4-2. WAN-Static IP settings

<b>IP Address</b>	Check with your ISP provider.
<b>Subnet Mask</b>	Check with your ISP provider.
<b>Default Gateway</b>	Check with your ISP provider.

Table 4-1. WAN-Static IP description

➤ **DHCP**

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:

WAN Port IP Assignment:  Static IP  DHCP  PPPoE

Host Name:  .

WAN Port MAC:  Original MAC (00:30:4F:4F:00:00)  Manual Setting

MTU:  bytes

MRU:  bytes

Set DNS server:  Manually  Automatically

Ping from WAN:  Allowed

Figure 4-3. WAN-DHCP settings

➤ **PPPoE**

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

**• WAN Setting**

NAT / Bridge Mode:

WAN Port IP Assignment:  Static IP  DHCP  PPPoE

Host Name:  .

WAN Port MAC:  Original MAC (00:30:4F:4F:00:00)  Manual Setting

PPPoE Username:

PPPoE Password:

Connect Type:

Max Idle Time:  seconds. (default:600)

MTU:  bytes

MRU:  bytes

Set DNS server:  Manually  Automatically

Ping from WAN:  Allowed

Figure 4-4. WAN-PPPoE settings

➤ **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. It is a computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address. Assign the domain name or IP address of your host computer. When the host operating system is set up it is given a name. This name may reflect the prime use of the computer. For example, a host computer that converts host names to IP addresses using DNS may be called cvs.IP-PBX.com and a host computer that is a web server may be

called [www.IP-PBX.com](http://www.IP-PBX.com). When we need to find the host name from an IP address we send a request to the host using its IP address. The host will respond with its host name.

### ➤ 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.

The WAN port allows your voice gateway to be connected to an Internet Access Device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet Cable. MAC addresses are uniquely set by the network adapter manufacturer and are sometimes called "physical addresses" for this reason. MAC assigns a unique number to each IP network adapter called the MAC address. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows: **00:3f:4f:88:81:18**. The first six hexadecimal digits of the address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number.

Some Internet service providers track the MAC address of a home router for security purposes. Many routers support a process called cloning that allows the MAC address to be simulated so that it matches one the service provider is expecting. This allows end-user to change their router (and their real MAC address) without having to notify the provider. For example, you could allow packets which have your name server's IP on them, but come from another MAC address (one way of spoofing packets).



Figure 4-5. WAN port MAC settings

### ➤ 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.

MRU stands for Maximum Receiving Unit. The largest physical packet size, measured in bytes that a network can receive. Any messages larger than the MRU are divided into smaller packets before being received.

The key is to be deciding how big your bandwidth pipe is and select the best MTU for your configuration. For example, you have a 33.6 modem, you use a MTU and MRU of 576, and if you have a larger pipe you may want to try 1500.

MTU	1500	bytes
MRU	1500	bytes

Figure 4-6. MTU and MRU settings

**Note**

For Static IP, both MTU and MRU are set to 1500 bytes as default value.  
 For DHCP, both MTU and MRU are set to 1500 bytes as default value.  
 For PPPoE, both MTU and MRU are set to 1492 bytes as default value.

➤ **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.ippbx.com](http://www.ippbx.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. When you run your DNS, web, and mail servers all on the same MACHine - if this MACHine goes down, it doesn't really matter that the backup DNS server still works.

The recommended practice is to configure the primary and secondary DNS servers on separate MACHines, on separate Internet connections, and in separate geographic locations.

Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1

Figure 4-7. DNS server settings

<b>Primary DNS Server</b>	Sets the IP address of the primary DNS server.
<b>Secondary DNS Server</b>	Sets the IP address of the secondary DNS server.

Table 4-2. DNS server description

➤ **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.

The default setting is allowed user can ping the host computer from remote site. If you disallow, the host computer doesn't response any user who issues Ping IP address command from any remote sites.

Ping from WAN  Allowed

Figure 4-8. Ping from wan settings

## ➤ LAN Setting

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 192.168.0.1 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. For example, devices in a home or office building would be considered part of a local area network.



• LAN Setting

LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DNS Proxy	<input checked="" type="checkbox"/> Enable

Figure 4-9. LAN settings

<b>LAN IP Address</b>	Assign the IP address of LAN server, default is 222.222.222.1
<b>Subnet Mask</b>	Select a subnet mask from the pull-down menu, default is 255.255.255.0

Table 4-3. LAN description

## ➤ 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

Figure 4-10. DNS proxy settings

## DHCP

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

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



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

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

Figure 4-11. DHCP server settings

When you enable the DHCP server, you are able to enter:

<b>Assigned DHCP IP Address</b>	Enter the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.
<b>DHCP IP Lease Time</b>	Assign the length of time for the IP lease, default setting is 86400 seconds.

Table 4-4. DHCP server description

## WLAN Setting (For IPX-300W)

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.

### ➤ 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.

**WLAN Setting**

WLAN  Enable

W-LAN Role

WLAN Mode

W-LAN Channel  Auto  (default: Channel 10 )

WLAN SSID  Hide SSID

Authentication Method  (default: OPEN )

Encryption Type

Figure 4-12. AP mode settings

<b>WLAN</b>	Enable / Disable WLAN Function
<b>WLAN Mode</b>	For wireless connected type 802.11 B/G mixed / 802.11b only / 802.11G only
<b>WLAN SSID</b>	Wireless stations associating to the access point must have the same SSID. Enter a descriptive name for the wireless LAN.(support 20 ACSII characters)
<b>Hide SSID</b>	Hide SSID prevents outside users from joining the network without knowing the wireless Network's ID, default is check SSID.
<b>WLAN Frequency</b>	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.
<b>WLAN Frequency Auto</b>	When the users select this option, the IP PBX automatically finds the channel with the least interference and uses that channel for wireless IP PBX 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.

Table 4-5. AP mode description

**Example:**

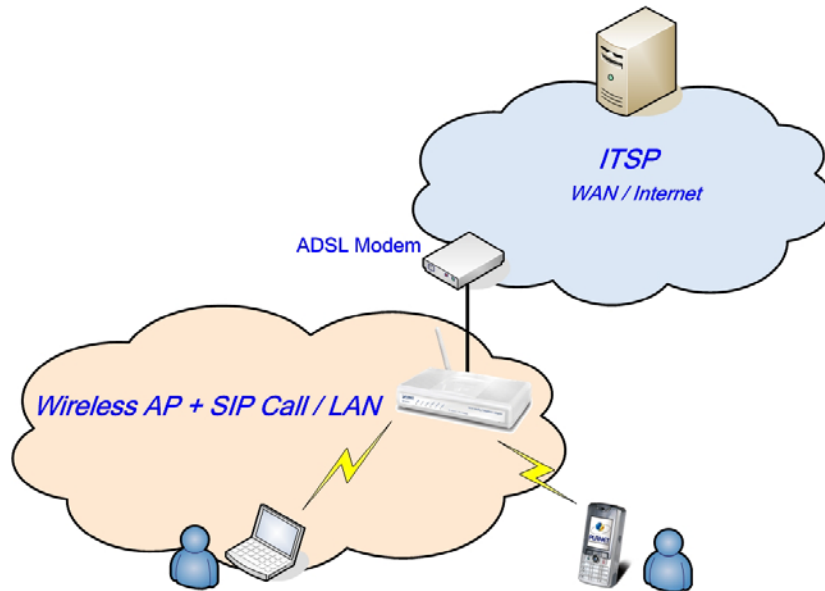


Figure 4-13. AP mode application

➤ **AP-Client Mode**

In this mode the IP PBX is used to access the Wireless Service Provider network by connecting wirelessly to the remote (Outdoor AP).

When the IPBX 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 Setting**

WLAN	<input checked="" type="checkbox"/> Enable
W-LAN Role	AP-Client
WLAN Mode	802.11 B/G mixed
Remote AP SSID	test_wps
<b>Attention:</b> Each AP and Client must have the same channel and encryption type.	
W-LAN NAT / Bridge	NAT
W-LAN Channel	<input type="checkbox"/> Auto 2.422GHZ (channel 3) (default: Channel 10 )
W-LAN IP Assignment	<input type="radio"/> Static IP <input checked="" type="radio"/> DHCP <input type="radio"/> PPPOE
Authentication Method	OPEN (default: OPEN )
Encryption Type	NONE

**Submit** **Reset**

Figure 4-14. AP-client mode settings

**Note**

When IP PBX 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

<b>WLAN Mode</b>	For wireless connected type 802.11 B/G mixed/ 802.11b only / 802.11G only
<b>Remote AP SSID</b>	Define the same as your Wireless Router uses.
<b>Remote AP KEY</b>	Enter the remote AP Authorization Key (WPA-PSK / WPA2-PSK / WPAPSK ,WPA2PSK Mix Mode to Show)
<b>W-LAN Channel</b>	Define the same as your Wireless Router uses.
<b>W-LAN IP Assignment</b>	1. DHCP client 2. Static IP Address
<b>Static IP</b>	Key in the W-LAN IP address, W-LAN Subnet mask and W-LAN Gateway from AP of WISP
<b>DHCP Client</b>	When the DHCP Client is enabled, the IP PBX will get the IP Address from Outdoor AP of WISP.
<b>PPPoE Client</b>	Enter User Name / Password provided by your ISP, the IP PBX will get the IP Address from Outdoor AP of WISP
<b>Remote AP SSID</b>	Define the same as your Wireless Router uses
<b>Authentication Method</b>	Define the same as your Wireless Router uses.(OPEN / SHARED Mode)
<b>Encryption Type</b>	Define the same as your Wireless Router uses. (OPEN / SHARED Mode)
<b>Scan usable network</b>	Select list to remote AP SSID (magnifying glass)

Table 4-6. AP-Client mode description

• **WLAN Setting**

WLAN  Enable

W-LAN Role

WLAN Mode

Remote AP SSID

Figure 4-15. AP-Client mode settings

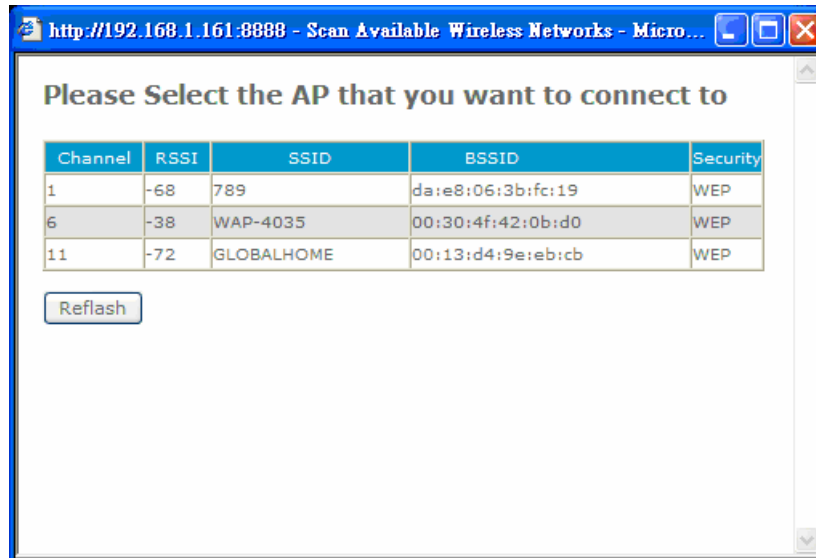


Figure 4-16. Search remote AP list page

**Note**

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

**Example:**

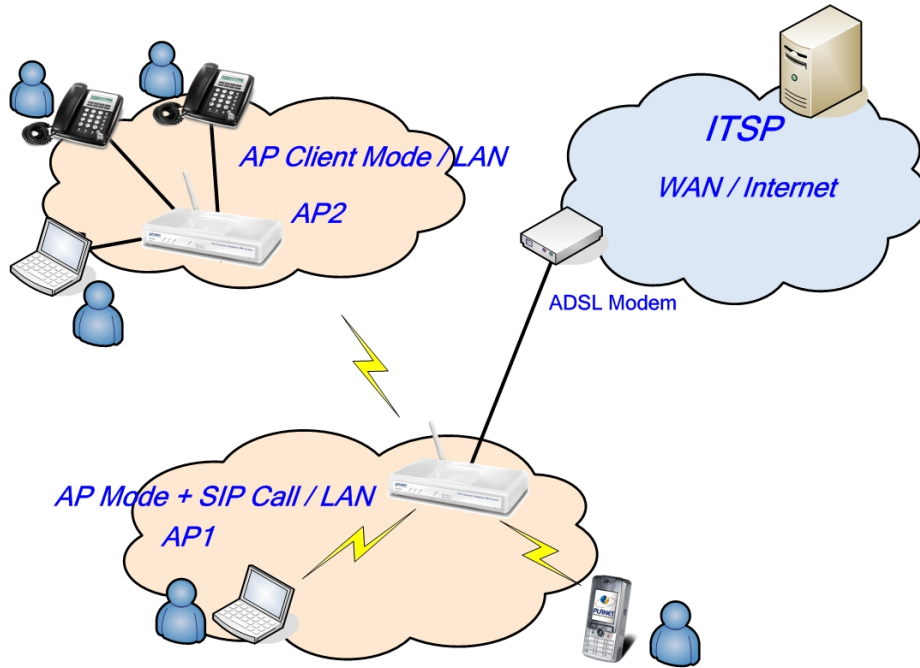


Figure 4-17. Ap-Client mode application

➤ **WISP & AP Mode**

The IP PBX 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.

• **WLAN Setting**

WLAN	<input checked="" type="checkbox"/> Enable
<b>AC Setting</b>	
W-LAN Role	WISP & AP
WLAN Mode	802.11 B/G mixed
Remote AP SSID	test_wps
Remote AP MAC	( Optional )
<b>Attention:</b> Each AP and Client must have the same channel and encryption type.	
W-LAN NAT / Bridge	NAT
W-LAN Channel	<input type="checkbox"/> Auto 2.422GHZ (channel 3) (default: Channel 10 )
W-LAN IP Assignment	<input type="radio"/> Static IP <input checked="" type="radio"/> DHCP <input type="radio"/> PPPOE
<b>AP Setting</b>	
WLAN SSID	IPPBX <input type="checkbox"/> Hide SSID
Authentication Method	OPEN (default: OPEN )
Encryption Type	NONE

Figure 4-18. WISP & AP mode settings

**Note**

When IP PBX 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.

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

Table 4-7. WISP & AP mode description

WLAN	<input checked="" type="checkbox"/> Enable
<b>AC Setting</b>	
W-LAN Role	WISP & AP
WLAN Mode	802.11 B/G mixed
Remote AP SSID	test_wps
Remote AP MAC	( Optional )

Figure 4-19. WISP & AP mode settings

**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

Refresh

Figure 4-20. 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:

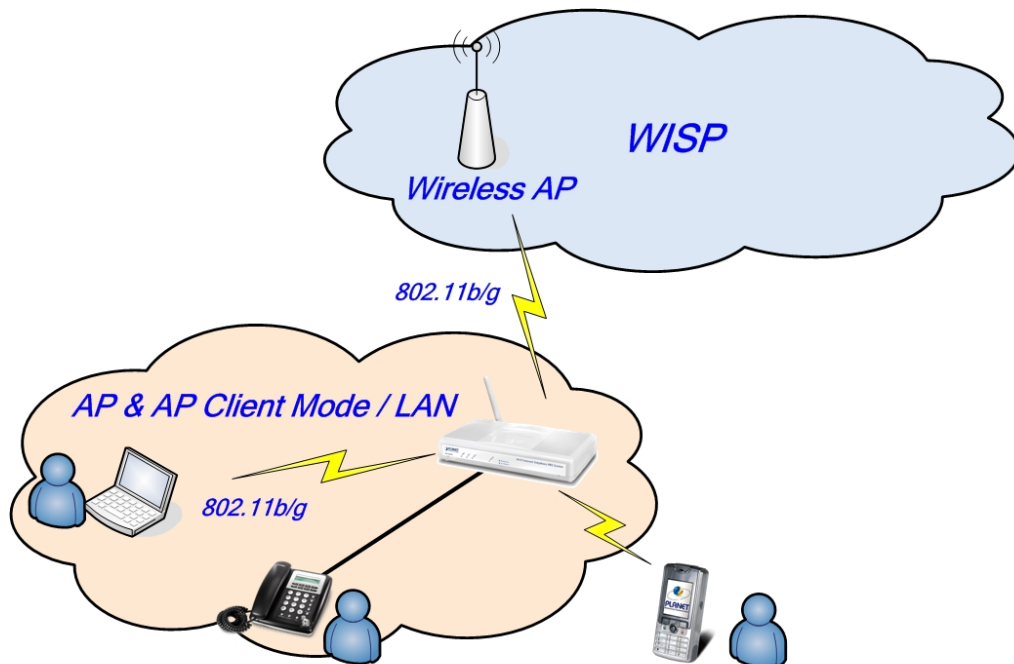


Figure 4-21. WISP & AP mode application

### Access Policy (For AP and WISP&AP mode)

**Access Policy**

In IP PBX security, an access control list is a list of “allow all / Reject all” to an MAC.

**Access Control List**    MAX MAC List : 64

Table 4-8. Access policy description

#### Network Settings

• **Access Policy Setting**

Access Policy

Allow all

Access Control List

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

Figure 4-22. Access policy settings

## Network Settings

- Access Policy Setting

Access Policy	Allow all ▼
Access Control List	<div style="border: 1px solid black; padding: 2px;">             Disable  <span style="background-color: #e0e0e0;">Allow all</span>              Reject all           </div>

Figure 4-23. Access policy settings

## Static Route

Static routes are special routes that the network administrator manually enters into the router configuration for local network management. 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 IP-PBX 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
<input type="checkbox"/>	Net ▼	<input type="text"/>	255.255.255.0 ▼	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Figure 4-24. Static route settings

<b>Enable</b>	Enable/Disable the static route.
<b>Type</b>	Indicates the type of route as follows, Host for local connection and Net for network connection.
<b>Target</b>	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.
<b>NetMask</b>	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.
<b>Gateway</b>	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.
<b>Action</b>	Insert a new Static Router entry or update a specified entry.

Table 4-9. Static route description

## NAT

NAT (Network Address Translation) serves three purposes:

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

**Network Settings**

- **NAT Setting**

Network Address Translation	<input checked="" type="checkbox"/> Enable
IPSec Pass Through	<input checked="" type="checkbox"/> Enable
PPTP Pass Through	<input checked="" type="checkbox"/> Enable
L2TP Pass Through	<input checked="" type="checkbox"/> Enable
SIP ALG	<input type="checkbox"/> Enable
NetMeeting ALG	<input type="checkbox"/> Enable
DMZ	<input type="checkbox"/> Enable

**Submit** **Reset**

- **Virtual Server Mapping**

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<b>Insert</b> <b>Change</b>

- **Port Trigger**

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	TCP	<b>Insert</b> <b>Change</b>

Figure 4-25. NAT settings

### ➤ NAT Setting

- **NAT Setting**

Network Address Translation	<input checked="" type="checkbox"/> Enable
IPSec Pass Through	<input checked="" type="checkbox"/> Enable
PPTP Pass Through	<input checked="" type="checkbox"/> Enable
L2TP Pass Through	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable
NetMeeting ALG	<input checked="" type="checkbox"/> Enable
DMZ	<input checked="" type="checkbox"/> Enable
DMZ LAN IP	<input type="text" value="192.168.0.11"/>

**Submit** **Reset**

Figure 4-26. NAT settings

<b>Network Address Translation</b>	Enable/Disable NAT.
<b>IPSec Pass Through</b>	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.
<b>PPTP Pass Through</b>	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.
<b>L2TP Pass Through</b>	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.
<b>SIP ALG</b>	SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.
<b>DMZ</b>	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 dIP-PBX. 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.
<b>DMZ IP LAN</b>	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.

Table 4-10. NAT description

### ➤ Virtual Server Mapping

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
<input checked="" type="checkbox"/>	80	TCP	192.168.0.17	80	<b>Insert</b> <b>Change</b>

Figure 4-27. Virtual server mapping settings

<b>Enable</b>	Enable/Disable the virtual server mapping, default setting is Disable.
<b>WAN Port</b>	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.
<b>Protocol</b>	The protocol used for the virtual service. Select a protocol type is TCP or UDP.
<b>LAN IP</b>	The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.
<b>LAN Port</b>	The port number of the service used by the Private IP computer. Enter the LAN port number.
<b>Action</b>	Insert a new WAN port or update a specified WAN port.

Table 4-11. Virtual server mapping description

➤ **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 DIP-PBXgram 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
<input checked="" type="checkbox"/>	40	TCP	40	TCP	<b>Insert</b> Change

Figure 4-28. Port trigger settings

<b>Enable</b>	Enable/Disable the port trigger, default setting is Disable.
<b>Trigger Port</b>	This is the port used to trigger the application. It can be either a single port or a range of ports.
<b>Trigger Type</b>	This is the protocol used to trigger the special application.
<b>Public Port</b>	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.
<b>Public Type</b>	This is the protocol used for the special application.
<b>Action</b>	Insert a new Port Trigger or update a specified Port Trigger.

Table 4-12. Port trigger description

## Packet Filter

Controlling access to a network by analyzing the incoming packets and letting them pass or halting them based on the IP addresses of the source. (This function 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
<input type="checkbox"/>			TCP	Always	All	00:00 ~ 00:00	<b>Insert</b> Change

LAN  Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
<input type="checkbox"/>			TCP	Always	All	00:00 ~ 00:00	<b>Insert</b> Change

MAC  Enable

Enable	MAC Address	Block	Day	Time	Action
<input type="checkbox"/>		Always	All	00:00 ~ 00:00	<b>Insert</b> Change

Figure 4-29. Packet filter settings

➤ WAN

<b>WAN Enable/Disable</b>	The WAN IP port packet filter function, control a network IP port, default setting is <i>Enable</i> .
<b>Enable</b>	Enable/Disable the Internet to WAN IP source port rules, default setting is <i>Disable</i> .
<b>Source IP</b>	This is the filter WAN IP address. <i>Example: 209.131.36.158</i>
<b>Dest. Port</b>	This is the port used for source IP service.
<b>Protocol</b>	This Protocol Used for the source IP service. Select either TCP or UDP.
<b>Block</b>	Wan IP Port Block time setting. Select <i>Always</i> or <i>By Schedule</i> .
<b>Day</b>	Block Day setting, select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
<b>Time</b>	Block Time setting, select time range is 00:00 to 23:59.

Table 4-13. Packet filter-WAN description

➤ LAN

<b>LAN Enable/Disable</b>	Internet to LAN filter function, default setting is <i>Enable</i> . A prohibitive rule set should only allow the necessary Internet/DMZ services to LAN (Local Area Network) clients.
<b>Enable</b>	Enable/Disable the WAN IP source port rules, default setting is <i>Disable</i> .
<b>Source IP</b>	This is the filter source IP address to LAN.
<b>Dest. Port</b>	This is the port used for source IP.
<b>Protocol</b>	This Protocol Used for the WAN Filter service. Select either TCP or UDP.
<b>Day</b>	Block Day setting, select All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
<b>Time</b>	Block Time setting, select time range is 00:00 to 23:59

Table 4-14. Packet filter-LAN description

➤ MAC

<b>MAC Enable/Disable</b>	Form internet MAC filter function, default setting is <i>Enable</i> .
<b>Block</b>	Wan IP Port Block time Setting. Select <i>Always</i> or <i>By Schedule</i> .

<b>Day</b>	Block Day setting, select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
<b>Time</b>	Block Time setting, select time range is 00:00 to 23:59

Table 4-15. Packet filter-MAC description

## 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	Client IP	URL Filter String	Action
<input checked="" type="checkbox"/>			Insert Change

Figure 4-30. URL filter settings

<b>Enable</b>	Enable/Disable the URL filter function, default setting is Disable.
<b>Enable</b>	Enable/Disable Block URL to the Client IP, default setting is Disable
<b>Client IP</b>	This is the Client IP is LAN address. <i>Example:</i> 192.168.0.100
<b>URL Filter String</b>	This is the filter URL. <i>Example:</i> "http://www.yahoo.com/"

Table 4-16. URL filter description

## Security

Intrusion Detection has powerful management and analysis tools that let your IT administrator see what's going on in your network. Such as whose 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





Figure 4-31. Security settings

---

**Intrusion Detection** Enable / Disable , network / internet security protection.

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

Table 4-17. Security description

## UPnP

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.



Figure 4-32. UPnP settings

---

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

Table 4-18. UPnP description

## Call Out Block List

The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. Without

DDNS, the users should use the WAN IP to reach internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported, you apply a DNS name (e.g., [www.IPPBX.com](http://www.IPPBX.com)) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the [www.IPPBX.com](http://www.IPPBX.com) regardless of the WAN IP.

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

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

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

**Network Settings**

- **DDNS Setting**

DDNS  Enable

DDNS Server Type

DDNS Username

DDNS Password

Confirmed Password

Hostname to register

DDNS Interval Registration  Enable

Figure 4-33. DDNS settings

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

Table 4-19. DDNS description

## SNTP

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 dIP-PBXbase schema, and a set of dIP-PBX objects.

Figure 4-34. SNMP settings

<b>Enable</b>	Enable/Disable the SNMP service, default setting is Disable. (Support SNMP version 1 or SNMP version 2c).
<b>SNMP Read Community</b>	SNMP Read Community string so that EPICenter can retrieve information.(default :public)
<b>SNMP Write Community</b>	Specifies the name of the SNMP write community to which the printer device that this actual destination represents belongs.(Default:private)
<b>SNMP Trap Host</b>	Defines an SNMP trap host to which AppCelera will send trap messages. (Default address is empty)
<b>SNMP Trap Community</b>	The SNMP trap community name. The community name functions as a password for sending trap notifications to the target SNMP manager. (Default: public).

Table 4-20. SNMP description

# Chapter 5 Management

# 5

## Admin Account

The administrator account can access the management interface through the web browser.

Figure 5-1. Management settings

<b>Administrator Name</b>	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; “_”.
<b>Administrator Password</b>	Assign an administrator password. Maximum 16 characters and minimum 6 characters with mix of digits and letters 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 “_”.
<b>Confirm Password</b>	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.
<b>Remote Administration</b>	Enable/Disable to access from remote site. Default setting is “Disable”.
<b>Http port for remote</b>	If you allowed the access from the remote site, assign the http port used to access the IP-PBX. Default port number is “8080”.
<b>Remote administration only from IP</b>	Internet IP address of the computer that has access to the IP-PBX. Assign the legal IP address. <i>Example:</i> 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.

Table 5-1. Management description

**Note**

- The administrator name and password are *case-sensitive* and the "blank" character is an *illegal character*
- Only the administrator account has the ability to change account password.

## Date & Time

### ➤ Manual Time Setting

#### Management

##### • Date/Time

Date Time Set By  Manual Time Setting  NTP Time Server

Time Zone

Daylight Saving

Date Value Setting Year:  Month:  Day:

Time Value Setting Hour:  Minute:  Second:

Figure 5-2. Date/Time-Manual time settings

Manual Time Setting	Set up the time manually.
---------------------	---------------------------

Table 5-2. Date/Time-Manual time description

### ➤ NTP Time Server

#### Management

##### • Date/Time

Date Time Set By  Manual Time Setting  NTP Time Server

Time Zone

Daylight Saving

NTP Update Interval  hours (1..1000, default:24)

NTP Server 1

NTP Server 2

Figure 5-3. Date/Time-NTP time settings

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

Table 5-3. Date/Time-NTP time description

## Ping Test

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping (Packet Internet Groper) and click Ping. *Example:* www.yahoo.com or 209.131.36.158



Figure 5-4. Ping test settings

<b>Ping Destination</b>	Assign a legal IP address.
-------------------------	----------------------------

Table 5-4. Ping test description

## Save & Restore

All settings can be saving to a local file. Pervious device configuration can also be restored by upload a local file back to the device.

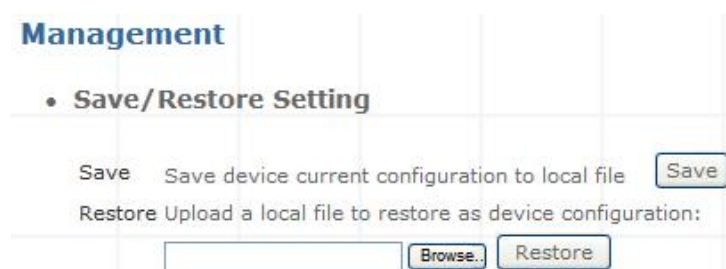


Figure 5-5. Save/Restore settings

## Factory Default

This function is used to restore all the parameters back to factory default setting. You can use the Save/Restore Setting 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**

Figure 5-6. Factory default settings

## Admin Account

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.



Figure 5-7. Firmware update settings

---

<b>Firmware Name</b>	Select that you want to upgrade Firmware version.
----------------------	---

---

Table 5-5. Firmware update description

# Chapter 6 Information

# 6

## System Information

**System Information** page indicates the current setup-status of the device, it includes LAN, WAN, (Status and MAC Address), Host Name / System Date time / Machines Life time and system firmware information. The information and options on this page will vary according to your WAN setting (Static IP, DHCP, or PPPoE).

-If your WAN connection is set up for *Dynamic IP address*, the page will display “Release” and “Renew” buttons. Use “Release” to disconnect from your ISP and use “Renew” to connect to your ISP.

-If your WAN connection is set up for *PPPoE*, the page will display “Connect” and “Disconnect” buttons. Use "Disconnect" to drop the PPPoE connection and use "Connect" to establish the PPPoE connection

System Information	
<b>• System</b>	
Firmware Version	IPPBX 0.0.10
Host Name	SIP.IPPBX
Date & Time	Mon Feb 25 11:48:27 CST 2008
Life Time	1 hour(s)20 min(s)42 sec(s)
Mode	NAT
<b>• WAN</b>	
WAN Type	Static IP
IP Address	172.16.0.1
Subnet Mask	255.255.0.0
Default Gateway	172.16.0.254
MTU	1500
DNS 1 (Primary)	168.95.1.1
DNS 2 (Secondary)	168.95.192.1
<b>• LAN</b>	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server Function	Enabled
<b>• Physical MAC</b>	
WAN	00:30:4F:50:00:06
LAN	00:30:4F:50:00:07

Figure 6-1. System Information



## PBX Extension Status

This page displays the information of Extension/Users Registration status.

• **Extension Status**

Num	Status	Num	Status	Num	Status
200	✗	101	✗	100	○

Figure 6-2. Extension Status




 <b>Register OK</b>	SIP device is connected to IPPBX
 <b>Talk on the telephone</b>	The connection from/to the other end of SIP device is established.
 <b>Register Unknown</b>	Sip device is not connected to IPPBX

Table 6-1. Extension Status description

## PBX Trunk Status

This page displays the information of Service Provider Registration status.

• **Service Provider Status**

Num	Status	Num	Status	Num	Status
0395413	✗	288929	○		

Figure 6-3. Service Provider Status



 <b>Register OK</b>	SIP Trunk is registered
 <b>Register Unknown</b>	SIP Trunk is not registered

Table 6-2. Service Provider Status description

## Call Detail Record

Call Detail Record (CDR) contains the call history of the extensions when calls was made or received.

Recorded information include: Source Number, Destination Number, Start Time, Answer Time, End Time, Duration Time and Status.

- Call Detail Record

<< [1] >>

Source No	Destination No	Start Time	Answer Time	End Time	Duration Time	Status
200	100	2007-11-28 14:23:51	2007-11-28 14:23:51	2007-11-28 14:24:16	25	ANSWERED
100	out	2007-11-28 14:24:41	2007-11-28 14:24:42	2007-11-28 14:24:47	6	ANSWERED
2010	s	2007-11-28 14:24:42	2007-11-28 14:24:42	2007-11-28 14:24:47	5	ANSWERED
100	out	2007-11-28 14:24:52	2007-11-28 14:24:57	2007-11-28 14:24:58	6	ANSWERED
431	100	2007-11-28 14:29:06	2007-11-28 14:29:07	2007-11-28 14:29:11	5	ANSWERED
431	100	2007-11-28 14:30:12	2007-11-28 14:30:14	2007-11-28 14:30:26	14	ANSWERED

Figure 6-4. Call Detail Record

Press << to go to the Next page; Press >> to go to the Previous page

<b>Source No</b>	Caller's ID
<b>Destination No</b>	ID of destination extension / user
<b>Start Time</b>	The date/time when the call initiated
<b>Answer Time</b>	The date/time when the call answered
<b>End Time</b>	The date/time when the call terminated
<b>Duration Time</b>	Duration of the call, in seconds, from Start Time to End Time.
<b>Status</b>	4 status available (1) Answered; (2) No Answer; (3) Busy; (4) Failed.

Table 6-3. Call Detail Record description

**Note**

- IPPBX / WIPPBX have save Maximum 500 Records to the memory. If you press Reset bottom or reboot the system, the record will be erased.

# Appendix A

## How to use Call Parking function

The followings are the Call Park function settings, and all of VoIP devices (ATA, GW and IP Phone) were registered with Wi-Fi IP PBX.

- **Extension to Dial for Parking Calls: 700**
- **Extensions to park calls on :701-720**

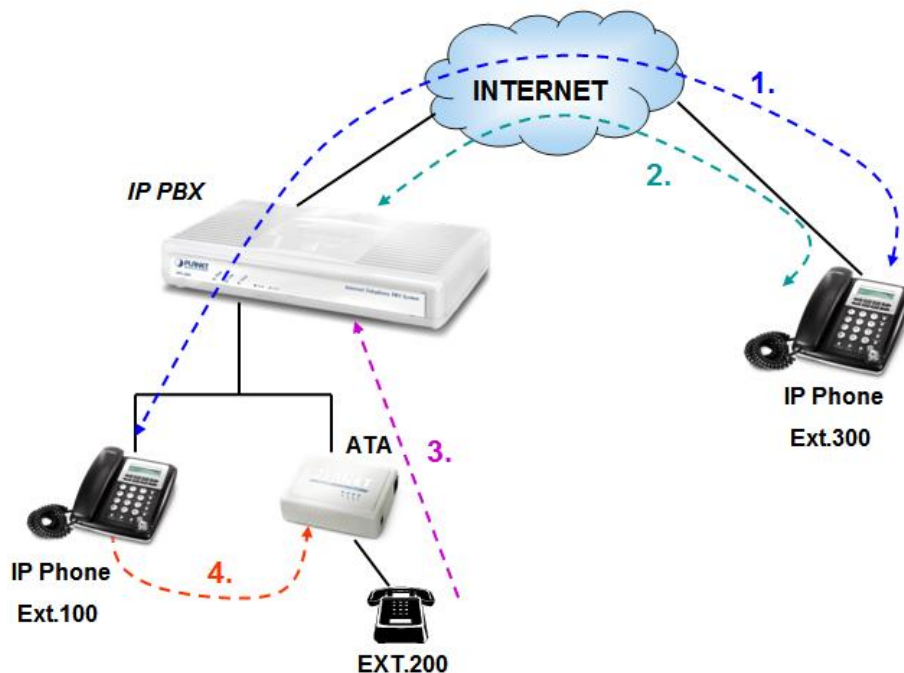


Figure A-1. Call Parking sample scenario

1. Ext.100 and Ext.300 are talking.
2. Ext.300 press Transfer button and dial "700#" to carry out the Call Parking function, and the voice guide will tell Ext.300 a retrieve number (ex:701) to set parking call (At this moment, the remote extension will hear the holding music.)
3. Ext.200 dial retrieve number (ex:701) to pick up call.
4. Ext.100 are talking with Ext.200

# Appendix B

## How to use Call Pickup function

The followings are the Call Pickup function settings, and all of VoIP devices (ATA, GW and IP Phone) were registered with IP PBX.

- **Pickup Extension: \*8**

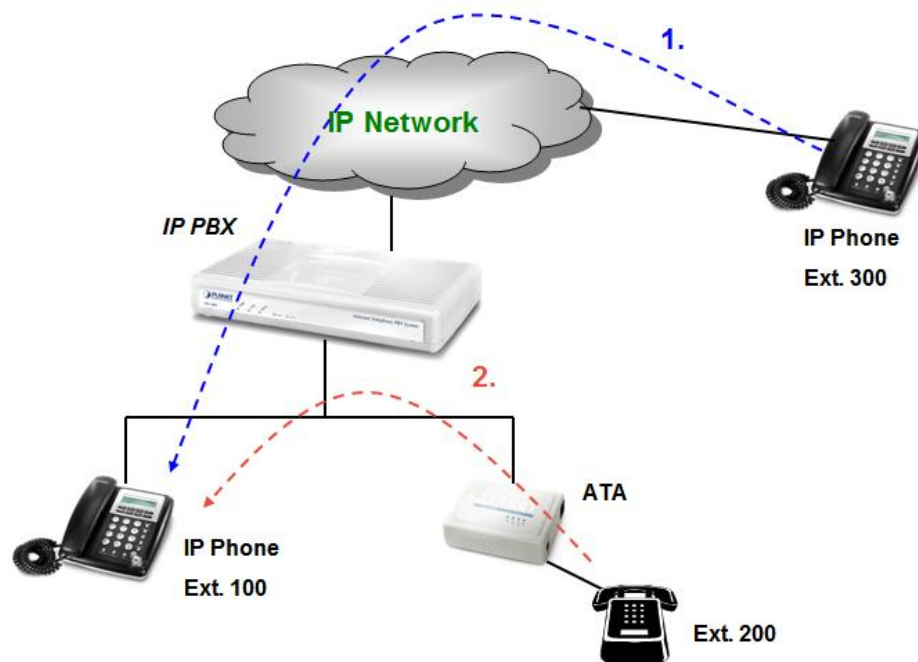


Figure B-1. Call Pickup sample scenario

1. Ext.300 call to Ext.100, and Ext.100 is ringing.
2. Ext.200 dial "**\*8#**" to pickup the call for Ext.100, and Ext.200 is talking with Ext.300.

# Appendix C

## Record Voice Guide Process

IPX-300W provides **Record Voice Menu by Phone** function. Please register your VoIP devices to Wi-Fi IP PBX at first, and then check the Record voice code from “**IP PBX Setup -> record Voice Menu**” page.

• Record Voice Menu		
Record voice	<input type="text" value="*9"/>	Ex:*9
Play voice	<input type="text" value="*10"/>	Ex:*10
Default voice	<input type="text" value="*11"/>	Ex:*11
Password	<input type="text" value="1234"/>	
<input type="button" value="Submit"/>		

Figure C-1. Record voice menu settings

VoIP devices dial **\*9** to enter the Record Voice Menu, then refer to the following record processes to record the Voice Menu.

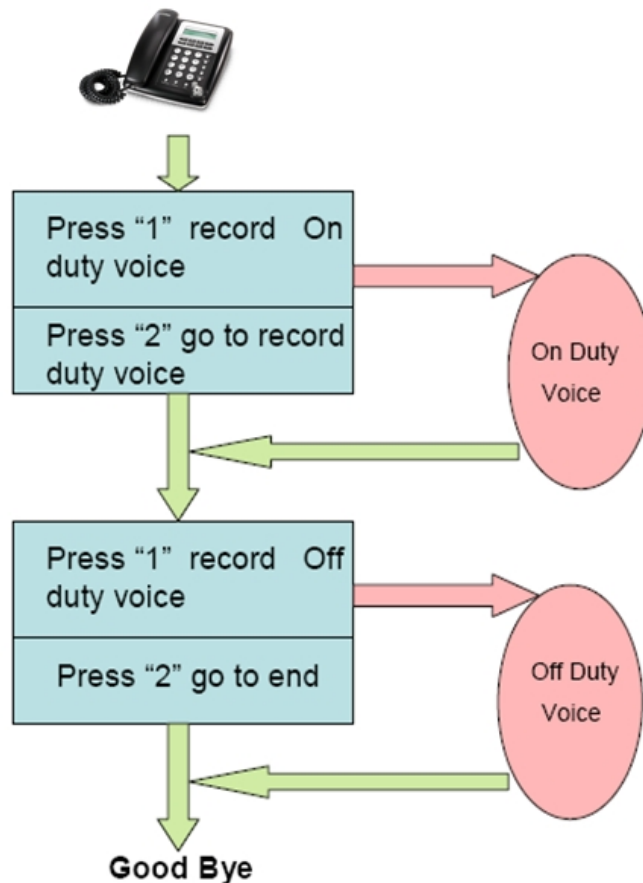


Figure C-2. Voice record processes

# Appendix D

## Voice Communication Samples

The chapter shows you the concept and command to help you configure your IP PBX System through sample configuration. And provide several ways to make calls to desired destination in IP PBX. In this section, we'll lead you step by step to establish your first voice communication via web browsers operations.

### IP Phone and Wi-Fi Phone register to IPX-300W

In the following samples, we'll introduce IP Phone and Wi-Fi Phone register to IP PBX applications.

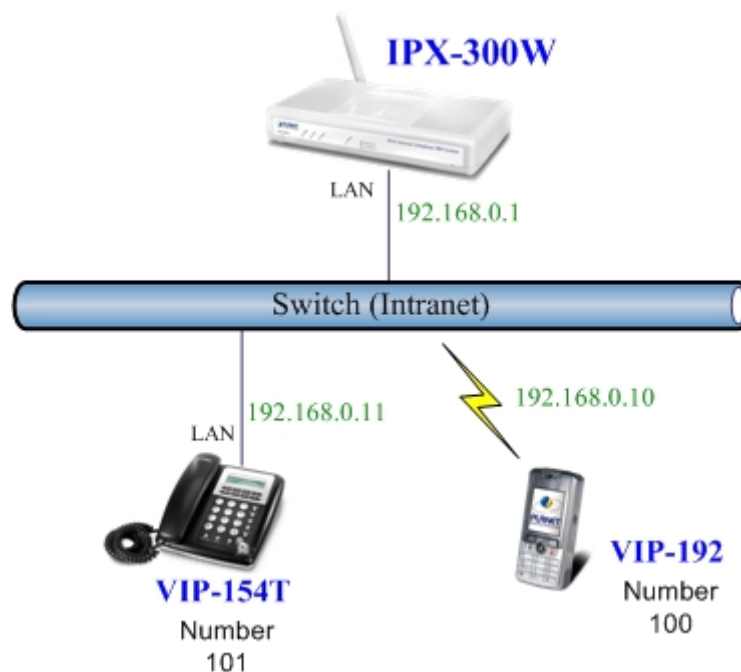


Figure D-1. Topology of instruction example

#### ➤ Machine Configuration:

##### STEP 1:

Please log in IP PBX via web browser and browse to “**Network Setup -> WLAN Setting**” configuration menu. Enable the WLAN and setup the related configuration. The sample configuration screen is shown below:

• **WLAN Setting**

WLAN	<input checked="" type="checkbox"/> Enable
W-LAN Role	AP Only
WLAN Mode	802.11 B/G mixed
W-LAN Channel	<input type="checkbox"/> Auto <input checked="" type="checkbox"/> 2.422GHZ (channel 3) (default: Channel 10 )
WLAN SSID	IPPBX <input type="checkbox"/> 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/Client enabled , and encryption type is WEP . AP and Client will use the same WEP key

<input checked="" type="radio"/> Key 1	<input checked="" type="radio"/> HEX <input type="radio"/> ASCII	1234567890
<input type="radio"/> Key 2	<input checked="" type="radio"/> HEX <input type="radio"/> ASCII	
<input type="radio"/> Key 3	<input checked="" type="radio"/> HEX <input type="radio"/> ASCII	
<input type="radio"/> Key 4	<input checked="" type="radio"/> HEX <input type="radio"/> ASCII	

Figure D-2. WLAN Setting of IPX-300W

**STEP 2:**

Browse to “**IP PBX Setup → User Extensions Setup**” configuration menu.

**IP PBX Setup**

• **User Extensions Setting**

Add New User Extensions

**Extensions List** Extension Max is 100

User Extension	Password	Caller Id	Action
----------------	----------	-----------	--------

Figure D-3. User extension setting of IP PBX

**STEP 3:**

Click the “**Add**” button to create extension account ext.100 and ext.101.

### User Extension Advance Setup

User Extension	<input type="text" value="100"/>
Password	<input type="text" value="123"/>
Caller Id	<input type="text" value="100"/>
<b>• Call group / Pickup group select</b>	
Call Group	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10
Pickup Group	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10
<b>• Call forward option</b>	
Call Forward Always	<input type="text"/>
Call Forward on Busy	<input type="text"/>
Call Forward on No Answer	<input type="text"/> IF Time out <input type="text" value="20"/> Sec
<b>• Voice mail</b>	
Voicemail	<input type="checkbox"/> Enable
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Figure D-4. Add extension setting of IP PBX

**STEP 4:**

Please log in VIP-154T and browser to “**SIP setting → Domain Service**” configuration menu. Insert the account/password information then save and reboot machine. The sample configuration screen is shown below:

## Service Domain Settings

You could set information of service domains in this page.

Realm 1 (Default)	
Active:	<input checked="" type="radio"/> On <input type="radio"/> Off
Display Name:	<input type="text" value="101"/>
Line Number:	<input type="text" value="101"/>
Register Name:	<input type="text" value="101"/>
Register Password:	<input type="text" value="•••"/>
Domain Server:	<input type="text" value="192.168.0.1"/>
Proxy Server:	<input type="text" value="192.168.0.1"/>
Outbound Proxy:	<input type="text"/>

Data match with Figure D-3. IP PBX's extension settings

The IP address of IP PBX

Figure D-5. Web page of VIP-154T

**STEP 5:**

Please take VIP-192 and setup the wireless network to connect with IP PBX (IPX-300W) by keypad menu method. Then log in VIP-192 via web browser and browser to “**SIP Settings**” configuration menu. Insert the Register and Outbound Proxy IP Address information.



SIP Phone Setting	
SIP Phone Port Number	5060 [1024 - 65535]
Registrar Server	
Registrar Server Domain Name/IP Address	192.168.0.1
Registrar Server Port Number	5060 [1024 - 65535]
Authentication Expire Time	3600 sec. (Default: 3600 sec.) [60 - 9999]
Outbound Proxy Server	
Outbound Proxy Domain Name/IP Address	192.168.0.1
Outbound Proxy Port Number	5060 [1024 - 65535]

Figure D-6. SIP settings of VIP-192

Then browse to **“SIP Account Settings”** configuration menu and fill in the account/password information. The sample configuration screen is shown below:

SIP Account Setting	
Default Account	Account 1
Account 1 Setting	
Account Active	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Display Name	100
SIP User Name	100
Authentication User Name	100
Authentication Password	●●●
Register Status	Register

Figure D-7. SIP account settings of VIP-192

**STEP 6:**

After both of devices have registered to IP PBX successfully, it could browse to **“Information -> PBX Extension Status”** page to show the registration status:

Information					
• Extension Status					
Num	Status	Num	Status	Num	Status
100		101			

Figure D-8. Extension status

➤ **Test the Scenario:**

1. VIP-154T pick up the telephone
2. Dial the number: 100 (VIP-192) shall be able to connect to the VIP-192
3. Then the VIP-192 should ring. Please repeat the same dialing steps on VIP-192 to establish the first voice communication from VIP-154T

## IP Phone and Wi-Fi Phone make off-Net calls via Gateway

In the following samples, we'll introduce VIP-154T and VIP-192 makes off-Net Calls (PSTN calls) via VIP-480FO applications.

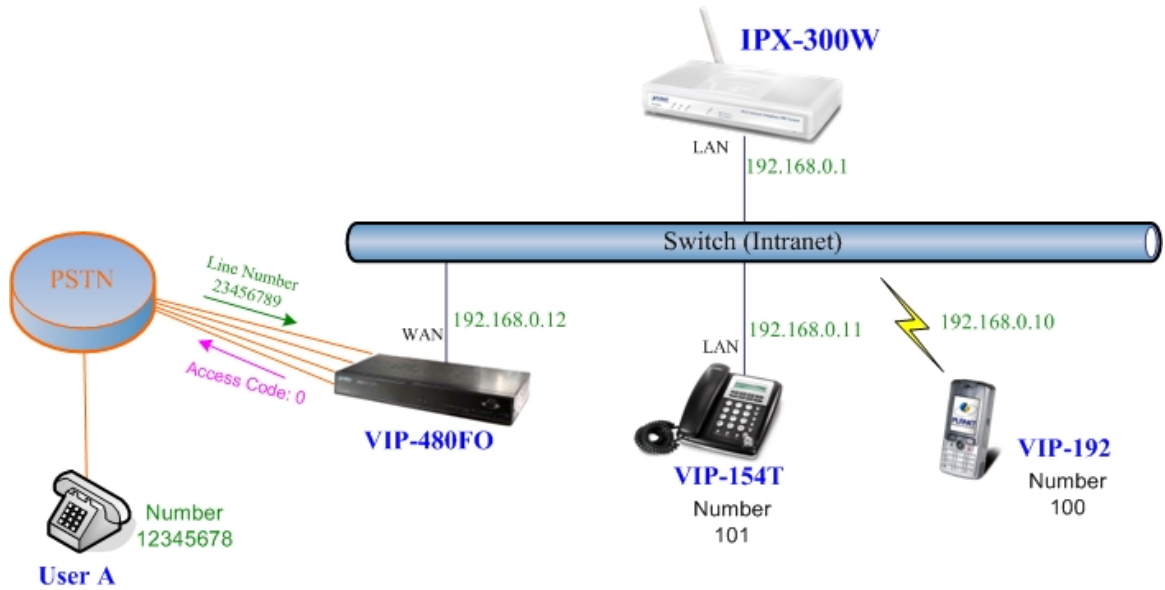


Figure D-9. Installation example with VIP-480FO

### ➤ Machine Configuration:

#### STEP 1:

Please refer to the first sample and let VIP-154T and VIP-192 register to IP PBX.

#### STEP 2:

Please log in IP PBX via web browser and browse to “**IP PBX Setup → User Extensions Setup**” configuration menu to add four accounts for VIP-480FO using.

• **User Extensions Setting**

Add New User Extensions

**Extensions List** Extension Max is 100

User Extension	Password	Caller Id	Action
100	123	100	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
101	123	101	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
200	123	200	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
201	123	201	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
202	123	202	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
203	123	203	<input type="button" value="Advance"/> <input type="button" value="Delete"/>

Figure D-10. Add accounts for VIP-480FO

**STEP 3:**

Browse to “**IP PBX Setup → Attendant Extension**” configuration menu. Assign an attendant number which inexistence extension in Extension List and the sample configuration screen is shown below:

• Attendant Extension	
Attendant Extension Number 1	<input type="text" value="555"/>
Attendant Extension Number 2	<input type="text"/>
Attendant Extension Number 3	<input type="text"/>
Attendant Extension Number 4	<input type="text"/>
Attendant Extension Number 5	<input type="text"/>
Attendant Extension Number 6	<input type="text"/>
Attendant Extension Number 7	<input type="text"/>
Attendant Extension Number 8	<input type="text"/>
Attendant Extension Number 9	<input type="text"/>
Attendant Extension Number 10	<input type="text"/>

Figure D-11. Assign an attendant number

Pressing the “**Submit**” button for activate the configuration.

**STEP 4:**

Browse to “**IP PBX Setup → Trunk Management → Gateway Trunk**” configuration menu. Fill in the IP address of VIP-480FO for connecting with VIP-480FO by peer-to-peer mode, and press the “**Insert**” button for activate the configuration.

• Gateway Trunk Setting		
Add Gateway trunk <span style="color: red;">Gateway trunk Max is 10</span>		
IP	Port	Action
<input type="text" value="192.168.0.12"/>	<input type="text" value="5060"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Figure D-12. Add an Gateway trunk for connecting with VIP-480FO

**STEP 5:**

Browse to “**IP PBX Setup → Trunk Management → Trunk Group**” configuration menu. Add a Trunk Group for making off-Net calls via VIP-480FO.

• **Trunk Group Setting**

Add New Grop Name

**Group Name List** Trunk Group Max is 10

Group Name	Group Number	Number	Action
VIP-480FO	0	192.168.0.12:5060	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure D-13. Add Trunk Group number for grabbing the FXO ports of VIP-480FO

**STEP 6:**

Please log in VIP-480FO via web browser and browse to “**Advance Setup → VoIP Setup → VoIP Basic**” configuration menu. Insert the account/password information and set up the hunting function. The sample configuration screen is shown below:

Port Number / Password Setting(MAX 20 digit) :

No.	Number	Reg	Account	Password	Register Status	Reason
1	<input type="text" value="200"/>	<input checked="" type="checkbox"/>	<input type="text" value="200"/>	<input type="text" value="..."/>	Success	OK
2	<input type="text" value="201"/>	<input checked="" type="checkbox"/>	<input type="text" value="201"/>	<input type="text" value="..."/>	Success	OK
3	<input type="text" value="202"/>	<input checked="" type="checkbox"/>	<input type="text" value="202"/>	<input type="text" value="..."/>	Success	OK
4	<input type="text" value="203"/>	<input checked="" type="checkbox"/>	<input type="text" value="203"/>	<input type="text" value="..."/>	Success	OK

Figure D-14. Set up the number of FXO ports of VIP-480FO

SIP Hunting Table :

No.	Hunting Member
1	<input checked="" type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/> Port 3 <input checked="" type="checkbox"/> Port 4
2	<input checked="" type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/> Port 3 <input checked="" type="checkbox"/> Port 4
3	<input checked="" type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/> Port 3 <input checked="" type="checkbox"/> Port 4
4	<input checked="" type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2 <input checked="" type="checkbox"/> Port 3 <input checked="" type="checkbox"/> Port 4

Figure D-15. Set up the Hunting Member of FXO ports

SIP Proxy Setting :

Domain/Realm	<input type="text" value="192.168.0.1"/>
SIP Proxy Server	<input type="text" value="192.168.0.1/5060"/> <input type="checkbox"/> use net2phone
Register Interval(seconds)	<input type="text" value="900"/>
SIP Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Outbound Proxy Server	<input type="text" value="0.0.0.0"/>

Figure D-16. Set up the Proxy Server IP address for register to IPX-300W

**STEP 7:**

Browse to **“Dialing Plan”** configuration menu. Add an Incoming Dial Plan (no.1x) for redirect the PSTN outgoing calls to FXO ports.

Incoming Dial Plan: (maximun 50 entries, maximun length of prefix digits is 16 digit, maximun length of number is 20 digit):

Item	Incoming no.	Length of Number	Delete Length	Prefix no.	Destination telephone port	Operation
1	1x	2 ~ 20	0	None	1	
	<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<b>ADD</b>

**DELETE** Inbound Dial Plan From  To

Figure D-17. Add an incoming dial plan

**STEP 8:**

Browse to **“Port Status”** configuration menu. Fill in the auto attendant number **555** to all of ports. ( Where 555 is the auto-attendant number of IP PBX )

Hot Line Number Setting (Hotline Setting)

Hotline Delay  Disable  Enable

Hotline Delay Time(Max. 20 sec)  sec

Port 1 number

Port 2 number

Port 3 number

Port 4 number

**Apply**

Figure D-18. Hot Line to auto-attendant of IPX-300W

**STEP 8:**

After all of devices have registered to IP PBX successfully, the **Extension Status** page will show the registration status:

• **Extension Status**

Register OK! 
  Talk on the Telephone ! 
  Register Unknown!

Num	Status	Num	Status	Num	Status
203	<input checked="" type="radio"/>	202	<input checked="" type="radio"/>	201	<input checked="" type="radio"/>
200	<input checked="" type="radio"/>	101	<input checked="" type="radio"/>	100	<input checked="" type="radio"/>

Figure D-19. Extension status page with Phone and Gateway registered

➤ **Test the Scenario:**

1. VIP-154T pick up the telephone
2. Dial the number: 0 will hear the dial tone, and dial the number: 12345678. This call will hunt the FXO port of VIP-480FO and shall be able connect to the User A.
3. Then the telephone of User A will ringing, User A can pick up the handset and talk with VIP-154T.
4. Both VIP-154T and User A hang up the calls.
5. User A pick up the telephone and dial the number: 23456789 should be able to connect to the Auto Attendant System of IP PBX.
6. The User A will hear the prompts, and dial the extension number: 100 shall be able connect to the VIP-192.
7. Then the VIP-192 should ringing, and it to pick up the call then talk with User A.

## IP Phone and Wi-Fi Phone make external SIP Proxy calls via SIP Trunk

In the following samples, we'll introduce VIP-154T and VIP-192 makes SIP Proxy calls via SIP Trunk applications.

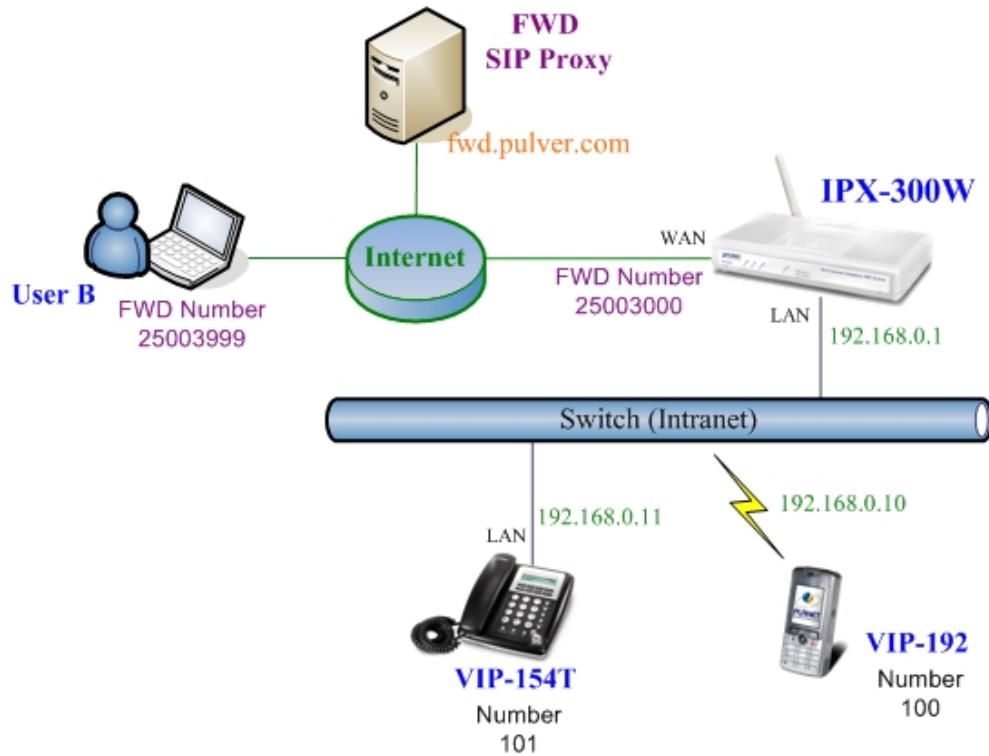


Figure D-20. Installation example with VIP-480FO

### ➤ Machine Configuration:

#### STEP 1:

Please refer to the first sample and let VIP-154T and VIP-192 register to IP PBX.

#### STEP 2:

Browse to “IP PBX Setup → Trunk Management → SIP Trunk” configuration menu. Add a new Service Provider account for registering to FWD SIP Proxy.

• **Server Providers Setting**

Add New Service Providers

**Providers List** Service Provider Max is 10

Caller Id	UserName	Password	Proxy	Port	Action
25003000	25003000	123	fwd.pulver.com	5060	<input type="button" value="Advance"/> <input type="button" value="Delete"/>

Figure D-21. Add a Service Provider account

### STEP 3:

Browse to “IP PBX Setup → Trunk Management → Trunk Group” configuration menu. Add a Trunk Group for making external SIP Proxy calls.



Figure D-22. Add Trunk Group number

### STEP 4:

After the SIP Trunk has registered to FWD SIP Proxy successfully, the **Service Provider Status** page will show the registration status:

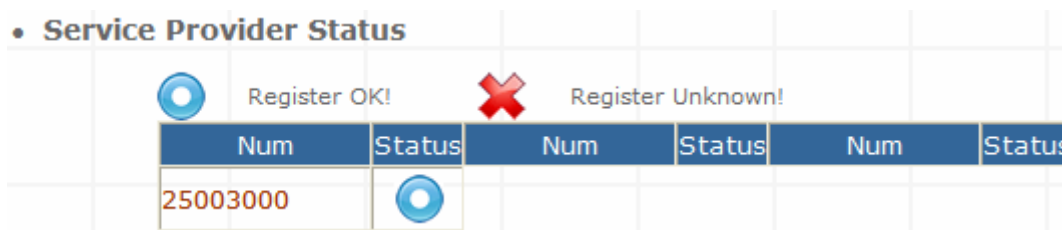


Figure D-23. Service Provider status page

### ➤ Test the Scenario:

1. VIP-154T pick up the telephone
2. Dial the number: **9** will hear the dial tone, and dial the number: 25003999. This call shall be able connect to the User B.
3. Then the softphone of User B will ringing, User B can answer the call and talk with VIP-154T.
4. Both VIP-154T and User B hang up the calls.
5. User B pick up and dial the number: 25003000 should be able to connect to the Auto Attendant System of IP PBX.
6. The User B will hear the prompts, and dial the extension number: 100 shall be able connect to the VIP-192.
7. Then the VIP-192 should ringing, and it to pick up the call then talk with User B.



# Appendix E

## IPX-300 Series Specifications

Product	Internet Telephony PBX System	Wi-Fi Internet Telephony PBX System
Model	IPX-300	IPX-300W
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)
LAN	1 RJ-45 (10/100Base-TX, Auto-Sensing/Switching)	
WAN	1 RJ-45 (10/100Base-TX, Auto-Sensing/Switching)	
Standards and Protocol		
Call control	SIP 2.0 (RFC3261) , SDP (RFC 2327), Symmetric RTP	
Registration	Max. 100 nodes / SIP IP phones/ ATA / FXO gateways	
Calls	Max. 30 concurrent calls	
Voice CODEC Support	G.723, G.726, G.729, G.711, GSM, iLBC	
Voice Processing	DTMF detection and generation In-Band and Out-of-Band (RFC 2833), (SIP INFO) Supports password authentication using MD5 digest	
PBX features	Auto Attendant (AA) Interactive Voice Response (IVR) Records IVR via IP Phone Voicemail Support (VM) Voicemail Send to E-mail Call Detailed Record (CDR) User Management via Web Browsers Web Firmware Upgrade	

	Backup and Restore Configuration file Call/Pickup Group Displays 100 Registered User's Status: Unregistered / Registered / On-Call Displays 20 Registered Trunk's Status: Unregistered / Registered Fax Support using G.711 Pass-Through or T.38**	
Call features	Caller ID Call Group Call Hold Call Waiting Call Transfer Call Forward (Always, Busy, No Answer) Call Pickup Call Park Call Resume Music on Hold Three-way conference with feature phones (VIP-154T series, VIP-155PT/350PT/550PT and ATA series: VIP-156/157/158/161W)	
Internet Sharing		
Protocol	TCP/IP, UDP/RTP/RTCP, HTTP, ICMP, ARP, NAT, DHCP, PPPoE, DNS	
Advanced Function	NAT/Bridge mode, DHCP server, Static Route, DMZ, Virtual Server, Port Trigger, Packet / URL Filter, UPnP, DDNS, SNMP, Ping test	
Network and Configuration		
Connection Type	Static IP, PPPoE, DHCP	
Management	HTTP Web Browser	
LED Indications	System: 1, PWR WAN: 1, LNK/ACT LAN: 1, LNK/ACT	System: 1, PWR WAN: 1, LNK/ACT LAN: 1, LNK/ACT WLAN: 1, LNK/ACT
Environment		
Dimension (W x D x H)	180 x 110 x 25 mm	
Operating Temperature	0~40 degree C, 0~90% humidity	
Power Requirement	12V DC	
EMC/EMI	CE, FCC Class B	
Remark	* Signal Range depends on the used antenna **T.38 support is dependent on fax machine, SIP provider and network / transport resilience	