
***4ipnet* WHG301**
User's Manual

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission of 4IPNET, INC.

Disclaimer

4IPNET, INC. does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights not the parent rights of others. 4IPNET further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

Trademarks

4IPNET (4ipnet) is a registered trademark of 4IPNET, INC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

FCC CAUTION

This equipment has been tested and proven to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment.

Table of Contents

1.	<i>Before You Start</i>	1
1.1	Preface	1
1.2	Document Conventions	1
2.	<i>System Overview</i>	2
2.1	Introduction of 4ipnet WHG301	2
2.2	System Concept	2
2.3	Specification	3
2.3.1	Hardware Specification	3
2.3.2	Technical Specification.....	3
3.	<i>Installation</i>	6
3.1	Hardware Installation.....	6
3.1.1	System Requirements.....	6
3.1.2	Package Contents.....	6
3.1.3	Panel Function Descriptions	7
3.1.4	Installation Steps.....	8
3.2	Quick Software Configuration.....	9
4.	<i>Web Interface Configuration</i>	19
4.1	System Configuration	21
4.1.1	Configuration Wizard	22
4.1.2	System Information	23
4.1.3	WAN1 Configuration	25
4.1.4	WAN2 Configuration	27
4.1.5	WAN Traffic Settings.....	29
4.1.6	LAN Port Mapping.....	31
4.1.7	Service Zones	34
4.2	User Authentication	39
4.2.1	Authentication Configuration.....	40
4.2.2	Black List Configuration	65
4.2.3	Group Configuration.....	67
4.2.4	Policy Configuration	71
4.2.5	Additional Configuration.....	78
4.3	AP Management	81
4.3.1	AP List.....	82
4.3.2	AP Discovery	86
4.3.3	Manual Configuration.....	88
4.3.4	Template Settings	89
4.3.5	Firmware Management.....	90







4.3.6	AP Upgrade	90
4.3.7	WDS Management.....	91
4.4	Network Configuration	92
4.4.1	Network Address Translation	93
4.4.2	Privilege List.....	96
4.4.3	Monitor IP List	98
4.4.4	Walled Garden List	99
4.4.5	Proxy Server Properties.....	100
4.4.6	Dynamic DNS	101
4.4.7	IP Mobility.....	101
4.4.8	VPN Configuration	102
4.5	Utilities	104
4.5.1	Change Password.....	105
4.5.2	Backup/Restore Settings	106
4.5.3	Firmware Upgrade	107
4.5.4	Restart.....	108
4.5.5	Network Utilities	109
4.6	Status.....	110
4.6.1	System Status	111
4.6.2	Interface Status	113
4.6.3	Routing Table	115
4.6.4	Current Users.....	116
4.6.5	Traffic History	117
4.6.6	Notify Configuration	120
4.7	Help	122
Appendix A.	Accepting Payment via Authorize.Net.....	123
Appendix B.	Accepting Payment via PayPal	132
Appendix C.	Service Zone Deployment Example.....	141
Appendix D.	Proxy Setting.....	150
Appendix E.	Session Limit and Session Log	155
Appendix F.	Network Configuration on PC & User Login.....	157
Appendix G.	Console Interface	173
Appendix H.	Local VPN.....	176
Appendix I.	Customizable Pages.....	180

1. Before You Start

1.1 Preface

This manual is for hotspot owners or network administrators to set up a network environment using the 4ipnet WHG301 system. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

	Represents essential steps, actions, or messages that should not be ignored.
	Contains related information that corresponds to a topic.
	Indicates that clicking this button will return to the homepage of this section.
	Indicates that clicking this button will return to the previous page.
	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear what you have set before these settings are applied.

2. System Overview

2.1 Introduction of 4ipnet WHG301

4ipnet WHG301 is an all-in-one product specially designed for wired and wireless data network environments in small to middle scaled businesses and hotspots. It features integrated management, secured data transmission, and enhanced accounting and billing. System administrators can effectively monitor wired or wireless users, including employees and guest users via its user management interface. Moreover, administrators can discover, configure, monitor, and upgrade all managed Access Points (APs) from a single, centralized AP management interface.

2.2 System Concept

4ipnet WHG301 is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external database server. Featured with user authentication and integrated with external payment gateway, WHG301 allows users to easily pay the fee and enjoy the Internet service using credit cards through Authorize.net or PayPal. With centralized AP management feature, the administrator does not need to worry about how to manage multiple wireless access point devices. Furthermore, WHG301 introduces the concept of Service Zones - multiple virtual networks, each with its own definable access control profiles. This is very useful for hotspot owners seeking to provide different customers or staff with different levels of network services. The following diagram is an example of WHG301 set to manage the Internet and network access services at a hotspot venue.

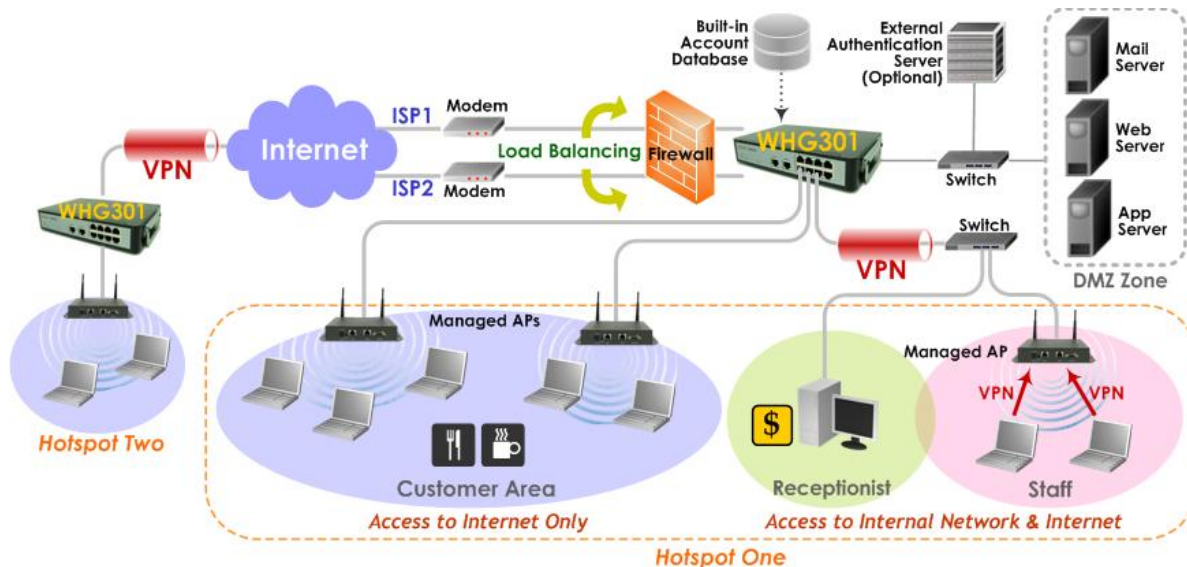


Figure-1: An example of managed network

2.3 Specification

2.3.1 Hardware Specification

General

- Ø Form Factor: Mini-desktop
- Ø Dimensions (W x D x H): 9.6" x 5.9" x 1.8" (243 mm x 150 mm x 45.5 mm)
- Ø Weight: 2.8 lbs (1.29 kg)
- Ø Operating Temperature: 0 ~ 45 °C
- Ø Storage Temperature: 0 ~ 65 °C
- Ø Power: 110~220 VAC, 50/60 Hz
- Ø Ethernet Interfaces: 10 x Fast Ethernet (10/100 Mbps)

Connectors and Display

- Ø WAN Ports: 2 x 10BASE-T/100BASE-TX RJ-45
- Ø LAN Ports: 8 x 10BASE-T/100BASE-TX RJ-45
- Ø Console Port: 1 x RJ-11
- Ø LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 8 x LAN

2.3.2 Technical Specification

Networking

- Ø Support NAT or Router mode
- Ø Support Static IP, DHCP, PPPoE on WAN interface
- Ø Choose freely which LAN is authentication-enabled LAN
- Ø Support NAT (a) IP/Port destination redirection (b) DMZ server mapping (c) virtual server mapping (d) H.323 pass-through
- Ø Built-in with DHCP Server and support DHCP relay
- Ø Support walled garden (free surfing zone)
- Ø Support SMTP redirection
- Ø Support MAC-address and IP-address pass-through
- Ø Support HTTP Proxy
- Ø Support IP Plug and Play (IP PnP)
- Ø Support configurable static routes
- Ø Contain built-in hardware-based VPN accelerator
- Ø Support dual uplinks, outbound load balancing and failover for more reliable Internet connection
- Ø Support SIP pass-through NAT

Service Zones

- Ø The network is divided into maximum eight Service Zones (plus one default zone), each defined by a pair of VLAN tag and ESSID
- Ø Each service zone has its own (a) login portal page (b) redirected home page (c) authentication options (d) LAN interface IP address (e) DHCP address range

- Ø Each service zone allows access to the selected groups
- Ø Each service zone assigns a network policy to each user group

User Management and Guest Accounts

- Ø Authentication methods supported: Local and On-demand accounts, POP3, LDAP, RADIUS, Windows Domain, and SIP authentication
- Ø Single-Sign-On for Windows Domain
- Ø Allow MAC address and user identity binding for local user authentication
- Ø Support MAC Access Control List
- Ø Support auto-expired guest accounts
- Ø Users can be divided into user groups
- Ø Each user group has its own network properties, including bandwidth, QoS, accessible service zones, and other privileges
- Ø Support QoS and WMM traffic types: Voice, Video, Best Effort and Background
- Ø Each group (role) may get different network policies in different service zones
- Ø Max concurrent user session (tcp/udp) limit
- Ø A setting for user-idle-timeout
- Ø Configurable user Black List
- Ø Instant guest account generation by authorized users
- Ø Export/Import local users list to/from a text file
- Ø Definable session limit in policy puts a cap to each user's concurrent sessions (tcp/udp)

Security Features

- Ø Support data encryption: WEP(64/128-bit), WPA, WPA2, IPsec VPN
- Ø Support various authentication methods: WPA-PSK, WPA2-PSK, IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP)
- Ø Provide VPN termination of IPsec tunnels
- Ø Support VPN pass-through (IPsec and PPTP)
- Ø Built-in DoS attack protection
- Ø AP Management
- Ø Provide centralized remote management via HTTP/SNMP interface
- Ø Auto Discovery for Managed APs
- Ø Enable or disable APs easily via user interface
- Ø Templates for Managed APs
- Ø Monitoring Managed AP for its status, the number of associated clients, and RF info
- Ø Recover APs automatically when the system fails
- Ø Upgrade managed APs centrally, including bulk upgrade
- Ø Monitor 3rd party non-integrated AP

Monitoring and Reporting

- Ø Status monitoring of online users
- Ø IP-based monitoring of network devices
- Ø Uplink (WAN) connection failure alert
- Ø Support Syslog for diagnosis and troubleshooting
- Ø User traffic history logging
- Ø Traffic history report via email to administrator
- Ø Users' session log can be sent to ftp or Syslog server

Accounting and Billing

- Ø Support local on-demand and external RADIUS server
- Ø Contain ten configurable billing plans for on-demand accounts
- Ø Support credit card billing system by Authorize.net and PayPal
- Ø Provide session expiration control for on-demand accounts
- Ø Provide detailed per-user network traffic history for both local and on-demand user accounts
- Ø Support automatic e-mail to report network traffic history

System Administration

- Ø Support web-based management user interface
- Ø Provide customizable login and logout portal page
- Ø SSH remote management
- Ø Remote firmware upgrade
- Ø NTP time synchronization
- Ø Menu driven console management interface
- Ø Utilities to backup and restore the system database

3. Installation

3.1 Hardware Installation

3.1.1 System Requirements

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Package Contents

The standard package of 4ipnet WHG301 includes:

- 4ipnet WHG301 x 1
- Quick Installation Guide (QIG) x 1
- CD-ROM (with User's Manual and QIG) x 1
- DC 12V Power Adaptor x 1

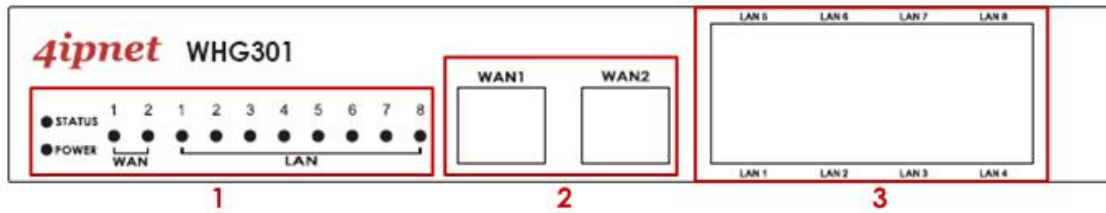
- Console Cable x 1
- Core x 1 (Don't Remove the core of Console Cable)



It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

3.1.3 Panel Function Descriptions

Front Panel



- ① **LED:** There are four kinds of LED, **Power**, **Status**, **WAN** and **LAN**, to indicate different status of the system.
 - ∅ **Power:** LED ON indicates power on.
 - ∅ **Status:** While system power is on, status OFF indicates BIOS is running; BLINKING indicates the OS is running, and ON indicates system is ready.
 - ∅ **WAN:** LED ON indicates connection to the WAN port.
 - ∅ **LAN:** LED ON indicates connection to the LAN port.
- ② **WAN1/WAN2:** Two WAN ports (10 Base-T / 100Base-TX RJ-45) are available on the system.
- ③ **LAN1~LAN8:** Client machines connect to WHG301 via LAN ports (10 Base-T / 100Base-TX RJ-45).

8 Note: By default, all LAN ports are set with Port-based Default Service Zone; for Service Zone configuration, please refer to **4.1.7. Service Zones**.

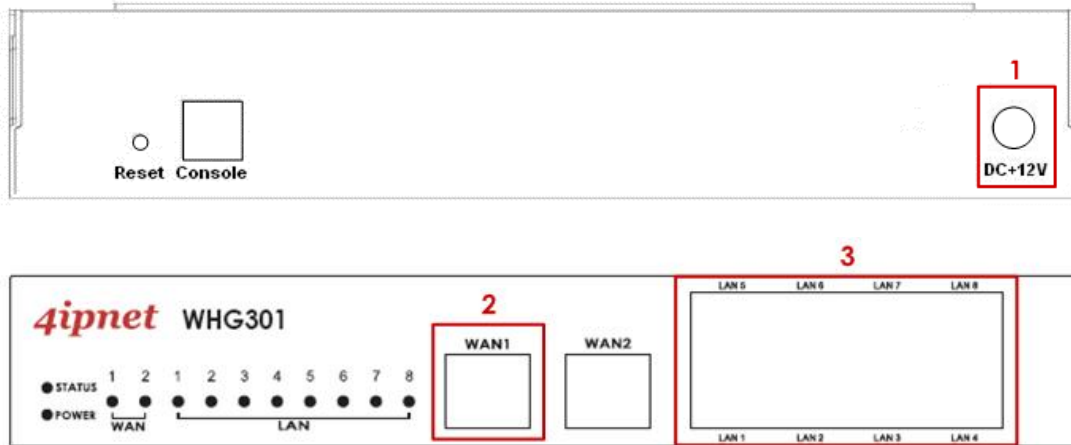
Rear Panel



- ① **Reset:** Press this button to restart the system
- ② **Console:** The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's HyperTerminal to login to the configuration console interface to change admin password or monitor system status, etc.
- ③ **Power Socket:** The power adapter attaches here.

3.1.4 Installation Steps

Please follow the steps below to install 4ipnet WHG301:



1. Connect the 12V power adapter to the power socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub on the LAN of a company/organization. The LED of this port should be on to indicate a proper connection.
3. Connect an Ethernet cable to one of the LAN1~LAN8 Ports on the front panel. Per your needs, connect the other end of the Ethernet cable to an administrator PC for configuring the WHG301 system, an AP for extending wireless coverage, a switch for connecting more wired clients, or a client PC. The LED of the connected port should be on to indicate a proper connection.



WHG301 supports Auto Sensing MDI/MDIX. You may use either a straight-through or a cross-over Ethernet cable to connect the Ethernet port.

3.2 Quick Software Configuration

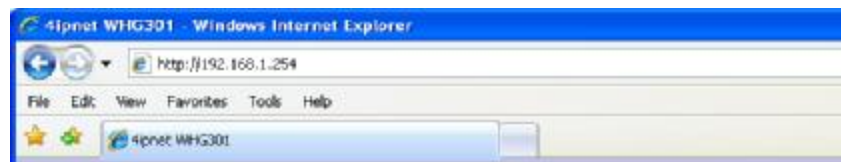
4ipnet WHG301 supports web-based configuration. Upon the completion of hardware installation, WHG301 can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox. There are two ways to configure the 4ipnet WHG301 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of six basic steps as follows. Follow the instructions of Configuration Wizard to enter the required information step by step, save your settings, and restart WHG301. The 6 steps of Configuration Wizard are listed below:

- Step 1. Change Admin's Password**
- Step 2. Choose System's Time Zone**
- Step 3. Set System Information**
- Step 4. Select Connection Type for WAN Port**
- Step 5. Add Local User Account (Optional)**
- Step 6. Save and Restart 4ipnet WHG301**

Please follow the following steps to complete the quick configuration:

- To access the web management interface, connect a PC to one of the LAN1~8 ports, and then launch a browser. **Make sure you have set DHCP in TCP/IP of your PC to get an IP address dynamically.**

Next, enter the gateway IP address of WHG301 at the address field. The default gateway IP address is "**https://192.168.1.254**" ("**https**" is used for a secured connection).



The administrator login page will appear. Enter "**admin**", the default username, and "**admin**", the default password, in the User Name and Password fields. Click **Enter** to log in.



After a successful login, a "Welcome to System Administration" page will appear on the screen.

For the first time, if WHG301 is not using a **trusted SSL certificate**, there will be a “**Certificate Error**”, because the browser treats WHG301 as an illegal website. Please press “**Continue to this website**” to continue. The default user login page will then appear in the browser. *For more information, please see 4.2.5 Additional Configuration.*



*If you can't get the login screen, the reasons may be: (1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port; (2) The IP address and the default gateway are not under the same network segment. Please use default IP address such as 192.168.1.xx in your network and then try it again. For the configuration on PC, please refer to **Appendix F**.*

4ipnet WHG301 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

Admin: The administrator can access all configuration pages of WHG301.

User Name: **admin**

Password: **admin**



Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts, but without the permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

The screenshot displays the 'User Authentication' configuration page. The navigation menu includes 'System Configuration', 'User Authentication', 'IP Management', 'Network Configuration', 'Users', and 'Status'. The 'User Authentication' section is active, showing a sidebar with 'Authentication Configuration', 'Black List Configuration', 'Group Configuration', 'Policy Configuration', and 'Additional Configuration'. The main content area is titled 'User Authentication' and contains the following sections:

- Authentication Configuration:** Each server allows only one type of authentication method and one protocol. Supported authentication servers: POP3(S), RADIUS, LDAP, NT Domain and GP.
- Black List Configuration:** System supports 0 Black List profiles for used within the authentication server. On-demand users are NOT sourced by the Black List.
- Group:** 0 sets of group profiles can be define and used to enforce the access control for defined groups of users.
- Policy Configuration:** A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Management can be defined.
- Additional Configuration:** Additional configurations are in this section. They are Last Session Control, Built-in RADIUS Server Settings, Customizer, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout, User Session Control, Time Actions are provided in built-in RADIUS server settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the session control of the system via sleep/MAC address in the MAC ACL (Access Control List).

Operator: The operator can only access the configuration page of **Create On-demand User** to create new on-demand user accounts and print out the on-demand user account receipts.

User Name: **operator**

Password: **operator**

The screenshot shows a login form with the following fields and buttons:

- User Name:** operator
- Password:** operator
- Buttons:** ENTER, CLEAR



After a successful login to WHG301, a web management interface with a welcome message will appear.



8 Note: To logout, simply click the **Logout** icon on the upper right corner of the interface to return to the login screen.

2. Now you are ready to run the Wizard.

To quickly configure WHG301 by using the **Configuration Wizard**, click **System Configuration** from the top menu to go to the **System Configuration** page. Then, click **Configuration Wizard** on the left.

Click the **Run Wizard** button to begin the **Configuration Wizard**. The **Configuration Wizard** will appear in a pop-up browser window. Click **Next** to begin.



3. Running Configuration Wizard

A welcome screen that briefly introduces the 6 steps will appear. Click **Next** to begin.



Configuration Wizard

Welcome to the Setup Wizard. The wizard will guide you through these 6 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

Step 3. Set System Information

Step 4. Select the Connection Type for WAN Port

Step 5. Add Local User Account (Optional)

Step 6. Save and Restart 4ipnet WHG301

Next

Exit

Note: During every step of the wizard, if you wish to go back to modify the settings, please click the **Back** button to go back to the previous step.

Step 1. Change Admin's Password

- † Enter a **New Password** for the admin account and retype it in the **Verify Password** field (20-character maximum and no spaces). *For security concern, it is strongly recommended to change the administrator's password.*
- † Click **Next** to continue.



Step 1. Change Admin's Password

You may change the Admin's account password by entering a new password. Click Next to continue.

New Password:

Verify Password:

Back

Next

Exit

Y Step 2. Choose System's Time Zone

- † Select a proper time zone from the drop-down list box.
- † Click **Next** to continue.



Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT-08:00)Pacific Time(US&Canada),Tijuana

Back

Next

Exit

Y Step 3. Set System Information

- † **Home Page:** Enter the URL that users should be initially directed to when successfully authenticated to the network.
- † **NTP Server:** Enter the URL of the external time server for 4ipnet WHG301 time synchronization or use the default setting.
- † **DNS Server:** Enter the IP Address of a DNS Server provided by your ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.
- † Click **Next** to continue.



Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page: -

(e.g. http://www.4ipnet.com)

NTP Server: -

(e.g. todt.usno.navy.mil)

DNS Server: -

Back

Next

Exit

Y Step 4. Select Connection Type for WAN Port

There are three types of WAN port to be selected from: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type and click **Next** to continue.

Ø Dynamic IP Address

If this option is selected, an appropriate IP address and related information will automatically be assigned.

Click **Next** to continue.



Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

- | | |
|---|--|
| <input type="radio"/> Static IP Address | Select it to set static IP address. |
| <input checked="" type="radio"/> Dynamic IP Address | Select it to obtain an IP address automatically. (For most cable modem users.) |
| <input type="radio"/> PPPoE Client | Enter the PPPoE Client's Username and Password. (For most DSL users.) |

Back Next Exit

Ø Static IP Address: Set WAN Port's Static IP Address

Enter the "IP Address", "Subnet Mask" and "Default Gateway" provided by your ISP.

Click **Next** to continue.



Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

- | | |
|--|--|
| <input checked="" type="radio"/> Static IP Address | Select it to set static IP address. |
| <input type="radio"/> Dynamic IP Address | Select it to obtain an IP address automatically. (For most cable modem users.) |
| <input type="radio"/> PPPoE Client | Enter the PPPoE Client's Username and Password. (For most DSL users.) |

Back Next Exit



Step 4 (Cont). Set WAN Port's Static IP Address

Click Next to continue.

IP Address:

Subnet Mask:

Default Gateway:

Back Next Exit

Ø PPPoE Client: Set PPPoE Client's Information

Enter the “Username” and “Password” provided by your ISP.

Click **Next** to continue.



Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

- Static IP Address Select it to set static IP address.
- Dynamic IP Address Select it to obtain an IP address automatically. (For most cable modem users.)
- PPPoE Client Enter the PPPoE Client's Username and Password. (For most DSL users.)

Back Next Exit

Y Step 5. Add Local User Account (Optional)

- Ø A new user can be added to the Local User database. To add a user here, enter the **Username** (e.g. test), **Password** (e.g. test), **MAC Address** (optional) and assign an **Applied Group** to this particular user (or use the default **None**).
- Ø More users can be added to this authentication method by clicking the **Add Now** button.
- Ø Click **Next** to continue.

4ipnet

Step 5 Add Local User Account (Optional)

Administrator can choose to add local user accounts for a quick trial.

Username:

Password:

MAC Address: (XXXXXXXXXXXX)

Applied Group: ▼

Y Step 6. Save and Restart 4ipnet WHG301

- Ø Click **Restart** to save current settings and restart 4ipnet WHG301. The Setup Wizard is now complete.

4ipnet

Step 6. Save and Restart 4ipnet WHG301

The Setup Wizard has completed. Click on Back to review or modify settings. Click Restart to save the settings and restart the system to have the current settings take effect.

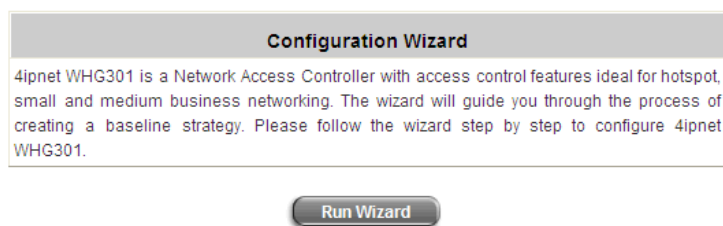
- Y **Restart:** When WHG301 is restarting, a “**Restarting now. Please wait for a moment.**” message will appear on the screen.

The logo for 4ipnet, featuring the word "4ipnet" in a stylized, red, lowercase font.

Setup Wizard

Restarting now. Please wait for a moment...

Please do NOT interrupt WHG301 restart process until the Configuration Wizard pop-up window has disappeared—which indicates the restart process has been completed. If all steps are done properly, you can start working on the system or refer to the user's manual for advanced settings.



4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of 4ipnet WHG301.

The screenshot shows the web interface for the 4ipnet WHG301. At the top left is the 4ipnet logo. To its right is the text "Wireless Hotspot Gateway WHG301". On the far right of the top bar are "Logout" and "Help" links. Below the top bar is a navigation menu with six buttons: "System Configuration", "User Authentication", "AP Management", "Network Configuration", "Utilities", and "Status". The main content area is titled "Welcome to System Administration" and contains a paragraph explaining the interface's purpose and a list of the six main categories.

4ipnet Wireless Hotspot Gateway WHG301 Logout Help

System Configuration User Authentication AP Management Network Configuration Utilities Status

Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into 6 main categories:
[System Configuration](#) , [User Authentication](#) , [AP Management](#) , [Network Configuration](#) , [Utilities](#) and [Status](#).

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Group Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Routing Table
	WAN2 Configuration	Policy Configuration	Template Settings	Walled Garden List	Restart	Current Users
	WAN Traffic Settings	Additional Configuration	Firmware Management	Proxy Server Properties	Network Utilities	Traffic History
	LAN Port Mapping		AP Upgrade	Dynamic DNS		Notification Configuration
	Service Zones		WDS Management	IP Mobility		
				VPN Configuration		



After finishing the configuration of the settings, please click **Apply** and pay attention to see if a **RESTART** message appears on the screen. If such message appears, the system must be restarted to allow the new settings to take effect. All on-line users will be disconnected during restart.

4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 Configuration**, **WAN Traffic Settings**, **LAN Port Mapping** and **Service Zones**.

System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be redirected to URL entered in the Home Page field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN1 Configuration	Set up WAN1 interface using the connection types: Static, Dynamic, PPTP, or PPPoE.
WAN2 Configuration	Set up WAN2 interface using the connection types: None, Static, Dynamic, or PPPoE.
WAN Traffic Settings	Overall traffic control features of WAN interface such as Load Balancing, WAN auto-failover, bandwidth management, and connection detection, etc.
LAN Port Mapping	A "Service Zone" in the system, by default, contains wired and wireless coverage areas in the organization. When "Port-Based" mode is enabled, each physical LAN port can be set individually to map to a specific Service Zone for later use. By contrast under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.
Service Zones	A table to display the Service Zones and related settings.

4.1.1 Configuration Wizard

There are two ways to configure the 4ipnet WHG301 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of 6 basic steps, providing a simple and easy way to go through the basic setups of WHG301. Please refer to **3.2 Quick Software Configuration** for the detailed description of **Configuration Wizard**.

Configuration Wizard

4ipnet WHG301 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure 4ipnet WHG301.

[Run Wizard](#)

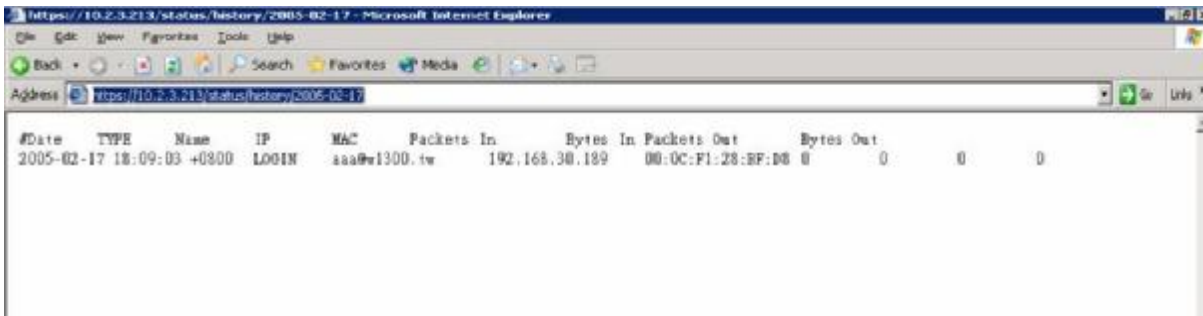
4.1.2 System Information

Main information about 4ipnet WHG301 is shown as follows:

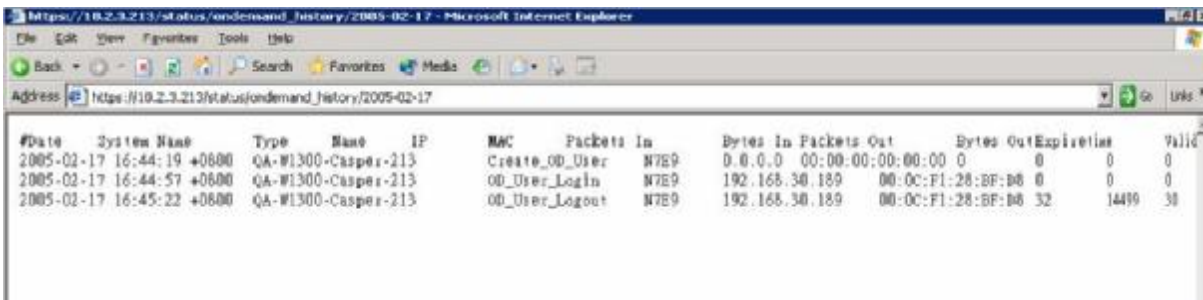
System Information	
System Name	<input type="text" value="Wireless Hotspot Gateway"/>
Device Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN for this device)
Home Page	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="text" value="http://www.4ipnet.com"/> (e.g. http://www.4ipnet.com)
Access History IP	<input type="text"/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
User Logon SSL	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Time	Device Time : 2007/12/23 22:16:48 Time Zone : <input type="text" value="(GMT-08:00)Pacific Time(US&Canada);Tijuana"/> <input type="button" value="v"/> <input checked="" type="radio"/> NTP Enable NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil) NTP Server 2: <input type="text" value="ntp1.fau.de"/> NTP Server 3: <input type="text" value="clock.cuhk.edu.hk"/> NTP Server 4: <input type="text" value="ntps1.pads.ufrj.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZ.AU"/> <input type="radio"/> Set Device Date and Time

- Y **System Name:** Set the system's name or use the default.
- Y **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name of the WHG301 as seen on client machines connected on LAN ports. A user on client machine can use this domain name to access WHG301 instead of its IP address. In addition, when **"Use the name on the security certificate"** option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.
- Y **Home Page:** Enter the URL of a Web server as the homepage. Once logged in successfully, users will be directed to this homepage, such as <http://www.4ipnet.com>, regardless of the original homepage set in their computers.
- Y **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of WHG301 with the predefined URLs. An example is provided as follows:

Traffic History : <https://10.2.3.213/status/history/2005-02-17>



On-demand History : https://10.2.3.213/status/ondemand_history/2005-02-17



- Y **Management IP Address List:** The IP address or subnet of remote management PCs. Only PCs within this IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, he or she can access the web management page.
- Y **SNMP:** If this function is enabled, the Manager IP and the community can be assigned to access to access the Management Information Base (MIB) of the system.
- Y **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- Y **Time:** NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT). The time can also be manually configured by selecting **“Set Device Date and Time”** and then entering the date and time in these fields.

Device Time : 2007/12/24 01:42:06

Time Zone :

(GMT-08:00)Pacific Time(US&Canada);Tijuana v

NTP Enable

Set Device Date and Time

-- v Year -- v Month -- v Day

-- v Hour -- v Minute -- v Second

4.1.3 WAN1 Configuration

There are 4 connection types for the WAN1 Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.

Y **Static IP Address:** Manually specifying the IP address of the WAN Port. The fields with red asterisks are required to be filled in.

IP Address: The IP address of the WAN1 port.

Subnet Mask: The subnet mask of the WAN1 port.

Default Gateway: The gateway of the WAN1 port.

Preferred DNS Server: The primary DNS server used by the system.

Alternate DNS Server: The substitute DNS server used by the system. This is an optional field.

The screenshot shows the 'WAN1 Configuration' form with the 'Static IP Address' radio button selected. The form includes the following fields:

- Static IP Address (selected)
- IP Address: []*
- Subnet Mask: []*
- Default Gateway: []*
- Preferred DNS Server: [168.95.1.1]
- Alternate DNS Server: []
- Dynamic IP Address (unselected)
- PPPoE Client (unselected)
- PPTP Client (unselected)

Y **Dynamic IP Address:** It is only applicable for the network environment where the DHCP server is available on the network. Click the **Renew** button to get an IP address automatically.

The screenshot shows the 'WAN1 Configuration' form with the 'Dynamic IP Address' radio button selected. A 'Renew' button is visible next to the 'Dynamic IP Address' option.

- Static IP Address (unselected)
- Dynamic IP Address (selected) [Renew]
- PPPoE Client (unselected)
- PPTP Client (unselected)

Y **PPPoE Client:** When selecting PPPoE to connect to the network, please set the “**User Name**”, “**Password**”, “**MTU**” and “**CLAMP MSS**”. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

The screenshot shows the 'WAN1 Configuration' form with the 'PPPoE Client' radio button selected. The form includes the following fields:

- Static IP Address (unselected)
- Dynamic IP Address (unselected)
- PPPoE Client (selected)
- Username: []*
- Password: []*
- MTU: [1492] bytes *(Range:1000~1492)
- CLAMP MSS: [1400] bytes *(Range:980~1400)
- Dial on Demand: Enabled Disabled
- PPTP Client (unselected)

- Y **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

WAN1 Configuration	
WAN1 Port	<input type="radio"/> Static IP Address
	<input type="radio"/> Dynamic IP Address
	<input type="radio"/> PPPoE Client
	<input checked="" type="radio"/> PPTP Client
	Type <input type="radio"/> Static <input checked="" type="radio"/> DHCP
	PPTP Server IP: <input type="text"/>
	Username: <input type="text"/>
Password: <input type="text"/>	
PPTP Connection ID/Name: <input type="text"/>	
Dial on Demand: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	

4.1.4 WAN2 Configuration

Select **None** to disable this WAN2 interface, or there are 3 connection types for the WAN2 port: **Static IP Address**, **Dynamic IP Address**, and **PPPoE Client**.

WAN2 Configuration	
WAN2 Port	<input checked="" type="radio"/> None <input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client

- Y **None:** The WAN2 Port is disabled.
- Y **Static IP Address:** Manually specifying the IP address of the WAN port. The red asterisks indicate required fields to be filled in.

WAN2 Configuration	
WAN2 Port	<input type="radio"/> None <input checked="" type="radio"/> Static IP Address IP Address: <input type="text"/> * Subnet Mask: <input type="text"/> * Default Gateway: <input type="text"/> * Preferred DNS Server: <input type="text"/> * Alternate DNS Server: <input type="text"/> <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client

IP address: the IP address of the WAN2 port.

Subnet mask: the subnet mask of the network WAN2 port connects to.

Default gateway: a gateway of the network WAN2 port connects to.

Preferred DNS Server: The primary DNS server used by the system.

Alternate DNS Server: The substitute DNS server used by the system. This is an optional field.

- Y **Dynamic IP address:** It is only applicable for the network environment where a DHCP server is available. Click the **Renew** button to get an IP address.

WAN2 Configuration	
WAN2 Port	<input type="radio"/> None <input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/> <input type="radio"/> PPPoE Client

- Y **PPPoE Client:** When selecting PPPoE to connect to the network, please set the “**User Name**” and “**Password**”. There is a **Dial on demand** function under PPPoE. If this function is enabled, **Maximum Idle Time can be set**. When the idle time is reached, the system will automatically disconnect itself.

WAN2 Configuration	
WAN2 Port	<input type="radio"/> None
	<input type="radio"/> Static IP Address
	<input type="radio"/> Dynamic IP Address
	<input checked="" type="radio"/> PPPoE Client
	Username: <input type="text"/>
	Password: <input type="text"/>
MTU:	<input type="text" value="1492"/> bytes · <small>(range: 1000~1492)</small>
Clamp MSS:	<input type="text" value="1400"/> bytes · <small>(range: 980~1400)</small>
Dial on Demand	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

4.1.5 WAN Traffic Settings

The section is for administrators to configure the control over the entire system's traffic through the WAN interface (WAN1 and WAN2 ports).

WAN Traffic Settings	
Available Bandwidth on WAN Interface	Uplink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small> Downlink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small>
Connection Detection & WAN Failover	Target for detecting Internet connection: IP/Domain Name: <input type="text" value="www.google.com"/> IP/Domain Name: <input type="text"/> IP/Domain Name: <input type="text"/> <input type="checkbox"/> Enable Load Balancing <input checked="" type="checkbox"/> Enable WAN Failover <input checked="" type="checkbox"/> Fall back to WAN1 when WAN1 is available again <input checked="" type="checkbox"/> Warning of Internet Disconnection When Internet connection is down, the system will display the message as: <input type="text" value="Sorry! The service is temporarily unavailable."/>

Available Bandwidth on WAN Interface:

- Y **Uplink:** It specifies the maximum uplink bandwidth that can be shared by clients of the system.
- Y **Downlink:** It specifies the maximum downlink bandwidth that can be shared by clients of the system.

Connection Detection & WAN Failover:

- Y **Target for detecting Internet connection:** These URLs are used by the system as the targets to detect Internet connection, for alerting Internet disconnection and WAN Failover. At least one URL is required to enable WAN Failover.
- Y **Enable Load Balancing:** Outbound load balancing is supported by the system. When enabled, the system will allocate traffic between WAN1 and WAN2 dynamically according to designed algorithms based on the weight ratio.
 - Ø **WAN1 Weight:** The percentage of traffic through WAN1. (Range: 1~99; by default, it is 50)
 - Ø **Base:** The weight ratio between WAN1 and WAN2 can be based on Sessions, Packets or Bytes. Packets and Bytes are based on historic data. New connection sessions will be distributed between WAN1 and WAN2 by a weight ratio using random number.
- Y **Enable WAN Failover:** Normally a Service Zone uses WAN1 as its primary WAN interface. When enabled and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a Service Zone's policy could also use WAN2 as its interface; in that case, if WAN2 is down, the WAN2's traffic under its policy will also be routed to WAN1.
 - Ø **Fall back to WAN1 when WAN1 is available again:** If WAN Failover is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. When **fall back to WAN1** is enabled, the routed traffic will be connected back to WAN1 when WAN1 connection is recovered.
- Y **Warning of Internet Disconnection:** When enabled, there is a text box available for the administrator to enter

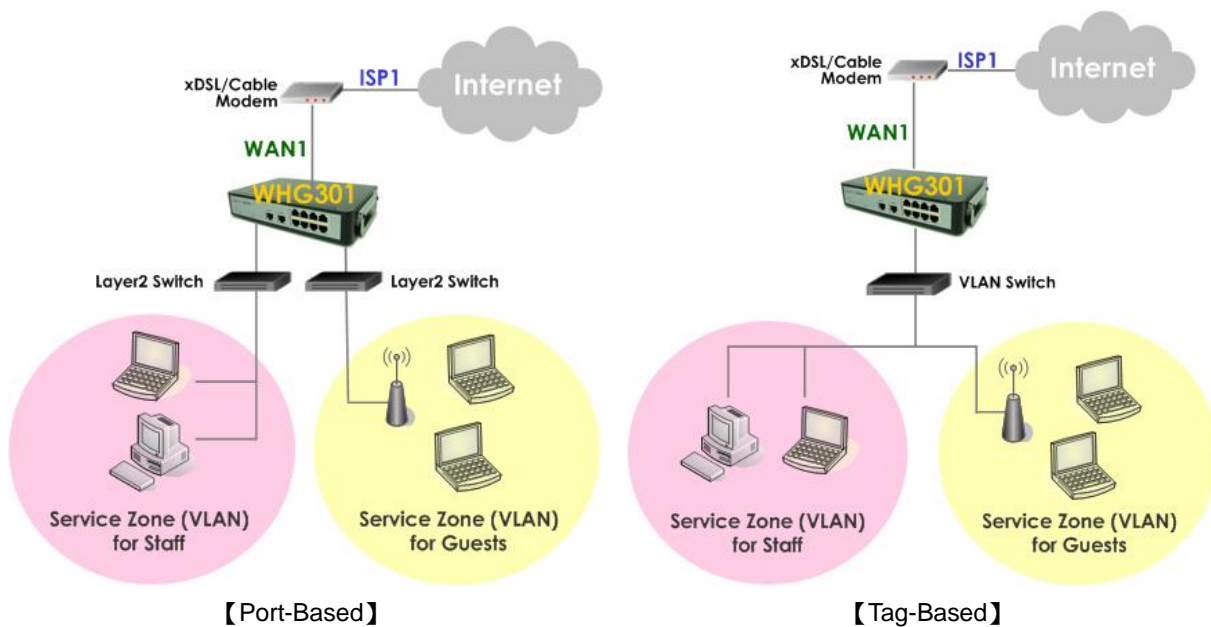
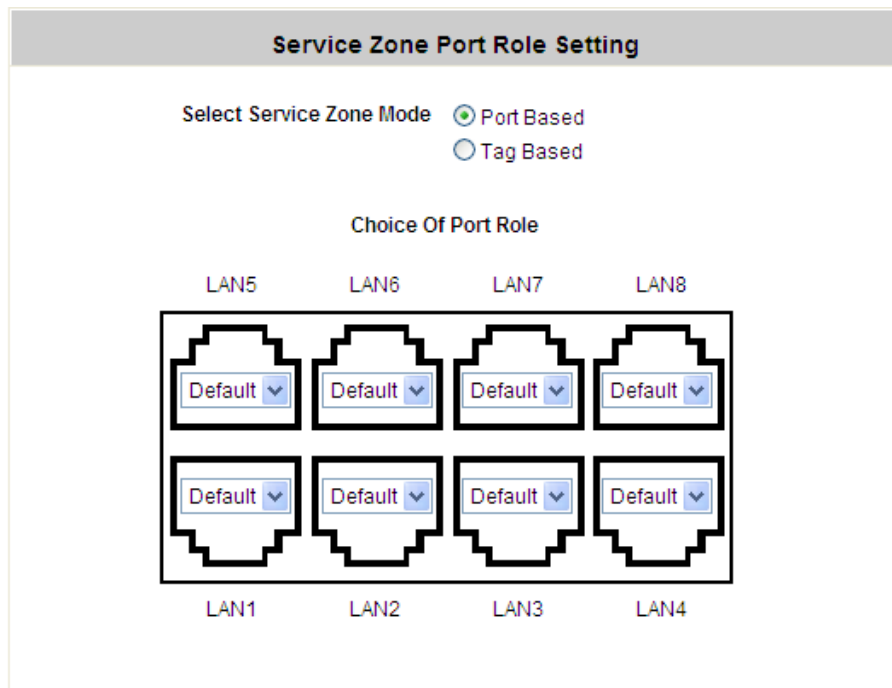
a reminding message. This reminding message will appear on clients' screens when Internet connection is down.



SIP authentication is exempt from Load Balancing and WAN Failover. A fixed WAN port is used for SIP traffic.

4.1.6 LAN Port Mapping

WHG301 supports multiple Service Zones in either of the two VLAN modes, **Port-Based** or **Tag-Based**, but not concurrently. In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone as each Service Zone is identified by physical LAN ports. In **Tag-Based** mode, each LAN port can serve traffic from any Service Zone as each Service Zone is identified by VLAN tags carried within message frames. **By default, the system is in Port-Based mode with Default Service Zone enabled and all LAN ports are mapped to Default Service Zone.** Compare the two figures below to see the differences.



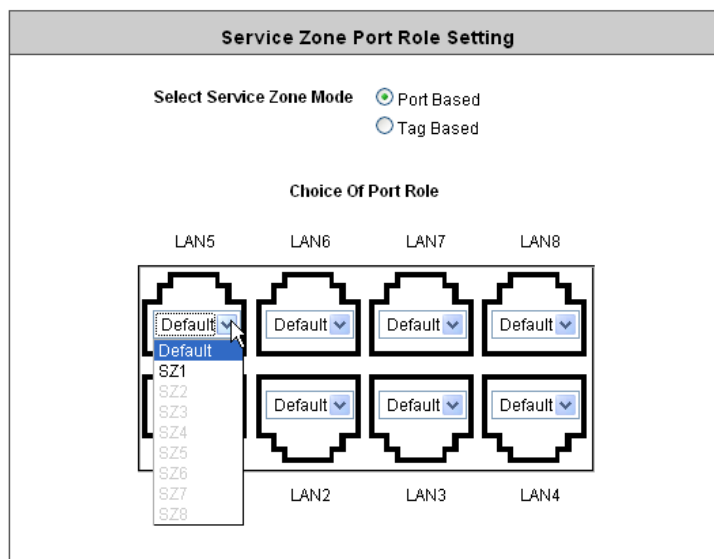
It is recommended that the administrator decides which mode is better for a multiple-service-zone deployment before proceeding further with the system configuration. Settings for the two VLAN modes are slightly different, for example, the VLAN Tag setting is required for Tag-Based mode.

¶ **Select Service Zone Mode:** Select a VLAN mode, either *Port-Based* or *Tag-Based*.



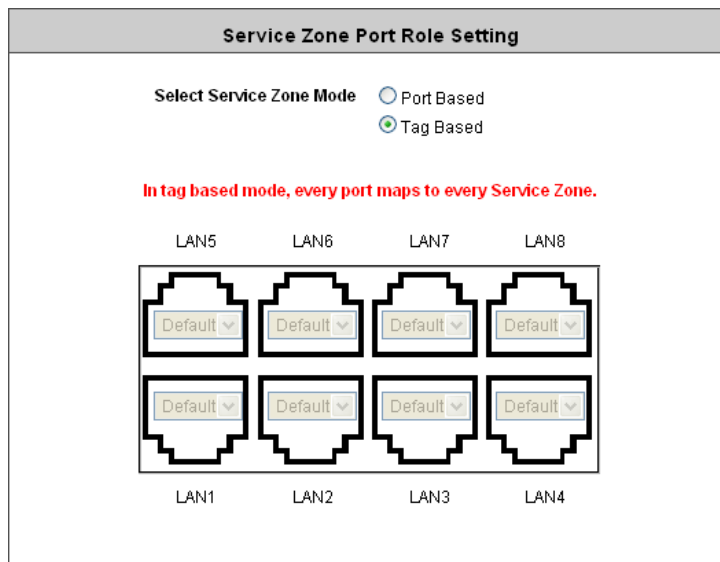
The switches deployed under WHG301 in Port-Based mode must be Layer2 Switches only. The switch deployed under WHG301 in Tag-Based mode must be a VLAN switch only.

- Ø **Port-Based:** When Port-Based mode is selected, traffic from different virtual Service Zones will be distinguished by physical LAN ports. Each LAN port can be mapped to a Service Zone in the form of a many-to-one mapping between ports and Service Zones.
 - **Specify a desired Service Zone for each LAN Port:** For each LAN port, select a Service Zone to which the LAN port is to be mapped from the drop-down list box. By factory default, all LAN ports are mapped to Default Service Zone; therefore, the administrator can enter the web management interface via any LAN port upon the first power up of the system. From the drop-down list box, all disabled Service Zones are gray-out; to activate any desired Service Zone, please configure the desired Service Zone under the **Service Zone** tab and enable its *Service Zone Status* (refer to **4.1.7. Service Zones**).



- Ø **Tag-Based:** When the Tag-Based mode is selected, traffic from different virtual Service Zones will be distinguished by VLAN tagging, instead of by physical LAN ports.

Select *Tag-Based* and then click **Apply** to activate the Tag-Based VLAN function. When a restart message screen appears, do NOT restart the system until you have completed the configuration under the **Service Zones** tab first.

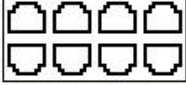


8 Note: For more information on enabling and configuring Service Zones, please refer to **Appendix C**.

4.1.7 Service Zones

A *Service Zone* is a logical network area to cover certain wired and wireless networks in an organization such as SMB or branch offices. By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical zones. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc.

There are up to nine Service Zones to be utilized; by default, they are named as: **Default, SZ1~SZ8**, as shown in the table below.

Service Zone Settings							
Service Zone Name	Port Map	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default		4ipnet	None	Policy 1	Server 1	Enable	Configure
SZ1		4ipnet-1	None	Policy 1	Server 1	Disable	Configure
SZ2		4ipnet-2	None	Policy 1	Server 1	Disable	Configure
SZ3		4ipnet-3	None	Policy 1	Server 1	Disable	Configure
SZ4		4ipnet-4	None	Policy 1	Server 1	Disable	Configure
SZ5		4ipnet-5	None	Policy 1	Server 1	Disable	Configure
SZ6		4ipnet-6	None	Policy 1	Server 1	Disable	Configure
SZ7		4ipnet-7	None	Policy 1	Server 1	Disable	Configure
SZ8		4ipnet-8	None	Policy 1	Server 1	Disable	Configure

- Y **Service Zone Name:** Mnemonic name of the Service Zone.
- Y **VLAN Tag:** The VLAN tag number that is mapped to the Service Zone.
- Y **SSID:** The SSID that is associated with the Service Zone.
- Y **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- Y **Applied Policy:** The policy that is applied to the Service Zone.
- Y **Default Authentication:** Default authentication method/server that is used within the Service Zone.
- Y **Status:** Each Service Zone can be enabled or disabled.
- Y **Details:** Configurable, detailed settings for each Service Zone.

Click **Configure** button to configure each Service Zone: **Basic Settings, SIP Interface Configuration, Authentication Settings, Wireless Settings, and Managed AP in Each Service Zone.**

1) Service Zone Settings – Basic Settings

Basic Settings	
Service Zone Status	Enable
Service Zone Name	Default
Network Settings	Operation Mode: <input checked="" type="radio"/> NAT <input type="radio"/> Router IP Address: <input type="text" value="192.168.1.254"/> * Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Settings	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server Start IP Address: <input type="text" value="192.168.1.1"/> * End IP Address: <input type="text" value="192.168.1.100"/> * Preferred DNS Server: <input type="text" value="168.95.1.1"/> * Alternate DNS Server: <input type="text"/> Domain Name: <input type="text" value="domain"/> * WINS Server IP: <input type="text"/> Lease Time: <input type="text" value="1 Day"/> * Reserved IP Address List <input type="radio"/> Enable DHCP Relay

- ∅ **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- ∅ **Service Zone Name:** The name of service zone could be input here.
- ∅ **Network Settings:**
 - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
 - **IP address:** The IP Address of this service zone.
 - **Subnet Mask:** The subnet Mask of this service zone.
- ∅ **DHCP Server Settings:** Related information needed on setting up the DHCP Server is listed here. Please note that when “*Enable DHCP Relay*” is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.
 - **Start IP Address / End IP Address:** A range of IP addresses that built-in DHCP server will assign to clients. Note: please change the Management IP Address List accordingly (at *System Configuration* → *System Information* → *Management IP Address List*) to permit the administrator to access the WHG301 admin page after the default IP address of the network interface is changed.
 - **Preferred DNS Server:** The primary DNS server that is used by this Service Zone.
 - **Alternate DNS Server:** The substitute DNS server that is used by this Service Zone.
 - **Domain Name:** Enter the domain name for this service zone.

- **WINS Server IP:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
- **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.
- **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with certain MAC address.

2) Service Zone Settings – SIP Interface Configuration

SIP Interface Configuration		
Enabled <input checked="" type="checkbox"/>	WAN Interface	WAN1

The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic can pass through NAT via a fixed WAN interface. The policy route setting of SIP Authentication must be configured carefully because it must cooperate with the fixed WAN interface for SIP authentication.

SIP Transparent Proxy can be activated in both NAT and Router mode. SIP Authentication must support in either mode. For users logging in through SIP authentication, a policy can be chosen to govern SIP traffic. The policy's login schedule profile will be ignored for SIP authentication. Specific route and firewall rules of the chosen policy will be applied to SIP traffic.

3) Service Zone Settings – Authentication Settings

Authentication Settings					
Authentication Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
	On-demand User	ONDEMAND	guest	<input type="radio"/>	<input checked="" type="checkbox"/>
	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Custom Pages	Login Page				<input type="button" value="Configure"/>
	Logout Page				<input type="button" value="Configure"/>
	Login Success Page				<input type="button" value="Configure"/>
	Login Success Page for On-demand User				<input type="button" value="Configure"/>
	Logout Success Page				<input type="button" value="Configure"/>
Group Permission for this Service Zone				<input type="button" value="Configure"/>	
Default Policy in this Service Zone			Policy 1 <input type="button" value="v"/>	<input type="button" value="Edit System Policies"/>	
Email Message for Login Reminding			<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="button" value="Edit Mail Message"/>	

Ø **Authentication Status:** When enabled, users must be authenticated before they get access to the network within this Service Zone.

Ø **Authentication Options:** There are total seven types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. For each Service Zone, up to six authentication options can be enabled, and one of them can be set as the default option – so that users do not have to type in the postfix string while entering username during login.

Ø **Custom Pages:** Related login and logout pages can be customized by administrators for each service zone. Please refer to **Appendix I. Customizable Pages** for more details.

Ø **Group Permission for this Service Zone:**

For each Service Zone, the administrator can set up multiple groups for that Service Zone. For each group, an associated policy can be assigned. Therefore, users in the same group follow the same policy and have the same privileges.

To configure Group permission based on the role of this Service Zone.

Click **Configure** to have further configuration or view the details.

Click **Enabled** of the desired Group option(s) to allow the clients of the selected Group(s) to log into this Service Zone after a successful authentication. Moreover, a pre-defined Policy can be applied to any Group in this Service Zone.

Click the hyperlink of the respective Group names in the **Edit Group Option** column to enter the **Group Configuration** tab, where zone permission and policy assignment can be further configured (refer to **4.2.3. Group Configuration**).

Group Permission - Service Zone : Default			
Group Option	Enabled	Policy	Edit Group Option
Group 1	<input checked="" type="checkbox"/>	Policy 1	Group 1
Group 2	<input checked="" type="checkbox"/>	Policy 2	Group 2
Group 3	<input checked="" type="checkbox"/>	Policy 3	Group 3
Group 4	<input checked="" type="checkbox"/>	Policy 4	Group 4
Group 5	<input checked="" type="checkbox"/>	Policy 5	Group 5
Group 6	<input checked="" type="checkbox"/>	Policy 6	Group 6
Group 7	<input checked="" type="checkbox"/>	Policy 7	Group 7
Group 8	<input checked="" type="checkbox"/>	Policy 8	Group 8

- Ø **Default Policy in this Service Zone:** For each Service Zone, one policy can be applied to enforce the access control over the users. Please refer to **4.2.4 Policy Configuration** for complete description.
- Ø **Email Message for Login Reminding:** When enabled, the system will automatically send an email to users if they attempt to send/receive their emails using POP3 email program (for example, Microsoft Outlook) before they are authenticated. Click **Edit Mail Message** to edit the message in HTML format:

4) Service Zone Settings – Wireless Settings

Wireless Settings	
Set SSID	4ipnet -
Access Point Security	Authentication: Open System <input type="checkbox"/> Enable 802.1X Authentication
	Encryption: none

- Ø **Set SSID:** Each service zone can be mapped with its own SSID.
- Ø **Access Point Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.

5) Service Zone Settings – Managed AP in this Service Zone

All managed APs that belong to this service zone are listed here.

Managed AP in this Service Zone			
AP Type	AP Name	IP Address	Status
		MAC Address	
EAP100	EAP100A	192.168.1.9	Offline
		11:22:33:44:55:66	

4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Group Configuration**, **Policy Configuration** and **Additional Configuration**.

The screenshot displays the web interface for the 4ipnet Wireless Hotspot Gateway WHG301. The top navigation bar includes the 4ipnet logo, the product name, and links for Logout and Help. Below this is a menu with System Configuration, User Authentication (selected), AP Management, Network Configuration, Utilities, and Status. The main content area is titled 'User Authentication' and contains a table with the following information:

User Authentication	
Authentication Configuration	Each server allows only one type of authentication method and one Black List Profile. System supports the following external authentication servers: POP3(S), RADIUS, LDAP, NT Domain and SIP.
Black List Configuration	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Group	8 sets of group profiles can be define and used to enforce the access control for different groups of users.
Policy Configuration	A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Limit Management can be defined.
Additional Configuration	Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout in User Session Control. Three functions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL (Access Control List).

At the bottom of the page, there are two red icons: a warning sign and an upward-pointing arrow.

4.2.1 Authentication Configuration

This section is for administrators to pre-configure authentication servers for the entire system's Service Zones. For a particular Service Zone, administrators can enable all the authentication servers which will be used and also specify a default authentication server in the page of *Service Zone Settings*. Concurrently up to four servers can be selected and pre-configured here by administrators from the five types of authentication databases (LOCAL, POP3, RADIUS, LDAP, and NTDOMAIN). In addition, there are two servers (On-demand User and SIP) that are selected by the system. For the Authentication Settings of each Service Zone, please see **4.1.7 Service Zones**.

Authentication Server Configuration			
Server Name	Auth Method	Postfix	Group
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	ondemand	Group 5
SIP	SIP	N/A	None

- Y **Server Name:** There are several authentication options supported by WHG301: Server 1 to Server 4, On-demand User, and SIP. Click the hyperlink of the respective Server Name to configure the authentication server.
- Y **Auth Method:** There are different authentication methods in WHG301: **LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND** and **SIP**.
- Y **Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated against the LOCAL authentication database.

Note: Concurrently only one server is allowed to be set as Local or NTDOMAIN authentication method.

- Y **Group:** An authentication option, such as POP3 or NT Domain, can be set as a Group with the same QoS or Privilege Profile setting.

For more information on Group, please refer to **4.2.3. Group Configuration**.



After clicking **Apply**, there will be a restart message. You must click **Restart** to apply the settings.

Y Authentication Server Configuration

WHG301 provides four authentication servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the configuration for that particular server. After completing and clicking **Apply** to save the settings, go back to the previous page to select a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

Server 1~4: There are 5 authentication methods, **Local User, POP3, RADIUS, LDAP** and **NTDomain**, to select from.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(its server name)</small>
Postfix	local <small>*(its postfix name)</small>
Black List	None
Authentication Method	Local <small>Local User Setting</small>
Group	

Local
POP3
RADIUS
LDAP
NT Domain

Apply Clear

Server Name: Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.

Postfix: A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.



The Policy Name cannot contain these words: MAC and IP.

Black List: There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from the drop-down menu and this black list will be applied to this specific authentication option.

Group: Select one Group from the drop-down list box for this specific authentication option.

Authentication Method: Select *Local* from the drop-down list box and then click **Local User Setting** button to enter the **Local User Settings**. Then, click the hyperlink of **Edit Local User List**.



Enabling two or more servers of the same authentication method is NOT allowed.

4.2.1.1 Authentication Method – Local

Choose “**Local User**” from the **Authentication Method** field, the button besides the pull-down menu will become “**Local User Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Postfix	local <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	Local <input type="button" value="v"/> <input type="button" value="Local User Setting"/>
Group	Group 1 <input type="button" value="v"/>

Click the button of **Local User Setting** for further configuration.

Local User Setting	
Edit Local User List	
RADIUS Roaming Out	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>(Local user database will be used as authentication database for roaming out users.)</small>
802.1x Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>(Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)</small>

Y **Edit Local User List:** It let the administrator view / add, and delete local user account. The **Upload User** button is for importing a list of user account from a text file. The **Download User** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a policy and applied Local VPN individually. Check the check box of individual local user account in the Enable Local VPN column to enable individually. MAC address of a networking device can be bound with a local user as well.

Users List				
Username	Password	MAC Address	Applied Group	<input type="button" value="Del All"/>
			Local VPN Enabled	
			Remark	
eric	eric	00:20:A6:4C:A1:05	None	Delete
			No	

- o **Add User:** Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **“Username”**, **“Password”**, **“MAC”**, and **“Remark”**. Select a desired **Group** to classify local users. Check to enable *Local VPN* in the **Enable Local VPN** column. Click **Apply** to complete adding the user(s).

For more information on Group configuration, please refer to **4.2.3. Group Configuration**.

Add User						
Item	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Group	Remark	Local VPN
1	test	****		Group 1		<input type="checkbox"/>

User 'test' has been added!

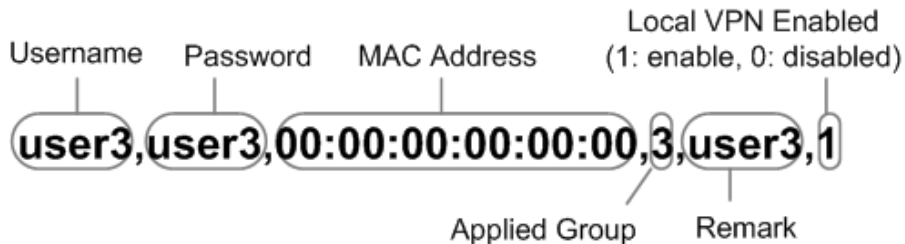
Add User						
Item	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Group	Remark	Local VPN
1				None		<input type="checkbox"/>

- o **Upload User:** Click **Upload User** to enter the **Upload User from File** interface. Click the **Browse** button to select the text file for uploading user accounts, then click **Upload** to complete the upload process.

Note 1: The format of each line is "ID, Password, MAC, Group, Remark, IPsec" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Note 2: If you want user Enabled Local VPN, please set IPsec field to 1, or 0 would disable.
Note 3: Only "0-9", "A-Z", "a-z", ".", "-", and "_" are acceptable for password field.

Upload User Account	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	

When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, and then, try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.



- ÿ **Download User:** Use this function to create a .txt file with all built-in user account information and then save it on disk.

Users List			
Username	Password	MAC	Group
			Local VPN Enabled
			Remark
eric	eric	00:20:A6:4C:A1:05	0
			0
ericz1	ericz1		0
			0
eric_d	eric_d		0
			0
test	1234		1
			0

[Download](#)

- ÿ **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.

Users List				
Username	Password	MAC Address	Applied Group	Del All
			Local VPN Enabled	
			Remark	
test	1234		Group 1	Delete
			No	

- ÿ **Del All:** Click on this button to delete all the users at once and click on **Delete** to delete the user individually.

- Y **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **User Profile** Interface for that particular user, and then modify or add any desired information such as *Username*, *Password*, *MAC Address* (optional), *Group* (optional), *Enable Local VPN* (optional) and *Remark* (optional). Click **Apply** to complete the modification.

User Profile	
Username	test *
Password	1234 *
MAC	
Group	Group 1 ▾
Enable Local VPN	<input type="checkbox"/>
Remark	

- Y **Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled, the link of this function will be available to define the authorized device with IP address, Subnet Mask, and Secret Key. Please see more explanation above in the section for **Roaming Out** and the section for **802.1X Authentication**.

Local User Setting	
Edit Local User List	
RADIUS Roaming Out	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled (Local user database will be used as authentication database for roaming out users.)
802.1x Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client List	

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	Roaming Out ▾		255.255.255.255 (/32) ▾	****
2	802.1x ▾	192.168.0.0	255.255.255.254 (/31) ▾	****
3	Disable ▾		255.255.255.252 (/30) ▾	****

Click the hyperlink **RADIUS Client List** to enter the **Radius Client Configuration** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1X**, and key in the 802.1X client's IP address and network mask and then click **Apply** to complete the settings.

802.1X Authentication: When **802.1X Authentication** is enabled, the Local authentication database will be used as a RADIUS database for connection with 802.1X enabled devices such as APs or switches.

Roaming Out: The system's local user database can also be an external RADIUS database to another system. When *Account Roaming Out* is enabled, local users can login from other domains with their original local user accounts. The authentication database with their original local user accounts acts as a RADIUS Server and roaming out local users act as RADIUS clients.

4.2.1.2 Authentication Method – POP3

Choose “**POP3**” from the **Authentication Method** field, the button beside the pull-down menu will become “**POP3 Setting**”.

Authentication Server - Server 2	
Server Name	Server 2 <small>*(Its server name)</small>
Postfix	pop3 <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	POP3 <input type="button" value="v"/> <input type="button" value="POP3 Setting"/>
Group	Group 1 <input type="button" value="v"/>
Enable Local VPN	<input type="checkbox"/>

Click the button of **POP3 Setting** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary POP3 Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Default: 110)</small>
SSL Setting	<input type="checkbox"/> Enable SSL Connection
Secondary POP3 Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
SSL Setting	<input type="checkbox"/> Enable SSL Connection

- ÿ **Server IP:** The IP address of the external POP3 Server.
- ÿ **Port:** The authentication port of the external POP3 Server.
- ÿ **SSL Setting:** The system supports POP3S. Check the check box beside to **Enable SSL Connection** to POP3.

4.2.1.3 Authentication Method – RADIUS

Choose “RADIUS” from the **Authentication Method** field, the button beside the pull-down menu will become “Radius Setting”.

Authentication Server - Server 3	
Server Name	Server 3 <small>*(Its server name)</small>
Postfix	radius <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	RADIUS <input type="button" value="v"/> <input type="button" value="Radius Setting"/>
Group	Group 1 <input type="button" value="v"/>
Enable Local VPN	<input type="checkbox"/>

Click the button of **Radius Setting** for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the **Apply** button.

RADIUS Setting	
802.1x Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Trans Full Name	<input type="radio"/> Complete (e.g. user1@company.com) <input checked="" type="radio"/> Only ID (e.g. user1)
NASID	<input type="text"/>
Class-Group Mapping	<input type="button" value="Edit Class-Group Mapping"/>
Primary RADIUS Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP Address)</small>
Authentication Port	<input type="text"/> <small>*(Default: 1812)</small>
Accounting Port	<input type="text"/> <small>*(Default: 1813)</small>
Secret Key	<input type="text"/>
Accounting Service	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Authentication Protocol	PAP <input type="button" value="v"/>
Secondary RADIUS Server	
Server IP	<input type="text"/> <small>(Domain Name/IP Address)</small>
Authentication Port	<input type="text"/>
Accounting Port	<input type="text"/>
Secret Key	<input type="text"/>
Accounting Service	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Authentication Protocol	CHAP <input type="button" value="v"/>

802.1X Authentication: The system supports 802.1X. When *802.1X Authentication* is enabled, the Local Authentication Database will be used as a RADIUS database for connection with 802.1X enabled devices such as access points or switches.

When the option is enabled, the hyperlink of **Radius Client List** will appear.

Click the hyperlink of **Radius Client List** to enter the **Radius Client Configuration** page. Choose a desired type from *Disable*, *Roaming Out* or *802.1X*. Enter the *IP Address*, *Segment (Subnet Mask)*, and *Secret Key* of 802.1X clients. Click **Apply** to complete the settings.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	Roaming Out		255.255.255.255 (/32)	****
2	802.1x	192.168.0.0	255.255.255.254 (/31)	****
3	Disable		255.255.255.252 (/30)	****

- ÿ **Trans Full Name:** When **Complete** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when **Only ID** option is checked, only the username will be transferred to the external RADIUS server for authentication.
- ÿ **NASID:** The Network Access Server (NAS) Identifier of the system for the external RADIUS server.
- ÿ **Class-Group Mapping**
- ÿ This function is to assign a *Group* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Group.

RADIUS Group Mapping - Server 3			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
No.	Class Attribute	Group	Remark
1	1	Group 1	
2	2	Group 1	
3	3	Group 1	

- ÿ **Server IP:** The IP address of the external RADIUS server.
- ÿ **Authentication Port:** Enter the authentication port of the RADIUS server.
- ÿ **Accounting Port:** The accounting port of the external RADIUS server.
- ÿ **Secret Key:** The Secret Key for RADIUS authentication.
- ÿ **Accounting Service:** The system supports RADIUS accounting that can be enabled or disabled.
- ÿ **Authentication Protocol:** The configuration of the system must match with that of the remote RADIUS server. **PAP** (Password Authentication Protocol) transmits passwords in plain text without encryption. **CHAP** (Challenge Handshake Authentication Protocol) is a more secure authentication protocol with hash encryption.

Note: If the RADIUS Server does not assign idle-timeout value, the WHG301 will use the local idle-timeout.

4.2.1.4 Authentication Method – LDAP

Choose “LDAP” from the **Authentication Method** field, the button beside the pull-down menu will become “LDAP Setting”.

Authentication Server - Server 4	
Server Name	<input type="text" value="Server 4"/> <small>*(Its server name)</small>
Postfix	<input type="text" value="ldap"/> <small>*(Its postfix name)</small>
Black List	<input type="text" value="None"/> <input type="button" value="v"/>
Authentication Method	<input type="text" value="LDAP"/> <input type="button" value="v"/> <input type="button" value="LDAP Setting"/>
Group	<input type="text" value="Group 1"/> <input type="button" value="v"/>
Enable Local VPN	<input type="checkbox"/>

Click the button of **LDAP Setting** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisk are necessary information which should be filled in. These settings will become effective immediately after clicking the **Apply** button.

Primary LDAP Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Ex: 389)</small>
Base DN	<input type="text"/> <small>*(CN=,dc=,dc=)</small>
Account Attribute	<input type="text"/> <small>*(Ex: uid)</small>
Secondary LDAP Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
Base DN	<input type="text"/>
Account Attribute	<input type="text"/>
Group Mapping	
Attribute-Group Mapping	Map LDAP Attributes to Group

- ÿ **Server IP:** The IP address of the external LDAP server.
- ÿ **Port:** The authentication port of the external LDAP server.
- ÿ **Base DN:** The Distinguished Name for the navigation path of LDAP account.
- ÿ **Account Attribute:** The attribute of LDAP accounts.
- ÿ **Attribute-Group Mapping:** This function is to assign a *Group* to a LDAP attribute sent from the LDAP server. When the clients classified by LDAP attributes log into the system via the LDAP server, each client will be mapped to its assigned Group. To get and show the attribute name and value from the configured LDAP server, enter *Username* and *Password* and click **Show Attribute**. Then, the table of attribute will be displayed. Enter the *Attribute Name* and *Attribute Value* chosen from the attribute table, and select a *Group* from the drop-down list box.

Attribute Name	Attribute Value
CN	USER01
C	TW

LDAP Group Mapping - Server 4				
<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
No.	LDAP Attribute Name	LDAP Attribute Value	Group	Remark
1	<input type="text" value="CN"/>	<input type="text" value="USER01"/>	<input type="text" value="Group 1"/>	<input type="text"/>
2	<input type="text" value="C"/>	<input type="text" value="TW"/>	<input type="text" value="Group 2"/>	<input type="text"/>

4.2.1.5 Authentication Method – NTDomain

Choose “**NTDomain**” from the **Authentication Method** field, the button beside the pull-down menu will become “**NT Domain Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Postfix	local <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	NT Domain <input type="button" value="v"/> <input type="button" value="NT Domain Setting"/>
Group	Group 1 <input type="button" value="v"/>
Enable Local VPN	<input type="checkbox"/>

Click the button of **NT Domain Setting** for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the **Apply** button.

Domain Controller	
Server IP	<input type="text"/> <small>*(IP Address)</small>
Transparent Login	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>(Windows 2000, 2003 or above)</small>

- Y **Server IP:** The IP address of the external NT Domain Server.
- Y **Transparent Login:** This function refers to Windows NT Domain single sign on. When *Transparent Login* is enabled, clients will log in to the system automatically after they have logged in to the NT domain, which means that clients only need to log in once.

4.2.1.6 Authentication Method – On-demand User

On-demand User Server Configuration: The administrator can enable and configure this authentication method to create on-demand user accounts. This function is designed for hotspot owners to provide temporary users with free or paid wireless Internet access in the hotspot environment. Major functions include accounts creation, users monitoring list, billing plan, billing report statistics, and external payment gateway support.

Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account List	View

1) General Settings

This is the common setting for the On-demand User authentication option. The generated on-demand users and all accounts related information such as postfix and unit will be shown in this list.

General Settings	
Postfix	<input type="text" value="ondemand"/>
Monetary Unit	<input checked="" type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> (Input other desired monetary unit, e.g. AU)
Group Name	<input type="text" value="Group 1"/>
WLAN ESSID	<input type="text" value="4ipnet"/>
Wireless Key	<input type="text"/>
Remaining Volume Sync Internal	<input checked="" type="radio"/> 10min(s) <input type="radio"/> 15min(s) <input type="radio"/> 20min(s)
Number of Tickets	<input checked="" type="radio"/> 1 <input type="radio"/> 2

Ÿ **Postfix:** Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Enter the postfix used for on-demand users.

Ÿ **Monetary Unit:** Select the desired monetary unit or specified the unit by users.

Ÿ **Group Name:** Select the desired group for on-demand user.

Ÿ **WLAN ESSID:** The administrator can enter the defined wireless ESSID in this field and it will be printed on the receipt for on-demand users' reference when accessing the Internet via wireless LAN service. The ESSIDs given here should be those of the Service Zones enabled for On-demand Users.

Ÿ **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the on-demand users' reference when accessing the Internet via wireless LAN service.

Ÿ **Remaining Volume Sync Internal:** While the on-demand user is still logged in, the system will update the

billing notice of the login successful page by the time interval defined here.

- Y **Number of Tickets:** Print one or duplicate receipts, when pressing the print button of the ticket printer which connected to serial port.

2) Ticket Customization

On-demand account ticket can be customized here and previewed on the screen.

Ticket Customization	
Receipt Header 1	<input style="width: 95%;" type="text" value="Welcome!"/>
Receipt Header 2	<input style="width: 95%;" type="text"/>
Receipt Footer	<input style="width: 95%;" type="text" value="Thank You!"/>
Background Image	<input type="radio"/> None <input checked="" type="radio"/> Default Image <input type="radio"/> Uploaded Image <input type="button" value="Edit"/>
<input type="button" value="Preview"/>	

- Y **Receipt Header:** There are two receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
- Y **Receipt Footer:** The entered content will be printed on the receipt. This footer is optional.
- Y **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose the default image or none. Click Browse to select the image file and then click upload. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.
- Y **Preview:** Click **Preview** button, the ticket will be shown including the information of username and password with the selected background. Print the ticket here.

3) Billing Plans

Administrators can configure several billing plans. Click **Edit** button to enter the page of Editing Billing Plan. Click **Apply** to save the plan that manually set up by the administrators. Go back to the screen of Billing Plans, click **Enable** button, and then the plan is activated.

Billing Plans					
Plan	Type	Quota	Price	Enable	Function
1	Time	2 hrs 0 mins	20	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
2	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
3	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
4	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
5	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
6	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
7	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
8	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
9	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>
0	N/A			<input type="checkbox"/>	<input type="button" value="Edit"/>

ÿ **Plan:** The number of the specific plan.

ÿ **Type:** This is the type of the plan, based on which it defines how the account can be used.

ÿ **Quota:** The limit on how On-demand users are allowed to access the network.

ÿ **Enable:** Click the radio button to activate the plan.

ÿ **Function:** Click the button **Edit** to add one billing plan.

- o **Time:** Total period of time (xx hrs yy mins), during which On-demand users are allowed to access the network.

Editing Billing Plan	
Plan	1
Type	Time
Quota	2 hr(s) 0 min(s) <small>(Range of min(s) : 0 ~ 59; they cannot both be zero.)</small>
Account Activation	First time login must be done within 3 day(s) 0 hour(s) <small>(Range of hour(s) : 0 ~ 23; they cannot both be zero.)</small>
Valid Period	After activation, account will be expired in 5 day(s) <small>(Must be larger than 0.)</small>
Price	20 <small>(Range : 0 ~ 100000, including two digits after decimal point, e.g. 1.00)</small>

- o **Volume:** Total traffic volume (xx Mbytes), up to which on-demand users are allowed to transfer data.

Editing Billing Plan	
Plan	2
Type	Volume
Quota	100 Mbyte(s) <small>(Range : 1 ~ 2000)</small>
Account Activation	First time login must be done within 3 day(s) 0 hour(s) <small>(Range of hour(s) : 0 ~ 23; they cannot both be zero.)</small>
Valid Period	After activation, account will be expired in 5 day(s) <small>(Must be larger than 0.)</small>
Price	20 <small>(Range : 0 ~ 100000, including two digits after decimal point, e.g. 1.00)</small>

- **Cut-off Time:** The time of day at which the on-demand account is cut off (made expired) by the system on that day. Please note that the “Grace Period” is an additional, short period of time after the account is cut off, during which a user is allowed to continue to use the on-demand account to access the Internet without paying additional fee.

Editing Billing Plan	
Plan	1
Type	Cut-off
Cut-off Time	12 : 00 <small>* Hour(s) range : 00:00 ~ 23:59</small>
Grace Period	Account remains usable for 1.5 hour(s) after cut-off.
Unit Price	20 per day <small>* Range : 0 ~ 100000, including two digits after decimal point, e.g. 1.99</small>

4) **External Payment Gateway**

This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access service to end customers who wish to pay for the service on-line.

The three options are **Authorize.Net**, **PayPal** and **Disable**.

External Payment Gateway		
<input type="radio"/> Authorize.Net	<input type="radio"/> PayPal	<input checked="" type="radio"/> Disable

§ **Authorize.Net**

Before setting up “Authorize.Net”, it is required that the merchant owners have a valid Authorize.Net account. Please see **Appendix A. Accepting Payments via Authorize.Net** for more information about opening an Authorize.Net account, relevant maintenance functions, and an example for end users.

Ø **Authorize.Net Payment Page Configuration**

External Payment Gateway		
<input checked="" type="radio"/> Authorize.Net	<input type="radio"/> PayPal	<input type="radio"/> Disable

Authorize.Net Payment Page Configuration	
Merchant Login ID	<input type="text"/> -
Merchant Transaction Key	<input type="text"/> -
Payment Gateway URL	<input type="text" value="https://secure.authorize.net/gateway/transact.dll"/> -
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Test Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="button" value="Try Test"/> -
MD5 Hash	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Merchant ID: This is the “Login ID” that comes with the Authorize.Net account

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

Payment Gateway URL: This is the default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net.

Test Mode: In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Authorize.Net.

Ø Service Disclaimer Content/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record

Service Disclaimer Content

We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

Choose Billing Plan for Authorize.Net Payment Page				
Plan	Enable/Disable		Quota	Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	2 hrs 0 mins	20
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

Client's Purchasing Record

Starting Invoice Number	Hotspot	-	00000001	-	<input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access -				
E-mail Header	Enjoy Online! -				

Service Disclaimer Content

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

Choose Billing Plan for Authorize.Net Payment Page

These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

Client's Purchasing Record

Starting Invoice Number: An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the

"Change the Number" checkbox to change it.

Description (Item Name): This is the item information to describe the product (for example, Internet Access).

Email Header: Enter the information that should appear in the header of the invoice.

Ø **Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content**

Authorize.Net Payment Page Fields Configuration		
Item	Displayed Text	Required
<input checked="" type="checkbox"/> Credit Card Number	Credit Card Number *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Credit Card Expiration Date	Credit Card Expiration Date *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Type	Card Type * <input checked="" type="checkbox"/> Visa <input checked="" type="checkbox"/> American Express <input checked="" type="checkbox"/> Master Card <input checked="" type="checkbox"/> Discover	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Code	Card Code *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> E-mail	E-mail *	<input type="checkbox"/>
<input type="checkbox"/> Customer ID	Room Number *	<input type="checkbox"/>
<input checked="" type="checkbox"/> First Name	First Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Last Name	Last Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Company	Company *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Address	Address *	<input type="checkbox"/>
<input checked="" type="checkbox"/> City	City *	<input type="checkbox"/>
<input checked="" type="checkbox"/> State	State *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Zip	Zip *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Country	Country *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Phone	Phone *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Fax	Fax *	<input type="checkbox"/>

*Displayed text fields must be filled.

Authorize.Net Payment Page Remark Content	
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If	

Ø **Authorize.Net Payment Page Fields Configuration**

Item: Check the box to show this item on the customer's payment interface.

Displayed Text: Enter what needs to be shown for this field.

Required: Check the box to indicate this item as a required field.

Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in the format of MMY. For example, an expiration date of July September 2009 should be entered as 0709.

Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

E-mail: An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

Customer ID: This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any format of information.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city is associated with either the billing address or shipping address of a transaction.

State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

Ø **Authorize.Net Payment Page Remark Content**

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

§ **PayPal**

Before setting up “PayPal”, it is required that the hotspot owners have a valid PayPal “Business Account”.

Please see **Appendix B. Accepting Payments via PayPal** for more information about setting up a PayPal Business Account, relevant maintenance functions, and an example for clients.

After opening a PayPal Business Account, the hotspot owners should find the “**Identity Token**” of this PayPal account to continue “PayPal Payment Page Configuration”.

Ø **External Payment Gateway / PayPal Payment Page Configuration**

External Payment Gateway

Authorize.Net
 PayPal
 Disable

PayPal Payment Page Configuration

Business Account	<input type="text"/>	-
Payment Gateway URL	<input type="text" value="https://www.paypal.com/cgi-bin/webscr"/>	-
Identity Token	<input type="text"/>	-
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Currency	<input type="text" value="USD (U.S. Dollar)"/>	-

Business Account: The “Login ID” (an email address) that is associated with the PayPal Business Account.

Payment Gateway URL: The default website address to post all transaction data.

Identity Token: This is the key used by PayPal to validate all the transactions.

Verify SSL Certificate: This is to help protect the system from accessing a website other than PayPal

Currency: The currency to be used for the payment transactions.

Ø **Service Disclaimer Content / Billing Configuration for Payment Page**

Service Disclaimer Content

We may collect and store the following personal information:
 email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
 If the information you provide cannot be verified, we may

Choose Billing Plan for PayPal Payment Page

Plan	Enable/Disable	Quota	Price
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	2 hrs 0 mins	20
2	<input type="radio"/> Enable <input type="radio"/> Disable		
3	<input type="radio"/> Enable <input type="radio"/> Disable		
4	<input type="radio"/> Enable <input type="radio"/> Disable		
5	<input type="radio"/> Enable <input type="radio"/> Disable		
6	<input type="radio"/> Enable <input type="radio"/> Disable		
7	<input type="radio"/> Enable <input type="radio"/> Disable		
8	<input type="radio"/> Enable <input type="radio"/> Disable		
9	<input type="radio"/> Enable <input type="radio"/> Disable		
10	<input type="radio"/> Enable <input type="radio"/> Disable		

Service Disclaimer Content: View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

Choose Billing Plan for PayPal Payment Page: These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

Ø Client's Purchasing Record / PayPal Payment Page Remark Content

Client's Purchasing Record	
Starting Invoice Number	Hotspot 00000001 <input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access -
Title for Message to Seller	Special Note to Seller -

PayPal Payment Page Remark Content
(A) Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,

Client's Purchasing Record:

Invoice Number: An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any kind of information.

Description: Enter the product/service description (e.g. wireless access service).

Title for Message to Seller: Enter the information that will appear in the header of the PayPal payment page.

PayPal Payment Page Remark Content: The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

5) On-demand Account Creation

On-demand accounts are listed and related. When at least one plan is enabled, the administrator can generate on-demand user accounts here. Click this to enter the On-demand Account Creation screen. Click on the **Create** button of the desired plan and an on-demand user account will be created. Click **Print** to print a receipt which will contain the on-demand user's information, including the username and password.

8 Note:

If no Billing plan is enabled, accounts cannot be created by clicking **Create** button. Please goes back to Billing Plans to active at least one Billing plan by clicking **Edit** button and **Apply** the setting to activate the plan. The printer used by **Print** is a pre-configured printer connected to the administrator's computer.

On-demand Account Creation					
Plan	Type	Quota	Price (\$)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	<input type="button" value="Create"/>
2	Time	12 hr(s)	3.99	Enabled	<input type="button" value="Create"/>
3	Volume	500 Mbyte(s)	5	Enabled	<input type="button" value="Create"/>
4	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
5	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
6	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
7	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
8	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
9	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>
0	N/A	N/A	N/A	Disabled	<input type="button" value="Create"/>

ÿ **Plan:** The number of a specific plan.

ÿ **Type:** Show one type of the plan in Time, Volume or Cut-off.

ÿ **Quota:** The Time Volume is how long the on-demand user is allowed to access the Internet.

ÿ **Price:** The unit price of each plan.

ÿ **Status:** Show the status in enabled or disabled.

ÿ **Function:** Press **Create** button for the desired plan; an On-demand user account will be created, and then click **Printout** to print a receipt which will contain this on-demand user's information.

On-demand Account Creation					
Plan	Type	Quota	Price	Status	Function
1	Time	2 hrs 0 mins	20	Enabled	<input type="button" value="Create"/>

↓

Creating an On-demand Account	
Plan : Type	1: Time
Quota	2 hrs 0 mins
Account Activation	First time login must be done within 3 day(s)
Valid Period	After activation, the account will be expired in 5 day(s)
Total Price	20
Operator's Remark	<input type="text"/> <small>Add a remark related to this account (for example, the customer's name)</small>
Please confirm the information and press Create button to create an account.	

↓

Welcome!


Username	9626@ondemand
Password	5jw34p96
Plan : Type	1 : Time
Quota	2 hrs 0 mins
Total Price	20
Remark	

ESSID : 4ipnet

Shared Wireless Key: None (Open System)

Your first time login must be done before 2008/01/27 10:03
The account is valid within 5 day(s) after your first login.

Thank You!



6) On-demand Account List

All created On-demand accounts are listed and related information on is also provided.

On-demand Account List					
Username	Password	Remaining Quota	Status	Account Valid Through	<input type="button" value="Delete All"/>
2z89	3n8rkq2p	1 hr(s) 2 min(s)	Normal	2007/11/21-20:30	Delete
cy87	u3u5s39m	1 hr(s) 2 min(s)	Normal	2007/11/21-20:35	Delete
3f2d	6mmx96aw	51 min(s)	Normal	2007/11/20-18:46	Delete
5vsc	4m5kqr3r	1 hr(s) 2 min(s)	Normal	2007/11/21-21:34	Delete
u944	58e5ns78	51 min(s)	Normal	2007/11/21-10:37	Delete

(Total:5) [First](#) [Previous](#) [Next](#) [Last](#)

Y **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.

Y **Username:** The login name of the user.

Y **Password:** The login password of the user.

Y **Remaining Quota:** The remaining time or volume that the user can continue to use to access the network.

Y **Status:** The status of the account.

- o **Normal:** the account is not currently in use and also does not exceed the quota limit.
- o **Online:** the account is currently in use.
- o **Expired:** the account is not valid any more, even there is remaining quota to be used.
- o **Out of Quota:** the account has exceeded the quota limit
- o **Redeemed:** the account has been applied for account renewal.

Y **Delete All:** This will delete all the users at once.

Y **Delete:** This will delete the users individually.

4.2.1.7 Authentication Method – SIP

The system provides SIP proxy for SIP clients (devices or soft clients) pass through NAT. After enable SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface.

Administrator will be able to add trusted SIP Registrars up to four of them. A group can be chosen to govern SIP traffic.

Authentication Server - SIP		
	IP Address	Remark
Trusted Registrar	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
Group	None <input type="button" value="v"/>	Group selection applied to clients login with SIP authentication.

- ÿ **SIP:** SIP authentication supports 4 Trusted SIP Registrar.
- ÿ **IP Address:** The IP address of the Trusted SIP Registrar.
- ÿ **Remark:** The administrator can enter extra information in this field for remark.
- ÿ **Group:** A Group option can be applied to the clients who login with SIP Authentication. Be noted that the specific route of the applied Policy for the selected Group cannot conflict with the assigned WAN interface for SIP authentication.

4.2.2 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include up to 40 users. Users' accounts that appear in the black list will be denied of network access. The administrator can use the pull-down menu to select the desired black list.

Black List Configuration		
Select Black List:	1:Blacklist1 ▾	
Name	Blacklist1	
User	Remark	<input type="button" value="Delete"/>
(Total:0) First Prev Next Last		
<input type="button" value="Add User(s)"/>		

- ÿ **Select Black List:** There are 5 lists to select from for the desired black list.
- ÿ **Name:** Set the black list name and it will show on the pull-down menu above.
- ÿ **Add User to List:** Click the hyperlink to add users to the selected black list.

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text" value="James"/>	<input type="text" value="Hacker"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

After entering the usernames in the “**Username**” blanks and the related information in the “**Remark**” blank (not required), click **Apply** to add the users.

User 'James' has been added!

 [Add Users to Blacklist](#)

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>

If removing a user from the black list is desired, select the user's “**Delete**” check box and then click the **Delete** button to remove that user from the black list.

Black List Configuration		
Select Black List:	1:Blacklist1 <input type="button" value="v"/>	
Name	Blacklist1	
User	Remark	<input type="button" value="Delete"/>
James	Hacker	<input checked="" type="checkbox"/>

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#)

4.2.3 Group Configuration

There are 8 groups to choose from. Local users can be classified by applying Group options. A Group which is allowed to access a Service Zone can be applied with a Policy within this zone. The same Group within different Service Zones can be applied with different Policies as well as different Authentication Options.

Group Configuration - Group 7			
Select Group:	Group 7 ▾		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark	<input type="text"/>		
Zone Permission Configuration & Policy Assignment - Group 7			
Name	Enabled	Policy	Edit Group Permission
Service Zone : Default	<input checked="" type="checkbox"/>	Policy 7 ▾	Default
Service Zone : SZ1	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ1
Service Zone : SZ2	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ2
Service Zone : SZ3	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ3
Service Zone : SZ4	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ4
Service Zone : SZ5	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ5
Service Zone : SZ6	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ6
Service Zone : SZ7	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ7
Service Zone : SZ8	<input checked="" type="checkbox"/>	Policy 7 ▾	SZ8
Remote VPN	<input checked="" type="checkbox"/>	Policy 7 ▾	Remote VPN

Y Group Configuration – Group 1~8

- Ø **QoS Profile:** Set parameters for traffic classification.

Group 1 - Traffic Configuration	
Traffic Class	Best Effort ▾
Group Total Downlink	Unlimited ▾
Individual Maximum Downlink	Unlimited ▾
Individual Request Downlink	None ▾
Group Total Uplink	Unlimited ▾
Individual Maximum Uplink	Unlimited ▾
Individual Request Uplink	None ▾

- **Traffic Class:** A Traffic Class can be chosen for a Group of users. There are four traffic classes: **Voice, Video, Best-Effort** and **Background**. Voice and Video traffic will be placed in the high priority

queue. When Best-Effort or Background is selected, more bandwidth management options such as Downlink and Uplink Bandwidth will appear.

- **Group Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
- **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
- **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
- **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client belonging to this Group. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

Ø Privilege Profile:

Group 1 - Privilege Configuration	
Change Password Privilege	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Change Password Privilege:** When **Change Password Privilege** is enabled, the authenticated local users within this Group are allowed to change their password via the Login Success Page.

Ÿ Zone Permission Configuration & Policy Assignment – Group 1~8

A Group can be assigned to one Service Zone or multiple Service Zones. Moreover, a Group can be applied with different Policies within different Service Zones. Remote VPN is considered as a zone, where clients log into the system via remote VPN.

Group Configuration - Group 1			
Select Group:	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Name	Enabled	Policy	Edit Group Permission
Service Zone : Default	<input checked="" type="checkbox"/>	Policy 1	Default
Service Zone : SZ1	<input checked="" type="checkbox"/>	Policy 1	SZ1
Service Zone : SZ2	<input checked="" type="checkbox"/>	Policy 1	SZ2
Service Zone : SZ3	<input checked="" type="checkbox"/>	Policy 1	SZ3
Service Zone : SZ4	<input checked="" type="checkbox"/>	Policy 1	SZ4
Service Zone : SZ5	<input checked="" type="checkbox"/>	Policy 1	SZ5
Service Zone : SZ6	<input checked="" type="checkbox"/>	Policy 1	SZ6
Service Zone : SZ7	<input checked="" type="checkbox"/>	Policy 1	SZ7
Service Zone : SZ8	<input checked="" type="checkbox"/>	Policy 1	SZ8
Remote VPN	<input checked="" type="checkbox"/>	Policy 1	Remote VPN

- Ø **Name:** The name of Service Zones and Remote VPN.
- Ø **Enabled:** Select *Enabled* to allow clients of this Group to log into the selected Service Zones. For example, the above figure shows that users in Group 1 can access network services via every Service Zone as well as Remote VPN under constraints of Policy 1.
- Ø **Policy:** Select a *Policy* that the Group will be applied with when accessing respective Service Zones.
- Ø **Edit Group Permission:** The relation between Group and Service Zone is many to many; every Group can access network services via more than one Service Zone, and meanwhile, each Service Zone can serve more than one Group.

Click the hyperlink in the **Edit Group Permission** column to enter the **Group Configuration** interface, which is based on the role of Service Zone, to configure the relation between Group and Zone.

Group Permission - Service Zone : Default			
Group Option	Enabled	Policy	Edit Group Option
Group 1	<input checked="" type="checkbox"/>	Policy 1	Group 1
Group 2	<input checked="" type="checkbox"/>	Policy 2	Group 2
Group 3	<input checked="" type="checkbox"/>	Policy 3	Group 3
Group 4	<input checked="" type="checkbox"/>	Policy 4	Group 4
Group 5	<input checked="" type="checkbox"/>	Policy 5	Group 5
Group 6	<input checked="" type="checkbox"/>	Policy 6	Group 6
Group 7	<input checked="" type="checkbox"/>	Policy 7	Group 7
Group 8	<input checked="" type="checkbox"/>	Policy 8	Group 8

- **Group Option:** The name of Group options available for selection.
- **Enabled:** Select *Enabled* to allow clients of the enabled Groups to log in to this Service Zone under

constraints of the selected Policies.

Check *Enabled* of each individual Group to assign it to the Service Zone listed. For example, the above figure shows, clients in Group 1~8 can access Default Service Zone, where they are governed by Policy 1~8 respectively.

- **Policy:** Select a *Policy* that the Group will be applied with when accessing this Service Zone.
- **Edit Group Option:** Click the hyperlink in the **Edit Group Option** column to enter **Zone Permission Configuration & Policy Assignment** interface, which is based on the role of Group, to configure the relation between Group and Zone.

4.2.4 Policy Configuration

WHG301 supports multiple Policies, including one **Global Policy** and 12 individual **Policy**. Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone.

The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is RADIUS, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute. When the type of authentication database is LDAP, the **Attribute-Group Mapping** function will be available to allow the administrator to assign a Group for LDAP attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute. When the type of database is SIP, the **Group** selection function will be available to allow the administrator to assign a Group option for all SIP clients.

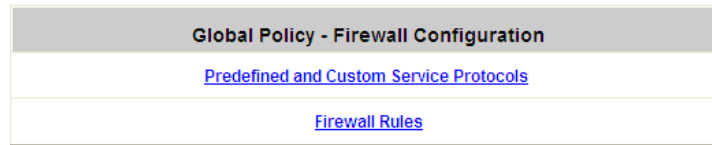
4.2.4.1 Global Policy

Global is the system's universal policy including **Firewall Rules**, **Specific Routes Profile** and **Maximum Concurrent Session** which will be applied to all users unless the user has been regulated and applied with another Policy.

Policy Configuration - Global Policy	
Select Policy:	Global ▼
Firewall Profile	Setting
Specific Route Profile	Setting
Maximum Concurrent Sessions	500 ▼ (Sessions per User)

- Ÿ **Select Policy:** Select **Global** to set the **Firewall Profile**, **Specific Route Profile** and **Privilege Profile**.
- Ÿ **Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- Ÿ **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- Ÿ **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

- Ø **Firewall Profile:** Click **Setting** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.



- **Predefined and Custom Service Protocols:** There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking **Add**, and delete the added protocols with **Select All** and **Delete** operations.

This link leads to a Service Protocols List where the administrator can define a list of service by protocols (TCP/UDP/ICMP/IP).

Global Policy - Service Protocols List			
No.	Name	Description	Select All
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP; Type: Any, Code: Any	<input type="checkbox"/>
5	FTP	TCP/UDP; Destination Port: 20;21	<input type="checkbox"/>
6	HTTP	TCP/UDP; Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP; Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP; Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP; Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP; Destination Port: 67;68	<input type="checkbox"/>

Add Delete

(Total: 27) [First](#) [Prev](#) [Next](#) [Last](#)

- **Firewall Rules:** Click the number of **Filter Rule No.** to edit individual rules and click **Apply** to save the settings. The rule status will show on the list. Check “**Active**” box and click **Apply** to enable that rule. This link leads to the Firewall Rules page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to Always, Recurring or One Time.

Global Policy - Firewall Rules							
No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	<input type="checkbox"/>	Block		ANY		ALL	Always
				ANY			
2	<input type="checkbox"/>	Block		ANY		ALL	Always
				ANY			

Selecting the Filter Rule Number 1 as an example:

Global Policy - Edit Filter Rule			
Rule Item	1		
Rule Name	<input type="text"/>		
Source		Destination	
Interface	ALL <input type="button" value="v"/>	Interface	ALL <input type="button" value="v"/>
IP Address <input type="button" value="v"/>	0.0.0.0	IP Address <input type="button" value="v"/>	0.0.0.0
Subnet Mask	0.0.0.0 (/0) <input type="button" value="v"/>	Subnet Mask	0.0.0.0 (/0) <input type="button" value="v"/>
IPSec Traffic	<input type="checkbox"/>	IPSec Traffic	<input type="checkbox"/>
MAC Address	<input type="text"/>		
Service	ALL <input type="button" value="v"/>		
Schedule	<input checked="" type="radio"/> Always <input type="radio"/> Recurring <input type="radio"/> One Time		
Action	<input checked="" type="radio"/> Block <input type="radio"/> Pass		

- **Rule Number:** This is the rule selected “1”. Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
 - **Rule Name:** The rule name can be changed here.
 - **Source/Destination – Interface/Zone:** There are choices of **ALL**, **WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
 - **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name filtering is not.
 - **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
 - **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
 - **Source/Destination – IPSec Encrypted:** Check the box for only filtering on the encrypted traffic.
 - **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
 - **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time**. **Recurring** is set with the hours within a week.
 - **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.
- Ø **Specific Route Profile:** Click the button of **Setting** for **Specific Route Profile**, the Specific Route Profile list will appear.

Global Policy - Specific Route Profile			
Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>

- **Route No.:** The number of route.
- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.

Ø **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

8 **Note:** For more information, please refer to **Appendix E. Session Limit and Session Log.**

4.2.4.2 Policy 1 ~ Policy 12

Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is RADIUS, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute. When the type of authentication database is LDAP, the **Attribute-Group Mapping** function will be available to allow the administrator to assign a Group for LDAP attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute. When the type of database is SIP, the **Group** selection function will be available to allow the administrator to assign a Group option for all SIP clients.

Policy Configuration - Policy 1	
Select Policy:	Policy 1 ▾
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Maximum Concurrent Sessions	500 ▾ (Sessions per User)

- Ÿ **Select Policy:** Select **Policy1~Policy12** to set the **Firewall Profile**, **Specific Route Profile**, **Schedule Profile** and **Maximum Concurrent Session**.
- Ÿ **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- Ÿ **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- Ÿ **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- Ÿ **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

Ø **Firewall Profile:** Click **Setting** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

Policy 1 - Firewall Configuration	
Predefined and Custom Service Protocols	
Firewall Rules	

- **Predefined and Custom Service Protocols:** This link leads to a Service Protocols List where the administrator can define a list of service by protocols (TCP/UDP/ICMP/IP). There are predefined service protocols available for firewall rules editing. The administrator is able to add new customized service protocols by clicking **Add**, and delete the added protocols by clicking **Delete**.

Policy 1 - Service Protocols List			
No.	Name	Description	Select All
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP; Type: Any, Code: Any	<input type="checkbox"/>
5	FTP	TCP/UDP; Destination Port: 20;21	<input type="checkbox"/>
6	HTTP	TCP/UDP; Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP; Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP; Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP; Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP; Destination Port: 67;68	<input type="checkbox"/>

- **Firewall Rules:** Click on the hyperlink in the **No.** column to edit individual rules and then click **Apply** to save the settings. The rule status will show on the list. Check the *Active* check box and click **Apply** to enable that rule. This link leads to the **Firewall Rules** page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by **Source**, **Destination** and **Pass/Block** action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to *Always*, *Recurring* or *One Time*.

Policy 1 - Firewall Rules							
No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	<input type="checkbox"/>	Block		ANY		ALL	Always
				ANY			
2	<input type="checkbox"/>	Block		ANY		ALL	Always
				ANY			

Below depicts an example of selecting Filter Rule Number 1:

Policy 1 - Edit Filter Rule			
Rule Item	1		
Rule Name	<input type="text"/>		
Source		Destination	
Interface	ALL <input type="button" value="v"/>	Interface	ALL <input type="button" value="v"/>
IP Address <input type="button" value="v"/>	0.0.0.0	IP Address <input type="button" value="v"/>	0.0.0.0
Subnet Mask <input type="button" value="v"/>	0.0.0.0 (/0)	Subnet Mask <input type="button" value="v"/>	0.0.0.0 (/0)
IP Sec Traffic	<input type="checkbox"/>	IPSec Traffic	<input type="checkbox"/>
MAC Address	<input type="text"/>		
Service	ALL <input type="button" value="v"/>		
Schedule	<input checked="" type="radio"/> Always <input type="radio"/> Recurring <input type="radio"/> One Time		
Action	<input checked="" type="radio"/> Block <input type="radio"/> Pass		

- **Rule Item:** This rule number of the selected rule. Rule No. 1 has the highest priority; Rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source / Destination – Interface/Zone:** There are choices of *ALL*, *WAN1*, *WAN2*, *Default* and the *Service Zones* to be applied to the traffic interface.
- **Source / Destination – IP Address/Domain Name:** Enter the source and destination IP addresses.
- **Source / Destination – Subnet Mask:** Enter the source and destination subnet masks.
- **Source / MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source / Destination – IPSec Traffic:** Check the box to filter the encrypted traffic only.
- **Service Protocol:** Select a defined protocol from the drop-down list box.
- **Schedule:** Defines the time when this firewall rule will be activated. When a schedule is selected, the clients assigned to this Policy are applied with the firewall rule only within the time selected. There are three options, *Always*, *Recurring* and *One Time*.
- **Action for Matched Packets:** There are two options, *Block* and *Pass*. Block is to prevent packets from passing, while Pass is to permit packets passing.

Ø **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a Policy. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.

Policy 1 - Specific Default Route			
Enable <input type="checkbox"/>	Default Gateway: IP Address <input type="button" value="v"/> <input type="text"/>		
Policy 1 - Specific Route Profile			
Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>

Click **Setting** of *Specific Route Profile* to enter the **Specific Route** page for further configuration.

- **Enable:** Check **Enable** box to activate this function or uncheck to inactivate it.
- **Destination / IP Address:** The destination network address or IP address of the destination host.
Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that are just entered and applied.
- **Destination / Subnet Netmask:** The subnet mask of the destination network. Select **255.255.255.255(/32)** if the destination is a single host.
- **Gateway / IP Address:** The IP address of the gateway or next router to the destination.

Ø **Schedule Profile:** Click **Setting** of *Schedule Profile* to enter the configuration page. Select **Enable** to show the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Check the desired time slots and click **Apply** to save the settings. These settings will become effective immediately after clicking **Apply**.

Enabled Disabled

Policy 1 - Login Schedule Profile							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
01:00~01:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
02:00~02:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03:00~03:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Ø **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

8 **Note:** For more information, please refer to **Appendix E. Session Limit and Session Log**.

4.2.5 Additional Configuration

Additional Configuration	
User Control	Idle Timer: <input type="text" value="10"/> *(Range: 1-1440)
	Multiple Login <input type="checkbox"/> (On-demand and RADIUS authentication do NOT support multiple login.)
Roaming Out Timer	Session Timeout: <input type="text" value="120"/> *(Range: 5-1440)
	Idle Timeout: <input type="text" value="10"/> *(Range: 1-120)
	Interim Update: <input type="text" value="5"/> *(Range: 1-120)
Upload File	Certificate
Credit Reminder	Volume <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Time and Cut-off <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Enhance User Authentication	Permit MAC Address List (Control list to manage which client devices are allowed to access the login page)

Y **User Control:** Functions under this section apply to all general users.

Idle Timer: If a user has idled with no network activities, the system will automatically kick out the user. The logout timer can be set between 1~1440 minutes, and the default logout time is 10 minutes.

Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication.)

Y **Roaming Out Timer:**

Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.

Idle Timeout: If a user has idled with no network activities, the system will automatically kick out the user.

Interim Update: The system will update the users' current status and usage according to this time period.

Y **Upload File**

Certificate: A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates. You can apply for a SSL certificate at CAs such as VeriSign.

If you already have an SSL Certificate, please Click Browse to select the file and upload it. Click **Apply** to complete the upload process.

Upload Private Key	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Upload Customer Certificate	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Without a valid certificate, users may encounter the following problem in IE7 when they try to open the login page.



Click “Continue to this website” to access the user login page.

To Use Default Certificate: Click *Use Default Certificate* to use the default certificate and key. Click **restart** to validate the changes.

You just overwrite the setting with default KEY & default CA file
You should restart the system to activate this. Click to [restart](#).

- Y **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.

Credit Reminder	Volume	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	<input type="text" value="1"/> Mbyte	*(Range: 1-10; Default: 1)
	Time	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	<input type="text" value="5"/> minutes	*(Range: 1-30; Default: 5)

- Y **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into WHG301. There are 40 users maximum allowed in this MAC address list. User authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click **Apply**.

MAC Address Control			
<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
Item	MAC Address	Item	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)



The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

4.3 AP Management

WHG301 supports to manage up to 12 access points (AP), and they can be configured in this section. This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management**, **AP Upgrade** and **WDS Management**.

AP Management	
AP List	The list shows the current AP summary including type, name, IP, MAC and online status. It also provides the operations for each AP on reboot, enable, disable, delete, apply a new template, and to do further examination or detailed configuration.
AP Discovery	This discovery function is to detect the unmanaged APs within LANs and assign the desired IPs for the future management. With the AP access information, administrator is able to manually or automatically discover AP on the selected LAN(s).
Manual Configuration	Administrators who are familiar with the new AP can set it up manually by filling in the necessary information. There are three templates from the drop-down box that can be chosen.
Template Settings	Administrators can edit template settings here. These templates are saved and can be used in "Manual Configuration" and "AP Discovery" sections.
Firmware Management	This page lets administrators manage firmwares and shows each firmware's information with operations of download and delete.
AP Upgrade	This page shows each AP on name, firmware version and the time previously being upgraded. Administrators can choose a firmware version from the drop-down box to upgrade APs. Several AP upgrades can be processed simultaneously by checking the upgrade boxes.
WDS Management	WDS (Wireless Distribution System) is a function to interconnect all the managed APs (access points) wirelessly to form a "Tree" connection with the structure of Parents and Children. The WDS Management provides the WDS tree status and enable the administrator to add, move and delete the WDS connections among the "Tree".

4.3.1 AP List

All of the APs under the management of WHG301 will be shown in the list. The AP can be edited by clicking the hyperlink of **AP Name** and the AP status can be got by clicking the hyperlink of **Status**.

AP List					
<input type="checkbox"/>	AP Type	AP Name	IP Address	Service Zone	Status
			MAC Address		
<input type="checkbox"/>	EAP100	EAP100A	192.168.1.9	Default	Online
			11:22:33:44:55:66		
<input type="checkbox"/>	EAP100	EAP100B	192.168.1.109	Default	Offline
			1A:2B:3C:4D:5E:6F		

(Total: 2) [First](#) [Prev](#) [Next](#) [Last](#)

Check any AP and then click the button below to **Reboot**, **Enable**, **Disable** and **Delete** the checked AP if desired.

AP List					
<input type="checkbox"/>	AP Type	AP Name	IP Address	Service Zone	Status
			MAC Address		
<input type="checkbox"/>	EAP100	EAP100A	192.168.1.9	Default	Online
			11:22:33:44:55:66		
<input checked="" type="checkbox"/>	EAP100	EAP100B	192.168.1.109	Default	Offline
			1A:2B:3C:4D:5E:6F		

(Total: 2) [First](#) [Prev](#) [Next](#) [Last](#)

Click **Apply Template** to select one template to apply to the AP.

Template

Template: TEMPLATE1	
Wireless b/g mode	802.11b+802.11g
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

Y AP Name

Click **AP Name** and enter the interface about related settings. There are four kinds of settings, **General Settings**, **LAN Interface Setting**, **Wireless Interface Setting** and **Access Control Setting**. Click the hyperlink to go on the configuration.

General Settings		
General	Name	EAP100B
	Firmware	1.00

LAN Interface Settings		
LAN	IP	192.168.1.109
	Gateway	192.168.1.254

Wireless Interface Settings		
Wireless LAN	Channel	Auto
	Data Rate	Auto

Access Control Settings		
Access Control	Status	Disabled
	Number of MAC Addresses	0

Ø **General Setting:** Click **Setting** to enter the **General Setting** interface. Firmware information can be observed here.

General Settings	
Name	<input type="text" value="EAP100B"/>
Admin Password	<input type="password" value="••••"/>
NTP	Time Zone (GMT+08:00)Taipei,Taiwan
	NTP Server 1: <input type="text" value="tick.stdtime.gov.tw"/>
	NTP Server 2: <input type="text" value="tock.stdtime.gov.tw"/>
SNMP	Disabled
SYSLOG	Disabled
Remark	<input type="text"/>
Firmware	

Ø **LAN Setting:** Click **LAN** to enter the **LAN Setting** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN Settings	
IP Address	<input type="text" value="192.168.1.109"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
Primary DNS	<input type="text" value="192.168.1.254"/>
Secondary DNS	<input type="text"/>

Y **Wireless LAN:** Click **Wireless LAN** to enter the **Wireless** interface.

Ø **Access Control:** In this function, when the status is “**Allowed**”, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP; on the other hand, when the status is “**Denied**”, the clients whose MAC addresses are listed in the list will be denied to connect to the AP. When “**Disabled**” is selected, all clients can connect to the AP. The default is **Disabled**.

- o **User Limit:** Limit the number of users connected to that AP.

Access Control			
Status	<input type="text" value="Allowed"/>		
User Limit	<input type="text" value="32"/>	<small>(Range: from 1 to 32)</small>	

MAC Address List			
<input type="text" value="12:13:14:1A:1B:1C"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="text" value="Disabled"/>
<input type="text"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="text" value="Disabled"/>
<input type="text"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="text" value="Disabled"/>
<input type="text"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="text" value="Disabled"/>
<input type="text"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="text" value="Disabled"/>

Y **Status**

After clicking the hyperlink in the Status column, there are two areas of information shown: **AP Status Summary** and **AP Status Details**. AP Status Summary includes **AP Name**, **AP Type**, **LAN Interface MAC address**, **Wireless Interface MAC address**, **Report Time**, **SSID**, and **Number of Associated Clients**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status Associated Client Status** and **Local Log Status**.

AP Status Summary	
AP Name	EAP100B
AP Type	EAP100
LAN MAC	
Wireless LAN MAC	
Report Time	N/A
SSID	4ipnet (Service Zone: Default)
Number of Associated Clients	0

AP Status Detail
System Status
LAN Status
Wireless LAN Status
Access Control Status
Associated Client Status
Local Log Status

4.3.2 AP Discovery

Use this function to detect and manage all of the APs in the network segments. Note that WHG301 can only manage APs that are connected to its LAN ports. Therefore, the AP discovery function is for adding locally connected APs to its management list. The administrator must know the local IP addresses of the APs he/she wishes to discover.

AP Discovery					
AP Type	EAP100				
Interface	Default <input type="button" value="v"/>				
Admin Settings Used to Discover	<input checked="" type="radio"/> Factory Default IP Address: 192.168.1.1 Login ID: admin Password: admin <input type="radio"/> Manual				
IP Addresses of APs after Discovery	Start IP Address: <input type="text" value="192.168.1.1"/>				
<input type="button" value="Scan Now"/>					
Background AP Discovery					
Status	Disabled				<input type="button" value="Configure"/>
Discovered AP List					
AP Type	IP Address	AP Name	Template	Service Zone	<input type="button" value="Add"/>
	MAC Address	Password	Channel		
(Total: 0) First Prev Next Last					
Last discovery was done at 23:44:25 December 20, 2007.					

Y To discover AP manually, please fill in the required data.

- Ø **AP Type:** Choose the type of AP you wish to discover.
- Ø **Interface:** Set to default.
- Ø **Admin Settings Used to Discover:** Choose from Factory Default or Manual.
- Ø **IP Addresses of APs after Discovery:** Start assigning from this IP address to discovered APs.

Then click the **Scan Now** button and the APs match the given settings will show in the list below. If one of the IP addresses intended is used, a warning message will show up. In this case, please change the IP range and then click **Scan Now** again. Input the desired name and password for the AP. Select one template check it and then click **Add** to add it under the managed list. (About the template, please see 4.3.4 Template Settings).

When the matched AP is discovered, it will show up in the list below and be given a new IP address set here (ex: 192.168.1.1). Check the **Add** box to add the AP and it will be listed to the AP list. When an AP is added, its MAC address will be automatically recorded into MAC Privilege List (please see 4.4.2 Privilege List) so its management page can be accessed.

Click **Configuring** to go on the related configuration. For the details, please refer to **4.3.1 AP List**.

AP List					
<input type="checkbox"/>	AP Type	AP Name	IP Address	Service Zone	Status
			MAC Address		
<input type="checkbox"/>	EAP100	EAP100A	192.168.1.9	Default	Offline
			11:22:33:44:55:66		

Y **Background AP Discovery:** Click **Configure** to enter Background AP Discovery interface to go on related configuration.

Background AP Discovery	
AP Type	
Interface	Default <input type="button" value="v"/>
Admin Settings Used to Discover	<input checked="" type="radio"/> Factory Default IP Address: 192.168.1.1 Login ID: admin Password: admin <input type="radio"/> Manual
IP Addresses of APs after Discovery	Start IP Address: <input type="text" value="192.168.1.1"/>
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

The **Interface** and **AP Access** configuration is the same as the settings mentioned above. When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and “Auto-Add AP” is enabled, it will be assigned an available IP from the starting IP address and apply the selected template. You can also set the channel the AP would use.



The scanning process may take a long time if the IP range assigned to scan is too wide.

4.3.3 Manual Configuration

The AP also can be added manually even though when it is offline. Input the related data of the AP and select a Template. After clicking **Add**, the AP will be added to the managed list.

Manual Configuration	
AP Type	EAP100
AP Name	<input type="text"/> -
Admin Password	<input type="text" value="admin"/>
AP IP	<input type="text"/> -
AP MAC	<input type="text"/> -
Remark	<input type="text"/>
Template	TEMPLATE1 <input type="button" value="v"/>
Channel	Auto <input type="button" value="v"/>

4.3.4 Template Settings

Template is a model that can be copied to every AP and not necessary to configure the AP individually. There are three templates provided. Click **Edit** to go on configuration.

Template Settings		
AP Type	EAP100	<input type="button" value="Edit"/>
Template Name	TEMPLATE1 <input type="button" value="v"/>	

Before configure the template, copy the configuration mode of an AP to the template by selecting a **Source AP**, and without configuring the template from the beginning, administrators can also revise some settings for demand. If copy is not desired, please select **NONE**. Input the **Template Name** and **Template Remark** and click the button of **Configure** to go on configuration.

Template Edit		
Template Name	TEMPLATE1 <input type="button" value="v"/>	<input type="button" value="Configure"/>
Template Source	None <input type="button" value="v"/>	
Template Remark	Template 1	

After entering the interface, revise the configuration for demand and change administrator's password if desired. About other function settings, please refer to **4.3.1 AP List**.

Y Template Editing

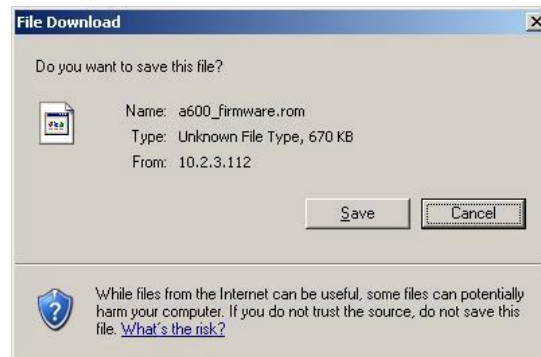
The administrator can set the template configuration manually. Click **Configure** button to have detailed configurations.

4.3.5 Firmware Management

Firmware Upload displays the current version of the AP's firmware. New firmware can be uploaded here to update the current firmware. To upload, click **Browse** to select the file and then click **Upload**.

Firmware Upload				
File Name	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>	

Firmware List				
File Name	AP Type	Version	Size	Actions
Checksum				



4.3.6 AP Upgrade

Check the APs which need to be upgraded and select the upgrade version of firmware, and click **Apply** to upgrade firmware.

AP List					
Name	Type	Version	Upgraded Time	New Version	Upgrade

4.3.7 WDS Management

WDS Management (Wireless Distribution System) is a function used to connect **APs** (Access Points) wirelessly. The WDS management function of the system can help administrators to setup a “Tree” structure of WDS network.

Default Settings for Newly Added WDS Tree			
Security	None	Channel	1 Edit

WDS Status			
WDS Tree	Security	Channel	Edit
Refresh Interval	Disable Auto Refresh <input type="button" value="v"/>		
No WDS operation has been done.			

WDS Update	
The Parent AP of this new connection.	<input type="button" value="v"/> <input type="button" value="Add"/>
The Child AP of this new connection.	<input type="button" value="v"/>
The Parent AP of this updated connection.	<input type="button" value="v"/> <input type="button" value="Move"/>
The Child AP of this updated connection, and the connection to the previous Parent AP will be deleted.	<input type="button" value="v"/>
The AP selected including all the Child APs of it will be deleted.	<input type="button" value="v"/> <input type="button" value="Delete"/>

- Y **WDS Status:** Status shows the added APs in the WDS Tree with the Security and Channel settings. The WDS could be set up more than one tree. Click the **Edit** is to change the **WDS connection settings** for the associated WDS Tree.
- Y **WDS Update:** Update the WDS connection with the following operations.
 - Ø **Add:** Add a new WDS connection with a Child AP not in the WDS and a Parent AP from the AP List. A new WDS Tree will be added if the selected Parent AP is not in any of the current WDS Trees. Click **Edit** is to change the **WDS connection settings** for the new added WDS Tree.
 - Ø **Move:** Update a WDS connection with a Child AP from WDS and a Parent AP which could be anymore from WDS, and the previous WDS connection of the Child AP to the previous Parent AP will be deleted.
 - Ø **Delete:** All the WDS connections of the selected AP will be deleted including the WDS connections to its Child APs, and the Child APs without wired connection will become unreachable.

4.4 Network Configuration

This section includes the following functions: **Network Address Translation, Privilege List, Monitor IP List, Walled Garden List, Proxy Server Properties, Dynamic DNS, IP Mobility** and **VPN Configuration**.

The screenshot shows the 'Network Configuration' page of the 4ipnet WHG301 interface. The page has a red header with the 4ipnet logo and the title 'Wireless Hotspot Gateway WHG301'. Below the header is a navigation bar with buttons for System Configuration, User Authentication, AP Management, Network Configuration (selected), Utilities, and Status. The main content area is titled 'Network Configuration' and contains a table with the following information:

Network Configuration	
Network Address Translation	4ipnet WHG301 provides 3 types of network address translation: DNZ (Demilitarized Zone), Public Accessible Server and IPPortRedirect.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List	System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hyperlink.
Walled Garden List	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties	4ipnet WHG301 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	4ipnet WHG301 supports dynamic DNS (DDNS) feature.
IP Mobility	System supports IP PNP Configuration.
VPN Configuration	PPTP Termination: a PPTP tunnel can be established between the system and the remote user over the Internet. Local VPN: an IPsec tunnel can be established between the system and the client located at the LAN side. Site-to-Site VPN: an IPsec tunnel can be constructed to be used to connect to other IPsec capable device over the Internet.