

## 4.4.1 Network Address Translation

Set the configuration for **DMZ**, **Public Accessible Server** and **Port and Redirect**.

Network Address Translation
<a href="#">DMZ (Demilitarized Zone)</a>
<a href="#">Public Accessible Server</a>
<a href="#">Port and IP Redirect</a>

### Y DMZ

The system supports up to 40 sets of Internal IP address (LAN) to External IP address (WAN) mapping in the Static Assignments. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN1) that will change dynamically if WAN1 Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN1 interface. Each **Static Assignment** could be bound with the chosen External Interface, WAN1 or WAN2. There are 40 sets of static **Internal IP Address** and **External IP Address** available. Enter **Internal** and **External** IP Addresses as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the **Apply** button.

Automatic WAN IP Assignment			
Enable	External IP Address	External Interface	Internal IP Address
<input type="checkbox"/>	10.2.3.100	WAN1	<input type="text"/>

Static Assignments			
Item	External IP Address	External Interface	Internal IP Address
1	<input type="text"/>	WAN1 ▼	<input type="text"/>
2	<input type="text"/>	WAN1 ▼	<input type="text"/>
3	<input type="text"/>	WAN1 ▼	<input type="text"/>
4	<input type="text"/>	WAN1 ▼	<input type="text"/>
5	<input type="text"/>	WAN1 ▼	<input type="text"/>
6	<input type="text"/>	WAN1 ▼	<input type="text"/>
7	<input type="text"/>	WAN1 ▼	<input type="text"/>
8	<input type="text"/>	WAN1 ▼	<input type="text"/>
9	<input type="text"/>	WAN1 ▼	<input type="text"/>
10	<input type="text"/>	WAN1 ▼	<input type="text"/>

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

**Public Accessible Server**

This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the “**External Service Port**”, “**Local Server IP Address**” and “**Local Server Port**”. Select “**TCP**” or “**UDP**” for the service’s type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the **Apply** button.

Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

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

**Port and IP Redirect**

This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the “**IP Address**” and “**Port**” of **Destination**, and the “**IP Address**” and “**Port**” of **Translated to Destination**. Select “**TCP**” or “**UDP**” for the service’s type. These settings will become effective immediately after clicking **Apply**.

Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

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

## 4.4.2 Privilege List

Set the configuration for **Privilege IP Address List** and **Privilege MAC Address List**.

Privilege List
<a href="#">Privilege IP Address List</a>
<a href="#">Privilege MAC Address List</a>

### Y Privilege IP Address List

If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in the “**Privilege IP Address List**”. The “**Remark**” field is not necessary but is useful to keep track. WHG301 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

Privilege IP Address List		
Item	Privilege IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total: 100) [First](#) [Prev](#) [Next](#) [Last](#)



*Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.*

### Y Privilege MAC Address List

In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in the “**Privilege MAC Address List**”. WHG301 allows 100 privilege MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking **Apply**.

Privilege MAC Address List		
Item	MAC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total: 100) [First](#) [Prev](#) [Next](#) [Last](#)



*Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems*

### 4.4.3 Monitor IP List

WHG301 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the necessary information, click **Apply** to save the settings. Click **Monitor** to check the current status of all the monitored IP. The system supports monitoring on 40 IP addresses listed in the “**Monitor IP List**”.

Monitor IP List							
Item	Protocol	IP Address	Link	Item	Protocol	IP Address	Link
1	http	<input type="text"/>	<input type="button" value="Add"/>	2	http	<input type="text"/>	<input type="button" value="Add"/>
3	http	<input type="text"/>	<input type="button" value="Add"/>	4	http	<input type="text"/>	<input type="button" value="Add"/>
5	http	<input type="text"/>	<input type="button" value="Add"/>	6	http	<input type="text"/>	<input type="button" value="Add"/>
7	http	<input type="text"/>	<input type="button" value="Add"/>	8	http	<input type="text"/>	<input type="button" value="Add"/>
9	http	<input type="text"/>	<input type="button" value="Add"/>	10	http	<input type="text"/>	<input type="button" value="Add"/>
11	http	<input type="text"/>	<input type="button" value="Add"/>	12	http	<input type="text"/>	<input type="button" value="Add"/>
13	http	<input type="text"/>	<input type="button" value="Add"/>	14	http	<input type="text"/>	<input type="button" value="Add"/>
15	http	<input type="text"/>	<input type="button" value="Add"/>	16	http	<input type="text"/>	<input type="button" value="Add"/>
17	http	<input type="text"/>	<input type="button" value="Add"/>	18	http	<input type="text"/>	<input type="button" value="Add"/>
19	http	<input type="text"/>	<input type="button" value="Add"/>	20	http	<input type="text"/>	<input type="button" value="Add"/>

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

On each monitored item with a WEB server running, administrators may add a link for the easy access by selecting a protocol, http or https, and click the **Add** button. After clicking **Add** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the **Del** button to remove the setting.

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	<span style="color: red;">●</span>
2	192.168.1.100	<span style="color: red;">●</span>

#### 4.4.4 Walled Garden List

This function provides certain free services for users to access the websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and click **Apply** to save the settings.

Walled Garden List			
Item	Address	Item	Address
1	<input type="text" value="www.paypal.com"/>	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"/>

## 4.4.5 Proxy Server Properties

WHG301 supports Internal Proxy Server and External Proxy Server functions.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

- Y **External Proxy Server:** Under the security management of WHG301, the system will match the External Proxy Server list to the clients' proxy settings. If there is not a match, the clients will not be able to reach the login page and thus unable to access the network. If there is a match, the clients will be directed to the system for authentication. After a successful authentication, the clients will be redirected back to the desired proxy servers depending on different situations.
- Y **Internal Proxy Server:** WHG301 has a built-in proxy server. If this function is enabled, the clients will be forced to treat WHG301 as the proxy server regardless of their original proxy settings.

For more details about how to set up the proxy servers, please refer to **Appendix D. Proxy Setting**.



## 4.4.6 Dynamic DNS

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. WHG301 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access WHG301's WAN. If the dynamic DHCP is activated at the WAN port, it will update the IP address of the DNS server periodically. These settings will become effective immediately after clicking **Apply**.

Dynamic DNS	
DDNS	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Provider	DynDNS.org(Dynamic) ▼
Host name	<input type="text"/>
Username/E-mail	<input type="text"/>
Password/Key	<input type="text"/>

- Ÿ **DDNS:** Enable or disable this function.
- Ÿ **Provider:** Select the DNS provider.
- Ÿ **Host name:** The IP address/domain name of the WAN port.
- Ÿ **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- Ÿ **Password/Key:** The register password for the DNS provider.

---

**8 Note:** To apply for free Dynamic DNS service, you may go to <http://www.dyndns.com/services/dns/dyndns/howto.html>.

---

## 4.4.7 IP Mobility

WHG301 supports IP PNP function.

IP Mobility	
IP PNP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

At the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is, authentication can still be performed through WHG301.

## 4.4.8 VPN Configuration

*Virtual Private Network*, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

VPN Configuration
<a href="#">Local VPN</a>
<a href="#">Remote VPN</a>
<a href="#">Site-to-Site VPN</a>

**Local VPN:** Local VPN allows to create the VPN tunnel between a user's device and WHG301, to encrypt the data transmission. In addition, only when this function is enabled (**Active**) here do users of the entire system are able to use Local VPN. Local VPN users can also be isolated from each other when **VPN Client Isolation** is enabled.

Local VPN For The Entire System	
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

IPSec Parameters	
Encryption	<input type="radio"/> DES <input checked="" type="radio"/> 3-DES
Integrity	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA-1
Diffie-Hellman	<input checked="" type="radio"/> Group 1 <input type="radio"/> Group 2

For more information about Local VPN, please see **Appendix H. Local VPN**.

**Remote VPN:** When the setting is enabled, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP. The system's VPN supports end-users' device under Windows 2000, Windows XP SP1, SP2 and Windows Vista. Start IP field must be entered when enabled. The supported Authentication Servers, Group Permission, Client Policy, and the Remote VPN login page also can be configured here. The system supports up to 10 PPTP connections.

Remote VPN for the Entire System					
Remote VPN Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
IP Address Range Assignment	Start IP Address: <input type="text" value="192.168.6.1"/> <small>*(Support up to 10 connections.)</small>				
SIP Configuration	Enable <input type="checkbox"/> WAN Interface WAN1				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	<a href="#">Server 1</a>	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">Server 2</a>	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">Server 3</a>	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">Server 4</a>	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Group Permission Configuration	<input type="button" value="Configure"/>				
Applied Policy to Remote Client	<input type="text" value="Policy 1"/> <input type="button" value="v"/>				
Remote VPN Login Page	<input type="button" value="Configure"/>				

**Site-to-site VPN:** When the setting is enabled, the system enables the IPSec VPN tunnel between two remote networks/sites to encrypt the data transmission. Click **Add A Remote Site** button to set configuration about remote VPN capable devices such as VPN gateway. Click **Add A Local Site** button to set configuration about local site.

Remote Site Configuration				
Name	IP Address	Pre-shared Key	Edit	Delete
<input type="button" value="Add A Remote Site"/>				

Local Site Configuration					
Local Subnet	Local Interface	Remote VPN Gateway	Remote Subnet	Edit	Delete
<input type="button" value="Add A Local Site"/>					

## 4.5 Utilities

This section provides four utilities to customize and maintain the system including **Change Password**, **Backup/Restore Settings**, **Firmware Upgrade**, **Restart** and **Network Utilities**.

The screenshot displays the web management interface for the 4ipnet Wireless Hotspot Gateway WHG301. The top navigation bar includes the 4ipnet logo, the device name, and links for Logout and Help. Below this is a menu with System Configuration, User Authentication, AP Management, Network Configuration, Utilities (highlighted), and Status. The main content area shows the Utilities section with a sidebar of utility buttons and a table of descriptions.

Utilities	
Change Password	Change the administration password.
Backup/Restore Settings	Backup and restore system settings. Administrator may also reset system settings to factory default.
Firmware Upgrade	Update 4ipnet WHG301 firmware.
Restart	Restart the system.
Network Utilities	Some network utilities such as Wake-on-LAN, web-based Ping, and ARP table are supported by the system.

## 4.5.1 Change Password

There are three levels of authorities: **admin**, **manager** or **operator**. The default usernames and passwords are 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 permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

**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 administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click **Apply** to activate this new password.

Change Admin Password	
Old Password	<input type="password"/>
New Password	<input type="password"/>
Verify Password	<input type="password"/>

Change Manager Password	
New Password	<input type="password"/>
Verify Password	<input type="password"/>

Change Operator Password	
New Password	<input type="password"/>
Verify Password	<input type="password"/>

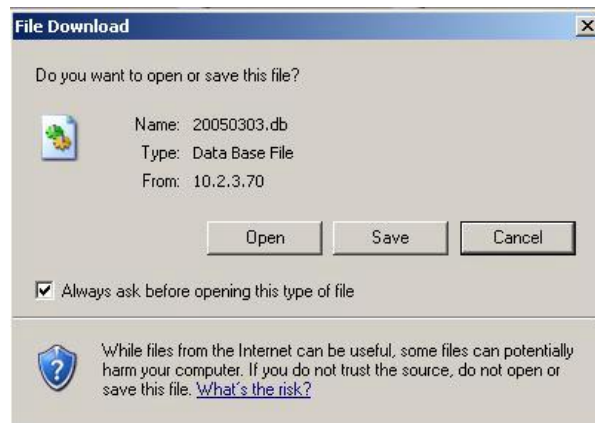


*If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface at the serial console port.*

## 4.5.2 Backup/Restore Settings

This function is used to backup/restore the 4ipnet WHG301 settings. Also, WHG301 can be restored to the factory default settings here.

- Y **Backup current system settings:** Click **Backup** to create a .db database backup file and save it on disk.



- Y **Restore system settings:** Click **Browse** to search for a .db database backup file created by WHG301 and click **Restore** to restore to the same settings at the time when the backup file was saved.
- Y **Reset to the factory-default settings:** Click **Reset** to load the factory default settings of WHG301.

### 4.5.3 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click **Browse** to search for the firmware file and click **Apply** for the firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to activate the new firmware.

Firmware Upgrade	
Current Version	1.00.00-EN-N
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Note: For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.



1. Firmware upgrade may cause the loss of some data. Please refer to the release notes for the limitation before upgrading.
2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.

## 4.5.4 Restart

This function allows the administrator to safely restart 4ipnet WHG301, and the process might take approximately three minutes. Click **YES** to restart WHG301; click **NO** to go back to the previous screen. If the power needs to be turned off, it is highly recommended to restart WHG301 first and then turn off the power after completing the restart process.

Do you want to **RESTART** the system?

**YES**      **NO**



*The connection of all online users of the system will be disconnected when system is in the process of restarting.*



## 4.5.5 Network Utilities

This function allows the administrators to manage functions including **Wake-on-LAN**, **Ping**, **Trace Route**, and showing **ARP Table** by entering IP or Domain Name.

Network Utilities	
Wake On Lan	<input type="text" value=""/> <small>(XX:XX:XX:XX:XX:XX)</small> <input type="button" value="Wake Up"/>
Ping	<input type="text" value="www.yahoo.com"/> <small>(IP/Domain Name)</small> <input type="button" value="Ping"/>
Trace Route	<input type="text" value=""/> <small>(IP/Domain Name)</small> <input type="button" value="Start"/> <input type="button" value="Stop"/>
ARP Table	<input type="button" value="Show"/>
Status	Done
Result	<pre> PING www.yahoo-ht3.akadns.net (209.131.36.158) 56(84) bytes of 64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s 64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s 64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s 64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s  --- www.yahoo-ht3.akadns.net ping statistics --- 4 packets transmitted, 4 received, 0% packet loss, time 3091ms rtt min/avg/max/mdev = 154.933/237.035/320.277/81.918 ms </pre>

- Ø **Wake on LAN:** It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled and is on the LAN side. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
- Ø **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.
- Ø **Trace Route:** It allows administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.
- Ø **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

## 4.6 Status

This section includes **System Status**, **Interface Status**, **Routing Table**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.

**4ipnet** Wireless Hotspot Gateway WHG301

System Configuration User Authentication AP Management Network Configuration Utilities Status

**Status**

Status	
System Status	Display current system settings.
Interface Status	Display the current settings of all network interfaces such as VLAN and service zone.
Routing Table	List all Policy Route rules and Global Policy Route rules. The System Route rules are shown here as well. The Policy Route rule has higher priority than the Global Policy route rule. The System Route rule has the lowest priority.
Current Users	Display online user information including Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
Traffic History	Display detail usage information by day. A minimum of 3 days of history can be logged in the system.
Notification Configuration	The system can send various reports via up to 3 email accounts such as Monitor IP report, Users log, and Session Log. The external SYSLOG server and FTP server are configured here.

## 4.6.1 System Status

This section provides an overview of the system for the administrator.

System Status		
Current Firmware Version		1.00.00-EN-N
Build		00400
System Name		Wireless Hotspot Gateway
Home Page		<a href="http://www.4ipnet.com">http://www.4ipnet.com</a>
SYSLOG server - Traffic History		N/A:N/A
SYSLOG server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
History	Retained Days	3 days
	Email To	N/A
		N/A
N/A		
Time	NTP Server	tock.usno.navy.mil
	Date Time	2007/12/27 09:41:43 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

The description of the above-mentioned table is as follows:

<b><u>Item</u></b>		<b><u>Description</u></b>
<b>Current Firmware Version</b>		The present firmware version of WHG301
<b>Build</b>		The current build number.
<b>System Name</b>		The system name. The default is WHG301
<b>Home Page</b>		The page the users are directed to after initial login success.
<b>Syslog server-Traffic History</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Syslog server-On demand User log</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Proxy Server</b>		Enabled/disabled stands for that the system is currently using the proxy server or not.
<b>Warning of Internet Disconnection</b>		Enabled/Disabled stands for the connection at WAN is normal or abnormal ( <b>Internet Connection Detection</b> ) and all online users are allowed/disallowed to log in the network.
<b>WAN Failover</b>		Enabled/Disabled stands for the function currently being used or not.
<b>Load Balancing</b>		Enabled/Disabled stands for the function currently being used or not.
<b>SNMP</b>		Enabled/disabled stands for the current status of the SNMP management function.
<b>History</b>	<b>Retained Days</b>	The maximum number of days for the system to retain the users' information.
	<b>Email To</b>	The email address to which the traffic history or user's traffic history information will be sent.
<b>Time</b>	<b>NTP Server</b>	The network time server that the system is set to align.
	<b>Date Time</b>	The system time is shown as the local time.
<b>User</b>	<b>Idle Timer</b>	The minutes allowed for the users to be inactive before their account expires automatically.
	<b>Multiple Login</b>	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
<b>DNS</b>	<b>Preferred DNS Server</b>	IP address of the preferred DNS Server.
	<b>Alternate DNS Server</b>	IP address of the alternate DNS Server.

## 4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **SZ Default-8**.

Interface Status		
WAN1	MAC Address	
	IP Address	
	Subnet Mask	255.255.255.0
WAN2	Disabled	
	WAN1	WAN2
Packets In	28583 (Δ 28153)	0 (Δ 0)
Packets Out	12887 (Δ 12862)	0 (Δ 0)
Bytes In	2957963 (Δ 2916864)	0 (Δ 0)
Bytes Out	9170109 (Δ 9167181)	0 (Δ 0)
Service Zone - Default	Mode	NAT
	MAC Address	
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	Disabled	

The description of the above-mentioned table is as follows:

<b><i>Item</i></b>		<b><i>Description</i></b>
<b>WAN1</b>	<b>MAC Address</b>	The MAC address of the WAN1 port.
	<b>IP Address</b>	The IP address of the WAN1 port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN1 port.
<b>WAN2</b>	<b>MAC Address</b>	The MAC address of the WAN2 port.
	<b>IP Address</b>	The IP address of the WAN2 port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN2 port.
<b>Packets In</b>		The total accumulated packets in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
<b>Packets Out</b>		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
<b>Bytes In</b>		The total accumulated bytes in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
<b>Bytes Out</b>		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
<b>Service Zone - Default DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server in Default Service Zone
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.
<b>Service Zone – Default</b>	<b>Mode</b>	The operation mode of the default SZ.
	<b>MAC Address</b>	The MAC address of the default SZ.
	<b>IP Address</b>	The IP address of the default SZ.
	<b>Subnet Mask</b>	The Subnet Mask of the default SZ.

### 4.6.3 Routing Table

All the **Policy** Route rules and **Global Policy** Route rules will be listed here. Also it will show the **System** Route rules specified by each interface.

Policy 1			
Destination	Subnet Mask	Gateway	Interface
Policy 2			
Destination	Subnet Mask	Gateway	Interface
Policy 3			
Destination	Subnet Mask	Gateway	Interface
Policy 4			
Destination	Subnet Mask	Gateway	Interface
Policy 5			
Destination	Subnet Mask	Gateway	Interface
Policy 6			
Destination	Subnet Mask	Gateway	Interface
Policy 7			
Destination	Subnet Mask	Gateway	Interface
Policy 8			
Destination	Subnet Mask	Gateway	Interface
Policy 9			
Destination	Subnet Mask	Gateway	Interface
Policy 10			
Destination	Subnet Mask	Gateway	Interface
Policy 11			
Destination	Subnet Mask	Gateway	Interface
Policy 12			
Destination	Subnet Mask	Gateway	Interface
Global Policy			
Destination	Subnet Mask	Gateway	Interface
System			
Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Default
10.2.3.0	255.255.255.0	0.0.0.0	WAN1
0.0.0.0	0.0.0.0	10.2.3.254	WAN1

Y **Policy 1~12:** Shows the information of the individual Policy from 1 to 12.

Y **Global Policy:** Shows the information of the Global Policy.

Y **System:** Shows the information of the system administration.

Ø **Destination:** The destination IP address of the device.

Ø **Subnet Mask:** The Subnet Mask IP address of the port.

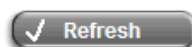
Ø **Gateway:** The Gateway IP address of the port.

Ø **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

## 4.6.4 Current Users

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Location** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of "**Logout**" and check the user access AP status by clicking the hyperlink of the AP name for "**Location**." Click **Refresh** is to update the current users list.

Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out





## 4.6.5 Traffic History

This function is used to check the traffic history of 4ipnet WHG301. The history of each day will be saved separately in the DRAM for at least 3 days (72 full hours). The system also keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months.

Traffic History		
Date	Size (Byte)	
<a href="#">2007-12-21</a>	65	
<a href="#">2007-12-22</a>	65	
<a href="#">2007-12-23</a>	65	
<a href="#">2007-12-24</a>	65	
On-demand User Log		
Date	Size (Byte)	
<a href="#">2007-12-21</a>	105	
<a href="#">2007-12-22</a>	105	
<a href="#">2007-12-23</a>	105	
<a href="#">2007-12-24</a>	105	
Roaming Out Traffic History		
Date	Size (Byte)	
<a href="#">2007-12-21</a>	106	
<a href="#">2007-12-22</a>	106	
<a href="#">2007-12-23</a>	106	
<a href="#">2007-12-24</a>	106	
Roaming In Traffic History		
Date	Size (Byte)	
<a href="#">2007-12-21</a>	112	
<a href="#">2007-12-22</a>	112	
<a href="#">2007-12-23</a>	112	
<a href="#">2007-12-24</a>	112	
SIP Call Usage Log		
Date	Call Count	
<a href="#">2007-12-21</a>	0	
<a href="#">2007-12-22</a>	0	
<a href="#">2007-12-23</a>	0	
<a href="#">2007-12-24</a>	0	
Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
<a href="#">2007-12</a>	0	<a href="#">Download</a>



Since the history is saved in the DRAM, if you need to restart the system, and at the same time, keep the history, please manually copy and save the traffic history information before restarting.



**Y SIP Call Usage Log**

The log provides the login and logout activities of SIP clients (device and soft clients) such as Start Time, Caller, Callee and Duration (seconds)

SIP Call Usage Log			
Start Time	Caller	Callee	Duration (seconds)

**Y Monthly Network Usage of Local User**

The system keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months. As shown in the following figure, each line in a monthly network usage of local user record consists of 6 fields, **System Name, Connection Time Usage, Packets In, Bytes In, Packets Out** and **Bytes Out** of user activities.

Monthly Report 2007-11					
Username	Connection Time Usage	Packets In	Bytes In	Packets Out	Bytes Out
user1	8 mins 42 secs	195	86.9K	202	23K
user2	1 min 43 secs	27K	23.1M	21.3K	12.1M

(Total: 2)

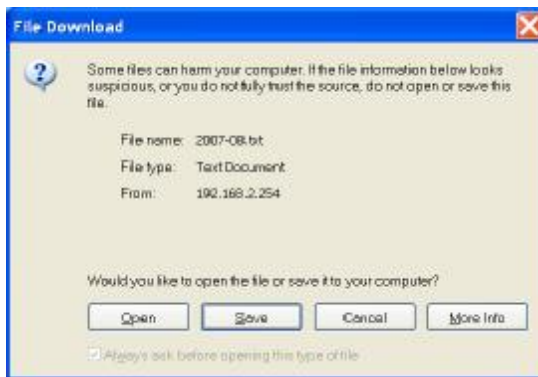
[First](#) [Previous](#) [Next](#) [Last](#)

- o **Username:** Username of the local user account.
- o **Connection Time Usage:** The total time used by the user.
- o **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
- o **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

**Ø Download Monthly Network Usage of Local User:** Click on the **Download** button for outputting the report manually to a local database.

Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
<a href="#">2007-12</a>	0	<a href="#">Download</a>

A warning message will then appear. Click **Save** to download the record into .txt format.



## 4.6.6 Notify Configuration

WHG301 can automatically send the notification of **Monitor IP Report**, **Traffic History**, **On-demand User Log**, **Session Log** and **AP status** to up to 3 particular e-mail address. The notification of AP Status is triggered by the event when a managed AP becomes unreachable while the other types of emails are sent periodically in given intervals such as 1 hour. A trial email is provided by the system for validation. In addition, the system supports recording Syslog of Traffic History, On-demand User Log and Session Log via external Syslog servers. In addition, the Session Log can be sent to a specified FTP server. Enter the related information and select the desired items and then apply the settings.

E-mail Notification Configuration					
Send To	Monitor IP Report	Traffic History	On-demand User Log	Session Log	AP Status
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interval	1 Hour <input type="button" value="v"/>	1 Hour <input type="button" value="v"/>	1 Hour <input type="button" value="v"/>	1 Hour <input type="button" value="v"/>	N/A
Send Test Email	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>
Send From	<input type="text"/>				
SMTP	<input type="text"/>				
Auth Method	None <input type="button" value="v"/>				

SYSLOG Configuration		
System Log	IP: <input type="text"/>	Port: <input type="text"/>
On-demand User Log	IP: <input type="text"/>	Port: <input type="text"/>
Session Log	IP: <input type="text"/>	Port: <input type="text"/>

FTP Server Settings	
Session Log	IP: <input type="text"/> Port: <input type="text"/> Send Log every Hours <small>*(Note: same as "Interval of Session Log" in the Notification E-mail Settings)</small> Using Anonymous <input checked="" type="radio"/> Yes <input type="radio"/> No FTP Setting Test <input type="button" value="Send Test Log"/>

### Y E-mail Notification Configuration:

- Ø **Send To:** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Traffic History, On-demand User Log and AP Status, and check which type of notification to be sent.
- Ø **Interval:** The time interval to send the e-mail report.
- Ø **Send Test Email:** To test the settings immediately.
- Ø **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the

sender's e-mail.

Ø **SMTP:** The IP address of the sender's SMTP server.

Ø **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or "**None**" to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.

- **NTLMv1** is not currently available for general use.
- **Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.
- Pegasus uses **CRAM-MD5** or **Login** but which method to be used can not be configured.

ÿ **Syslog Configuration:** There are 3 types of Syslog supported: System Log, On-demand User Log, and Session Log. Enter the IP address and Port number to specify which and from where the report should be sent to.

---

**8 Note:**

When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this Syslog server.

---

#### ÿ **FTP Server Settings**

**Session Log:** Log each connection created by users and tracking the source IP and destination IP. If Syslog is enabled, Session Log will be sent to the Syslog server automatically during every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file will be sent to the FTP server once the file size reaches its maximum size or periodical time interval.

## 4.7 Help

On the screen, the **Help** button is on the upper right corner.

Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.

### Online Help

[Overview](#)

[System Configuration](#)

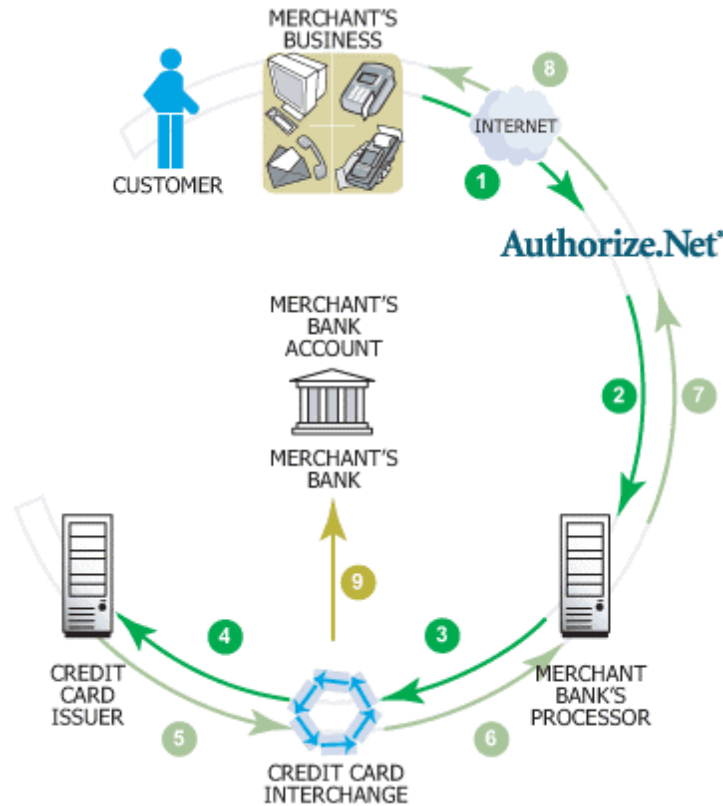
- [Configuration Wizard](#)
- [System Information](#)
- [WAN1 Configuration](#)
- [WAN2 Configuration](#)
- [WAN Traffic Settings](#)
- [LAN Port Mapping](#)
- [Service Zones](#)

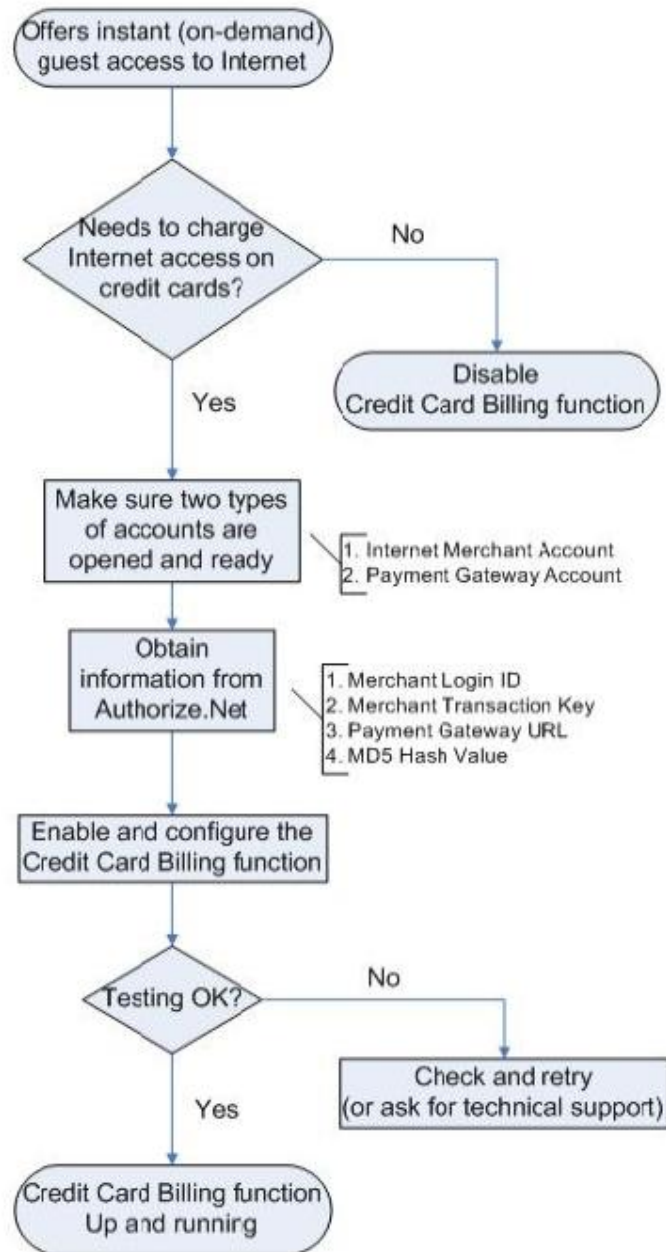
[User Authentication](#)

- [Authentication Configuration](#)
  - [Authentication Server Configuration](#)
    - [Auth Method - Local](#)
    - [Auth Method - POP3](#)
    - [Auth Method - RADIUS](#)
    - [Auth Method - LDAP](#)
    - [Auth Method - NT Domain](#)
    - [Auth Method - ONDEMAND](#)
    - [Auth Method - SIP](#)

## Appendix A. Accepting Payment via Authorize.Net

This section is to show independent Hotspot owners how to configure related settings in order to accept credit card payments via Authorize.Net, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their credit cards.





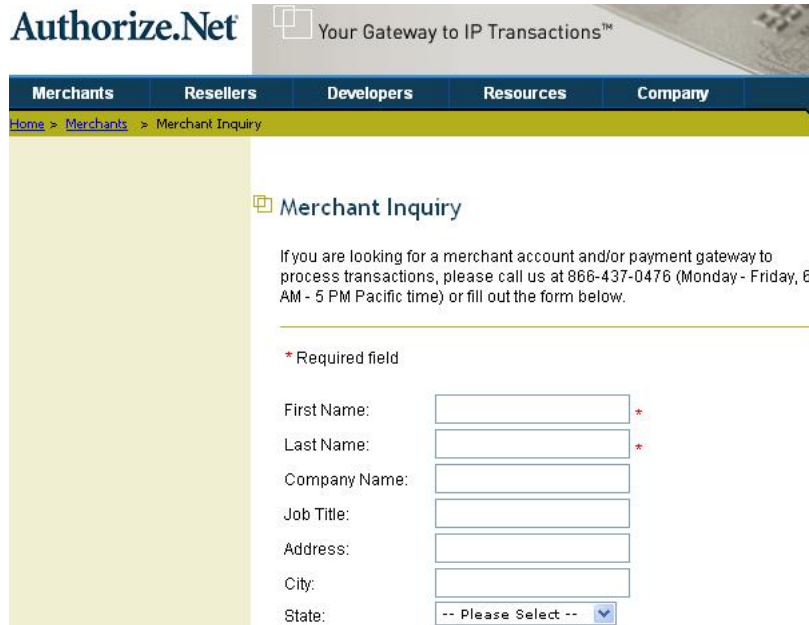


# 1. Setting Up

## 1.1 Open Accounts

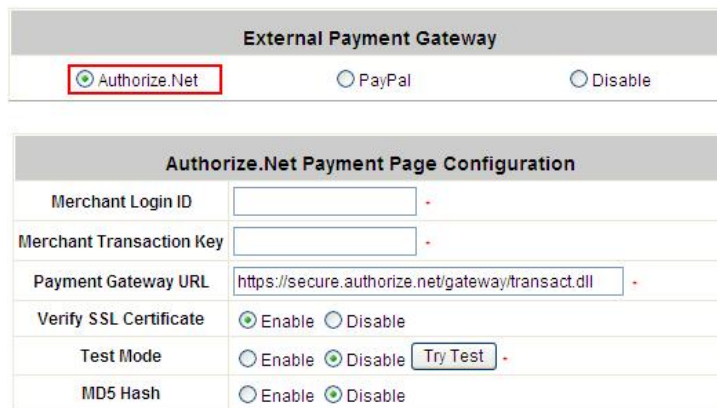
To set up 4ipnet WHG301 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on <http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/>.



## 1.2 Configure 4ipnet WHG301 using an Authorize.Net account

Please log in 4ipnet WHG301. **User Authentication >> Authentication Configuration >> Click the server name *On-demand User* >> External Payment Gateway >> Click *Configure* >> External Payment Gateway >> Select *Authorize.Net***



Some major fields are required:

Setting	Description
<b>Merchant Login ID</b>	This is the "Login ID" that comes with the Authorize.Net account.
<b>Merchant Transaction Key</b>	To get a new key, please log in Authorize.Net >> Click <b>Settings and Profile</b> >> Go to the " <b>Security</b> " section >> Click <b>Obtain Transaction Key</b> >> Enter " <b>Secret Answer</b> " >> Click <b>Submit</b> .
<b>Payment Gateway URL</b>	<a href="https://secure.authorize.net/gateway/transact.dll">https://secure.authorize.net/gateway/transact.dll</a> (default gateway address)
<b>MD5 Hash</b>	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: " <b>MD5 Hash Value</b> ".

**8 Note:** For detailed description, please see **4.2.1.6 Authentication Method – On-demand User**.

### 1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of 4ipnet WHG301

Settings of the merchant account on Authorize.Net should be matched with the configuration of 4ipnet WHG301:

Setting	Description
<b>MD5 Hash</b>	To configure " <b>MD5 Hash Value</b> ", please log in Authorize.Net >> Click <b>Settings and Profile</b> >> Go to the " <b>Security</b> " section >> Click <b>MD5 Hash</b> >> Enter " <b>New Hash Value</b> " & " <b>Confirm Hash Value</b> " >> Click <b>Submit</b> .
<b>Required Card Code</b>	If the " <b>Card Code</b> " is set up as a required field, please log in Authorize.Net >> Click <b>Settings and Profile</b> >> Go to the " <b>Security</b> " section >> Click <b>Card Code Verification</b> >> Check the <b>Does NOT Match (N)</b> box >> Click <b>Submit</b> .
<b>Required Address Fields</b>	After setting up the required address fields on the " <b>Credit Card Payment Page Billing Configuration</b> " section of 4ipnet WHG301, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net >> Click <b>Settings and Profile</b> >> Go to the " <b>Security</b> " section >> Click <b>Address Verification System (AVS)</b> >> Check the boxes accordingly >> Click <b>Submit</b> .

### 1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between 4ipnet WHG301 and Authorize.Net, please log in 4ipnet WHG301. **User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **External Payment Gateway** >> Click **Configure** >> **External Payment Gateway** >> Select **Authorize.Net** >> Go to "**Authorize.Net Payment Page Configuration**" section >> **Enable** the "**Test Mode**" >> Click **Try Test** and follow the instructions

**External Payment Gateway**

Authorize.Net     
  PayPal     
  Disable

**Authorize.Net Payment Page Configuration**

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

## 2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as 4ipnet WHG301.

### 2.1 Void A Transaction and Remove the On-demand Account Generated on 4ipnet WHG301

Sometimes, a transaction (as well as the related user account on 4ipnet WHG301) may have to be canceled before it has been settled with the bank.

- a. To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions** >> Locate the specific transaction record on the “**List of Unsettled Transactions**” >> Click the **Trans ID** number >> Confirm and click **Void**.

---

**8 Note:** To find the on-demand account name, click **Show Itemized Order Information** on the “**Order Information**” page >> Username can be found in the “**Item Description**”.

---

- b. To remove the specific account from 4ipnet WHG301, please log in 4ipnet WHG301. **User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **On-demand Account List** >> Click **View** >> **On-demand Account List** >> Click **Delete** on the record with the account name. Click **Delete All** to delete all users at once.

On-demand Account List					
Username	Password	Remaining Quota	Status	Remark	<input type="button" value="Delete All"/>
<a href="#">3r23</a>	qxr86b47	2 hr(s)	Normal		<a href="#">Delete</a>

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

### 2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on 4ipnet WHG301

- a. To refund a credit card payment, please log in Authorize.Net. Click **Virtual Terminal** >> Select a Payment Method >> Click **Refund a Credit Card** >> **Payment/Authorization Information** >> Type information in at least three fields: **Card Number**, **Expiration Date**, and **Amount** >> Confirm and click **Submit**.
- b. To remove the specific account from 4ipnet WHG301, please log in 4ipnet WHG301. **User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **On-demand Account List** >> Click **View** >> **On-demand Account List** >> Click **Delete** on the record with the account name.

### 2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions** >> Try to locate the specific transaction record on the “**List of Unsettled Transactions**” >> Click the **Trans ID** number >> Click **Show Itemized Order Information** in the “**Order Information**” section >> Username and Password can be found in the “**Item Description**”.

### 2.4 Send An Email Receipt to A Customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via Authorize.Net. To change the information on the receipt for customer, please

log in 4ipnet WHG301. **User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> External Payment Gateway >>** Click **Configure >> External Payment Gateway >>** Select **Authorize.NET >>** Scroll down to **Client's Purchasing Record** section of the page >> Type in information in the text boxes: **"Description"** and **"E-mail Header"** >> Confirm and click **Apply**.

Client's Purchasing Record	
Starting Invoice Number	HotspotYK 00000004 * <input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

### 2.5 Send an Email Receipt for Each Transaction to the Merchant Owner

A copy of email receipt with payment details for each successful transaction will also be automatically sent to the merchant owner/administrator via Authorize.Net.

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile >>** Go to the **"General"** section >> Click **Manage Contacts >>** Click **Add New Contact** to >> Enter necessary contact information on this page >> Check the **"Transaction Receipt"** box >> Click **Submit**.

## 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

### 3.1 Transaction Statistics by Credit Card Type during the Period.

Please log in Authorize.Net. >> Click **Reports >>** Check **"Statistics by Settlement Date"** radio button >> Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria >> Click **Run Report**.

### 3.2 Transaction Statistics by Different Location

- To deploy more than one 4ipnet WHG301, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in 4ipnet WHG301. **User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> External Payment Gateway >>** Click **Configure >> External Payment Gateway >>** Select **Authorize.NET >>** Scroll down to **"Client's Purchasing Record"** section of the page >> Check the **"Reset"** box >> A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number"** >> Confirm and click **Apply**.

Client's Purchasing Record	
Starting Invoice Number	HotspotYK 00000004 * <input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

- b. Please log in Authorize.Net >> Click **Search and Download** >> Specify the transaction period (or ALL Settled, Unsettled) in “**Settlement Date**” section >> Go to “**Transaction**” section >> Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A\*) in the “**Invoice #**” text box >> Click **Search** >> If transaction records can be found, the number of accounts sold is the number of search results >> Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

### 3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click **Search and Download** >> Enter the information for a specific customer as criteria >> Click **Search** >> Click the **Trans ID** number to view the transaction details.

---

**8 Note:** For more information about **Authorize.Net**, please see <http://www.authorize.net>.

---

## 4. Examples of Making Payment for End Users

**Step 1:** Click the link below the login window to pay for the service by credit card via Authorize.Net.

**Step 2:** Choose **I agree** to accept the terms of use and click **Next**.

**Step 3:** Please fill out the form and Click **Submit** to send out this transaction. There will be a confirm dialog box.

Rate Plan	Price
<input type="radio"/> 2 hrs 0 mins	\$ 5
<input checked="" type="radio"/> 6 hrs 0 mins	\$ 8
<input type="radio"/> 12 hrs 0 mins	\$ 12
<input type="radio"/> 600 Mbyte	\$ 5
<input type="radio"/> 1000 Mbyte	\$ 8
<input type="radio"/> 2000 Mbyte	\$ 12

Credit Card & Contact Information	
Credit Card Number	45631234567890
Credit Card Expiration Date	1208 (MMYY)
Card Type	Visa
Card Code	527
E-mail	1223@yahoo.com
First Name	Tom
Last Name	Lee
Company	
Address	
City	
State	
Zip	
Country	
Phone	
Fax	

Fields denoted by an asterisk(\*) are required.

Submit Clear Back

**Step 4:** Please confirm the data and the click **OK** to go on the transaction or click **Cancel** to revise the data or cancel this transaction. After clicking OK, there will be another dialog box showing up to confirm this transaction again.

Microsoft Internet Explorer

?

Please check the data you input:

Credit Card Number: 4567123456780000  
 Credit Card Expiration Date: 1208  
 Card Type: Visa  
 Card Code: 527  
 E-mail: 1223@yahoo.com  
 Room Number:  
 First Name: Tom  
 Last Name: Lee  
 Company:  
 Address:  
 City:  
 State:  
 Zip:  
 Country:  
 Phone:  
 Fax:

Do you want to continue the credit card payment process?

OK Cancel

**Step 5:** Click **OK** to complete the process or click **Cancel** to revise the data or cancel this transaction.



**Step 6:** Click **Start Internet Access** to use the Internet access service.




---

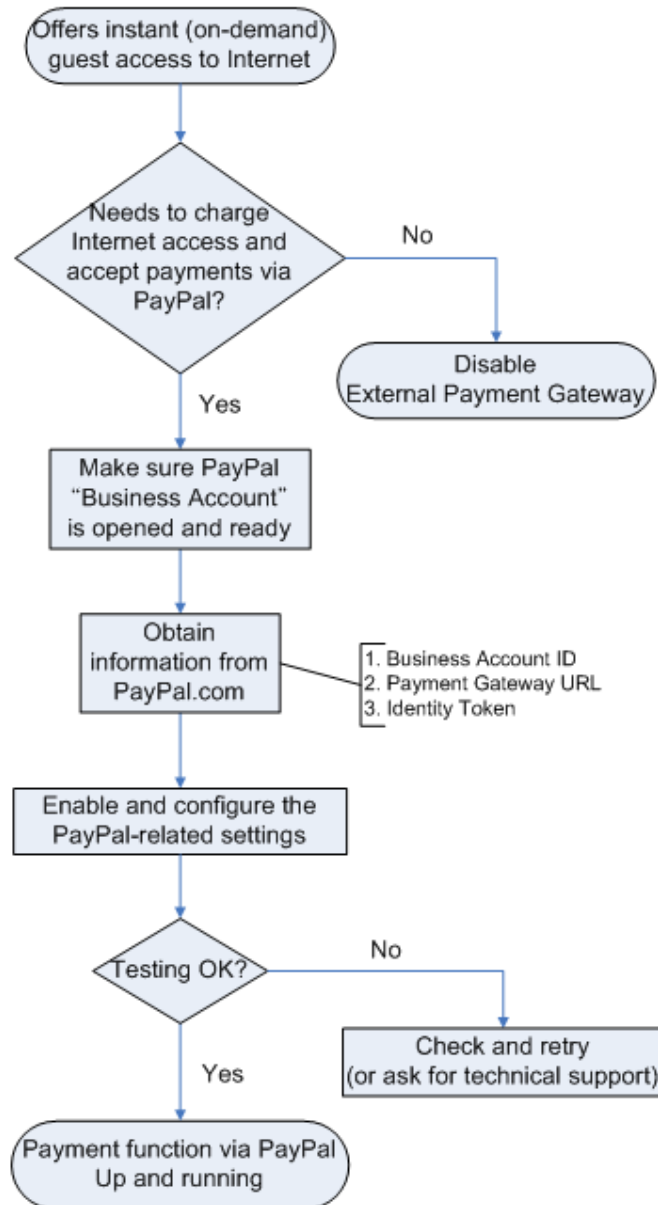
**8 Note:**

The clients 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 clients choose to enter the e-mail addresses, clients will receive confirmation letters for reference.

---

## Appendix B. Accepting Payment via PayPal

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their PayPal accounts or credit cards.





## 1. Setting Up

As follows are the basic steps to open and configure a “**Business Account**” on **PayPal**.

### 1.1 Open An Account

#### Step 1: Sign up for a PayPal Business Account and login.

Here is a link: [https://www.paypal.com/cgi-bin/webscr?cmd=\\_registration-run](https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run)

The screenshot shows the PayPal sign-up process. At the top, there are navigation links: "Choose Account Type" (selected), "Enter Information", "Confirm", and "Done". The main heading is "Sign Up for a PayPal Account". Below this, a message states: "Anyone with an email address can use PayPal to send and receive money online. [What is PayPal?](#)".

There are three account options, each with a radio button:

- Personal Account**: Ideal for shopping online. It's a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a [low fee](#). [Learn more](#)
- Premier Account**: Perfect for buying and selling on eBay or merchant websites. Accept all payment types for [low fees](#). Do business under your own name.
- Business Account** (selected): The right choice for your online business. Accept all payment types for [low fees](#). Do business under a company or group name. [Learn more](#)

A yellow box on the right says: "Already have a PayPal Account? [Upgrade your account](#)".

Below the account options is a "Member Log-In" section with a "Log In" button. It includes links for "Forgot your email address?" and "Forgot your password?". There are input fields for "Email Address" and "Password".

#### Step 2: Edit necessary settings in “Website Payment Preferences”

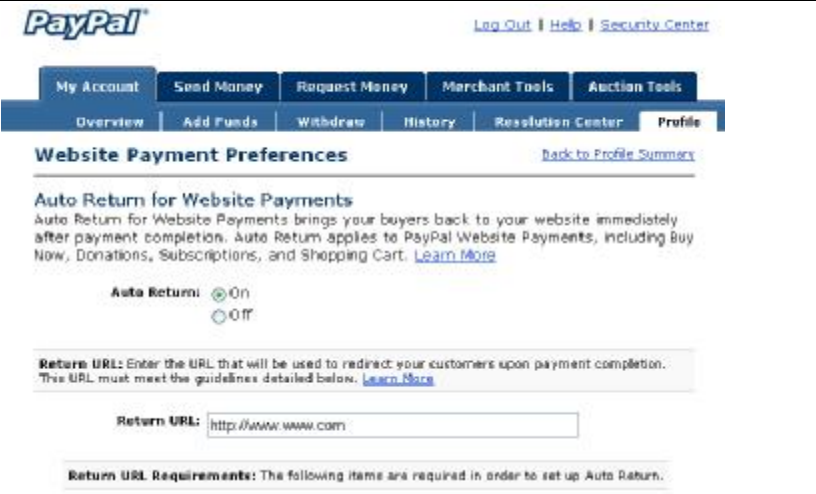
Click **Profile** >> Click **Website Payment Preferences** in the **Selling Preferences** section

The screenshot shows the PayPal Profile Summary page. At the top, there is the PayPal logo and navigation links: "Log Out", "Help", and "Security Center". Below the logo is a navigation bar with tabs: "My Account", "Send Money", "Request Money", "Merchant Tools", and "Auction Tools". Under "My Account", there are sub-tabs: "Overview", "Add Funds", "Withdraw", "History", "Resolution Center", and "Profile" (highlighted with a red box).

The main heading is "Profile Summary". Below this, a message states: "To edit your Profile information, please click on a link below." There are three columns of links:

- Account Information**: [Email](#), [Street Address](#), [Phone](#), [Password](#), [Notifications](#), [Multi-User Access](#), [API Access](#), [Business Information](#), [Close Account](#)
- Financial Information**: [Credit Cards](#), [Bank Accounts](#), [Currency Balances](#), [Gift Certificates](#), [Monthly Account Statements](#), [Preapproved Payments](#)
- Selling Preferences**: [Auctions](#), [Regional Tax](#), [Shipping Calculations](#), [Payment Receiving Preferences](#), [Instant Payment Notification Preferences](#), [Reputation](#), [Customer Service Message](#), [Seller Eligibility for PayPal Buyer Protection](#), [Website Payment Preferences](#) (highlighted with a red box), [Encrypted Payment Settings](#), [Custom Payment Pages](#), [Invoice Templates](#), [Language Encoding](#)

Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click **Save** at the end of the page.

Settings	Screenshots
<p><b>Auto Return (On)</b></p> <p><b>Return URL (Redirect Webpage)</b></p> <p>Type <a href="http://www.www.com">http://www.www.com</a> or other URL.</p>	 <p>The screenshot shows the PayPal 'Website Payment Preferences' page. At the top, there are navigation tabs: 'My Account', 'Send Money', 'Request Money', 'Merchant Tools', and 'Auction Tools'. Below these are sub-tabs: 'Overview', 'Add Funds', 'Withdraw', 'History', 'Resolution Center', and 'Profile'. The main heading is 'Website Payment Preferences' with a link to 'Back to Profile Summary'. The section is titled 'Auto Return for Website Payments' and explains that it brings buyers back to the website. The 'Auto Return' radio button is selected 'On'. Below, there is a text box for 'Return URL' containing 'http://www.www.com'. A note at the bottom states: 'Return URL Requirements: The following items are required in order to set up Auto Return.'</p>
<p><b>Payment Data Transfer (On)</b></p>	<p><b>Payment Data Transfer (optional)</b></p> <p>Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your <a href="#">system configuration</a> and your Return URL. Please note that in order to use Payment Data Transfer, you <b>must</b> turn on Auto Return.</p> <p><b>Payment Data Transfer:</b> <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><b>Block Non-encrypted Website Payment (Off)</b></p>	<p><b>Encrypted Website Payments</b></p> <p>Using encryption enhances the security of website payments by decreasing the possibility that a 3rd party could manipulate the data in your button code. If you plan on only using encrypted buttons you can block payments from non-encrypted ones.</p> <p><a href="#">Learn more about Encrypted Website Payments</a></p> <p><b>Note:</b> If you enable Encrypted Website Payments, all of your Buy Now, Donations, and Subscriptions buttons <b>must</b> be encrypted via one of the following methods:</p> <ul style="list-style-type: none"> <li>• Using the <a href="#">Button Factory</a> with the security settings enabled.</li> <li>• Using your own code, you encrypt all website payments before sending them to PayPal.</li> </ul> <p>By enabling this feature, any Buy Now, Donation, or Subscription button that is not encrypted will be rejected by PayPal.</p> <p><b>Block Non-encrypted Website Payment:</b> <input type="radio"/> On <input checked="" type="radio"/> Off</p>
<p><b>PayPal Account Optional (Off)</b></p>	<p><b>PayPal Account Optional</b></p> <p>When this feature is turned on, your customers will go through an optimized checkout experience. This feature is available for Buy Now, Donations, and Shopping Cart buttons, but not for Subscription buttons. <a href="#">Learn More</a></p> <p><b>PayPal Account Optional:</b> <input type="radio"/> On <input checked="" type="radio"/> Off</p>
<p><b>Contact Telephone Number (Off)</b></p> <p><b>Click Save.</b></p>	<p><b>Contact Telephone Number</b></p> <p>When you activate this option, your customers will be asked to include a Contact Telephone Number with their payment information. <a href="#">Learn More</a></p> <p><b>Note:</b> Selecting <b>On (Required Field)</b> could have a negative effect on buyer conversion.</p> <p><b>Contact Telephone:</b> <input type="radio"/> On (Optional Field) <input type="radio"/> On (Required Field) <input checked="" type="radio"/> Off (PayPal recommends this option)</p> <p style="text-align: right;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </p>

## 1.2 Configure 4ipnet WHG301 with a PayPal Business Account

Please log in 4ipnet WHG301:

**User Authentication >> Authentication Configuration >> Click the server *On-demand User* >> External Payment Gateway >> Click *Configure* >> External Payment Gateway >> Select *PayPal***

Three fields are required:

Setting	Description
<b>Business Account ID</b>	This is the "Login ID" (email address) that is associated with the PayPal Business Account.
<b>Payment Gateway URL</b>	<a href="https://www.paypal.com/cgi-bin/webscr">https://www.paypal.com/cgi-bin/webscr</a> (default URL for PayPal)
<b>Identity Token</b>	<p>Please log in PayPal after saving the above settings &gt;&gt; Click <b>Profile</b> &gt;&gt; Click <b>Website Payment Preferences</b> in the <b>Selling Preferences</b> section &gt;&gt; Scroll down to the section, <b>Payment Data Transfer (optional)</b>.</p> <hr/> <p><b>Payment Data Transfer (optional)</b>                      Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your <a href="#">system configuration</a> and your Return URL. Please note that in order to use Payment Data Transfer, you must turn on Auto Return.</p> <p>Payment Data Transfer: <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>Identity Token: <span style="border: 1px solid red; padding: 2px;">FIY4CqLV-EMdUbg8D_3y7kLG1C8iGdxF-z6f6kCo-K5d0F5QoKZkCBQru</span></p> <hr/> <p>Copy the <b>Identity Token</b> in the above page to the section "<b>PayPal Payment Page Configuration</b>" of 4ipnet WHG301.</p>

### 1.3 Requirements for Building a Secure PayPal-based E-Commerce Site

To deploy the PayPal function properly, it is required that the merchant register an **Internet domain name** (for example, [www.StoreName.com](http://www.StoreName.com)) for this subscriber gateway device.

System Information	
System Name	<input type="text"/>
Administrator Info	Sorry! The service is temporarily unavailable. <small>(It'll appear when Internet connection fails.)</small>
Device Name	<input type="text" value="www.StoreName.com"/> <small>(FQDN for this device)</small>

In addition, it is necessary to sign up for a **SSL certificate**, licensed from a “**Certificate Authority**” (for example, **VeriSign**), for this registered Internet domain name.

Thus, by meeting these two requirements, it will allow end customers or subscribers to pay for the Internet access in a securer and convenient way.

## 2. Basic Maintenance

In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as 4ipnet WHG301.

### 2.1 Refund a completed payment and remove the on-demand account generated on 4ipnet WHG301

(1) To refund a payment, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Click **Refund Payment** at the end of the details page >> Type in information: **Gross Refund Amount** and/or **Optional Note to Buyer** >> Click **Submit** >> Confirm the details and click **Process Refund**

(2) To remove the specific account from 4ipnet WHG301, please log in 4ipnet WHG301:

**User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **On-demand Account List** >> Click **View** >> **On-demand Account List** >> Click **Delete** on the record with the account ID. Click **Delete All** to delete all users at once.

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
<a href="#">V34Q</a>	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	<a href="#">Delete</a>

### 2.2 Find the username and password for a specific customer

(1) To find the username, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Username can be found in the “**Item Title**” field

(2) To find the password associated with a specific username, please log in 4ipnet WHG301:

**User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **On-demand Account List** >> Click **View** >> **On-demand Account List**. Search for the specific username. Password can be found in the same record

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
V34Q	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	Delete

**8 Note:**

As stated by PayPal, you can issue a full or partial refund for any reason and for **60 days** after the original payment was sent. To find the on-demand account name for a specific payment, click **Details** of the payment listing in the activity history log >> **Username** can be found in the **"Item Title"** field.

### 2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in 4ipnet WHG301:

**User Authentication >> Authentication Configuration >> Click the server *On-demand User* >> On-demand User Server Configuration >> External Payment Gateway >> Click *Configure* >> External Payment Gateway >> Select *PayPal* >> Go to "Client's Purchasing Record" section >> Type in information in the text boxes: **Invoice Number** and **Description (Item Name)** >> Confirm and click **Apply****

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

### 2.4 Send an email receipt for each transaction to the merchant

A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

### 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

#### 3.1 Transaction activity during a period

(1) Please log in PayPal >> Click **History** >> Choose activity type from the **Show** field as the search criteria >> Specify the dates (**From** and **To** fields) for the period >> Click **Search**

The screenshot shows the PayPal History page with the following search criteria:

- Show:** All Activity - Simple View
- Within:** The Past Day
- From:** 12 / 31 / 2006 (Month, Day, Year)
- To:** 1 / 30 / 2007 (Month, Day, Year)
- Search** button

Below the search criteria, there is a summary line: **All Activity - Simple View from Dec. 31, 2006 to Jan. 30, 2007**. Below this is a table header with columns: Date, Type, To/From, Name/Email, Status, Details, Action, Egress, Fee, Net Amount.

#### 3.2 Search for the transaction details for a specific customer

Please log in PayPal >> Click **History** >> Click **Advanced Search** >> Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or First Name in the **In** field >> Specify the time period >> Click **Submit** >> Click **Details** to view the transaction details


The screenshot shows the PayPal History page with the following advanced search criteria:

- Search For:** HotSpot00000001
- In:** Invoice ID
- Within:** The Past Day
- From:** 12 / 31 / 2006 (Month, Day, Year)
- To:** 1 / 30 / 2007 (Month, Day, Year)
- Submit** button

**Note:** For more information about **PayPal**, please see <http://www.paypal.com>.

## 4. Examples of Making Payment for End Users

**Step 1:** Click the link below the login window to pay for the service via PayPal.



Welcome To User Login Page!  
Please Enter Your User Name and Password To Sign In.

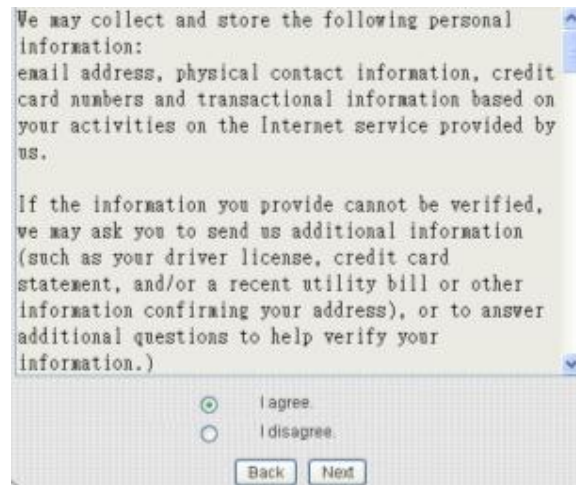
User Name:

Password:

Submit Clear Remaining

Click here to purchase by PayPal or Credit Card Online.

**Step 2:** Choose *I agree* to accept the terms of use and click **Next**.



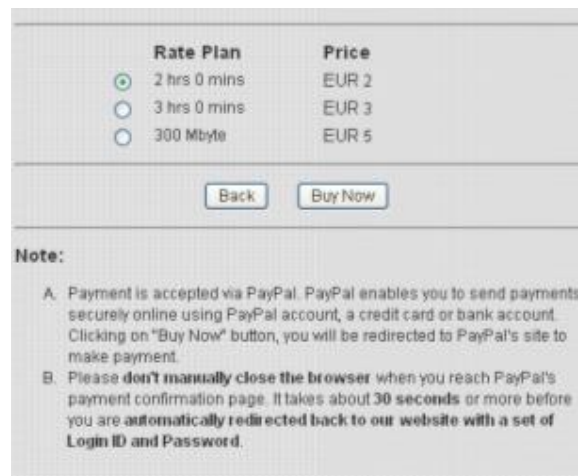
We may collect and store the following personal information:  
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

I agree  
 I disagree

Back Next

**Step 3:** Please fill out the form and Click **Submit** to send out this transaction. There will be a confirm dialog box.



Rate Plan	Price
<input checked="" type="radio"/> 2 hrs 0 mins	EUR 2
<input type="radio"/> 3 hrs 0 mins	EUR 3
<input type="radio"/> 300 Mbyte	EUR 5

Back Buy Now

**Note:**

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, you will be redirected to PayPal's site to make payment.

B. Please **don't manually close the browser** when you reach PayPal's payment confirmation page. It takes about **30 seconds** or more before you are **automatically redirected back to our website with a set of Login ID and Password**.



Microsoft Internet Explorer

Do you want to purchase the internet service through PayPal's website?  
(Note: You don't necessarily need a PayPal account to do a credit card payment on PayPal's website.)

OK Cancel

**Step 4:** You will be redirected to PayPal website to complete the payment process.

**YK Cafe**

Home > Home > Home

### Enter Payment Information

Wireless Internet Access at YK Cafe (2 hrs 0 mins) [View Item Details](#)

[Secure Transaction](#)

Payment For	Quantity	Price
Wireless Internet Access at YK Cafe (2 hrs 0 mins)	1	€2.00 EUR
	Subtotal:	€2.00 EUR
	Total Amount:	€2.00 EUR

**Pay Fast With PayPal**  
It's free and secure. You don't even need your credit info.

---

**YK Cafe**

Home > Review > Home

### Review Your Payment

[Secure Transaction](#)

Payment For	Quantity	Price
Wireless Internet Access at YK Cafe (2 hrs 0 mins)	1	€2.00 EUR
	Subtotal:	€2.00 EUR
	Tax:	€0.00 EUR
	Total Amount:	€2.00 EUR

Review the payment details and click **Pay** to complete your secure payment.

[Cancel and Refund to Merchant](#)

---

**YK Cafe**

### You Made A Payment

Your payment of €2.00 EUR has been received.

You are now being redirected to YK Cafe.

If you are not redirected within 30 seconds: [click here](#).

**Step 5:** Click **Start Internet Access** to use the Internet access service.

Login ID	<b>KM7B@ondemand</b>
Password	<b>6288C7X7</b>
Price	<b>EUR 2.00 (Tax: EUR 0.00)</b>
Usage	<b>2 hrs 0 mins</b>
ESSID: YK-Cafe-TEST2	
Your first time login must be done before 2007/01/31 18:35:28	
The account is valid within 2 days after your first login. <b>Please write down our login ID and Password immediately!</b>	
<input type="button" value="Start Internet Access"/>	

**8 Note:**

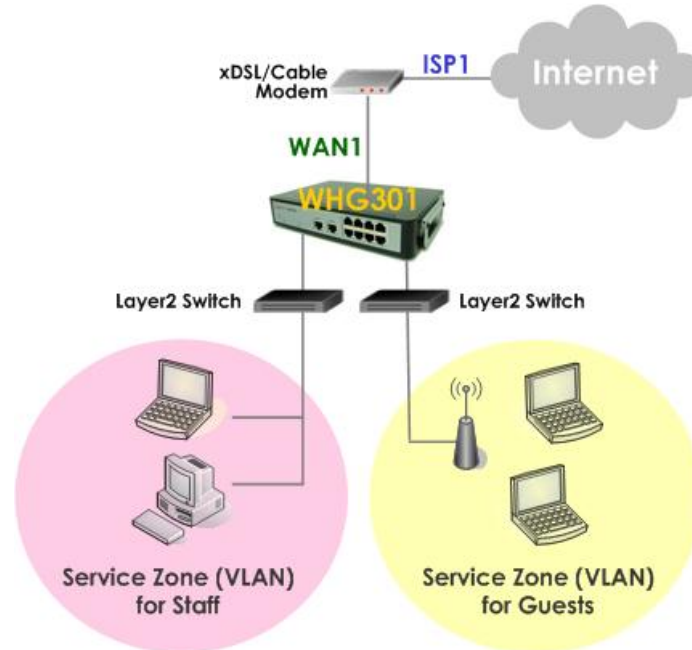
- Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on **Buy Now** button, you will be redirected to PayPal's site to make payment.
- Please **do not manually close the browser** when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are **automatically redirected back to our website with a set of Login ID and Password**.



## Appendix C. Service Zone Deployment Example

### § Port-Based Service Zone

In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Staff** and one for **Guests**.



The switches deployed under WHG301 in Port-Based mode must be Layer 2 switches only.

### Ÿ Configuration Steps for Port-Based Service Zones:

#### Step 1: Configure Service Zone 1 for Guests

Assume that **LAN1** is assigned to the **Service Zone 1 (SZ1)** for **Guests**. Click the **System Configuration** menu and select the **Service Zones** tab. Click **Configure** of SZ1.

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	<a href="#">Configure</a>
SZ1		4ipnet-1	None	Policy 1	Server 1	Disable	<a href="#">Configure</a>

#### Step 2: Configure Basic Settings for SZ1

Check the **Enable** radio button of **Service Zone Status** to activate SZ1. Enter a name for SZ1 (e.g. **"Guests"**) in the **Service Zone Name** field.

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Zone Name	Guests
Network Settings	Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router IP Address : 192.168.2.254 * Subnet Mask : 255.255.255.0 *

### Step 3: Configure Authentication Settings for SZ1

Check the **Enable** radio button to enable *Authentication Required for the Zone*.

Check the **Default** button and **Enabled** box of *Guest Users* to set **ONDEMAND** authentication method as default.

Disable all other authentication options. Then, click **Apply** to activate the settings made so far. A warning message **“You should restart the system to activate the changes.”** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

Authentication Settings					
Authentication Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	<a href="#">Server 1</a>	LOCAL	local	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 2</a>	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 3</a>	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 4</a>	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">On-demand User</a>	ONDEMAND	ondemand	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">SIP</a>	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>

### Step 4: Configure LAN Port Mapping for SZ1

Select the **LAN Port Mapping** tab from the **System** menu to enter the **LAN Ports and Service Zone Mapping** page. Select *Guests* from the drop-down list box of LAN1. Click **Apply** to save the selection.

Service Zone Port Role Setting			
Select Service Zone Mode <input checked="" type="radio"/> Port Based <input type="radio"/> Tag Based			
Choice Of Port Role			
LAN5	LAN6	LAN7	LAN8
Default	Default	Default	Default
Guest	Default	Default	Default
LAN1	LAN2	LAN3	LAN4

A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

LAN1 is now configured for **Guests**.

**Step 5: Configure Service Zone 2 for Staff**

Assume that LAN2 is assigned to the **Service Zone 2 (SZ2)** for **Staff**. Select the **Service Zones** tab and click **Configure** of SZ2.

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	<a href="#">Configure</a>
Guest		4ipnet-1	None	Policy 1	On-demand User	Enable	<a href="#">Configure</a>
SZ2		4ipnet-2	None	Policy 1	Server 1	Disable	<a href="#">Configure</a>

**Step 6: Configure Basic Settings for SZ2**

Check the **Enable** radio button of *Service Zone Status* to activate SZ2. Enter a name for SZ2 (e.g. “**Staff**”) in the *Service Zone Name* field.

**Step 7: Configure Authentication Settings for SZ2**

Check the **Enable** radio button to enable *Authentication Required for the Zone*.

Check the **Default** button and **Enabled** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options. Then, click **Apply** to activate the settings made so far. A warning message **“You should restart the system to activate the changes.”** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

Authentication Settings					
Authentication Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	<a href="#">Server 1</a>	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">Server 2</a>	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 3</a>	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 4</a>	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">On-demand User</a>	ONDEMAND	ondemand	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">SIP</a>	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>









**Step 8: Configure LAN Port Mapping for SZ2**

Select the **LAN Port Mapping** tab from the **System** menu to enter the **LAN Ports and Service Zone Mapping** page. Select *Staff* from the drop-down list box of LAN2. Click **Apply** to save the selection.

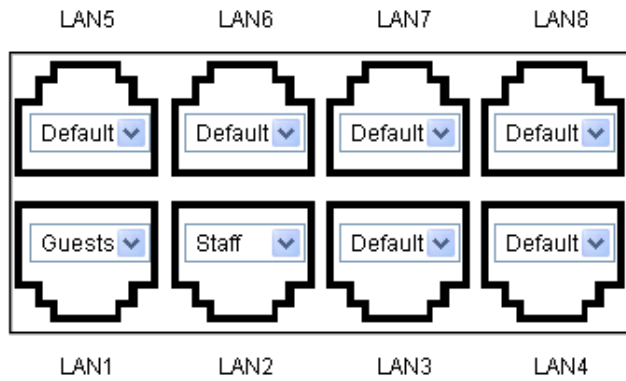
**Service Zone Port Role Setting**

Select Service Zone Mode:  Port Based  Tag Based

Choice Of Port Role

LAN5	LAN6	LAN7	LAN8
			
Default	Default	Default	Default
			
Guest	Staff	Default	Default
LAN1	LAN2	LAN3	LAN4

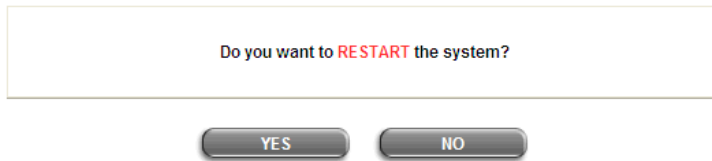
A warning message **“You should restart the system to activate the changes.”** will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all configurations.



You should restart the system to activate the changes. [Restart](#)

### Step 9: Restart the System

A confirmation message of “Do you want to restart the system?” will appear. Click **Yes** to start the restarting process. A confirmation dialog box will then pop out. Click **OK** to continue.



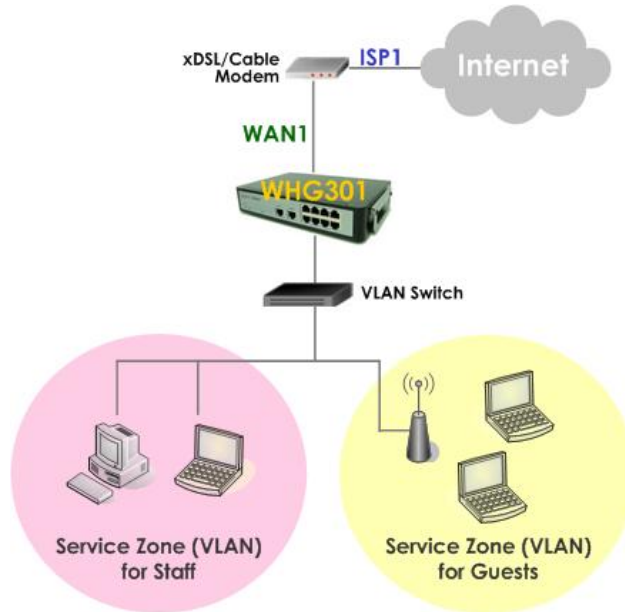
Please do not interrupt the system during the restarting process.

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

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	<a href="#">Configure</a>
Guest		4ipnet-1	None	Policy 1	On-demand User	Enable	<a href="#">Configure</a>
Staff		4ipnet-2	None	Policy 1	Server 1	Enable	<a href="#">Configure</a>

## § Tag-Based Service Zone

VLAN tags carried within message frames. An example of network application diagram is shown as below: one Service Zone for **Staff** and another for **Guests**.



The switch deployed under WHG301 in **Tag-Based** mode must be a **VLAN switch** only.

## ÿ Configuration Steps for Tag-Based Service Zones:

The following example assumes the system is in factory default status and just powered up.









### Step 1: Set Tag-Based mode

Click the **System** menu and select the **LAN Port Mapping** tab. Select **Tag-Based** mode and click **Apply**. A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

**Service Zone Port Role Setting**

Select Service Zone Mode  Port Based  
 Tag Based

In tag based mode, every port maps to every Service Zone.

LAN5	LAN6	LAN7	LAN8
			
			
LAN1	LAN2	LAN3	LAN4

### Step 2: Configure Service Zone 1 for Staff

Select the **Service Zones** tab and click **Configure** of SZ1.

Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	4ipnet	None	Policy 1	Server 1	Enable	<a href="#">Configure</a>
Guest	1	4ipnet-1	None	Policy 1	On-demand User	Enable	<a href="#">Configure</a>
Staff	2	4ipnet-2	None	Policy 1	Server 1	Enable	<a href="#">Configure</a>

### Step 3: Configure Basic Settings for SZ1

Check the **Enable** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. "Employee") in the *Service Zone Name* field.

Enter a VLAN tag for SZ1 (e.g. "1111") in the *VLAN Tag* field.

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Zone Name	<input type="text" value="Employee"/>
Network Settings	VLAN Tag <input type="text" value="1111"/> * (range: 1 ~ 4094)
	Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router
	IP Address : <input type="text" value="192.168.2.254"/> *
	Subnet Mask : <input type="text" value="255.255.255.0"/> *

### Step 4: Configure Authentication Settings for SZ1

Check the **Enable** radio button to enable *Authentication Required for the Zone*.

Check the **Default** button and **Enabled** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options.

Authentication Settings					
Authentication Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	<a href="#">Server 1</a>	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	<a href="#">Server 2</a>	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 3</a>	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">Server 4</a>	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	<a href="#">On-demand User</a>	ONDEMAND	ondemand	<input type="radio"/>	<input type="checkbox"/>
<a href="#">SIP</a>	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	

**Step 5: Set Policy SZ1**

Select **Policy 1** from the drop-down list box.

Click **Apply** to activate the settings made so far. A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

Group Permission for this Service Zone	Configure	
Default Policy in this Service Zone	Policy 1	Edit System Policies
Email Message for Login Reminding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Edit Mail Message

**Step 6: Configure Service Zone 2 for Guests**

Follow **Step 2** to **Step 5** to configure SZ2.

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Zone Name	Guest
Network Settings	VLAN Tag: 222 (range: 1 ~ 4094)
	Operation Mode: <input checked="" type="radio"/> NAT <input type="radio"/> Router
	IP Address: 192.168.12.254
	Subnet Mask: 255.255.255.0

In the **Authentication Settings** section, check the **Default** button and **Enable** box of **Guest Users** to set **ONDEMAND** authentication method as default. Disable all other authentication options.

Authentication Settings					
Authentication Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input type="radio"/>	<input type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	

**Step 7: Restart the System**

Click **Apply** to activate the settings. A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all changes you have made.

Group Permission for this Service Zone	Configure	
Default Policy in this Service Zone	Policy 1	Edit System Policies
Email Message for Login Reminding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Edit Mail Message



A confirmation message of **“Do you want to restart the system?”** will appear. Click **Yes** to start the restarting process. A confirmation dialog box will then pop out. Click **OK** to continue.

Do you want to **RESTART** the system?



*Please do not interrupt the system during the restarting process*

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

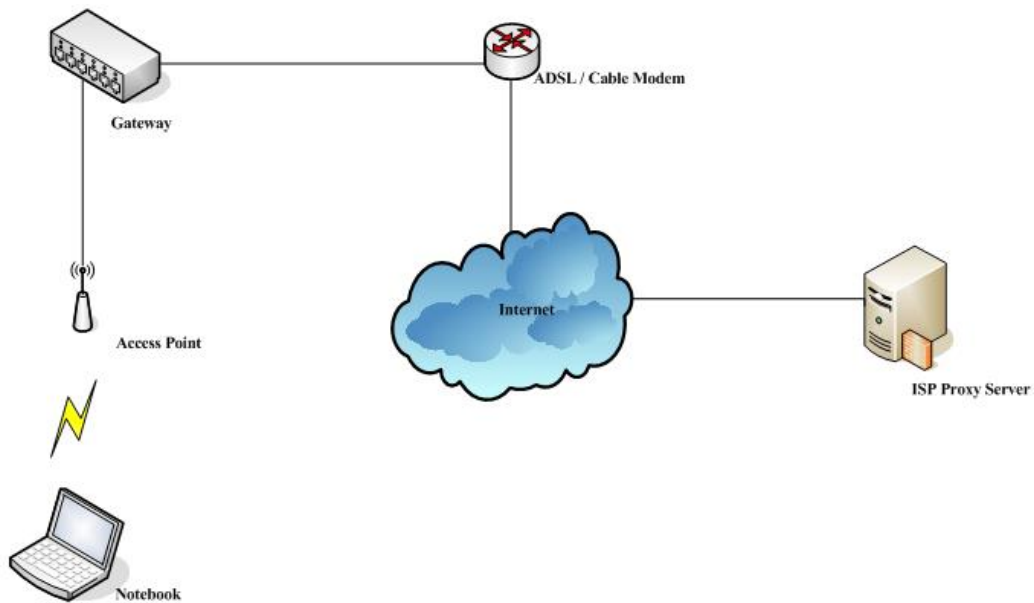
Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	4ipnet	None	Policy 1	Server 1	Enable	<input type="button" value="Configure"/>
Employee	1111	4ipnet-1	None	Policy 1	Server 1	Enable	<input type="button" value="Configure"/>
Guest	222	4ipnet-2	None	Policy 1	On-demand User	Enable	<input type="button" value="Configure"/>

## Appendix D. Proxy Setting

Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of WHG301.

### § Using Internet Proxy Server

The first scenario is that a proxy server is placed outside the LAN environment or in the Internet. For example, the following diagram shows that a proxy server of an ISP will be used.



Follow the following steps to complete the proxy configuration:

**Step 1.** Log into the system by using the **admin** account.

**Step 2.** **Network >> Proxy Server >> External Proxy Servers** page. Add the IP address (leaving it blank means any IP address) and port number of the proxy servers into **External Proxy Servers** setting. Enable the **Built-in Proxy Server**. Click **Apply** to save the settings.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text" value="8080"/>
3	<input type="text"/>	<input type="text" value="8023"/>
4	<input type="text"/>	<input type="text" value="3128"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

**Step 3.** Make sure that the proxy server settings match with at least one of the proxy server setting of the system – for example, in this case, 203.125.142.1:3128 matches with blank:3128.

**Local Area Network (LAN) Settings**

Automatic configuration  
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

Automatically detect settings

Use automatic configuration script

Address:

Proxy server

Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address:  Port:  **Advanced**

Bypass proxy server for local addresses

OK Cancel

**Proxy Settings**

**Servers**

Type	Proxy address to use	Port
HTTP:	208.125.142.1	3128
Secure:		
ETP:		
Socks:		

Use the same proxy server for all protocols

**Exceptions**

Do not use proxy server for addresses beginning with:

Use semicolons ( ; ) to separate entries.

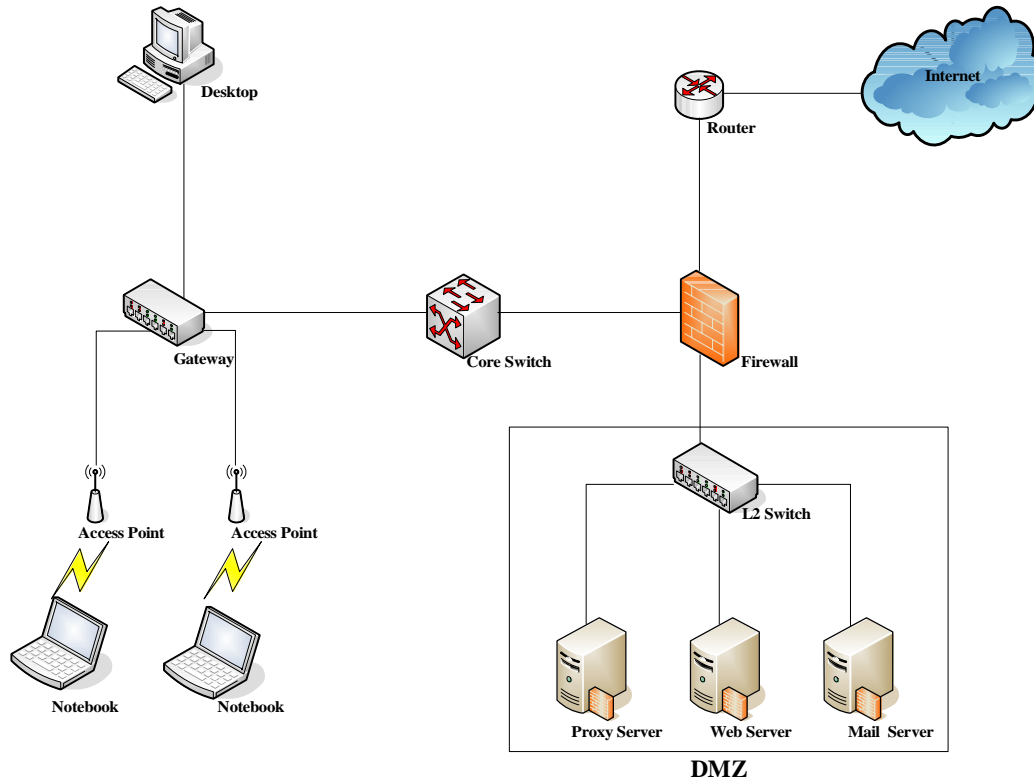
OK Cancel



- 1 *It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*
- 2 *When the **Built-in Proxy Server** is enabled, all the outgoing proxy traffic will be automatically redirected to the built-in proxy server.*

## § Using Extranet Proxy Server

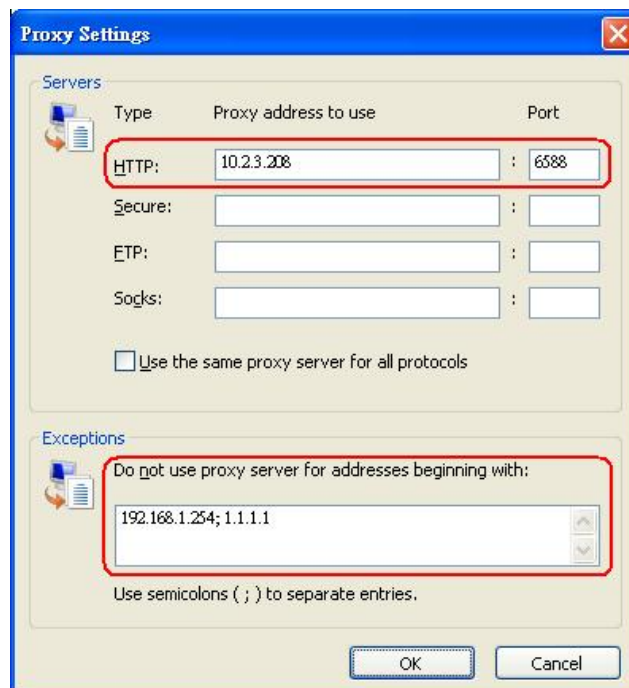
The second scenario is that a proxy server is placed in the Extranet (such as DMZ), which all users from the Intranet or the Internet are able to access. For example, the following diagram shows that a proxy server of an organization in the DMZ will be used.



*A special scenario is that a proxy server is placed in a zone like Intranet – where users can reach each other without going through the system. In this case, whenever any one of users in the Intranet has been authenticated and connects to the network via the proxy server, other users using the same proxy setting in their browsers will be able to access the network without any authentication. Therefore, to stop the risk, it is strongly recommended to put all proxy servers outside the Intranet.*

Follow the following steps to complete the proxy configuration:

- Step 1.** Log in the system by using the **admin** account.
- Step 2.** **Network >> Proxy Server >> External Proxy Servers** page. Add the IP address and port number of the proxy server into External Proxy Servers setting. Click **Apply** to save the settings.
- Step 3.** Make sure that clients use the same proxy server settings. Please also configure appropriate exceptions if there is any traffic which is not needed to go through proxy server – for example, there is no need to use proxy server for the Default Gateway (192.168.1.254).



*It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*

## Appendix E. Session Limit and Session Log

### § Session Limit

To prevent ill-behaved clients or malicious software from using up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

- ∅ The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- ∅ When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350 and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a Syslog server.
- ∅ Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

### § Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- ∅ The description of the fields of a session log record is shown as below:

Field	Description
Date and Time	The date and time that the session is established
Session Type	[New]: This is a newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user. When it shows "N.A.", it indicates that the user or device does not need to log in with a username, for example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Change the account name accordingly, if the name is not identifiable in the record. <b>8 Note:</b> Only 31 characters are allowed for the combination of Session Type plus Username.
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the user's computer or device
SIP	The source IP address of the user's computer or device
SPort	The source port number of the user's computer or device
DIP	The destination IP address of the user's computer or device
DPort	The destination port number of the user's computer or device

Ø An example of session log data is shown as below:

```
31 Aug 12:35:05 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
31 Aug 12:35:05 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
31 Aug 12:35:06 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
31 Aug 12:35:06 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
31 Aug 12:35:07 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
31 Aug 12:35:09 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
31 Aug 12:35:10 2007 [New]user1 @local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80
```



## Appendix F. Network Configuration on PC & User Login

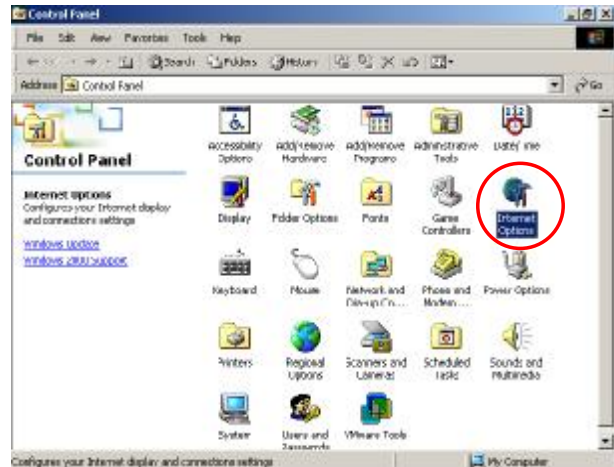
### § Network Configuration on PC

After 4ipnet WHG301 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

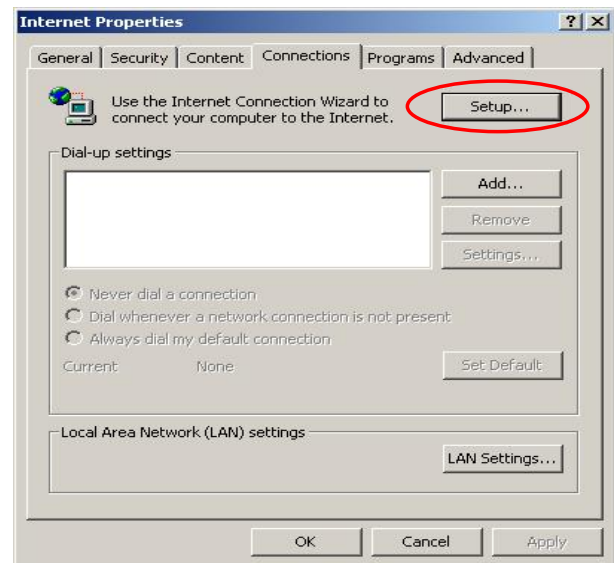
#### ¶ Internet Connection Setup

##### § Windows 9x/2000

- 1) Choose **Start >> Control Panel >> Internet Options**.



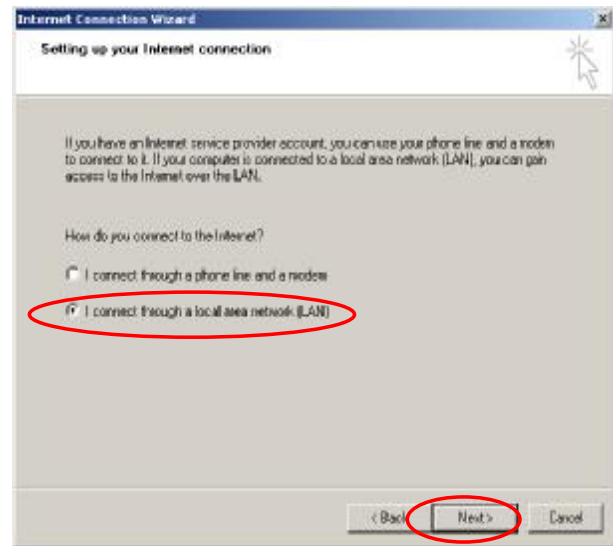
- 2) Choose the **Connections** tab, and then click **Setup**.



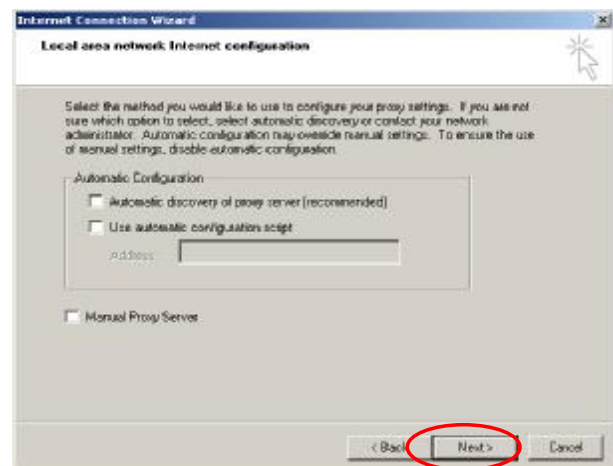
- 3) Choose “I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)”, and then click **Next**.



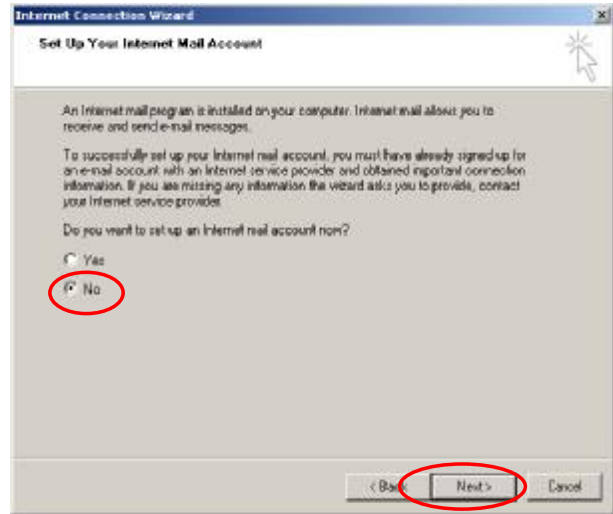
- 4) Choose “I connect through a local area network (LAN)” and then click **Next**.



- 5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click **Next**.



- 6) Choose “**No**” and then click **Next**.



- 7) Finally, click **Finish** to exit the **Internet Connection Wizard**. Now, the set up is completed.

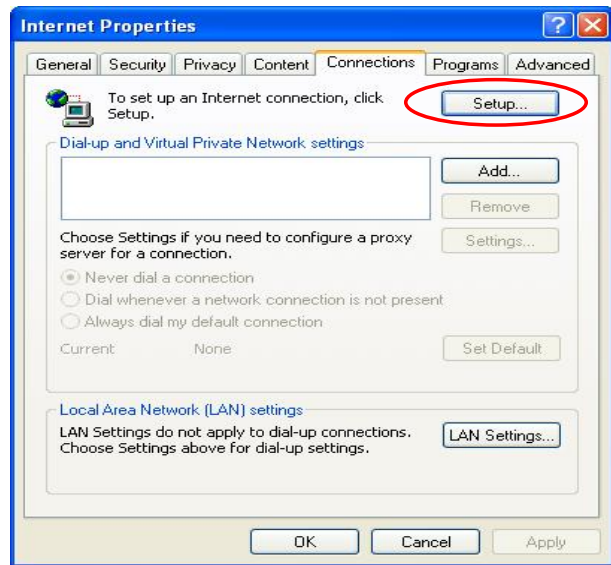


## § Windows XP

- 1) Choose **Start >> Control Panel >> Internet Option**.



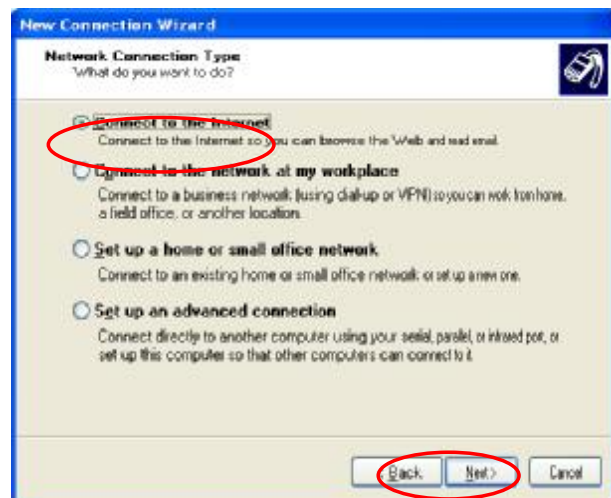
- 2) Choose the **Connections** tab, and then click **Setup**.



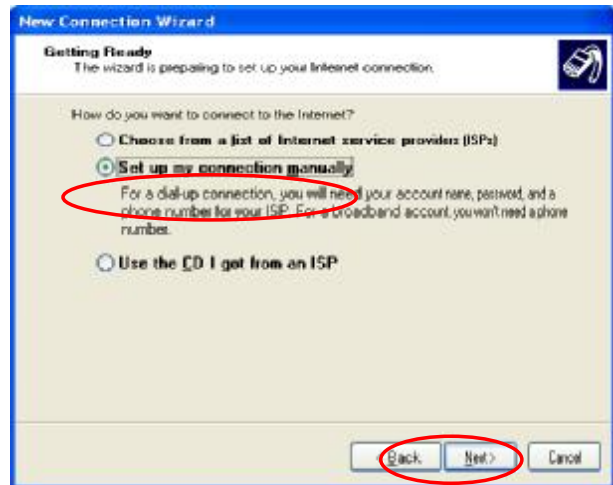
- 3) When the **Welcome to the New Connection Wizard** window appears, click **Next**.



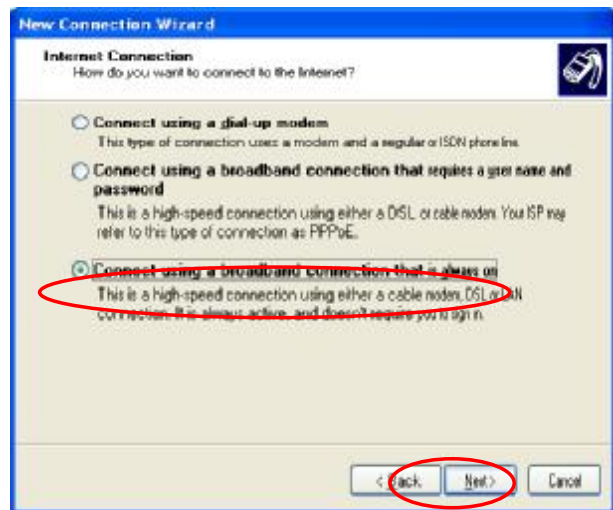
- 4) Choose **“Connect to the Internet”** and then click **Next**.



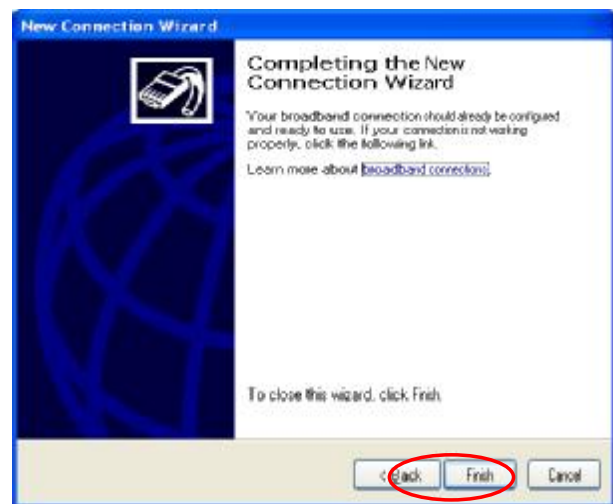
- 5) Choose “**Set up my connection manually**” and then click **Next**.



- 6) Choose “**Connect using a broadband connection that is always on**” and then click **Next**.



- 7) Finally, click **Finish** to exit the **Connection Wizard**. Now, the setup is completed.

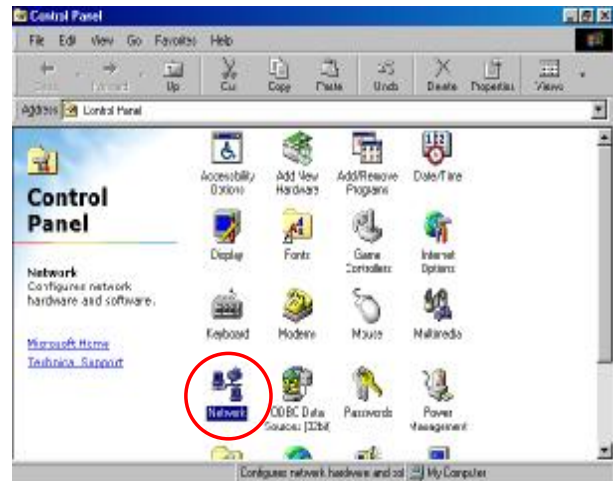


## Y TCP/IP Network Setup

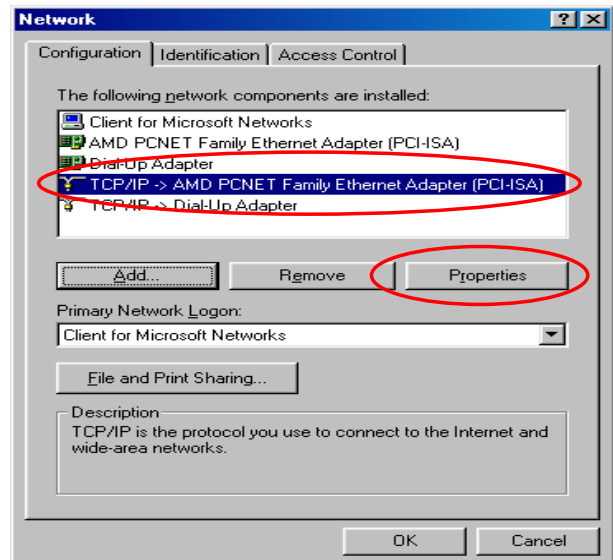
If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any changes to directly start/restart the system. With the factory default settings, during the process of starting the system, 4ipnet WHG301 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called “**Obtain an IP address automatically**”. If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

### § Check the TCP/IP Setup of Window 9x/ME

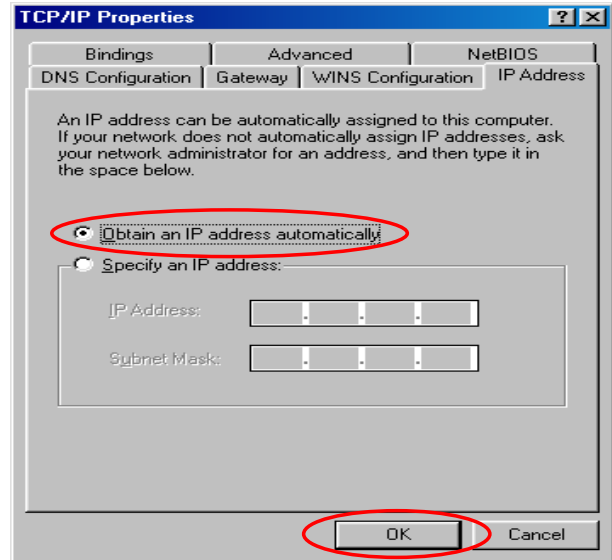
- 1) Choose **Start >> Control Panel >> Network**.



- 2) Click on the **Configuration** tab and select “**TCP/IP >> AMD PCNET Family Ethernet Adapter (PCI-ISA)**”, and then click **Properties**.  
Now, you can choose to use DHCP or a specific IP address.



- 3) **Using DHCP:** If you want to use DHCP, click on the **IP Address** tab and choose “**Obtain an IP address automatically**”, and then click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG301.

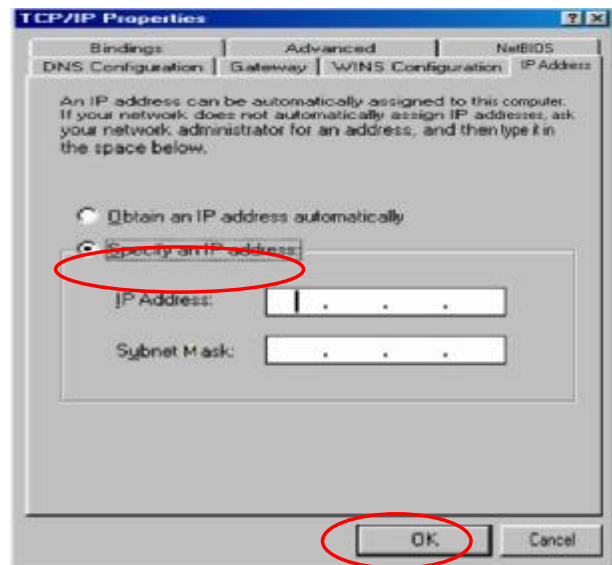


- 4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG301.

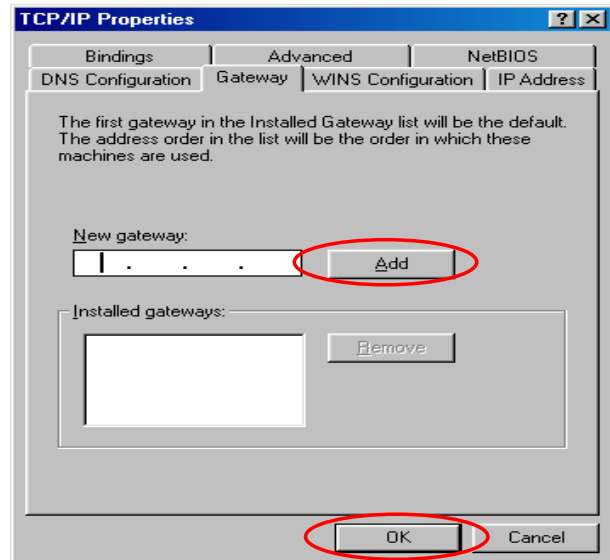


If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

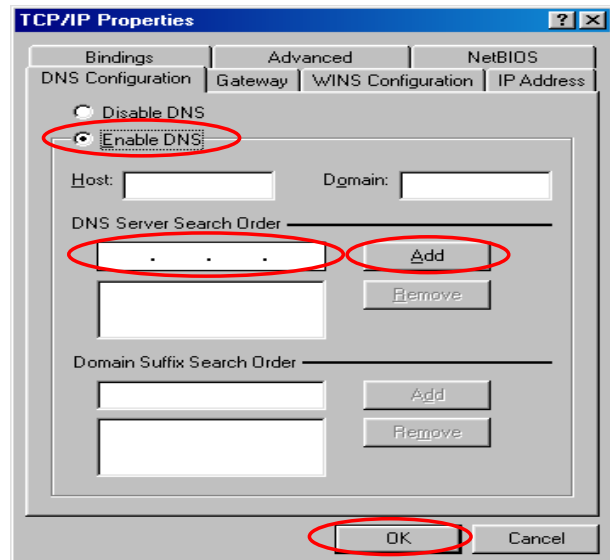
- 4.1) Click on the **IP Address** tab and choose “**Specify an IP address**”. Enter the *IP Address*, *Subnet Mask* and then click **OK**.



- 4.2) Click on the **Gateway** tab. Enter the gateway address of WHG301 in the **“New gateway”** field and click **Add**. Then, click **OK**.

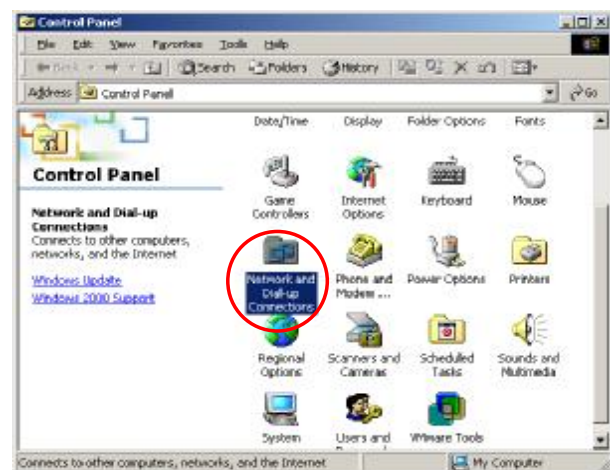


- 4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **“Enable DNS”** and enter *DNS Server address*. Click **Add**, and then click **OK** to complete the configuration.



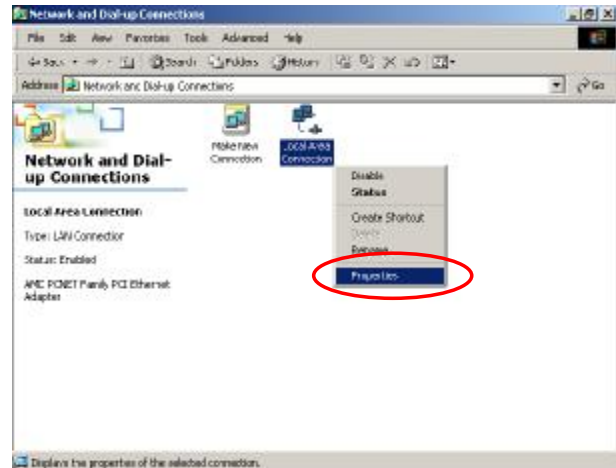
## § Check the TCP/IP Setup of Window 2000

- 1) Select **Start >> Control Panel >> Network and Dial-up Connections**.

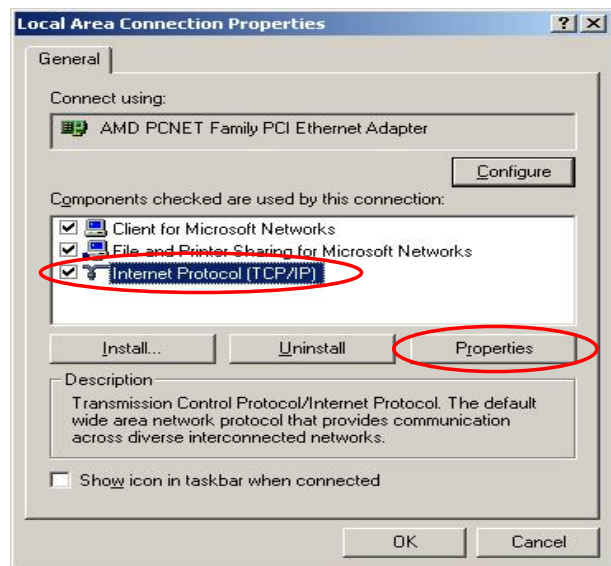




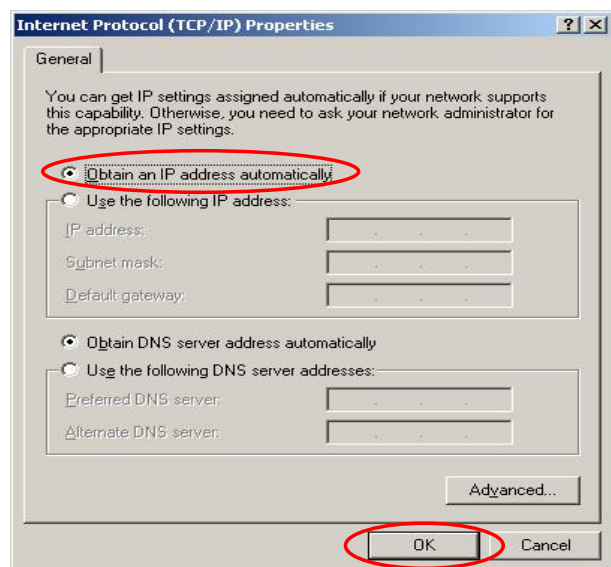
- 2) Right click on the **Local Area Connection** icon and select **“Properties”**.



- 3) Select **“Internet Protocol (TCP/IP)”** and then click **Properties**. Now, you can choose to use DHCP or a specific IP address.



- 4) **Using DHCP:** If you want to use DHCP, choose **“Obtain an IP address automatically”**, and then click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG301.



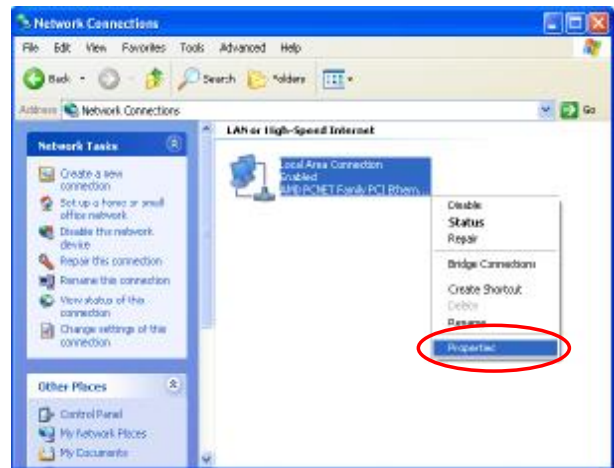


## § Check the TCP/IP Setup of Window XP

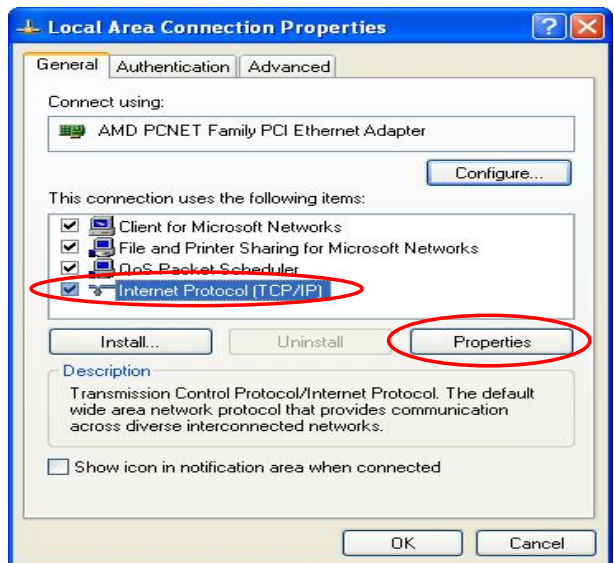
- 1) Select **Start >> Control Panel >> Network Connection**.



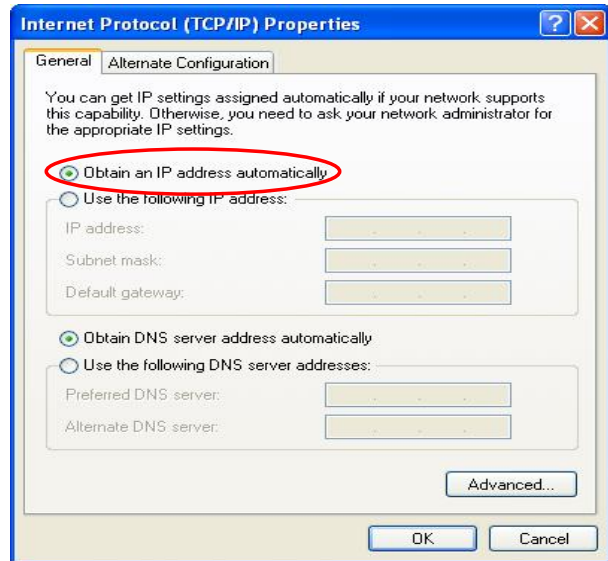
- 2) Right click on the **Local Area Connection** icon and select **"Properties"**.



- 3) Click on the **General** tab and choose **"Internet Protocol (TCP/IP)"**, and then click **Properties**. Now, you can choose to use DHCP or a specific IP address.



- 4) **Using DHCP:** If you want to use DHCP, choose **“Obtain an IP address automatically”** and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG301.

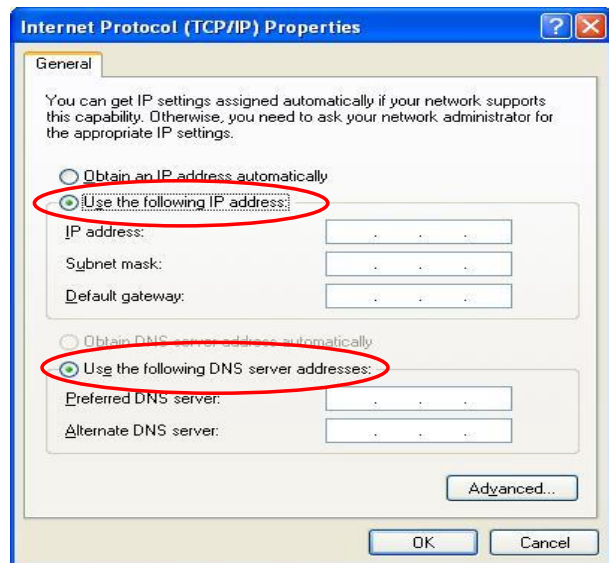


- 5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG301.

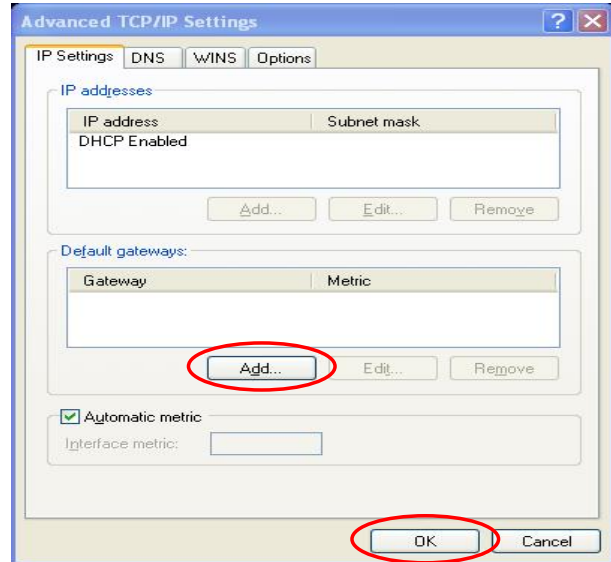


If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

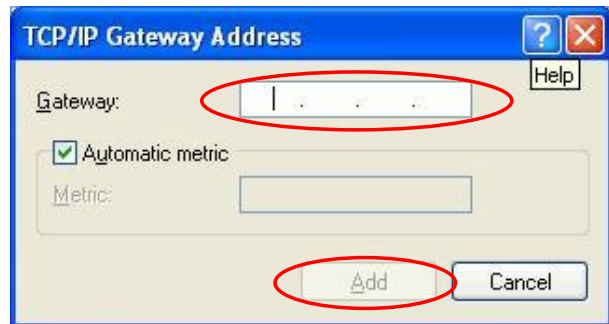
- 5.1) Choose **“Use the following IP address”** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **“Using the following DNS server addresses”** and enter the *DNS Server address*. Then, click **OK**.
- 5.2) Click **Advanced** to enter the **Advanced TCP/IP Settings** window.



- 5.3) Click on the **IP Settings** tab and click **Add** below the “**Default gateways**” column and the **TCP/IP Gateway Address** window will appear.



- 5.4) Enter the gateway address of WHG301 in the “**Gateway**” field, and then click **Add**. After back to the **IP Settings** tab, click **OK** to finish the configuration.



## § An Example of User Login

Normally, users will be authenticated before they get network access through WHG301. This section presents the basic authentication flow for end users. Please make sure that the WHG301 is configured properly and network related settings are done.

1. Open an Internet browser and try to connect to any website (in this example, we try to connect to [www.google.com](http://www.google.com)).
  - a) For the first time, if the WHG301 is not using a trusted SSL certificate (for more information, please see [4.2.5 Additional Configuration](#)), there will be a "Certificate Error", because the browser treats WHG301 as an illegal website.



- b) Please press "Continue to this website" to continue.
  - c) The default user login page will appear in the browser.



2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click **Submit** button. If the **Remember Me** check box is checked, the browser will remember this user's name and password so that he/she can just click Submit next time he/she wants to login.

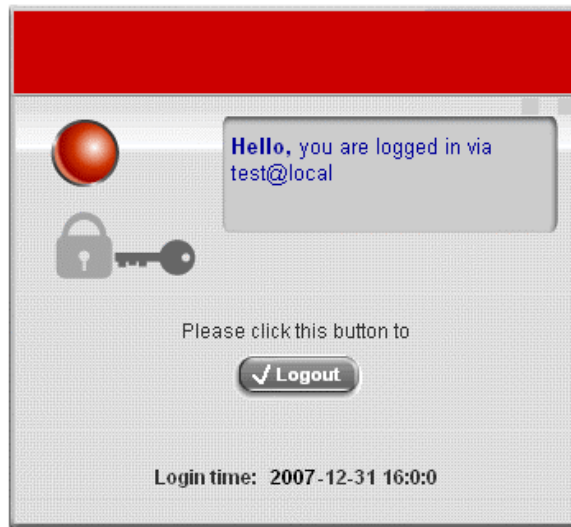
Check the **Remember Me** box to store the username and password on the current computer in order to automatically login to the system at next login. Then, click the **Submit** button.

The **Remaining** button on the **User Login Page** is for on-demand users only, where they can check their Remaining Usage time.



The screenshot shows a web browser window with a red header bar containing the text "User Login Page". Below the header, the text reads "Welcome To User Login Page!" and "Please Enter Your User Name and Password To Sign In.". There are two input fields: "User Name:" with the value "test@local" and "Password:" with masked characters "\*\*\*\*". Below the input fields are three buttons: "Submit", "Clear", and "Remember Me" (which is checked). The "Remember Me" checkbox is located below the buttons.

3. Successful! The **Login Successful** page appearing means WHG301 has been installed and configured successfully. Now, you are connected to the network and Internet!



The screenshot shows a web browser window with a red header bar. The main content area has a grey background with a red sphere icon and a key icon. A message box says "Hello, you are logged in via test@local". Below the message, it says "Please click this button to" and there is a "Logout" button. At the bottom, it says "Login time: 2007-12-31 16:0:0".

---

**Note:** When On-demand accounts are used (for example, we use **7ksc@ondemand** here), the system will display more information, as shown below.

---

4. **Remaining Usage:** The remaining quota of this On-demand account that the user can surf the Internet.



5. **Redeem:** When the remaining quota is insufficient, the user can add up the quota by purchasing an additional account. Please enter the new username and password in the Redeem Page and click **ENTER** button to merge the two accounts so that there will be more quota for the original account.



**8 Note:**

---

The maximum session time/data transfer is 24305 days/9,999,999 Mbytes. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

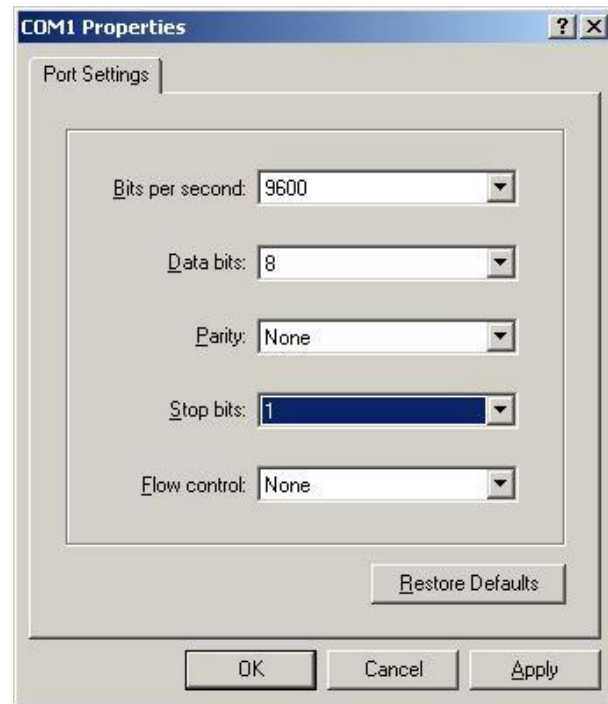
---



## Appendix G. Console Interface

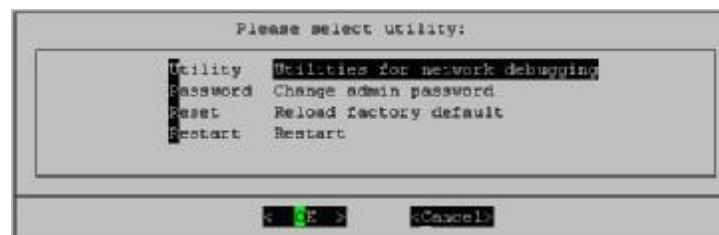
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of 4ipnet WHG301, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600,8,n,1**.



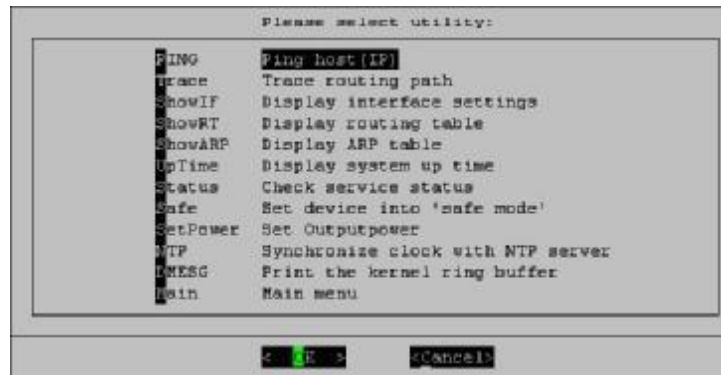
*The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.*

3. Once the console port of 4ipnet WHG301 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system, where the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



## Y Utilities for network debugging

The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:



- Ø Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- Ø Trace routing path: Trace and inquire the routing path to a specific target.
- Ø Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
- Ø Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Ø Display ARP table: The internal ARP table of the system is displayed.
- Ø Display system up time: The system live time (time for system being turn on) is displayed.
- Ø Check service status: Check and display the status of the system.
- Ø Set device into "safe mode": If the administrator is unable to use Web Management Interface via browser for the system failed inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
- Ø Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- Ø Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
- Ø Main menu: Go back to the main menu.

## Y **Change admin password**

Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator's password again.



*Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the 4ipnet WHG301 Admin username and password after logging in the system for the first time.*

## Y **Reload factory default**

Choosing this option will reset the system configuration to the factory defaults.

## Y **Restart 4ipnet WHG301**

Choosing this option will restart 4ipnet WHG301.

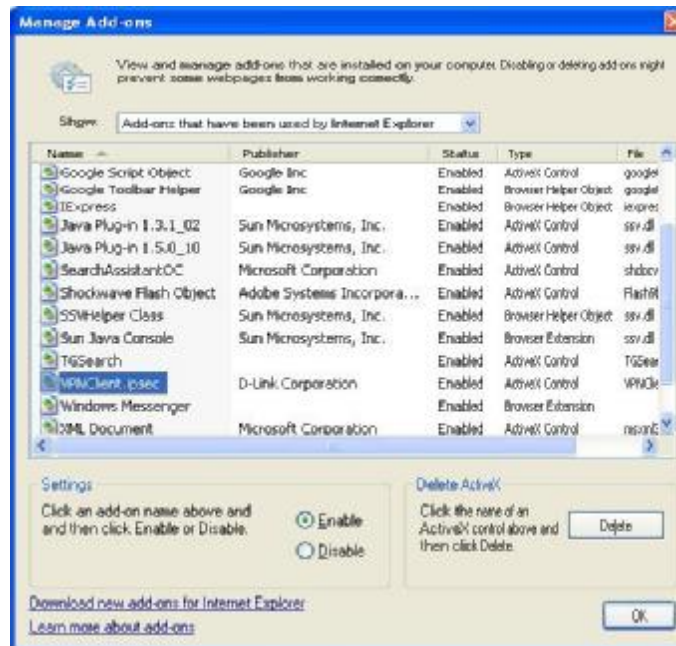
## Appendix H. Local VPN

The system is equipped with IPSec VPN feature. To utilize IPSec VPN supported by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, the system implements IPSec VPN tunneling technology between client's windows devices and the system itself regardless of wired or wireless network.

By pushing down ActiveX to the client's Windows device from the system, no extra client software is required to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is then configured automatically. At the end of this setup, a build-in IPSec VPN feature will be enabled and ready to serve once it is launched for setup. The goal of this design is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of the system is based on ActiveX and the built-in IPSec VPN client of Windows OS.

- **ActiveX Component**

The ActiveX is a software component running inside Internet Explorer. The ActiveX component can be checked by the following windows.



**Windows Internet Explorer:** From the **Tools** menu, click on **Internet Options**. Select the **Programs** tab and click **Manage add-ons** button to enter the **Manage add-ons** dialogue box, where you can see **VPNClient.ipsec** is enabled.

During the first-time login to WHG301, Internet Explorer will ask clients to download an ActiveX component of IPSec VPN. Once this ActiveX component is downloaded, it will run in parallel with the “Login Success Page” after the page being brought up successfully. The ActiveX component helps set up individual IPSec VPN tunnels between clients and WHG301 and check the validity of IPSec VPN tunnels between them. If the connection is down, the ActiveX component will detect the broken link and decompose the IPSec tunnel. Once the IPSec VPN tunnel was built, all sent packets will be encrypted. Without connecting to the original IPSec VPN tunnel, a client has no alternative way to gain network connection beyond this. IPSec VPN feature supported by WHG301 directly solves possible data security leak problem between clients and the system via either wireless or wired connections without extra hardware or client software installed.

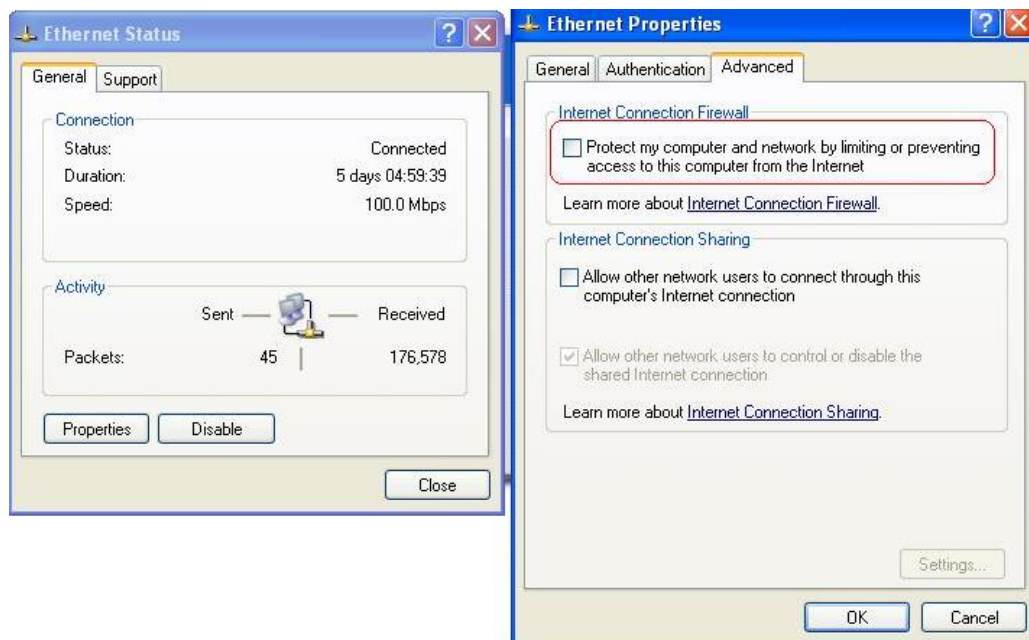
## • Limitations

The limitation on the client side due to ActiveX and Windows OS includes:

- Ø Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPSec protocol. It shall be turned off to allow IPSec packets to pass through.
- Ø Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.
- Ø The forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes that IPSec tunnel cannot be cleared properly at client device. A reboot of client device is needed to clear the IPSec tunnel.
- Ø The crash of Windows Internet Explorer may cause the same result.

## • Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPSec. Internet Connection Firewall will drop packets from tunneling of IPSec VPN. Please **TURN OFF** Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.



- **ICMP and Active Mode FTP**

In Windows XP SP2 without patching by KB889527, it will drop ICMP packets from IPsec tunnel. This problem can be fixed by upgrading patch KB889527. Before enabling IPsec VPN function on client devices, please access the patch from Microsoft's web at <http://support.microsoft.com/default.aspx?scid=kb:en-us:889527>. This patch also fixes the problem of supporting active mode FTP inside IPsec VPN tunnel of Windows XP SP2. Please **UPDATE** clients' Windows XP SP2 with this patch.

- **The Termination of ActiveX**

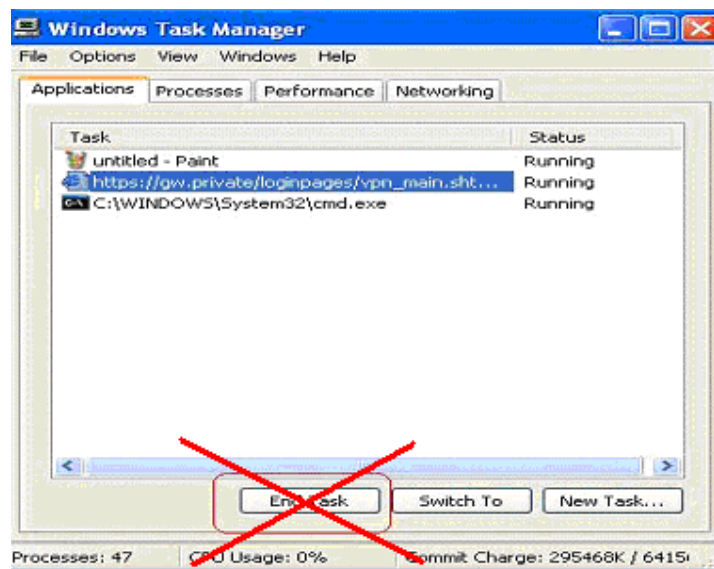
The ActiveX component for IPsec VPN is running in parallel with the web page of "Login Success". To ensure that the built-in IPsec VPN tunnel is always alive, unless clients decide to close the session and to disconnect from WHG301, **the following conditions or behaviors, which may cause the Internet Explorer to stop the ActiveX, should be avoided.**

(1) **The crash of Internet Explorer on running ActiveX.**

*If it happens, please reboot the client computer. Once Windows service is resumed, go through the login process again.*

(2) **Termination of the Internet Explorer Task from Windows Task Manager.**

*Do NOT terminate this VPN task of Internet Explorer.*



(3) **Execution of instructions given by the following Windows messages:**

- † Close the Windows Internet Explorer.
- † Click **Logout** on Login Success page.
- † Click **Back** or **Refresh** of the same Internet Explorer browser page.
- † Enter a new URL in the same Internet Explorer browser page.
- † Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.

*Click **Cancel** if you do not intend to stop the IPsec VPN connection.*

- **Non-supported OS and Browser**

Currently, Windows Internet Explorer is the only browser supported by the system. Windows XP and Windows 2000 are the only two supported OS along with this release.

- **FAQ**

(1) How to clean IPsec client?

ANS:

Open a command prompt window and type the commands as follows.

```
C:\> cd %windir%\system32
```

```
C:\> Clean_IPSEC.bat
```

Or

```
C:\> cd %windir%\system32
```

```
C:\> ipsec2k.exe stop
```

(2) How to remove ActiveX component in client's computer?

ANS:

- ① Uninstall and delete ActiveX component
- ② Close all Internet Explorer windows
- ③ Open a command prompt window and type the commands as follows

```
C:\> cd %windir%\system32
```

```
C:\> regsvr32 /u VPNClient_1_5.ocx
```

```
C:\> del VPNClient_1_5.ocx
```

(3) What can I do if unable establish IPsec connection for Windows XP SP1?

ANS:

Disable Windows XP firewall

## Appendix I. Customizable Pages

There are five users' login and logout pages for each service zone that can be customized by administrators.

Go to System Configuration >> Service Zone >> Service Zone Settings Configure >> Custom Pages.

Click the button of **Configure**, the **Login (Logout)** page will appear, including **Login page**, **Logout Page**, **Login Success Page**, **Login Success Page for On-demand User** and **Logout Success Page**.

Click the radio button of page selections to have further configuration.

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 Ondemand User	<input type="button" value="Configure"/>
	Logout Success Page	<input type="button" value="Configure"/>

### 1 Custom Pages >> Login Page

The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from a designated website. After finishing the setting, click **Preview** to see the login page.

#### Y Custom Pages >> Login Page >> Default Page

Choose Default Page to use the default login page.

Login Page Selection for Users - Service Zone: Default	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting - Service Zone: Default
<p>This is default login page for users.            You could click preview link to preview the default login page.            Thanks.</p> <p style="text-align: center;"><a href="#">Preview</a></p>

#### Y Custom Pages >> Login Page >> Template Page

Choose Template Page to make a customized login page. Click Select to pick up a color and then fill in all of the blanks. You can also upload a background image file for your template. Click **Preview** to see the result first.



Login Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	E1F4FD <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	034E42 <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	FFFFFF <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	595959 <a href="#">Select</a> (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Remember Me	Remember Me
Logo Image File	<a href="#">Preview and Edit the Image File</a>
Background Image File	<a href="#">Preview and Edit the Image File</a>
<a href="#">Preview</a>	

Y *Custom Pages >> Login Page >> **Uploaded Page***

Choose Uploaded Page and upload a login page.

Login Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <a href="#">Browse...</a>
<a href="#">Submit</a>	

Existing Image Files:	
Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <a href="#">Browse...</a>
<a href="#">Submit</a>	
<a href="#">Preview</a>	

The user-defined login page must include the following HTML codes to provide the necessary fields for user name and password.

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

And if the user-defined login page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

```
Remote VPN      : <img src=images/xx.jpg">
Default Service Zone: <img src=images0/xx.jpg">
Service Zone 1  : <img src=images1/xx.jpg">
Service Zone 2  : <img src=images2/xx.jpg">
Service Zone 3  : <img src=images3/xx.jpg">
Service Zone 4  : <img src=images4/xx.jpg">
```

Click the **Browse** button to select the file to upload. Then click **Submit** to complete the upload process.

Next, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the **Use Default Page** button to restore it to default.

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click **Delete** to delete the file.

After the upload process is completed and applied, the new login page can be previewed by clicking **Preview** button at the bottom.

#### Y Custom Pages >> Login Pages >> External Page

Login Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

Choose the **External Page** selection and get the login page from a designated website. In the External Page Setting, enter the URL of the external login page and then click **Apply**.

After applying the setting, the new login page can be previewed by clicking **Preview** button at the bottom of this page.

The user-defined logout page must include the following HTML codes to provide the necessary fields for username and password.

```

<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>

```

## 2 Custom Pages >> Logout Page

The administrator can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page >> Uploaded Page" instructions for more details.

**Upload Logout Page - Service Zone: Default**

File Name	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Submit"/>		<input type="button" value="Use Default Page"/>

Existing Image Files:

Total Capacity: 512 K  
 Now Used: 0 K

**Upload Image Files - Service Zone: Default**

Upload Images	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Submit"/>		

[Preview](#)

### 8 Note:

The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the customized logout page can be previewed by clicking **Preview** at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "Use Default Page" button.

```

<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>

```

## 3 Custom Pages >> Login Success Page

The users can apply their own Login Success page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

### Y Custom Pages >> Login Success Page >> Default Page

Choose Default Page to use the default login success page.

Login Success Page Selection for Users - Service Zone: Default	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting - Service Zone: Default
This is default login success page for users. You could click preview link to preview the default login success page.
<a href="#">Preview</a>

Y Custom Pages >> Login Success Page >> **Template Page**

Choose Template Page to make a customized login success page. Click Select to pick up a color and then fill in all of the blanks. Click Preview to see the result first.

Login Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Success Page"/>
Welcome	<input type="text" value="Hello"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Login Time	<input type="text" value="Login Time"/>
<input type="button" value="Preview"/>	

Y Custom Pages >> Login Success Page >> **Uploaded Page**

Choose Uploaded Page and get the login success page to upload. Click the Browse button to select the file for the login success page upload. Then click Submit to complete the upload process.

After the upload process is completed and applied, the new login success page can be previewed by clicking Preview button at the bottom.

Login Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <a href="#">Browse...</a>
<a href="#">Submit</a>	

Existing Image Files:

Total Capacity: 512 K	Now Used: 0 K
-----------------------	---------------

Upload Image Files	
Upload Images	<input type="text"/> <a href="#">Browse...</a>
<a href="#">Submit</a>	
<a href="#">Preview</a>	

Y *Custom Pages >> Login Success Page >> External Page*

Choose the External Page selection and get the login success page from a designated website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking **Preview** button at the bottom of this page

Login Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL	<input type="text" value="http://"/>
<a href="#">Preview</a>	

4 *Custom Pages >> Login Success Page for On-demand User*

The users can apply their own Login Success page for on-demand Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

Y *Custom Pages >> Login Success Page for On-demand Users >> Default Page*

Choose Default Page to use the default login success page for on-demand account

Login Success Page Selection for on-demand Users - Service Zone: Default	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting - Service Zone: Default
This is default login success page for on-demand users. You could click preview link to preview the default login success page. Thanks.
<a href="#">Preview</a>

Y Custom Pages>> Login Success Page for On-demand Users>> **Template Page**

Choose Template to make a customized login success for on-demand account. Click *Select* to pick up a color and then fill in all of the blanks. Click **Preview** to see the result.

**Login Success Page Selection for on-demand Users - Service Zone: Default**

Default Page       Template Page  
 Uploaded Page       External Page

**Template Page Setting**

Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Success Page for Guest Users"/>
Welcome	<input type="text" value="Welcome"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Remaining Usage	<input type="text" value="Remaining Usage"/>
Day	<input type="text" value="Day"/>
Hour	<input type="text" value="Hour"/>
Min	<input type="text" value="Min"/>
Sec	<input type="text" value="Sec"/>
Login Time	<input type="text" value="Login Time"/>
Redeem	<input type="text" value="Redeem"/>

Y Custom Pages>> Login Success Pages for On-demand Users>> **Uploaded Page**

Choose Uploaded Page and get the login success page for on-demand users by uploading. Click the **Browse** button to select the file for the login success page for Instant upload. Then click **Submit** to complete the upload process.

**Login Success Page Selection for On-demand Users - Service Zone: Default**

Default Page       Template Page  
 Uploaded Page       External Page

**Upload Login Success Page for On-demand User**

File Name:

Existing Image Files:

Total Capacity: 512 K  
Now Used: 0 K

Upload Image Files

Upload Images:

[Preview](#)

¶ *Custom Pages >> Login Success Pages for On-demand Users >> External Page*

Choose the External Page selection and get the login success page from a designated website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking **Preview** button at the bottom of this page.

Login Success Page Selection for on-demand Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

5 *Custom Pages >> Logout Success Page*

The administrator can apply their own Logout Success page for Users in the menu. As the process is similar to that of the Login Page, please refer to the “Login Page” instructions for more details.

¶ *Custom Pages >> Logout Success Page >> Default Page*

Choose **Default Page** to use the default logout success page.

Logout Success Page Selection for Users - Service Zone: Default	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting - Service Zone: Default	
This is default logout success page for users. You could click preview link to preview the default logout success page.	
<a href="#">Preview</a>	

¶ *Custom Pages >> Logout Success Page >> Template Page*

Choose Template Page to make a customized logout success page. Click **Select** to pick up a color and then fill in all of the blanks. Click **Preview** to see the result first.

Logout Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Logout Success Page"/>
Information	<input type="text" value="Logout successfully"/>
<input type="button" value="Preview"/>	

Y Custom Pages >> Logout Success Page >> **Uploaded Page**

Choose Uploaded Page and get the logout success page to upload. Click the **Browse** button to select the file for the logout success page upload. Then click **Submit** to complete the upload process.

After the upload process is completed and applied, the new logout success page can be previewed by clicking **Preview** button at the bottom.

Logout Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Upload Logout Success Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
Existing Image Files:	
Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

Y Custom Pages >> Logout Success Page >> **External Page**

Choose the External Page selection and get the logout success page from a designated website. Enter the website address in the External Page Setting field and then click Apply. After applying the setting, the new logout success page can be previewed by clicking **Preview** button at the bottom of this page.

Logout Success Page Selection for Users - Service Zone: Default	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	