



LevelOne

Secure WLAN Controller

WHG-311/315/401/505/515/707

User Manual

Copyright

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

Disclaimer

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

Trademarks

LevelOne is a registered trademark of Digital Data Communications Group. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.



About 4ipnet

The LevelOne **Secure WLAN Controller** series is powered by 4ipnet. **LevelOne** is partnered with 4ipnet to deliver most feature-rich product yet simple deployment in wireless networking infrastructure solution.

4ipnet is a leading provider of wireless networking solution software design house for manageable, reliable, and secure wireless access. In an effort to meet changing market demands at the least possible cost, 4ipnet delivers a diverse array of turnkey, high-performance products and mission-critical applications to bring reliability and manageability to increasingly complex wireless networks.

4ipnet's complete WLAN infrastructure solution portfolio addresses the needs of different network operation environments ranging from the ISP to the SOHO, with an emphasis on simplified network deployment, centralized network management, and enhanced network performance.



FCC CAUTION

WHG-311

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

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

WHG-315, WHG-401, WHG-505, WHG-515, WHG-707

These equipments has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Table of Contents

1.	<i>Before You Start</i>	8
1.1.	Preface.....	8
1.2.	Document Conventions	8
2.	<i>WHG Controllers Installation Guide</i>	9
2.1.	WHG Controller Capacity Table	9
2.2.	WHG Controller Hardware Overview	10
2.2.1.	WHG-311 Hardware.....	10
2.2.2.	WHG-315 Hardware.....	11
2.2.3.	WHG-401 Hardware.....	12
2.2.4.	WHG-505 Hardware.....	13
2.2.5.	WHG-515 Hardware.....	14
2.2.6.	WHG-707 Hardware.....	15
2.3.	Preparation before the Installation	16
2.4.	Unpacking & Installing	17
2.4.1.	WHG-311 Package & Installation.....	17
2.4.2.	WHG-315 Package & Installation	17
2.4.3.	WHG-401 Package & Installation	18
2.4.4.	WHG-505 Package & Installation	19
2.4.5.	WHG-515 Package & Installation	19
2.4.6.	WHG-707 Package & Installation	20
3.	<i>System Overview</i>	22
3.1.	System Concept.....	22
3.2.	Service Zone Concept.....	26
3.3.	AP Management Concept.....	28
4.	<i>Getting Started</i>	29
4.1.	Accessing Web Management Interface	29
4.2.	Home Page	31
4.2.1.	Setup Wizard.....	32
4.2.2.	Quick Links.....	33
4.2.3.	System Overview	34
4.2.4.	Main Menu	35
4.2.5.	Online Help	36
5.	<i>Initial Network Setup</i>	37
5.1.	Network Requirement.....	37
5.2.	Managing System Date & Time	37
5.3.	WAN1 & WAN2 Setup	38
5.4.	WAN Traffic Control.....	40
5.5.	LAN Port & Service Zone Mapping	41
5.6.	LAN Partition -- Service Zone	44
5.6.1.	Planning Your Internal Network.....	46
5.6.2.	Configure Service Zone Network	47
5.6.3.	WISPr Attributes in Service Zone.....	51
5.7.	IPv6.....	52
6.	<i>User Authentication and Grouping</i>	54
6.1.	Overview of User Authentication Database.....	54
6.1.1.	Configuring On-demand.....	56
6.1.2.	Configuring RADIUS	73
6.1.3.	Configuring Local	78
6.1.4.	Configuring LDAP	79
6.1.5.	Configuring POP3	81
6.1.6.	Configuring NT Domain.....	82
6.1.7.	Configuring SIP	83
6.1.8.	Choosing Your Networks' Authentication method	85
6.2.	Users Group.....	87
6.2.1.	Assign users to a Group	88
6.2.2.	Permission in Service Zone	90
6.2.3.	QoS Traffic Class and Bandwidth Control.....	93

6.3.	User Login	94
6.3.1.	An Example of User Login	94
6.3.2.	Default Authentication	96
6.3.3.	Login with Postfix	96
7.	<i>Policies and Access Control</i>	97
7.1.	Policy	97
7.1.1.	Firewall	99
7.1.2.	Routing	104
7.1.3.	Schedule	105
7.1.4.	Session Limit	106
7.2.	User Access Control	107
7.3.	Session Limit & Session Log	111
8.	<i>Users' Login and Logout</i>	113
8.1.	Before User Login	113
8.1.1.	Login with SSL	113
8.1.2.	Internal Domain Name with Certificate	114
8.1.3.	Walled Garden	116
8.1.4.	Walled Garden AD List	117
8.1.5.	Mail Message	119
8.2.	After User Login	120
8.2.1.	Portal Home Page	120
8.2.2.	Idle Timer	121
8.2.3.	Multiple Login	122
8.2.4.	Change Password Privilege	123
8.2.5.	Proxy Server	124
9.	<i>Local Area AP Management</i>	126
9.1.	Multiple Type of AP	127
9.2.	Configure AP Template	128
9.3.	AP Discovery	131
9.3.1.	AP Background Discovery	133
9.4.	Manually add AP	134
9.5.	AP with Service Zone	135
9.6.	AP Security	137
9.7.	Change managed AP settings	138
9.8.	AP Operations from AP List	141
9.8.1.	Reboot, Enable, Disable and Delete the AP	141
9.8.2.	Apply Template	142
9.8.3.	Apply Service Zone (Tag-Based Only)	143
9.9.	Firmware management and upgrade	144
9.10.	WDS Management	145
9.11.	Rogue AP Detection	146
9.12.	AP Load Balancing	148
10.	<i>Wide Area AP Management</i>	151
10.1.	AP Discovery	152
10.2.	Manually add AP	153
10.3.	Manage AP Lists	154
10.4.	Manage Third Party AP	156
10.5.	Map	157
10.5.1.	Register key from Google	158
10.5.2.	Create a Map	159
10.5.3.	Marking APs on your Map	160
10.5.4.	Operations from Map page	163
10.6.	AP Operations from AP List	164
10.7.	WDS List	166
10.8.	Backup Config	167
10.9.	Firmware management and upgrade	168
10.10.	CAPWAP	169
11.	<i>Networking Features of a Gateway</i>	170
11.1.	DMZ	170
11.2.	Virtual Server	171

11.3.	Client Mobility	172
11.4.	DNS Cache	173
11.5.	Dynamic Domain Name Service	174
11.6.	Port and IP Forwarding.....	175
11.7.	Dynamic Route.....	176
12.	<i>System Management and Utilities</i>	179
12.1.	System Time	179
12.1.1.	NTP	179
12.1.2.	Manual Settings	180
12.2.	Management IP	181
12.3.	Access History IP	182
12.4.	SNMP.....	183
12.5.	Change Password.....	184
12.6.	Backup / Restore and Reset to Factory Default.....	185
12.7.	Firmware Upgrade.....	186
12.8.	Restart	187
12.9.	Network Utility	188
12.10.	Certificate	190
12.11.	Administrator Account.....	193
12.12.	Monitor IP.....	196
12.13.	Console Interface	197
13.	<i>System Status and Reports</i>	200
13.1.	View the Status	200
13.1.1.	System Status	201
13.1.2.	Interface Status	203
13.1.3.	HW	205
13.1.4.	Routing Table	206
13.1.5.	Online Users	207
13.1.6.	Non-Login Users	208
13.1.7.	Session List.....	209
13.1.8.	User Logs.....	210
13.1.9.	Local User Monthly Network Usage.....	212
13.1.10.	Logs	213
13.1.11.	DHCP Lease	214
13.2.	Notification	215
13.2.1.	SMTP Settings	216
13.2.2.	SYSLOG Settings	217
13.2.3.	FTP Settings	218
13.2.4.	Notification Settings	219
13.2.5.	System Report	222
14.	<i>Virtual Private Network (VPN)</i>	223
14.1.	Local VPN	223
14.2.	Remote VPN	227
14.3.	Site-to-Site VPN	228
15.	<i>Customization of Portal Pages</i>	230
15.1.	Customizable Pages	230
15.2.	Loading a Customized Login Page.....	231
15.3.	Using an External Login Page	234
15.4.	Load a Customized Logout Page	235
15.5.	How External Page Operates	236
15.6.	Disclaimer Page	251
16.	<i>Payment Gateways</i>	253
16.1.	Payments via Authorize.Net.....	253
16.2.	Payments via PayPal.....	257
16.3.	Payments via SecurePay	259
16.4.	Payments via WorldPay	261
17.	<i>Additional Applications</i>	264
17.1.	Upload / Download Local Users Accounts	264
17.2.	Backup / Restore and Upload New On-demand Users Accounts.....	265

17.3.	Account Roaming Out	266
17.4.	Seamless Cross Gateway Roaming	267
Appendix A. Certificate Settings for IE6 and IE7.....		269
Appendix B. Network Configuration on PC & User Login.....		278
Appendix C. Policy Priority.....		291
Appendix D. RADIUS Accounting.....		292
Appendix E. VLAN Port Location Mapping and PMS Middleware.....		299









1. Before You Start

1.1. Preface

This WHG Controller User Manual is for WLAN service providers or network administrators to set up a network environment using the WHG Controllers. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with basic network system knowledge to complete the installation.

Besides this document, there is a “Quick Installation Guide” (QIG), which is for starting up WHG Controller quickly. It is recommended to start with the QIG, and then refer to this manual for further details. Some special topics are addressed separately in the Appendixes.

1.2. Document Conventions

	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear what you have set before the settings are applied.
	The red asterisk indicates that information in this field is compulsory.
	Log out the system.
	Access Online Help interface.
	Access Home interface.
	Represents essential steps, actions, or messages that should not be ignored.
 Note:	Contains related information that corresponds to a topic.

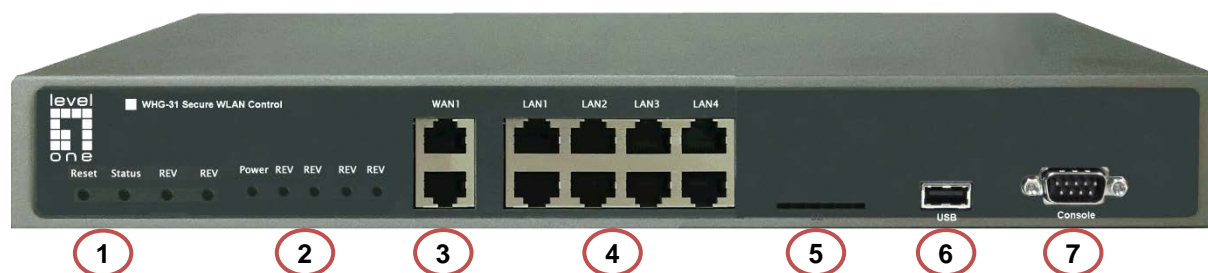
2. WHG Controllers Installation Guide

2.1. WHG Controller Capacity Table

Capacity	WHG-311	WHG-315	WHG-401	WHG-505	WHG-515	WHG-707
Form Factor	13" Mini-book	19" (1U)	19" (1U)	19" (1U)	19" (1U)	19" (1U)
WAN	2 x GbE	2 x GbE	2 x GbE	2 x GbE	2 x GbE	2 x GbE, 2 x Combo SFP
LAN	8 x GbE	8 x GbE	2 x GbE	2 x GbE	4 x GbE	4 x GbE, 2 x SFP
Local Accounts	3000	4000	5000	6000	10000	15000
On-demand Accounts	3000	4000	5000	6000	10000	15000
Managed AP Capacity (Local & Wide Combined)	30	50	150	200	250	500
LevelOne AP Model	EAP-110 EAP-200 EAP-300	EAP-110 EAP-200 EAP-300	EAP-110 EAP-200 EAP-300 OWL800	EAP-110 EAP-200 EAP-300 OWL800	EAP-110 EAP-200 EAP-300 OWL800	EAP-110 EAP-200 EAP-300 OWL800
Monitored IP	100	100	200	200	250	500
Service Zones	Default + 8	Default + 8	Default + 8	Default + 8	Default + 8	Default + 8
User Groups	8	8	16	24	24	24
User Policies	Global + 12	Global + 12	Global + 24	Global + 40	Global + 40	Global + 40

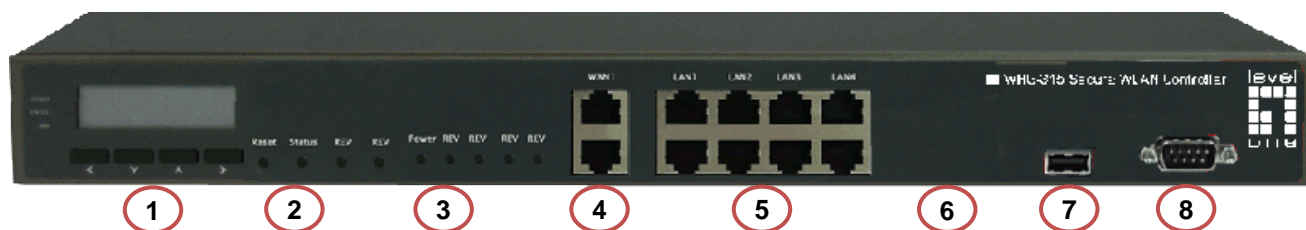
2.2. WHG Controller Hardware Overview

2.2.1. WHG-311 Hardware



1	Quick Buttons	<ul style="list-style-type: none">• Reset: Press and hold the Reset button for over 3 seconds and status of LED on front panel will start to blink, release button at this stage to restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will turn from blinking to off, release at this stage to reset the system to default configuration.• Quick-Restore: This button is the firmware switch button. Press this button while system is powering up and release when the “Quick-Restore” LED lights up, the system will switch to the other firmware image and boot up with that firmware.• Quick-VPN: Function reserved for future release.• Quick-Offload: Function reserved for future release.
2	LED Displays	<ul style="list-style-type: none">• Power: Power LED lights up as constant green when power supply is on.• Status: Status LED is Blue. Blinking indicates that system OS is booting up, when lit up constantly indicates that the system is ready for operation.• Quick-Restore: This is used to indicate that the system will now switch to the other F/W partition for operation.• Quick-VPN: Function reserved for future release.• Quick-Offload: Function reserved for future release.
3	WAN1/ WAN2	Two Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
4	LAN1~ LAN8	Eight Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).
5	SD Disk	Used for system storage, please do not remove during operation.
6	USB	Function Reserved for future use.
7	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.

2.2.2. WHG-315 Hardware

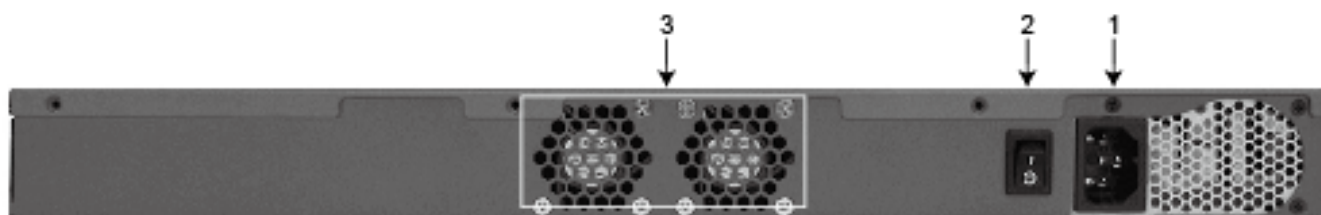


1	LCD Display	<ul style="list-style-type: none"> Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigations buttons from left to right respectively are “Sleep”, “Esc”, “Up”, “Down”, and “Enter”.
2	Quick Buttons	<ul style="list-style-type: none"> Reset: Press and hold the Reset button for over 3 seconds and status of LED on front panel will start to blink, release button at this stage to restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will turn from blinking to off, release at this stage to reset the system to default configuration. Quick-Restore: This button is the firmware switch button. Press this button while system is powering up and release when the “Quick-Restore” LED lights up, the system will switch to the other firmware image and boot up with that firmware. Quick-VPN: Function reserved for future release. Quick-Offload: Function reserved for future release.
3	LED Displays	<ul style="list-style-type: none"> Power: Power LED lights up as constant green when power supply is on. Status: Status LED is Blue. Blinking indicates that system OS is booting up, when lit up constantly indicates that the system is ready for operation. Quick-Restore: This is used to indicate that the system will now switch to the other F/W partition for operation. Quick-VPN: Function reserved for future release. Quick-Offload: Function reserved for future release.
4	WAN1/ WAN2	Two Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
5	LAN1~ LAN8	Eight Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).
6	SD Disk	Used for system storage, please do not remove during operation.
7	USB	Function Reserved for future use.
8	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.

2.2.3. WHG-401 Hardware



1	LED Indicators	There are three kinds of LED, Power , Status and Hard-disk , to indicate different status of the system.
2	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigation buttons from left to right respectively are “Esc”, “Up”, “Down”, and “Enter”.
3	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
4	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
5	USB	Reserved for future use.
6	Mgmt	For management use only, it always will open WMI (Web Management Interface) homepage.
7	WAN1/ WAN2	Two Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
8	LAN1/ LAN2	Two Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).

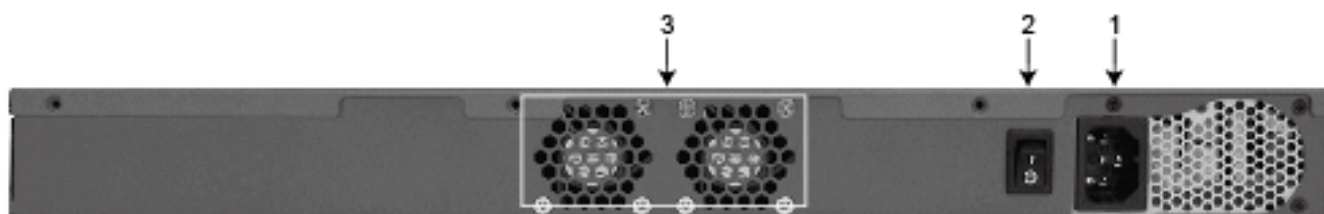


1	Power Supply Socket	Connecting the power cord to the built-in open-frame power supply (Input: 100~240 VAC, 50/60 Hz).
2	Power Switch	Power-On () & Power-Off (O).
3	Device Cooling Fan	Don’t block the cooling fans. Leave enough open space for ventilation.

2.2.4. WHG-505 Hardware

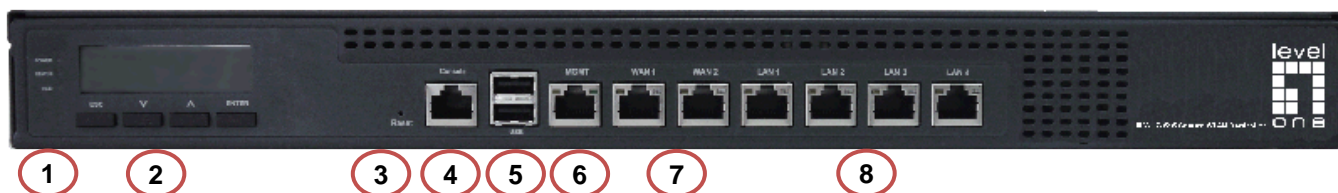


1	LED Indicators	There are three kinds of LED, Power , Status and Hard-disk , to indicate different status of the system.
2	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigations buttons from left to right respectively are “Esc”, “Up”, “Down”, and “Enter”.
3	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
4	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
5	USB	Reserved for future use.
6	Mgmt	For management use only, it always will open WMI (Web Management Interface) homepage.
7	WAN1/ WAN2	Two Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
8	LAN1/ LAN2	Two Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).



1	Power Supply Socket	Connecting the power cord to the built-in open-frame power supply (Input: 100~240 VAC, 50/60 Hz).
2	Power Switch	Power-On () & Power-Off (O).
3	Device Cooling Fan	Don’t block the cooling fans. Leave enough open space for ventilation.

2.2.5. WHG-515 Hardware



1	LED Indicators	There are three kinds of LED, Power , Status and Hard-disk , to indicate different status of the system.
2	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigations buttons from left to right respectively are “Esc”, “Up”, “Down”, and “Enter”.
3	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
4	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
5	USB	Reserved for future use.
6	Mgmt	For management use only, it always will open WMI (Web Management Interface) homepage.
7	WAN1/ WAN2	Two Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
8	LAN1 ~ LAN4	Four Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).



1	Power Supply Socket	Connecting the power cord to the built-in open-frame power supply (Input: 100~240 VAC, 50/60 Hz).
2	Device Cooling Fan	Don't block the cooling fans. Leave enough open space for ventilation.
3	Power Switch	Power-On () & Power-Off (O).

2.2.6. WHG-707 Hardware



1	WAN1/ WAN2 (SFP)	Two combo WAN ports (SFP) are connected to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
2	LAN5/ LAN6 (SFP)	Client machines connect to WHG Controller via these LAN ports (SFP).
3	LED Indicators	There are four kinds of LED, WAN1, WAN2, LAN4, and LAN5, to indicate the traffic status of the SFP ports.
4	WAN1/ WAN2	Two WAN ports (10/100/1000 Base-T RJ-45) are connected to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
5	LAN1 ~ LAN4	Client machines connect to WHG Controller via these LAN ports (10/100/1000 Base-T RJ-45).
6	USB	Reserved for future use.
7	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
8	LED Indicators	There are three kinds of LED, Power, Status and Hard-disk, to indicate different status of the system.
9	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigations buttons from left to right respectively are "Esc", "Up", "Down", and "Enter".



1	Power Supply Socket	Connecting the power cord to the built-in open-frame power supply (Input: 100~240 VAC, 50/60 Hz).
2	Power Switch	Power-On () & Power-Off (O).
3	Device Cooling Fan	Don't block the cooling fans. Leave enough open space for ventilation.

2.3.Preparation before the Installation

Before you start the installation by either following this User Manual or the Quick Installation Guide, below is a short preparation list to do.

1. Unpack the WHG Controller and go through the package checklist.
2. Review the front panel and the back panel and identify each control and network interface that is described in the Hardware & Specification section.
3. Prepare Ethernet cables with RJ-45 connectors.
4. Prepare a PC with Web browser for accessing the Web Management Interface.
5. Identify an upstream device for WHG Controller to connect to in your network, such as ADSL, CABLE modem or other edge devices. Collect the DNS server address provided by your ISP.

If you are using WHG Controller product for the first time, it is recommended that you follow the Quick Installation Guide to start up the WHG Controller in a near default state with minimum configuration changes (such as WAN settings and admin password), then refer to this manual later when you want to configure the system for specific application needs.

The recommended general steps for the configuration are:

- ♦ Set up system's Time Zone, NTP server, DNS server and WAN1 address
- ♦ Configure LAN address range for at least one Service Zone, and enable its authentication. The Default Service Zone is enabled to require authentication by the factory default.
- ♦ Create user accounts to test the login page via wire line in the enabled Service Zone.
- ♦ Try to generate on-demand user and test the account.
- ♦ Configure Wireless Settings of Service Zone, then add in AP.
- ♦ Configure more Service Zones base on your application.
- ♦ Set up Group and Policy (including Firewall rules and Session Limit).
- ♦ Customize the portal login page and add walled garden Advertisement links if needed.
- ♦ Set up Payment gateway if you want to use credit card for the on-demand accounts.
- ♦ Load SSL certificate for the Web Server before operation.
- ♦ Monitor the status pages and reports generated.
- ♦ Perform other advanced setting for your specific application.

2.4. Unpacking & Installing

2.4.1. WHG-311 Package & Installation

▪ Package Checklist

The standard package of WHG-311 includes:

- ♦ WHG-311 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 Console Cable x 1
- ♦ Ethernet Cable x 1
- ♦ Power Adaptor (12VDC, 2A) x 1



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

▪ Installation

- Connect the power adaptor to the power socket on the rear panel. The Power LED should be on to indicate a proper connection.
- Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
- Connect an Ethernet cable to a LAN Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the system. Connect an Ethernet cable to the LAN1 or LAN2 Port on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

2.4.2. WHG-315 Package & Installation

▪ Package Checklist

The standard package of WHG-315 includes:

- ♦ WHG-315 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 Console Cable x 1
- ♦ Ethernet Cable x 1
- ♦ Power Cord x 1

- ♦ Rack Mounting Bracket (with Screws) x 1



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

▪ Installation

- Connect the power cord to the power socket on the rear panel.
- Turn on (|) the power switch on the rear panel. The Power LED should be on to indicate a proper connection.
- Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
- Connect an Ethernet cable to a LAN Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the system. Connect an Ethernet cable to the LAN1 or LAN2 Port on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

2.4.3. WHG-401 Package & Installation

▪ Package Checklist

The standard package of WHG-401 includes:

- ♦ WHG-401 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 to RJ45 Console Cable x 1
- ♦ Ethernet Cable x 1
- ♦ Straight-through Ethernet Cable x 1
- ♦ Power Cord x 1
- ♦ Rack Mounting Bracket (with Screws) x 1



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

▪ Installation

- Connect the power cord to the power socket on the rear panel.
- Turn on (|) the power switch on the rear panel. The Power LED should be on to indicate a proper connection.
- Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
- Connect an Ethernet cable to the Mgmt Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the system. Connect an Ethernet cable to the LAN1 or LAN2 Port on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for

connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

2.4.4. WHG-505 Package & Installation

▪ Package Checklist

The standard package of WHG-505 includes:

- ♦ WHG-505 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 to RJ45 Console Cable x 1
- ♦ Ethernet Cable x 1
- ♦ Straight-through Ethernet Cable x 1
- ♦ Power Cord x 1
- ♦ Rack Mounting Bracket (with Screws) x 1



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

▪ Installation

1. Connect the power cord to the power socket on the rear panel.
2. Turn on (|) the power switch on the rear panel. The Power LED should be on to indicate a proper connection.
3. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
4. Connect an Ethernet cable to the Mgmt Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the system. Connect an Ethernet cable to the LAN1 or LAN2 Port on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

2.4.5. WHG-515 Package & Installation

▪ Package Checklist

The standard package of WHG-505 includes:

- ♦ WHG-515 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 to RJ45 Console Cable x 1

- ♦ Ethernet Cable x 1
- ♦ Straight-through Ethernet Cable x 1
- ♦ Power Cord x 1
- ♦ Rack Mounting Bracket (with Screws) x 1



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

▪ Installation

- Connect the power cord to the power socket on the rear panel.
- Turn on (|) the power switch on the rear panel. The Power LED should be on to indicate a proper connection.
- Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
- Connect an Ethernet cable to the Mgmt Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the system. Connect an Ethernet cable to the LAN1 or LAN2 Port on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

2.4.6. WHG-707 Package & Installation

▪ Package Checklist

The standard package of WHG-707 includes:

- ♦ WHG-707 x 1
- ♦ CD-ROM (with User's Manual and QIG) x 1
- ♦ Quick Installation Guide (QIG) x 1
- ♦ RS-232 DB9 Console Cable x 1
- ♦ Ethernet Cable x 2
- ♦ Power Cord x 1
- ♦ Rack Mounting Bracket (with Screws) x 1



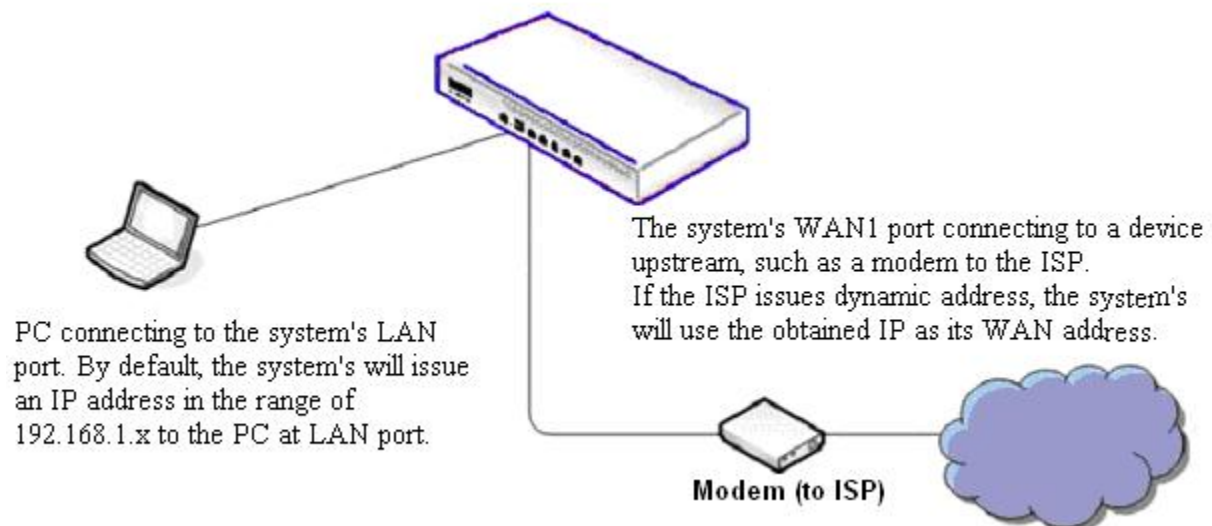
It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

▪ Installation

1. Connect the power cord to the power socket on the rear panel.
2. Turn on the power switch on the rear panel.
3. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
4. Connect an Ethernet cable to the LAN Ports on the front panel; connect the other end of the Ethernet cable

to an administrator PC for configuring the WHG Controller system. Connect an *Ethernet* cable to the LAN1 or LAN2 Port on the front panel; connect the other end of the Ethernet cable to an AP for extending wireless coverage, a switch for connecting more wired clients, or a client PC. The LED of this port should be on to indicate a proper connection.

Start with this simple network topology to set up WHG Controller for the first time; it helps to plan a more sophisticated network topology to suits your specific application needs later.



【A simple network diagram for the initial setup】

3. System Overview

3.1. System Concept

If you have experienced other LevelOne WLAN WHG Controller products before and are familiar with its system concept, you may skip the concept description below. **Please proceed to the next section on (Getting Started).**

WHG Controller is capable of managing user authentication, authorization and accounting (AAA). The user account information is stored in the local database or a specified external database server. Featured with user authentication and integrated with external payment gateway, WHG Controllers allows users to easily pay the fee and enjoy the Internet service using credit cards through Authorize.Net, PayPal, SecurePay, or WorldPay.

With centralized AP management feature, the administrator does not need to worry about how to manage multiple wireless access point devices. WHG Controllers and LevelOne APs combined provides flexible network solution which supports overlay deployment where traffics from remote sites are tunnelled back and centrally controlled by WHG Controller.

Furthermore, WHG Controller introduces the concept of Service Zones - multiple virtual networks, each with its own definable access control profiles. This is very useful for hotspot owners seeking to provide different customers or staff with different levels of network services.

The following portion of this section explains the basic concepts of WHG Controller. With the understanding of these concepts, the administrator will be able to do more advanced network planning and to manipulate the configurations of WHG Controller to suit his own specific application. It is sufficient for most of administrators to use the default configuration with minor WAN/DNS address changes for simple deployments.

Gateway is a network node where a small network attaches to a bigger network. WHG Controller is a kind of gateway in a network environment; hence it has those features a typical gateway has, such as NAT, DHCP, DMZ, Firewall and etc. Conventionally, the bigger network is referred as the gateway's **WAN side** or upstream network, while the small network is referred as the gateway's **LAN side**. The Ethernet ports leading to the WAN side network is called **WAN ports**. The Ethernet ports leading to the LAN side network is called **LAN ports**.

Local User is a type of user with its account credential stored in a built-in database named "Local" within WHG Controller. The WHG Controller's "Local" database capacity varies with different model. A local user account does not have an expiration date once they are created. If administrator wishes to terminate the account, he must remove it manually from the database. A local database can be used as an external RADIUS database for another WHG Controller product for account roaming.

On-demand User is a type of user with its account credential stored in a built-in database named "On-demand" within WHG Controller. The WHG Controller's "On-demand" database capacity varies with different model.. On-demand User is used for short term usage purpose; it has an expiration period. An on-demand account record will be recycled for creating new on-demand account if it has expired for over 15 days or has been deleted by the

Administrator/Manager manually.

External Authentication Database is a user account database that is not built inside WHG Controller. Besides Local database and On-demand database, WHG Controller allows up to three additional External Authentication databases simultaneously. The types of external Authentication databases supported are RADIUS, POP3, LDAP (including Active Directory), and NTDomain (Win2K's NTDS). The database of another WHG Controller device can be used as an external RADIUS database. External Authentication Database is useful for implementing account roaming; for example, multiple WHG Controller devices in multiple campuses can share one common external database. A user needs only one account in the common database to access the network from different campuses.

Service Zone is a logic partition of WHG Controller's LAN network. The concept of Service Zone is similar to the concept of virtual LAN (VLAN), which can be used to group the network traffic or network services for clients on the same VLAN segment, regardless of the clients' physical locations. That is, several VLAN segments may be in service at one physical network location as well as devices belonging to one VLAN segment may spread across multiple physical locations.

Each Service Zone can also be viewed a virtual machine of WHG Controller because each Service Zone can define its own customized login portal page, and its own gateway properties (such as LAN IP address, DHCP on/off and address range). The feature of Multiple Service Zone is also useful to service multiple hotspot franchises in shopping malls or airport terminals by a single WHG Controller.

A Service Zone is uniquely defined by a VLAN tag id (under Tag-Based) and an associated SSID attribute. When a managed access point (MAP) is added to a Service Zone through WHG Controller's AP Management feature by the administrator, the associated SSID will be activated in the MAP along with the VLAN tag of the corresponding Service Zone.

For example, in the following Figure 2, the administrator plans three logical Service Zones for an academic campus:

- ♦ The first Service Zone (with SSID='Student', and VLAN tag=1) is for students.
- ♦ The second (with SSID='Faculty' and VLAN tag=2) for faculties.
- ♦ The third (SSID='Guest' and VLAN tag=3) for guests.

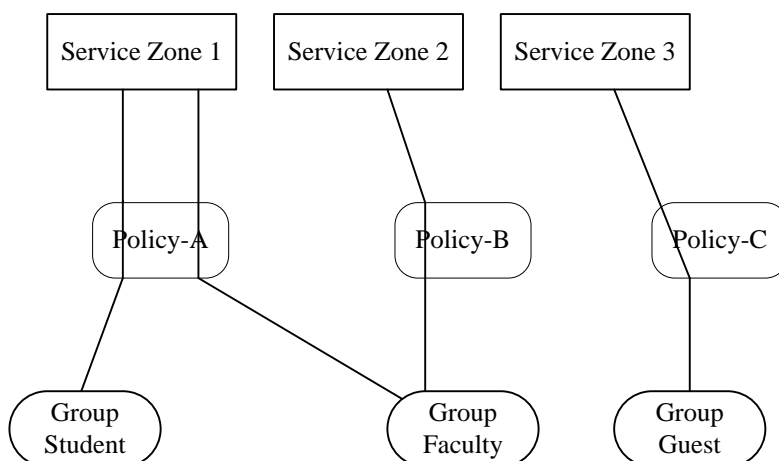
A Service Zone may or may not require client authentication, depending on how the administrator sets it up. If a Service Zone requires user authentication, the client will be prompted for the login in first before using the network services, no matter whether the client is connecting to its SSID wirelessly or a switch port via wired line,.

Group is a group of user accounts sharing the same access privileges, QoS properties and network policies. Each client account belongs to a Group. Each Group may or may not be allowed to access a particular Service Zone, depending on the how the administrator define its access mapping. If the administrator does not assign a new account to any specific Group, the account belongs to a catch-all group named "**None**" by default.

Policy is for defining rules, privileges or properties for managing users. Each user group is bound by a Policy within a given Service Zone. The same group may or may not be bound to the same policy in different Service zones. There are two tiers of Policies. The first tier is a policy named 'Global-Policy'. The Global-Policy is a base policy which will be applied to all users if not applied with another policy. The second tier is called 'Group-Policy' or simply

'Policy', which can be chosen to bound the network behaviors of a Group. The administrator can define the Firewall Profile, Route Profile, Schedule Profile and Max Sessions in a Policy.

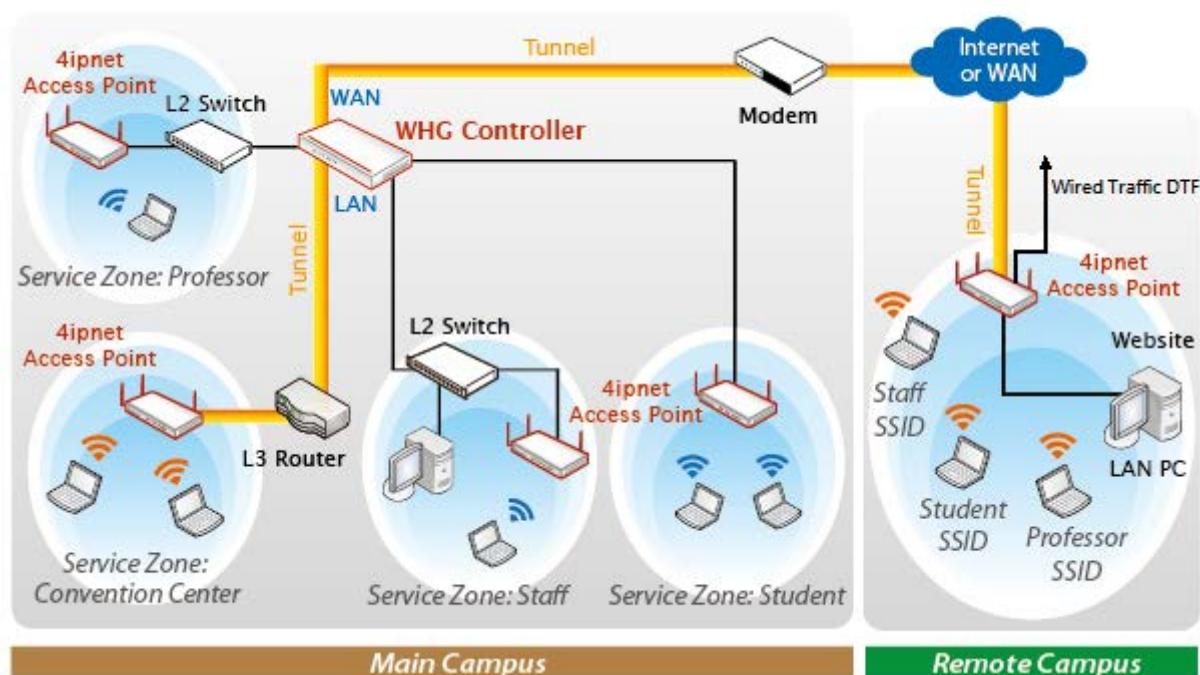
The following Figure depicts an example relationship of Service Zone, Group and Policy. In this example, Students and faculties logging into Service Zone 1 will be governed by Policy-A. Guests only have the access of Service Zone 3, and will be bounded by Policy-C. Faculties have the access to both Service Zone 1 and Service Zone 2 under two different policies.



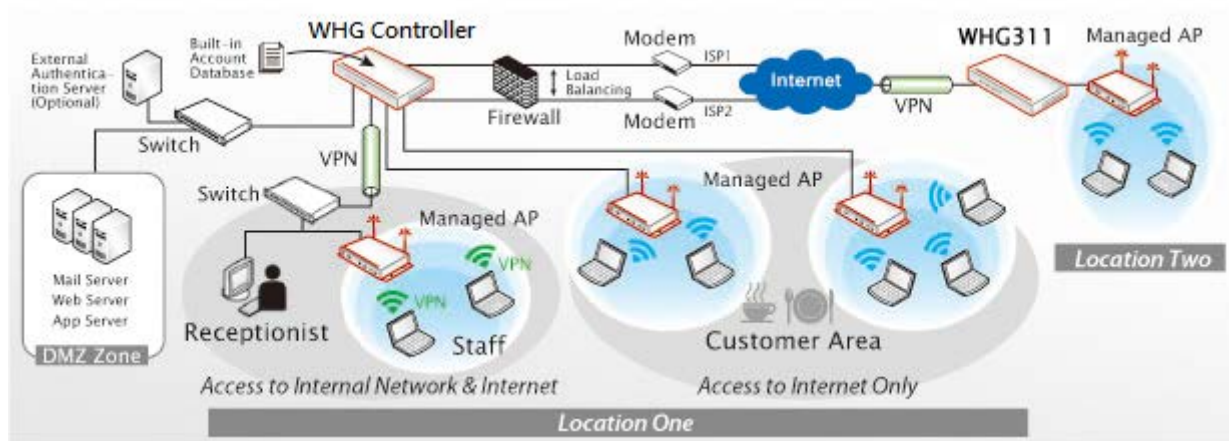
An example relationship of Service Zone, Group and Policy

The following Figure depicts an example using WHG Controller in managing network/internet access in an academic campus environment. Imagine the network administrator may wish to set different privileges and bandwidth limits for staff, students, and professors; he could use several Service Zones of WHG Controller – one for staff, one for students, and one for the professors. He also uses one zone for some shared servers in the diagram.

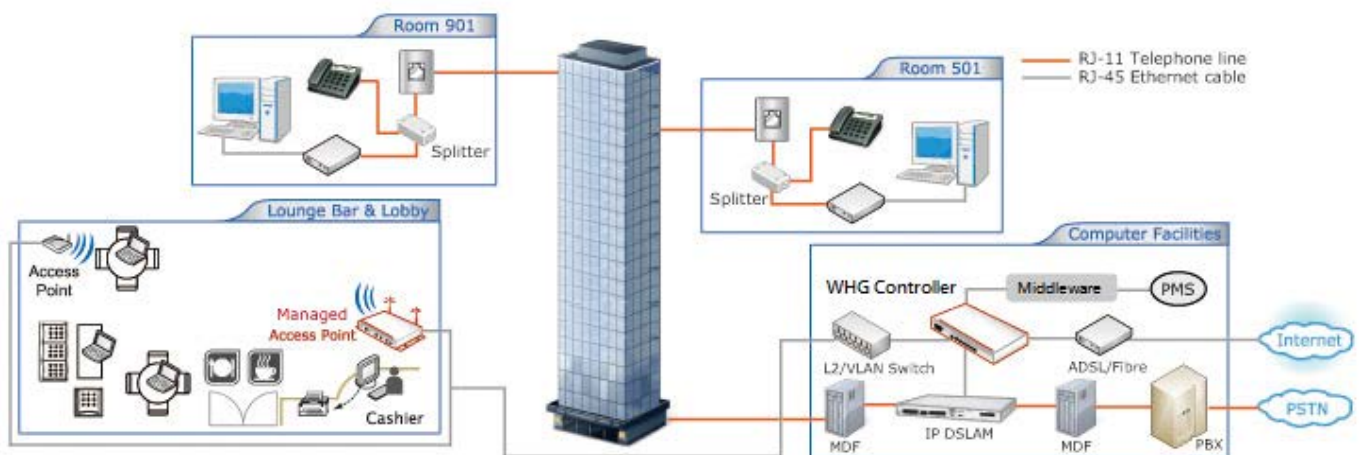
There traffic of students, professors, and guests can be segregated by thereby different VLAN segments.



An example of managed network in a Campus environment



WHG Controller in a Business Headquarter



WHG Controller in a Hotel – Capable of integrating with DSLAM and PMS

3.2. Service Zone Concept

LevelOne Service Zones are virtual machines that has its' own network interface, DHCP server, authentication configuration, user pages as well as security and user policy settings.

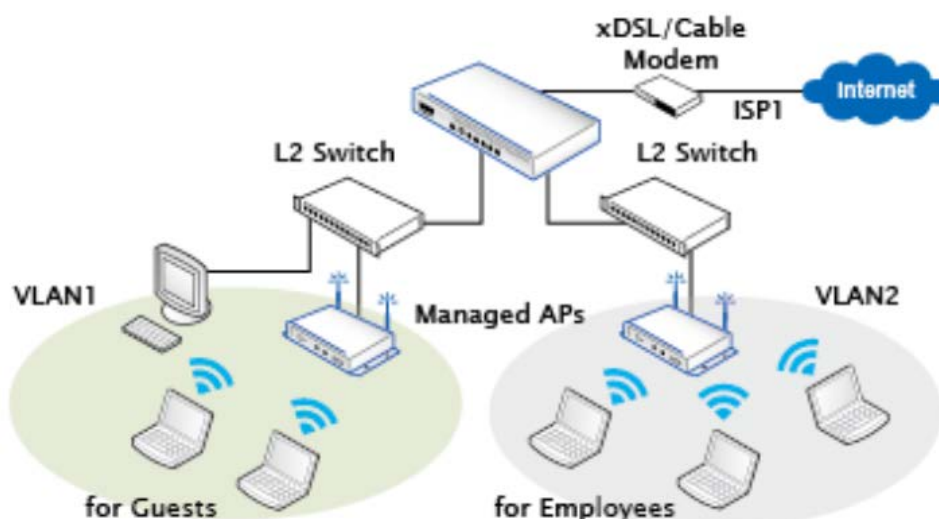
By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical networks isolated from one another. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc.

There are nine Service Zone profiles in total, Default Service Zone and Service Zones 1 ~ 8.

Service Zone Settings							
Service Zone Name	SSID	Applied Policy	IP Address	Network Alias	DHCP Pool	VLAN Tag	Details
	WLAN Encryption	Default Authen Option	IPv6 Address			Status	
Default	SSID0	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100	N/A	Configure
	None	Server 1	N/A			Enabled	
SZ1	SSID1	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100	1	Configure
	None	Server 1	N/A			Disabled	

■ Simple network environment

For most simple internal network, such as there are just only two subnets. Using Port-Based model is an easy and better way. In **Port-Based** mode (configurable in Port Location Mapping tab page), 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 **Employees** and one for **Guests**.

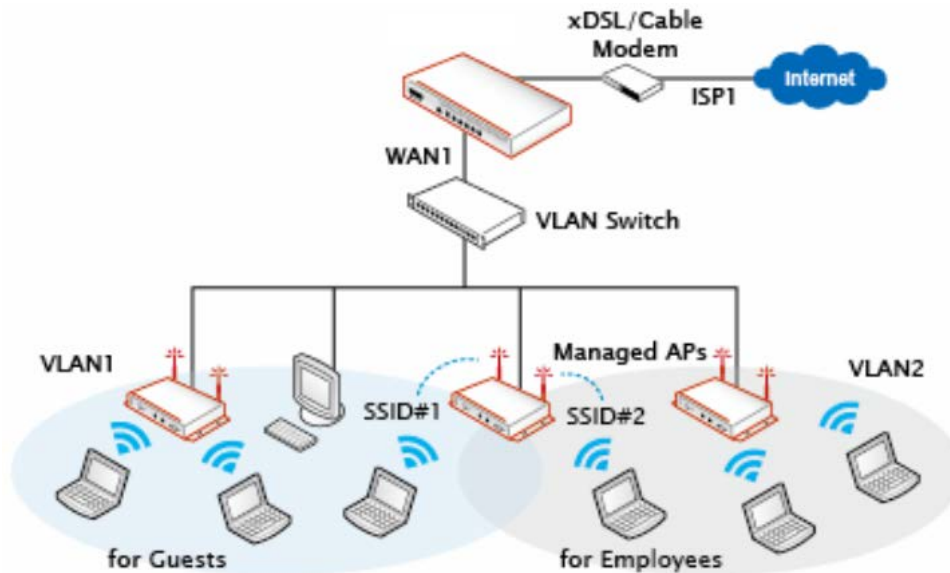


The switches deployed under Controller in Port-Based mode must be Layer 2 switches only.

■ Multi subnet network environment

On the other hand, if the internal network is a **Multi subnets network environment**, Tag-Based model will satisfy to your conditions. In **Tag-Based** mode, each LAN port will serve traffics from different Service Zones; a VLAN switch or VLAN AP is required to take care of the VLAN tags carried within the message frames.

An example of network application diagram is shown as below: more than two Service Zones for different departments.

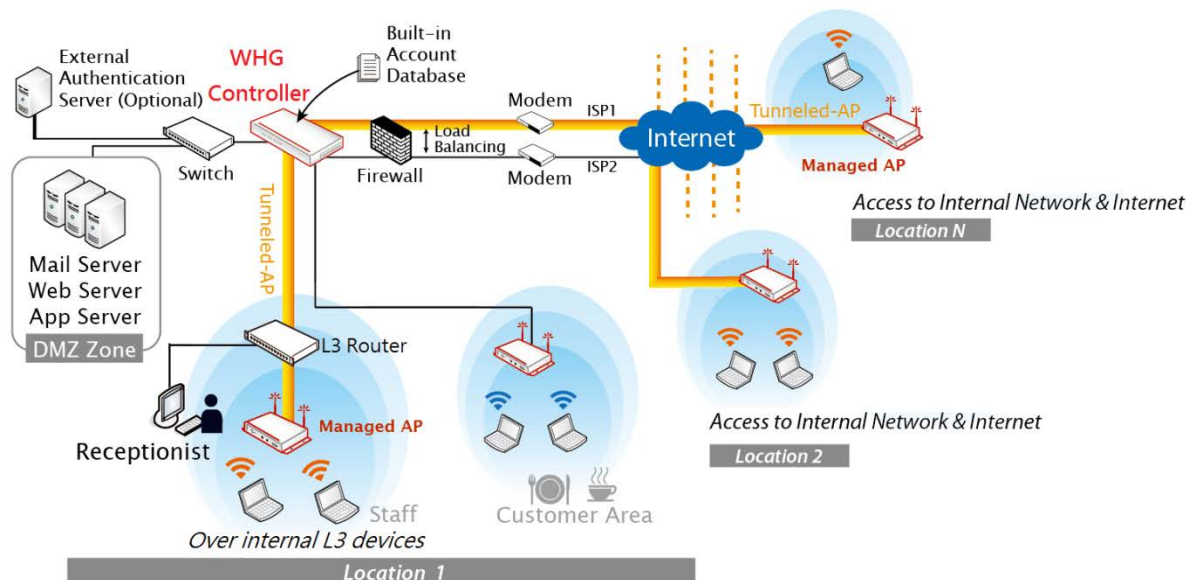


The switch deployed under Controller in **Tag-Based** mode must be a **VLAN switch** only.

3.3. AP Management Concept

AP Management feature is designed not only for internal network AP deployment, but also overlay deployment at remote locations over the cloud.

WHG Controllers can manage from 30 to 500 LevelOne Access Points depending on model. For overlay AP deployment, WHG Controllers establish a secure tunnel between the managed AP and Controller.



Certain AP models with additional Ethernet ports can also provide wired network service. When managed remotely over the internet, the APs wired user traffic can be forwarded into the internet without having to be tunneled back and centrally forwarded by the AC. This feature is an example of Distributed Traffic Forwarding (DTF).

4. Getting Started

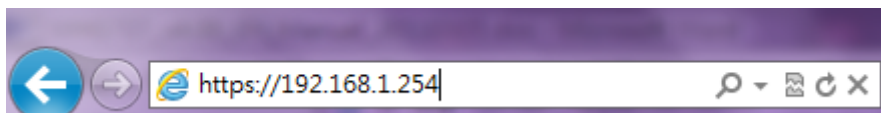
4.1. Accessing Web Management Interface

When you have completed the hardware installation of your WHG Controller, system configurations can be performed via built-in Web Management Interface (WMI).

Step 1. Connect your PC to any of the LAN ports of your WHG Controller.

Step 2. Set the TCP/IP settings on your PC to “Obtain an IP address automatically”.

Step 3. Launch a web browser and enter the WHG Controller’s default LAN IP address “192.168.1.254”. If you are connected to a Mgmt port (WHG-401, WHG-505, WHG-515) please enter the mgmt port IP address “172.30.0.1”.



Step 4. Enter the default administrator account and password “admin” to login. Once logged into the WMI, the system’s Home Page will be displayed.



If your PC is connecting to the LAN port, and you can't get the Administrator's login screen, the reasons may be:

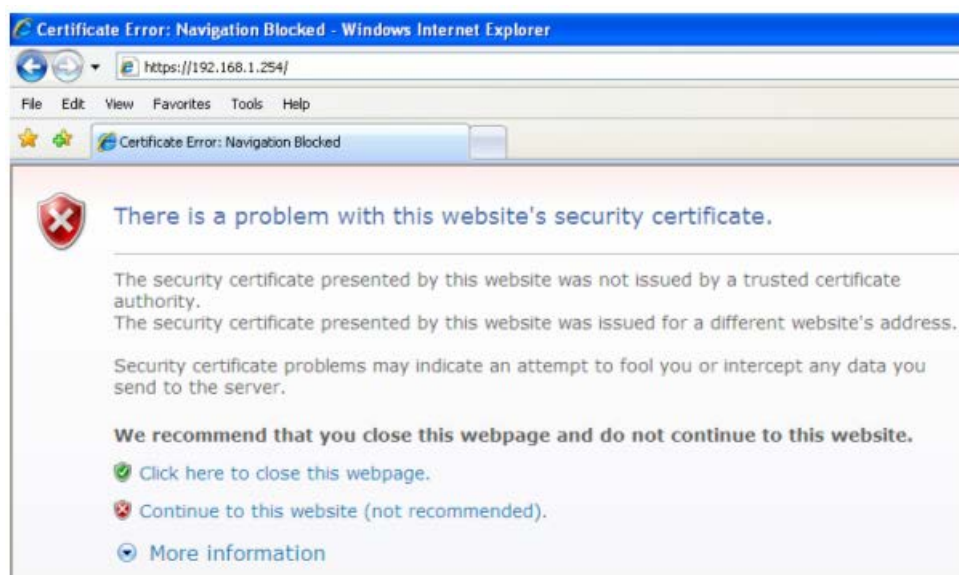
- (1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the built-in DHCP Server;*
- (2) The IP address and the default gateway are not under the same network segment.*

Please use default IP address such as 192.168.1.xx in your network and then try again.

After a successful login, a Home Page will appear on the screen.



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



4.2.Home Page

Home page lists four buttons **Setup Wizard**, **Quick Links**, **System Overview** and **Main Menu** respectively. Each button will be described in detail in the following section.



4.2.1. Setup Wizard

Using the configuration wizard

Configuration wizard provides a fast and easy way to configure the WHG Controller's system time, change Administrator password, WAN interfaces, as well as local user accounts. Follow the instructions given at each step to change the system admin password, select time zone, configure WAN1 interface, and create local user account (optional). Upon completing the Setup Wizard procedures, the system needs to be restarted to have the settings take effect. The system is ready for operation after restart with minimal configurations.

■ Running the Wizard

Click **Setup Wizard** button from the Home page and the **Setup Wizard** page will appear.

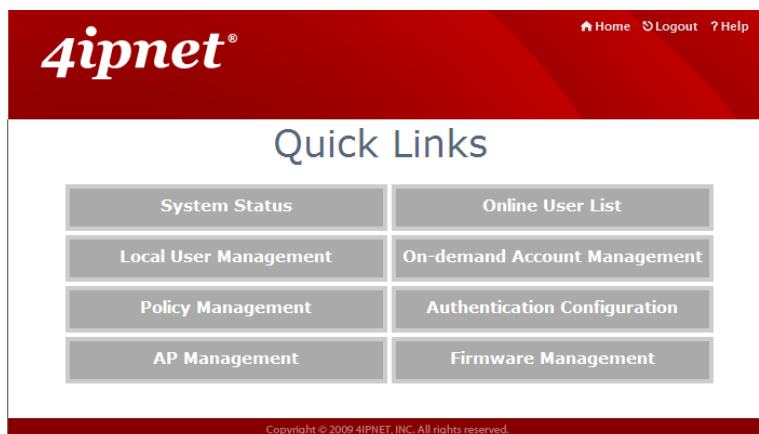
Please read tips provided for each step to complete the configuration.



The screenshot shows the 4ipnet Setup Wizard interface. At the top is a red header with the 4ipnet logo and navigation links: Home, Logout, and Help. The main content area is titled "Setup Wizard" and "General". On the left, there is a sidebar with five buttons: Step 1 (highlighted in orange), Step 2, Step 3, Step 4, and Exit. Below Step 1, a note reads: "It is recommended to change administrator's password and select an appropriate time zone for the system." The main form area contains three fields: "New Password:" with a masked input field, "Verify Password:" with a masked input field, and "Time Zone:" with a dropdown menu showing "(GMT+08:00)Taipei". A "Next" button is located below the Time Zone field. At the bottom of the page, a small copyright notice reads: "Copyright © 2009 4IPNET, INC. All rights reserved."

4.2.2. Quick Links


The **Quick Links** provide eight shortcut links for administrators to directly access frequently used functions of the web management interface. The eight functional links are: **System Status**, **Local User Management**, **Policy Management**, **AP Management**, **Online User List**, **On-demand Account Management**, **Authentication Configuration** and **Firmware Management**.



4.2.3. System Overview


This page displays important system related information that the administrator might need to be aware of at a glance, which includes General System settings, Network Interface and Online Users etc. A drop-down menu is available for selecting the information refresh rate for this page.

System Overview




System

System Time	2011/06/13 14:36:20+0800
Up Time	25 days, 2:59
F/W Version	5.00.00



Access Points


Total Managed	0
Down	0
Associated Clients	0



Network Interfaces


	IP Address	Status
WAN1	172.28.0.254	↓ Down
WAN2	118.168.240.65	↓ Down

	IP Address	SSID	Status
testszo	192.168.1.254	sz0ssid	Enabled
SZ1	172.21.0.254	SSID1	Enabled
SZ2	172.22.0.254	SSID2	Disabled
SZ3	172.23.0.254	SSID3	Disabled
SZ4	172.24.0.254	SSID4	Disabled
SZ5	172.25.0.254	SSID5	Disabled
SZ6	172.26.0.254	SSID6	Disabled
SZ7	172.27.0.254	SSID7	Disabled
SZ8	172.28.0.254	SSID8	Disabled




Wide Area APs

Total Managed	0
Down	0
Active WDS Links	0
Backup Links	0
Disconnected Links	0



Users

Total Online	0
On-demand	0



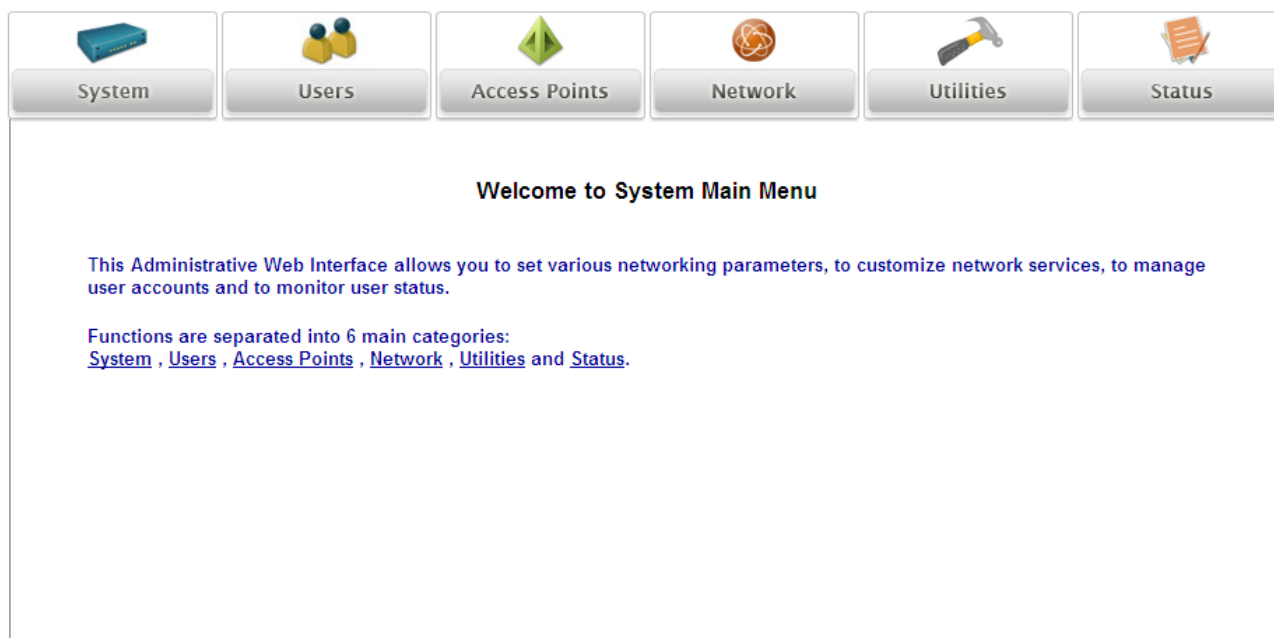
VPN Sessions

Local VPN	0
Remote VPN	0

Refresh every seconds

4.2.4. Main Menu

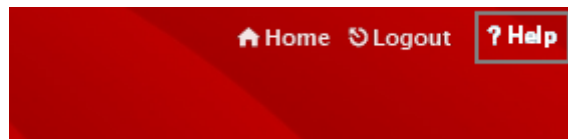
This feature leads to all the detailed configuration pages on the Web Management Interface, allowing you to set various networking parameters, enable and customize network services, manage user accounts and monitor user status. Administration functions are separated into 6 categories: **System**, **Users**, **Access Points**, **Network**, **Utilities** and **Status**.



4.2.5. Online Help

The **Help** button is at the upper right corner of the WHG Controller display screen.

Click **Help** for the **Online Help** window, and then click the hyperlink of the relevant information required.



Online Help Corner

5.Initial Network Setup

5.1. Network Requirement

Typically, in a network environment, WHG Controller plays the role of a gateway. On a gateway device, a network port leading upstream to the Internet or the backbone network is called a ‘WAN port’ or an uplink port, while a network port used for branching out to the service the clients downstream is referred as ‘LAN port’.

WHG Controller consists of two WAN ports, which are normally linked up to different routers or modems leading to ISP. A gateway needs one WAN port only, but if you want dual-homing or dual -uplink to add reliability and throughput, the second WAN port lets you achieve that goal.

5.2. Managing System Date & Time

Go to Main Menu > System > General page. The system time can be configured manually or calibrated automatically through external NTP Servers. Accurate system time is critical when it comes to billing and online payment.

Calibrate system time using NTP servers, fill in at least one valid NTP server address and apply.

Time	System Time : 2011/05/09 17:14:31	
	Time Zone :	
	<div>(GMT+08:00)Taipei</div>	
	<input checked="" type="radio"/> NTP	
	NTP Server	1: <div>tock.usno.navy.mil</div> <small>*(e.g. tock.usno.navy.mil)</small>
	NTP Server	2: <div>ntp1.fau.de</div>
	NTP Server	3: <div>clock.cuhk.edu.hk</div>
	NTP Server	4: <div>ntp1.pads.ufrj.br</div>
	NTP Server	5: <div>ntp1.cs.mu.OZ.AU</div>
	<input type="radio"/> Manually set up	

Manually set system time and apply.

Time	System Time : 2011/05/09 17:14:31	
	Time Zone :	
	<div>(GMT+08:00)Taipei</div>	
	<input type="radio"/> NTP	
	<input checked="" type="radio"/> Manually set up	
	<div>2011<div>▼</div>Year05<div>▼</div>Month09<div>▼</div>Day</div> <div>16<div>▼</div>Hour23<div>▼</div>Minute00<div>▼</div>Second</div>	

5.3. WAN1 & WAN2 Setup

WHG Controllers are designed with 2 WAN ports for load balancing and failover support. To configure WAN port settings, go to Main Menu > System > WAN1 / WAN2.

➤ WAN1

WAN1 port supports four connection types: **Static**, **Dynamic**, **PPPoE** and **PPTP**. These connection types are enough to support most ISP.

WAN1 Interface Setting	
WAN1	<input type="radio"/> Static (Use the following IP settings)
	<input checked="" type="radio"/> Dynamic (IP settings assigned automatically) Renew
	<input checked="" type="checkbox"/> Learn DNS Server Address During Negotiation.
	Preferred DNS Server: <input type="text" value="168.95.1.1"/>
	Alternate DNS Server: <input type="text"/>
	<input type="radio"/> PPPoE
	<input type="radio"/> PPTP

Depending on ISP or the upstream device the WAN port connects, you only need to select one connection type for the port. For example, if your ISP is Cable modem issuing Dynamic address, then you would select Dynamic connection when setting up the WAN ports.

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

- **IP Address:** The IP address of the WAN1 port.
- **Subnet Mask:** The subnet mask of the WAN1 port.
- **Default Gateway:** The gateway of the WAN1 port.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

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

- **Learn DNS Server Address During Negotiation:** When this check box is selected, the Controller will automatically learn the IP address of DNS server through DHCP messages received.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

PPPoE: If your ISP provides PPPoE Dialup connection, then the ISP will issue you an account with a password. You would need to enter the account credential in the WAN configuration page for dialing up to the ISP.

- **Username:** The username issued by your ISP as dial-up account.
- **Password:** The dial-up password issued by your ISP.
- **MTU:** Maximum Transmission Unit of a PPPoE frame. The PPPoE protocol allows an Ethernet frame's size to be up to 1492 bytes, but some ISP's network equipments may support a smaller frame size of than

1492 bytes. In that case, you have to enter a smaller number MTU number to meet the ISP's networking requirement.

- **Clamp MSS:** Short for Maximum Segment Size for a TCP connection. An end-to-end TCP connection over PPPoE will consume additional overhead out of each packet. At least 40 bytes are used for the address. Hence, MSS must be smaller than MTU by at least 40.
- **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.
- **Learn DNS Server Address During Negotiation:** When this check box is selected, the Controller will automatically learn the IP address of DNS server through DHCP messages received.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

PPTP: Although not a popular method, PPTP protocol for dialup connections is adapted by some ISPs (in European Countries). Your PPTP ISP will issue you an account with a password as well as the PPTP server address.

- **Type:** Select **Static** or **DHCP**. Select **Static** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically.
- **PPTP Server IP Address:** Specify your ISP's PPTP server IP address.
- **Username:** The username issued by your ISP as dial-up account.
- **Password:** The dial-up password issued by your ISP.
- **PPTP Connection ID:**
- **Dial on demand** function under PPTP: If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.

➤ WAN2

If you want to use a second Internet feed, select one of the three connection types for your WAN2 port: **Static**, **Dynamic**, and **PPPoE**. Please note that WAN load balancing and WAN failover features are only available when WAN2 is configured.

WAN2 Interface Setting	
WAN2	<p><input checked="" type="radio"/> None</p> <p><input type="radio"/> Static (Use the following IP settings)</p> <p><input type="radio"/> Dynamic (IP settings assigned automatically)</p> <p><input type="radio"/> PPPoE</p>

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

- **IP Address:** The IP address of the WAN1 port.
- **Subnet Mask:** The subnet mask of the WAN1 port.
- **Default Gateway:** The gateway of the WAN1 port.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

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

- **Learn DNS Server Address During Negotiation:** When this check box is selected, the Controller will automatically learn the IP address of DNS server through DHCP messages received.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

PPPoE: If your ISP provides PPPoE Dialup connection, then the ISP will issue you an account with a password. You would need to enter the account credential in the WAN configuration page for dialing up to the ISP.

- **Username:** The username issued by your ISP as dial-up account.
- **Password:** The dial-up password issued by your ISP.
- **MTU:** Maximum Transmission Unit of a PPPoE frame. The PPPoE protocol allows an Ethernet frame's size to be up to 1492 bytes, but some ISP's network equipments may support a smaller frame size of than 1492 bytes. In that case, you have to enter a smaller number MTU number to meet the ISP's networking requirement.
- **Clamp MSS:** Short for Maximum Segment Size for a TCP connection. An end-to-end TCP connection over PPPoE will consume additional overhead out of each packet. At least 40 bytes are used for the address. Hence, MSS must be smaller than MTU by at least 40.
- **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.
- **Learn DNS Server Address During Negotiation:** When this check box is selected, the Controller will automatically learn the IP address of DNS server through DHCP messages received.
- **Preferred DNS Server:** Statically designate the primary DNS server to be used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

5.4. WAN Traffic Control

WAN Bandwidth

The entire system's uplink and downlink bandwidth can be customized. Go to Main Menu > System > WAN Traffic

WAN Traffic Settings			
Available Bandwidth on WAN Interface	<input checked="" type="checkbox"/> Enable Bandwidth limitation on WAN		
	Uplink	<input type="text" value="2000000"/>	Kbps *(Range: 10-2000000)
	Downlink	<input type="text" value="2000000"/>	Kbps *(Range: 10-2000000)

The Uplink and Downlink bandwidth configured here is the combined bandwidth for WAN1 and WAN2. However, please note that the actual bandwidth is still bounded by the network speed of your ISP operator. For instance the network speed of your ISP is limited to 1Gbps, then the total throughput will not be greater than 1Gbps even if you configure 2Gbps on the Controller.

WAN Failover & Load Balancing

When both WAN1 and WAN2 are properly configured with uplink to the internet, WAN failover and Load Balancing feature becomes available.

WAN Failover & Connection Detection	
	<div>Target for detecting Internet connection</div> <div>IP/Domain Name <input type="text"/></div> <div>IP/Domain Name <input type="text"/></div> <div>IP/Domain Name <input type="text"/></div> <div> <input type="checkbox"/> Enable Load Balancing <input type="checkbox"/> Enable WAN Failover <input type="checkbox"/> Warning of Internet Disconnection </div>

Load Balancing: Administrator can spread the system traffic across WAN1 and WAN2 ports based on percentage load, calculated using session, bytes, or packets.

☒ Enable Load Balancing
 WAN1 Weight: *(Range: 1-99)
☐ Warning of Internet Disconnection

Base:

Sessions

Sessions

Packets

Bytes

Apply

Cancel

WAN Failover: Once enabled, whenever WAN1 is down, WAN2 will service the traffics originally handled by WAN1 until WAN1 link is up again and vice versa. This feature is not available to be used concurrently with Load Balancing.

☐ Enable Load Balancing
☒ Enable WAN Failover
☒ Fall back to WAN1 when WAN1 is available again
☐ Warning of Internet Disconnection

WAN Connection Detection

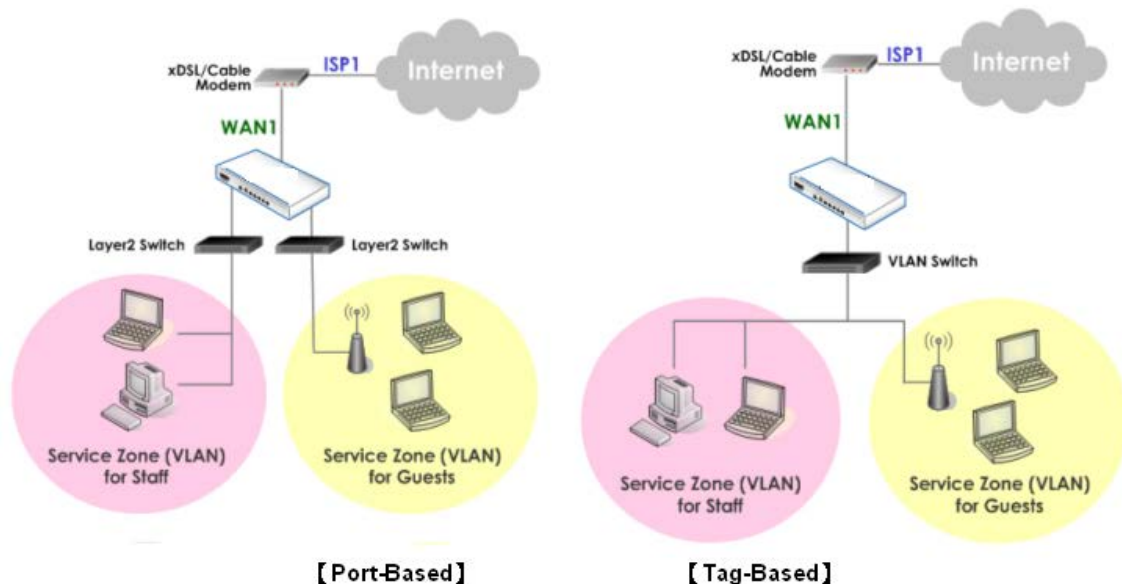
The system will periodically check to see if the Internet (uplink) connection is down by seeing if it can get responses from three target sites.

WAN Failover & Connection Detection	
	<div>Target for detecting Internet connection</div> <div>IP/Domain Name <input type="text" value="www.google.com"/></div> <div>IP/Domain Name <input type="text" value="www.yahoo.com"/></div> <div>IP/Domain Name <input type="text" value="www.apple.com"/></div> <div> <input type="checkbox"/> Enable Load Balancing <input type="checkbox"/> Enable WAN Failover <input checked="" type="checkbox"/> Warning of Internet Disconnection When Internet connection is down, the system will display the message as: <input type="text" value="Sorry! The service is temporarily unavailable."/> * </div>

Warning of Internet Disconnection: When check box is checked, the entered message will be displayed on clients' web browser when outbound internet connection is down.

5.5. LAN Port & Service Zone Mapping

WHG Controllers support 2 types of VLAN modes, Port-Based and Tag-Based. Go to Main Menu > System > LAN Port Mapping



In Port-Based mode each LAN port can be mapped to an enabled Service Zone or disabled, this means the maximum number of Service Zones available to provide service is determined by the number of LAN ports on the Controller.

LAN Ports and Service Zone Mapping						
<p>Select the mode for Service Zone <input checked="" type="radio"/> Port-Based <input type="radio"/> Tag-Based</p>						
<p>Specify a desired Service Zone for each LAN Port:</p>						
<div style="border: 1px solid black; padding: 2px; display: inline-block;">SZ1</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Disable</div>
LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	
Trusted Port						<div style="border: 1px solid black; padding: 2px; display: inline-block;">None</div>

Trusted Port: When a LAN port is selected, clients under this port will not require authentication regardless of the settings in the corresponding Service Zone profile this LAN port maps to.

In Tag-Based mode, Service Zones are mapped to VLAN tags. This means that each LAN port can service any service zone traffic.

LAN Ports and Service Zone Mapping

Select the mode for Service Zone ☐ Port-Based
☒ Tag-Based

Notice: Under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.

Disable ▾

LAN1

Disable ▾

LAN2

Disable ▾

LAN3

Disable ▾

LAN4

Disable ▾

LAN5

Disable ▾

LAN6

Select the mode for Isolation ☒ Enabled
☐ Disabled

Select the mode for Isolation: When enabled, network traffic will be isolated by VLAN tag, which means that inter-VLAN devices are segregated from each other. Please note that this check option is not available for WHG-311 and WHG-315 and are always enabled.

5.6. LAN Partition -- Service Zone


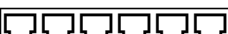
Configure Service Zone; go to: **System >> Service Zones.**

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

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

Service Zone Settings							
Service Zone Name	SSID	Applied Policy	IP Address	Network Alias	DHCP Pool	VLAN Tag	Details
	WLAN Encryption	Default Authen Option	IPv6 Address			Status	
Default	QQQ-EAP300-2.1	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100	N/A	Configure
	None	Server 1	2001:CB46:5359:1::1			Enabled	
SZ1	QA-707	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100	1	Configure
	WEP	Server 1	2001:CB46:5359:2::1			Enabled	

Tag-Based Mode

Service Zone Settings							
Service Zone Name	SSID	Applied Policy	IP Address	Network Alias	DHCP Pool	LAN Port Mapping	Details
	WLAN Encryption	Default Authen Option	IPv6 Address			Status	
Default	QQQ-EAP300-2.1	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100		Configure
	None	Server 1	2001:CB46:5359:1::1			Enabled	
SZ1	QA-707	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100		Configure
	WEP	Server 1	2001:CB46:5359:2::1			Enabled	

Port-Based Mode

- **Service Zone Name:** Mnemonic name of the Service Zone. **SSID:** The SSID that is associated with the Service Zone.
- **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- **Applied Policy:** The policy that is applied to the Service Zone.

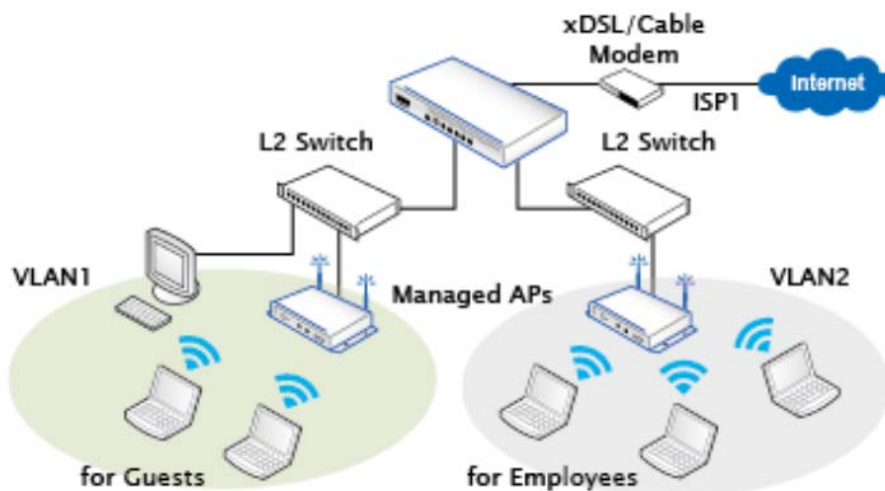
- **Default Authen Option:** Default authentication method/server that is used within the Service Zone.
- **IP Address:** The IPv4 address of this service zone interface.
- **IPv6 Address:** The IPv6 address of this service zone interface.
- **Network Alias:** Administrator may optionally set many alias network segments for a service zone. This feature can allow a single service zone to be seen as many service zones, also hide the IP address of a Service Zone's network interface and to some degree, provide protection from possible attacks from LAN clients.
- **DHCP Pool:** Displays the DHCP pool range configured for this service zone.
- **VLAN Tag (Tag Base only):** The VLAN tag number that is mapped to the Service Zone.
- **LAN Port Mapping (Port Base only):** The physical port that is mapped to this service zone, indicated by green light icon.
- **Status:** Each Service Zone can be enabled or disabled.
- **Details:** Configurable, detailed settings for each Service Zone.

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

5.6.1. Planning Your Internal Network

■ Simple network environment

For most simple internal network, such as there are just only two subnets. Using Port-Based model is an easy and better way. 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 **Employees** and one for **Guests**.

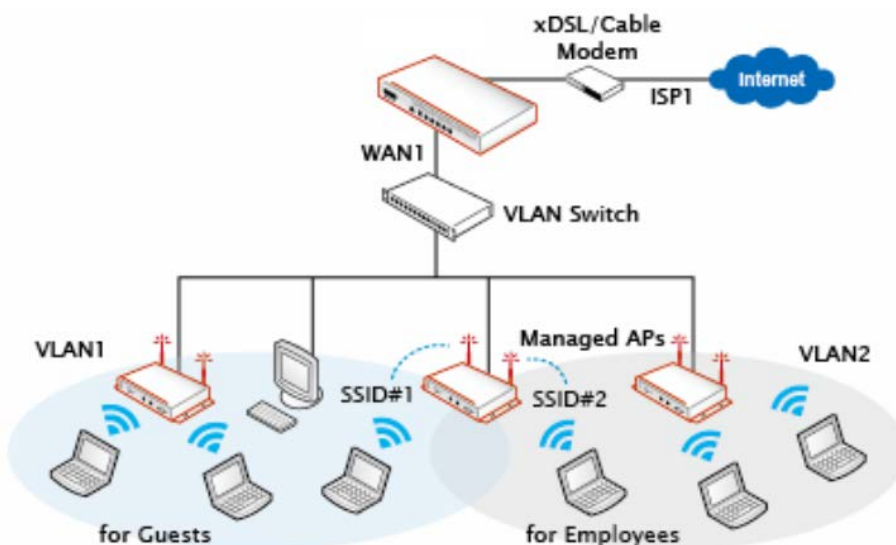


The switches deployed under WHG Controller in Port-Based mode must be Layer 2 switches only.

■ Multi subnet network environment

On the other hand, if the internal network is a **Multi subnets network environment**, Tag-Based model will satisfy to your conditions. In **Tag-Based** mode, each LAN port will serve traffics from different Service Zones; a VLAN switch or VLAN AP is required to take care of the VLAN tags carried within the message frames.

An example of network application diagram is shown as below: more than two Service Zones for different departments.



The switch deployed under WHG Controller in Tag-Based mode must be a VLAN switch only.

5.6.2. Configure Service Zone Network

Configure Service Zone; go to: **System >> Service Zones >> Service Zone Configuration.**

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Zone Name	SZ1
Network Interface	Inter LAN Port Isolation <input checked="" type="radio"/> Enable <input type="radio"/> Auth Required <input type="radio"/> Disable
	Operation Mode <input type="radio"/> NAT <input checked="" type="radio"/> Router
	IP Address 172.21.0.254 *
	Subnet Mask 255.255.0.0 *
	Network Alias List <button>Configure</button>
DHCP Server	Enable DHCP Server <input type="button" value="Configure"/>
	DHCP Server Configuration <input type="button" value="Configure"/>
	Reserved IP Address List <input type="button" value="Configure"/>
	DHCP Lease Protection <input type="radio"/> Enable <input checked="" type="radio"/> Disable

Router Mode

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Zone Name	SZ1
Network Interface	VLAN Tag 1 * (Range: 1 ~ 4094)
	Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router
	IP Address 172.21.0.254 *
	Subnet Mask 255.255.0.0 *
	Network Alias List <input type="button" value="Configure"/>
DHCP Server	Enable DHCP Server <input type="button" value="Configure"/>
	DHCP Server Configuration <input type="button" value="Configure"/>
	Reserved IP Address List <input type="button" value="Configure"/>
	DHCP Lease Protection <input type="radio"/> Enable <input checked="" type="radio"/> Disable

NAT Mode

- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.
- **Network Interface:**
 - **VLAN Tag (Tag Base Only):** The VLAN tag number that is mapped to the Service Zone.
 - **Inter LAN Port Isolation (Port Base Only):** Select **Enable**, **Auth Required** or **Disable**. When the option is “Enabled”, clients under different LAN ports cannot ping each other. When the option is “Disabled”, clients under different LAN ports can ping each other. When the option is “Auth Required”, clients under different LAN ports cannot ping each other unless both of them has successfully authenticated.
 - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
 - **IP Address:** The IP Address of this service zone.
 - **Subnet Mask:** The subnet Mask of this service zone.

- **IPv6 Settings:** The IPv6 Address and configuration of this service zone (When IPv6 enabled).
- **Network Alias List:** Administrator may optionally set many alias network segments for a service zone. This feature can allow a single service zone to be seen as many service zones, also hide the IP address of a Service Zone's network interface and to some degree, provide protection from possible attacks from LAN clients.
 - ◆ Click the **Configure** button to enter the Network Alias List page.

Network Alias List for Service Zone SZ1				
No	IP Address	Subnet Mask	Operation Mode	Enable
1	<input type="text"/>	255.255.255.255 (/32) ▼	<input checked="" type="radio"/> NAT <input type="radio"/> Router	<input type="checkbox"/>
2	<input type="text"/>	255.255.255.255 (/32) ▼	<input checked="" type="radio"/> NAT <input type="radio"/> Router	<input type="checkbox"/>
3	<input type="text"/>	255.255.255.255 (/32) ▼	<input checked="" type="radio"/> NAT <input type="radio"/> Router	<input type="checkbox"/>
4	<input type="text"/>	255.255.255.255 (/32) ▼	<input checked="" type="radio"/> NAT <input type="radio"/> Router	<input type="checkbox"/>
5	<input type="text"/>	255.255.255.255 (/32) ▼	<input checked="" type="radio"/> NAT <input type="radio"/> Router	<input type="checkbox"/>

- ◆ Fill in the desired alias IP address and select the preferred Subnet Mask, Operation mode, check the Enable box and click **Apply** button to activate the settings.

- **DHCP Server:** From the drop down menu, DHCP server for this particular service zone may be Disabled, Enabled or Relayed.

Please note that when “*Enable DHCP Relay*” is enabled, fill in the IP address of the external DHCP Server, and the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone. Please note that Controller should be in the same subnet as the DHCP server.

DHCP Server	Enable DHCP Relay ▼
	<div style="border: 2px solid red; padding: 2px;"> DHCP Server IP Address <input type="text"/> * </div>

When Enable DHCP Server option is selected, click **Configure** button to enter settings page.

DHCP Server	Enable DHCP Server ▼
	<div style="border: 2px solid red; padding: 2px;"> DHCP Server Configuration <input type="button" value="Configure"/> </div>
	Reserved IP Address List <input type="button" value="Configure"/>

DHCP Server Configuration for Service Zone SZ1		
DHCP Pool 1	Start IP Address	<input type="text" value="172.21.0.1"/> *
	End IP Address	<input type="text" value="172.21.0.100"/> *
	Preferred DNS Server	<input type="text" value="172.21.0.254"/> *
	Alternate DNS Server	<input type="text"/>
	Domain Name	<input type="text" value="domain.com"/>
	WINS Server	<input type="text"/>
	Lease Time	<input type="text" value="1440"/> * 2 minutes ~ 10080 minutes (7 days)
	Ignore Client Name	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DHCP Pool 2		<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Item	Description
DHCP Server 1	
Start IP Address / End IP Address	A range of IP addresses that built-in DHCP server will assign to clients. Note: please change the Management IP Address List accordingly (at <i>System Configuration >> System Information >> Management IP Address List</i>) to permit the administrator to access the WHG CONTROLLER admin page after the default IP address of the network interface is changed.
Preferred DNS Server	The primary DNS server that is used by this Service Zone.
Alternate DNS Server	The substitute DNS server that is used by this Service Zone.
Domain Name	Enter the domain name for this service zone.
WINS Server	The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
Lease Time	This is the time period that the IP addresses issued from the DHCP server are valid and available.
Ignore Client Name	When enabled the system will not record the name of the device requesting for an IP address. On the other hand, when disabled is selected, the system will record the device's name when issuing IP addresses. The devices name (Host Name) can be seen under DHCP Lease tab.
DHCP Server 2	
Enable/Disable	When Enabled, an additional DHCP server can be configured to assign IP address to clients associated to the alias IP of this Service Zone. The configurable fields are the same as DHCP Server 1.

Reserved IP Address List: Each service zone can reserve specific IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. Click the **Configure** button to edit the Reserved IP List.

DHCP Server	Enable DHCP Server <input type="button" value="v"/>	
	DHCP Server Configuration	<input type="button" value="Configure"/>
	Reserved IP Address List	<input type="button" value="Configure"/>

The administrator can reserve a list of specific IP addresses for special device with certain MAC address. Fill a set of IP address and MAC address as reserve, additional information can be entered in the Description field. Click **Apply** to activate your settings.

Reserved IP Address List - Service Zone SZ1			
No.	Reserved IP Address	MAC Address	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>

DHCP Lease Protection: When “Enabled”, whenever the Service Zone's built-in DHCP server receives a DHCP request, it will automatically bind the MAC address with an IP address permanently. This means that once all the IP address has been assigned once, it will be bound with the MAC address that first acquired this IP, subsequent devices with new MAC address will be unable to acquire an IP address. When “Disabled” DHCP server will operate as usual, assigning available IP addresses upon DHCP request.

DHCP Server	Enable DHCP Server <input type="button" value="v"/>	
	DHCP Server Configuration	<input type="button" value="Configure"/>
	Reserved IP Address List	<input type="button" value="Configure"/>
	DHCP Lease Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

5.6.3. WISPr Attributes in Service Zone

WISPr or Wireless Internet Service Provider roaming - Pronounced "whisper," WISPr is a draft protocol submitted to the Wi-Fi Alliance that allows users to roam between wireless internet service providers, in a fashion similar to that used to allow cell phone users to roam between carriers. A RADIUS server is used to authenticate the subscriber's credentials.

To configure WISPr attributes in Service Zone, go to: **System >> Service Zones >> WISPr Configuration.**

If a RADIUS server has been configured, the WISPr attributes used during RADIUS authentication can be defined here in this Service Zone.

WISPr Configuration	
WISPr Smart Client	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Smart Client Black List	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="text"/> (Separate by comma)
WISPr Location ID	ISO Country Code <input type="text"/> (e.g. US)
	E.164 Country Code <input type="text"/> (e.g. 1)
	E.164 Area Code <input type="text"/> (e.g. 408)
	Network (SSID/ZONE) <input type="text"/> (e.g. MYWIFI)
WISPr Location Name	Hostpot Operator <input type="text"/> (e.g. MYISP)
	Location <input type="text"/> (e.g. Lobby_of_Airport)
WISPr Billing Time	<input type="text" value="0"/> : <input type="text" value="0"/> (HH:MM)

- **WISPr Smart Client:** Select **Enable** if you wish to allow customers with a roaming account from a WISPr agent (iPass, WiFi Skype, Boingo, and etc.) to access your internet. Make sure to **Enable** the **HTTPS Protected Login** field under System >> General in order for roaming software on the client's device to work properly.
- **Smart Client Black List:** Fill in the WISPr agent names and enable to block users from that particular WISPr roaming agent to access your internet. For example, if you fill in "ipassconnect" the iPass clients will be denied roaming access in your network.
- **WISPr Location ID:** These attributes, which enable wireless hotspot providers to customize their web portals, are based on the client device location and are RADIUS vendor-specific attributes (VSAs).
- **WISPr Location Name:** These attributes, which enable wireless hotspot providers to customize their web portals, are based on the client device location and are RADIUS vendor-specific attributes (VSAs).
- **WISPr Billing Time:** Set RADIUS account billing time.

5.7.IPv6

Configure Service Zone; go to: **System >> IPv6**

System implements IPv6 feature and supports operating in IPv6 networking environment. When IPv6 is enabled, administrator may assign IPv4 IP address as well as IPv6 address to each interface such as WAN1, WAN2, Default Service Zone, Service Zone1, etc.

- **Status:** Enable or Disable the use of IPv6 addressing standard.
- **External Interface:** Select the external interface of the device that will be configured with an IPv6 address.
- **Type:** Choose the desired way of your IPv6 connection.
 - **Static:** Manually enter all the related IPv6 information. Red asterisk are mandatory fields.

IPv6 Setting	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
External Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Type	<div><input checked="" type="radio"/> Static (Use the following IPv6 settings)</div> <div><div>IPv6 Address:</div><div><input type="text"/></div><div>*</div></div> <div><div>Prefix Length:</div><div><input type="text"/></div><div>*</div></div> <div><div>Default Gateway:</div><div><input type="text"/></div><div>*</div></div> <div><div>Preferred DNS Server:</div><div><input type="text"/></div></div> <div><div>Alternate DNS Server:</div><div><input type="text"/></div></div> <div><input type="radio"/> 6to4</div> <div><input type="radio"/> go6</div>

- **IPv6 Address:** Enter the desired IPv6 IP address.
- **Prefix Length:** Set the desired length of your IPv6 mask.
- **Default Gateway:** The IPv6 default gateway of the selected interface.
- **Preferred DNS Server:** The primary DNS server used for this connection.
- **Alternate DNS Server:** The substitute DNS server used for this connection.

- **6to4:** 6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 internet) without the need to configure explicit tunnels. 6to4 option can only be chosen when the selected WAN interface was set with a static IPv4 address.

Type	<input type="radio"/> Static (Use the following IPv6 settings)	
	<input checked="" type="radio"/> 6to4	
	Mode:	<input checked="" type="radio"/> Automatic <input type="radio"/> Configured
	IPv6 Address:	<input type="text"/>
	Prefix Length:	<input type="text"/>
	Preferred DNS Server:	<input type="text"/>
	Alternate DNS Server:	<input type="text"/>
<input type="radio"/> go6		

- **Mode:** Select **Automatic** if you do not have a specified default router, or choose **Configured** to assign a default router to forward packet from IPv6 network to IPv4 network.
- **IPv6 Address:** Enter the desired IPv6 IP address.
- **Prefix Length:** Set the desired length of your IPv6 mask.
- **Default Router:** The default router that routes packets from IPv6 to IPv4 network.
- **Preferred DNS Server:** The primary DNS server used for this connection.
- **Alternate DNS Server:** The substitute DNS server used for this connection.

- **go6:** go6 is a platform that connects the world to the new Internet with IPv6 products, community and services. You may choose this connection option if you have a registered account.

Type	<input type="radio"/> Static (Use the following IPv6 settings)	
	<input type="radio"/> 6to4	
	<input checked="" type="radio"/> go6	
	User Name:	<input type="text"/>
	Password:	<input type="text"/>
	Server Address:	<input type="text"/>
	Preferred DNS Server:	<input type="text"/>
	Alternate DNS Server:	<input type="text"/>
Assign Broker Address: <input type="radio"/> Enable <input checked="" type="radio"/> Disable		

- **Username:** Username of your go 6 account.
- **Password:** Password of your go6 account.
- **Server Address:** The servicing go6 server address.
- **Preferred DNS Server:** The primary DNS server used for this connection.
- **Alternate DNS Server:** The substitute DNS server used for this connection.
- **Assign Broker Address:** Select **Enable** if you wish to use tunnel broker service.
- **Broker Address:** The address of your broker.

6. User Authentication and Grouping

6.1. Overview of User Authentication Database

- Built-in User Databases**

Local and On-demand are Controller's built-in user databases designed to house static and temporary accounts respectively. Local database is ideal for storing long term accounts for instance employee accounts while On-demand database is ideal for generating temporary accounts for guest usage.

Authentication Settings			
Auth Option	Auth Database	Postfix	Group
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	ondemand	Group 1
SIP	SIP	N/A	Group 1

- External User Database**

System supports 4 types of external user databases (POP3, RADIUS, LDAP, NT Domain) and 4 SIP (voice/video) servers.

Authentication Option - Server 2	
Name	Server 2 *
Postfix	pop3 *
Black List	None ▼
Authentication Database	POP3 ▼ Configure
Group	
Enable Local VPN	

LOCAL
POP3
RADIUS
LDAP
NT Domain

Apply

Cancel

Authentication Server - SIP		
Trusted Registrar	IP Address	Remark
Group	Group 1 ▼	Group selection applied to clients login with SIP authentication.

►► **Note:**

Concurrently only one server is allowed to be set as Local or NTDOMAIN authentication method simultaneously. For example, you can set two RADIUS authentication servers simultaneously.

- Authentication Option Configuration**

Go to Main Menu > Users > Authentication

Click on the server name to set the configuration for that particular server. After completing and clicking **Apply** to save the settings. Then go back to System > Service Zones and enable or disable any server in each service zone as you prefer. For each Service Zone, one of the authentication servers can be set as default, users can log into the default authentication server without the postfix to allow faster login process.

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

Authentication Option - Server 1	
Name	<input type="text" value="Server 1"/> *
Postfix	<input type="text" value="local"/> *
Black List	<input type="text" value="None"/> ▼
Authentication Database	<div><div>LOCAL ▼</div><div>LOCAL POP3 RADIUS LDAP NT Domain</div></div> <input type="button" value="Configure"/>
Group	

- **Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.
- **Postfix:** A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Black List:** There are 10 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop-down menu and this black list will be applied to this specific authentication option.
- **Authentication Database:** Click **Configure** button to enter the configuration page. For example, select *Local* from the drop-down list box and then click **Configure** button to enter the **Local User Database Settings**. Then, click the hyperlink of **Local User List**.
- **Group:** Select one Group from the drop-down list box for this specific authentication option.

6.1.1. Configuring On-demand

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

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

1) General Settings

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

General Settings	
Postfix	<input type="text" value="ondemand"/>
Currency	<input checked="" type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="text"/> (Input other desired monetary unit, e.g. AU)
Group Name	Group 1 ▾
WLAN ESSID	<input type="text" value="SSID0"/>
Wireless Key	<input type="text"/>
Remaining Volume Sync Interval	<input checked="" type="radio"/> 10min(s) <input type="radio"/> 15min(s) <input type="radio"/> 20min(s)
Terminal Server	Configuration
Expired Account Keep Days	<input type="text" value="15"/> *(1~30 days)
Delete All Expired Accounts	Delete

- **Postfix:** Postfix is used to inform the system which type of authentication database as account belongs to for authentication when multiple databases are concurrently in use. Enter the string to be used as postfix for on-demand users.
- **Currency:** Select the desired monetary unit or specify other unit in the input field.
- **Group Name:** Select the desired group for on-demand user.
- **WLAN ESSID:** The administrator can enter the defined wireless ESSID in this field and it will be printed on the receipt for on-demand users' reference when accessing the Internet via wireless LAN service. The ESSID given here should be ESSID of Service Zones that has enabled On-demand database as an authentication server.
- **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the on-demand users' reference when accessing the Internet via wireless LAN service.
- **Remaining Volume Sync Interval:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.
- **Terminal Server:** Terminal Configuration is a list of serial-to-Ethernet devices that communicate with the

system only; never get online and no need to go through authentication. NetTicketGen is an example of terminal server that is required to be configured here before it can operate with Controller.

Terminal Server Configuration				
Item	Server IP	Port	Location	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **Expired Account Keep Days:** When an Ondemand account expires, it will remain on the ondemand account list for a certain amount of time. The number of days to retain an expired ondemand account can be specified here.
- **Delete All Expired Accounts:** A click of the “Delete” button will delete all expired accounts on the Ondemand account list and recycle these accounts ready for new account generation.

2) Ticket Customization

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

Ticket Customization	
Receipt Header 1	<input type="text" value="Welcome!"/>
Receipt Header 2	<input type="text"/>
Receipt Header 3	<input type="text"/>
Receipt Footer 1	<input type="text" value="Thank You!"/>
Receipt Footer 2	<input type="text"/>
Receipt Footer 3	<input type="text"/>
Remark	<input type="text"/>
Background Image	<input type="radio"/> None <input checked="" type="radio"/> Default Image <input type="radio"/> Uploaded Image <input type="button" value="Edit"/>
Number of Tickets	<input type="radio"/> 1 <input checked="" type="radio"/> 2
Remark	<input type="text" value="Remark2"/>



SN:xxxxxx

Welcome!

Username	xxxx@ondemand
Password	xxxxxxxxxx
Plan : Account Type	1 : Usage-time
Quota	xx hr(s) xx min(s)
Total Price	1.99
Reference	Customer xxx
External ID	

Shared Wireless Key: None (Open System)

Your account is activated at

Your first time login must be done before 2011/05/11 15:45

You have to login before

The account will be expired in after account activation.

Thank You!

- **Receipt Header:** There are 3 receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
- **Receipt Footer:** The entered content will be printed on the receipt. This footer is optional.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose the default image or none. Click **Browse** to select the image file and then click **upload**. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.
- **Twin Ticket:** Enable this function to print duplicate receipts.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Preview:** Click **Preview** button, the ticket will be shown including the information of username and password with the selected background. Print the ticket here.

3) Billing Plans

Billing plan profiles defines the terms and conditions of guest internet access. Click **Edit** button to enter the configuration page of a selected Billing Plan profile. Once you have finished configuring a billing plan profile, go back to the screen of **Billing Plans**, check the **Enable** checkbox and click **Apply** to activate.

Billing Plans							
Plan	Account Type	Quota	Price	Enable	Quick Account Creation	Group	Function
1	Usage-time	1 day(s) 1 hr(s) 1 min(s) of connection time quota with expiration	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Group 1	<button>Edit</button>
2	N/A			<input type="checkbox"/>	<input type="checkbox"/>	Group 1	<button>Edit</button>
3	N/A			<input type="checkbox"/>	<input type="checkbox"/>	Group 1	<button>Edit</button>

- **Plan:** The number of the specific plan.
- **Account Type:** The account type chosen for this plan. Different account types have different properties. A suitable account type should be selected that will best meet guest usage requirements.
- **Quota:** The usage terms on how much or how long an On-demand users are allowed to access the

network.

- **Price:** The unit price of the respective billing plan.
- **Enable:** Check the checkbox to activate the plan. Deactivated billing plans cannot be used to generate ondemand guest accounts.
- **Quick Account Creation:** Check the checkbox to enable Quick Account Creation. Static users with "Ondemand Account Privilege" (an attribute in Group profile) enabled can see "Quick Account Creation" checked billing plans and can generate ondemand accounts.
- **Group:** Group assignment of on-demand users associated with the respective billing plan.
- **Function:** Click the button **Edit** to configure the respective billing plan profile.

4) Ondemand Account Types

- **Usage-time with Expiration Time:** Can access internet as long as account valid with remaining quota (usable time). Need to activate the purchased account within a given time period by logging in for the first time. Ideal for short term usage. For example in coffee shops, airport terminals etc. Only deducts quota while using, however the count down to Expiration Time is continuous regardless of logging in or out. Account expires when **Valid Period** has been used up or quota depleted.
 - **Quota** is the total period of time (xx days yy hrs zz mins), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.
 - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
 - **Valid Period** is the valid time period for using. After this time period, even with remaining quota the account will still expire.
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

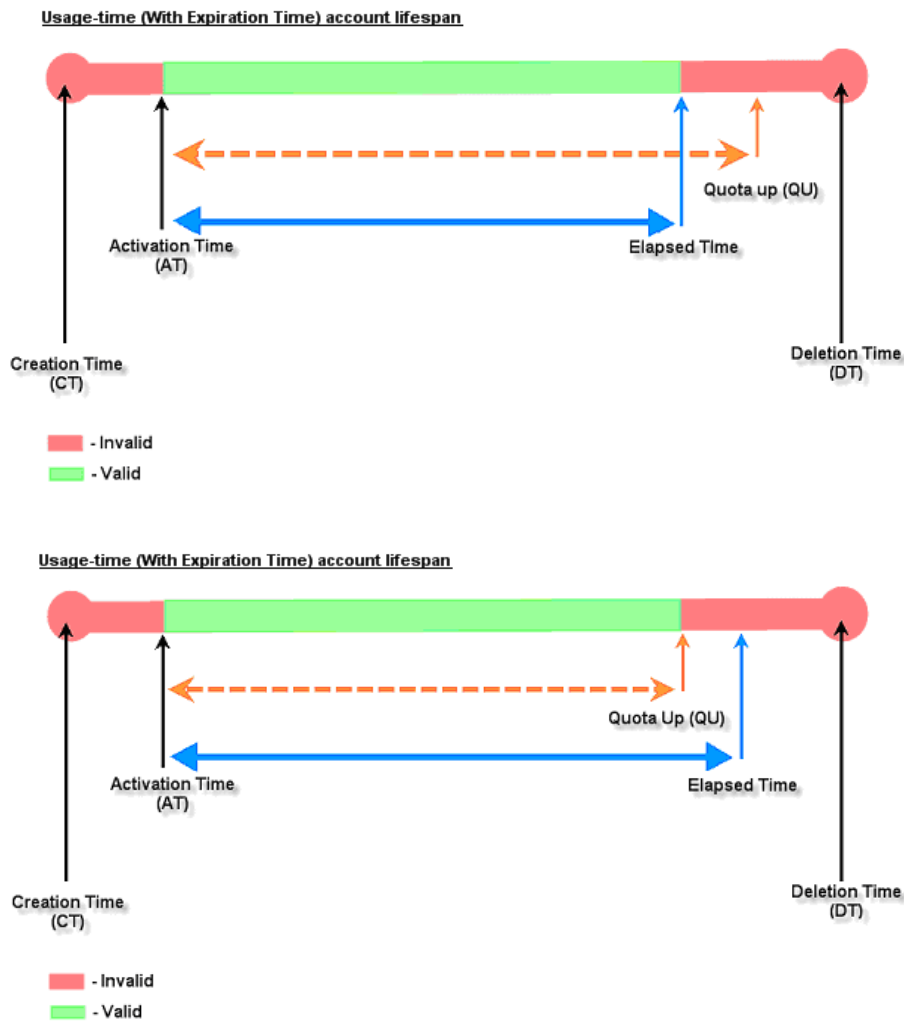
Editing Billing Plan	
Plan	3
Account Type	Usage-time ▾
Expiration Time	<input checked="" type="radio"/> With Expiration Time <input type="radio"/> No Expiration Time
Quota	<input type="text"/> day(s) <input type="text"/> hr(s) <input type="text"/> min(s) <small>*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)</small>
Account Activation	First time login must be done within <input type="text"/> day(s) <input type="text"/> hour(s) <small>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</small>
Valid Period	After activation, account will be expired in <input type="text"/> day(s) <small>*(Must be larger than 0)</small>
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▾
Reference	<input type="text"/>

TIP:

If the Account Type is "Usage Time", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (connection time). Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply

Cancel



- **Usage-time with No Expiration Time:** Can access internet as long as account has remaining quota (usable time). Need to activate the purchased account within a given time period by logging in for the first time. Ideal for short term usage. For example in coffee shops, airport terminals etc. Only deducts quota while using. Account expires only when quota depleted.
 - **Quota** is the total period of time (xx days yy hrs zz mins), during which On-demand users are allowed to access the network. The total maximum quota is “364Days 23hrs 59mins 59secs” even after redeem.
 - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Usage-time ▾
Expiration Time	<input type="radio"/> With Expiration Time <input checked="" type="radio"/> No Expiration Time
Quota	<input type="text"/> day(s) <input type="text"/> hr(s) <input type="text"/> min(s) <small>*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)</small>
Account Activation	First time login must be done within <input type="text"/> day(s) <input type="text"/> hour(s) <small>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</small>
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▾
Reference	<input type="text"/>

TIP:

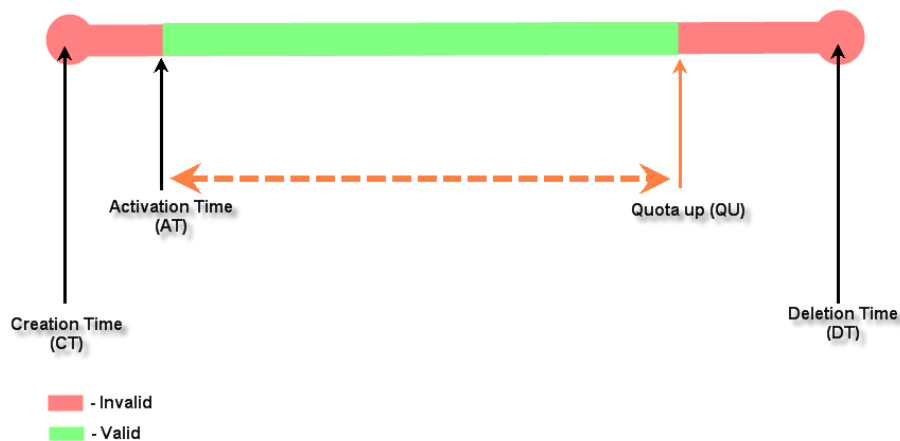
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (connection time).

Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply

Cancel

Usage-time (No Expiration) account lifespan



- **Hotel Cut-off-time:** **Hotel Cut-off-time** is the clock time (normally check-out time) at which the on-demand account is cut off (made expired) by the system on the following day or many days later. On the account creation UI of this plan, operator can enter a Unit value which is the number of days to Cut-off-time according to customer stay time. For example: Unit = 2 days, Cut-off Time = 13:00 then account will expire on 13:00 two days later. **Grace Period** is an additional, short period of time after the account is cut off that allows user to continue to use the on-demand account to access the Internet without paying additional fee. **Unit Price** is a daily price of this billing plan. Mainly used in hostel venues to provide internet service according to guests' stay time. **Group** will be the applied Group to users created from this plan. **Reference** field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Hotel Cut-off-time ▾
Hotel Cut-off Time	<input type="text"/> : <input type="text"/> *(HH:MM; range : 00:00 ~ 23:59)
Grace Period	Account remains usable for <input type="text"/> hour(s) after cut-off.
Unit Price	<input type="text"/> per day *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1 ▾
Reference	<input type="text"/>

TIP:

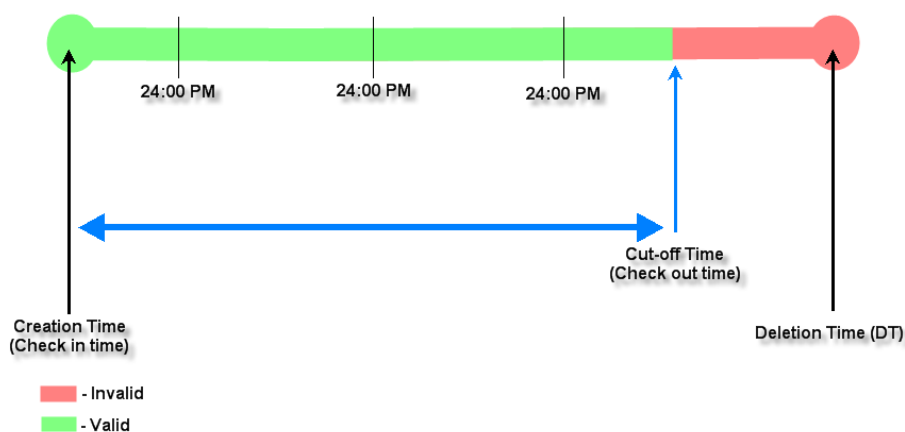
The "Hotel Cut-off-time" Account Type is designed for hotel applications and conforms to check-in/out scenario. For cut-off applications within one day (for example, the account expires upon bookstore's closing hour -11PM) please select "Duration Time".

One-day-stay in Hotel terms is counted from a customer's check-in time to the check-out time on the following day. When a tenant checks in for one or multiple days, the operator can generate an account ticket based on the number of the over-night stay. The account will be cut-off on the specified cut-off-time (normally the hotel's check-out-time) after the number of nights specified. Since guests may hang around in the lobby for a short while after checking out, the hotel may want to specify a "Grace period" for their tenants.

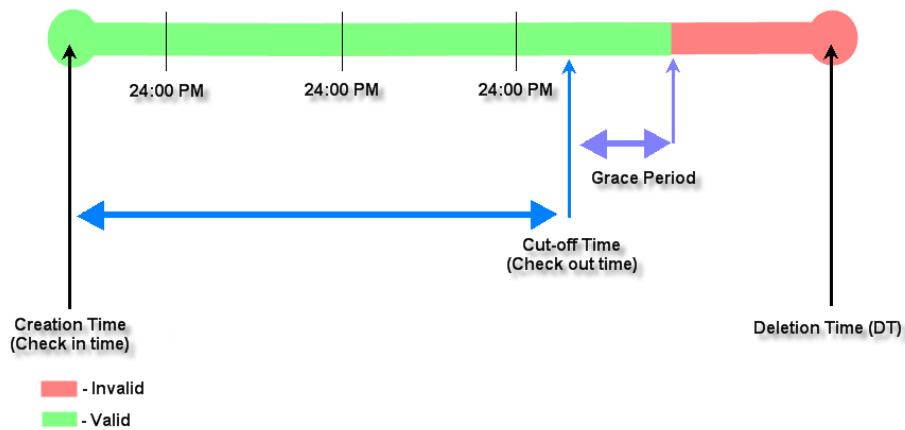
Apply

Cancel

Hotel Cut-off-time account lifespan (3 night stay example)



Hotel Cut-off-time account lifespan (3 night stay example with Grace Period)



- **Volume:** Can access internet as long as account valid with remaining quota (traffic volume). Account expires when *Valid Period* has been used up or quota depleted. Ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous regardless of logging in or out.
 - **Quota** is the total Mbytes (1~1000000), during which On-demand users are allowed to access the network.
 - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
 - **Valid Period** is the valid time period for using. After this time period, even with remaining quota the account will still expire.
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

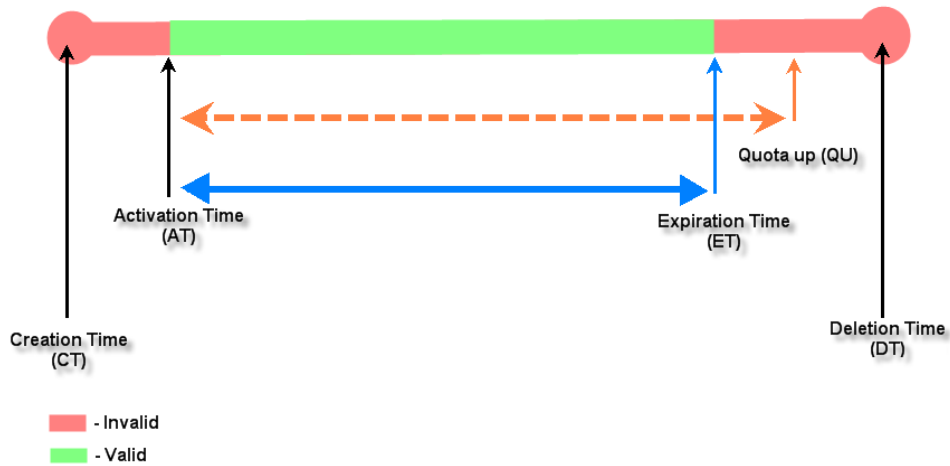
Editing Billing Plan	
Plan	3
Account Type	Volume ▾
Quota	<input type="text"/> Mbyte(s) <small>*(Range : 1 ~ 1000000)</small>
Account Activation	First time login must be done within <input type="text"/> day(s) <input type="text"/> hour(s) <small>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</small>
Valid Period	After activation, account will be expired in <input type="text"/> day(s) <small>*(Must be larger than 0)</small>
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▾
Reference	<input type="text"/>

TIP:
If the Account Type is "Volume", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (traffic volume).
Customer also needs to activate the issued account within a given time period by logging in for the first time.

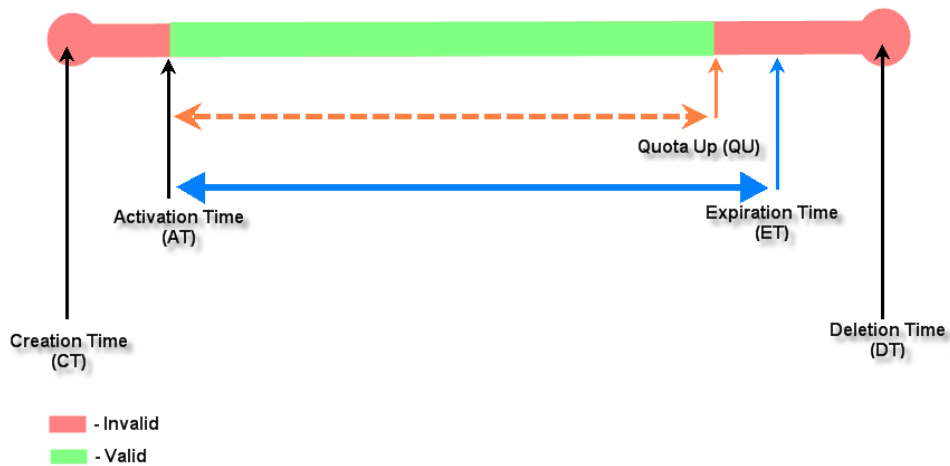
Apply

Cancel

Volume account lifespan



Volume account lifespan



- **Duration-time with Elapsed Time:** Account activated upon the account creation time. Count down begins immediately after account created and is continuous regardless of logging in or out. Account expires once the *Elapsed Time* has been reached. Ideal for providing internet service immediately after account creation throughout a specific period of time.
 - **Begin Time** is the time that the account will be activated for use. It is set to account creation time.
 - **Elapsed Time** is the time interval for which the account is valid for internet access (xx hrs yy mins).
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Duration-time ▼
Counting Method	<input checked="" type="radio"/> Elapsed Time <input type="radio"/> Begin-and-end Time <input type="radio"/> Cut-off Time
Begin Time	Upon Account Creation
Elapsed Time	<input type="text"/> day(s) <input type="text"/> hr(s) <input type="text"/> min(s) <small>*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)</small>
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	<input type="text"/>

TIP:

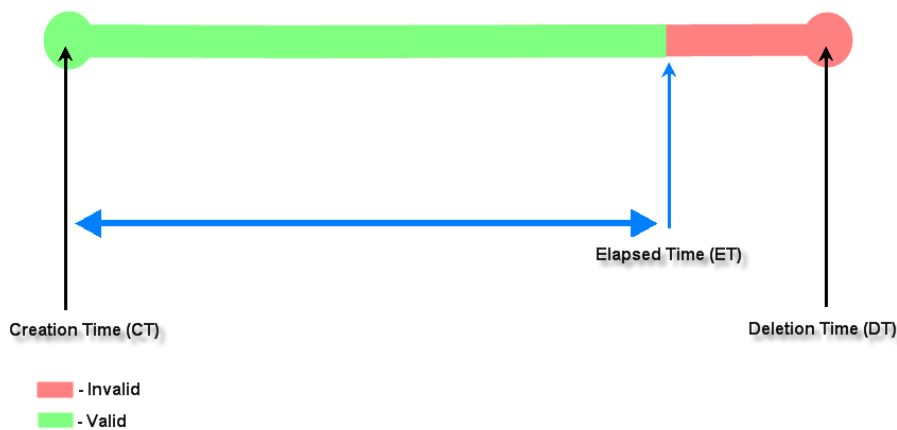
When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.

1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Time" specifies that the account is valid between the two time points.

Apply

Cancel

Duration-time (Elapsed Time) account lifespan



- **Duration-time with Cut-off Time:** **Cut-off Time** is the clock time at which the on-demand account is cut off (made expired) by the system on that day. For example a shopping mall closing hour is 23:00; operators selling on-demand tickets can create use this plan to create ticket set to be Cut-off on 23:00. If an account of this kind is created after the Cut-off Time, the account will automatically expire.
 - **Begin Time** is the time that the account will be activated for use. It is set to account creation time.
 - **Cut-off Time** is the clock time when the account will expire.
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Duration-time
Counting Method	<input type="radio"/> Elapsed Time <input type="radio"/> Begin-and-end Time <input checked="" type="radio"/> Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	<input type="text"/> : <input type="text"/> <small>*(HH:MM; range : 00:00 ~ 23:59)</small>
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1,99)</small>
Group	Group 1
Reference	<input type="text"/>

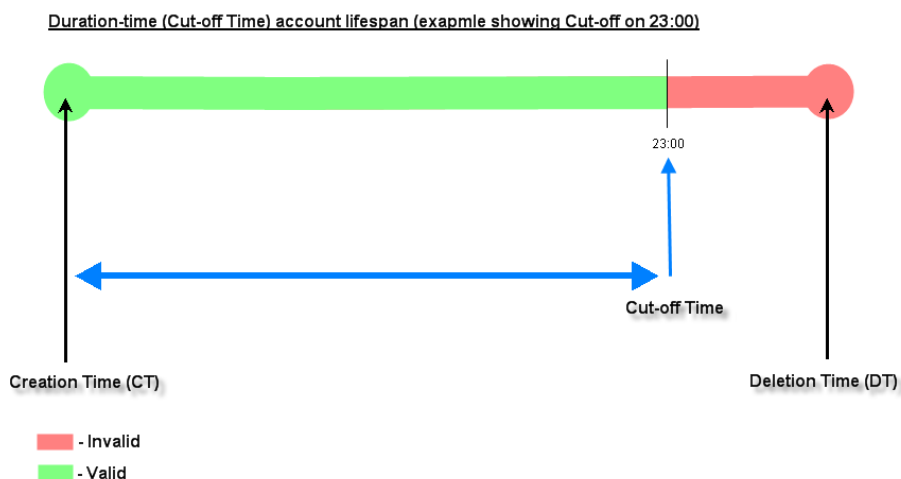
TIP:

When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.

1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Time" specifies that the account is valid between the two time points.

Apply

Cancel



- **Duration-time with Begin-and End Time:** Define explicitly the *Begin Time* and *End Time* of the account. Count down begins immediately after account activation and expires when the *End Time* has been reached. Ideal for providing internet service throughout a specific period of time. For example during exhibition events or large conventions such as Computex where each registered participant will get an internet account valid from 8:00 AM Jun 1 to 5:00 PM Jun 5 created in batch like coupons.
 - **Begin Time** is the time that the account will be activated for use, defined explicitly by the operator.
 - **End Time** is the time that the account will become expired and not able to use any more, defined explicitly by the operator.
 - **Price** is the unit price of this plan.
 - **Group** will be the applied Group to users created from this plan.
 - **Reference** field allows administrator to input additional information.

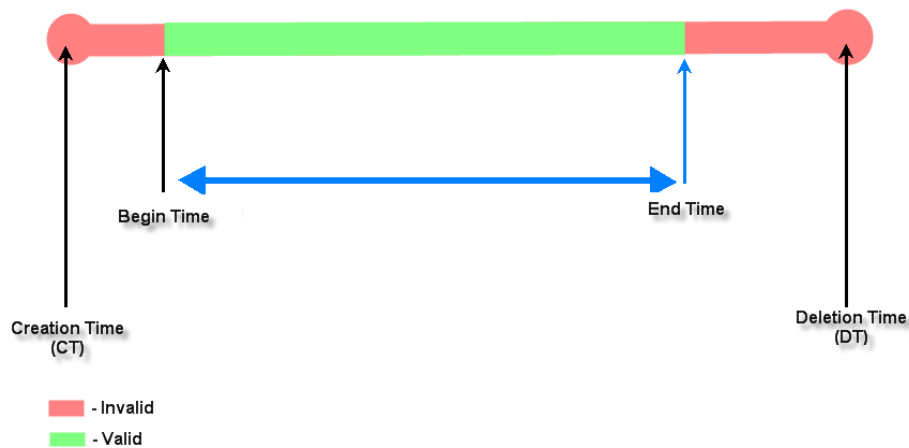
Editing Billing Plan	
Plan	3
Account Type	Duration-time ▼
Counting Method	<input type="radio"/> Elapsed Time <input checked="" type="radio"/> Begin-and-end Time <input type="radio"/> Cut-off Time
Begin Time	-- ▼ : -- ▼ , -- ▼ -- ▼ ---- ▼
End Time	-- ▼ : -- ▼ , -- ▼ -- ▼ ---- ▼
Price	<input type="text"/> <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	<input type="text"/>

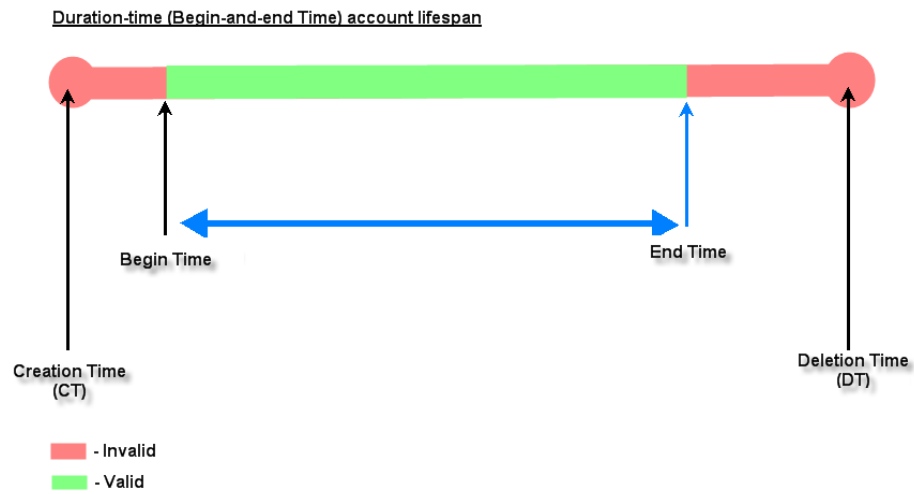
TIP:

When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.

1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Time" specifies that the account is valid between the two time points.

Duration-time (Begin-and-end Time) account lifespan





5) External Payment Gateway

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

The four options are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** and **Disable**.

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

6) On-demand Account Creation

After at least one plan is enabled, the administrator can generate on-demand user accounts here. Click on the **Create** button of the desired plan and an on-demand user account will be created.

After the account is created, you can print the ticket with all of the necessary on-demand user's information, including the username and password.

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

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Volume	1.1 Mbyte(s) of traffic volume quota	20	Enabled	<button>Create</button>
2	Usage-time	9 hr(s) 59 min(s) of connection time quota with expiration	57	Enabled	<button>Create</button>

- **Plan:** The number of the specific plan.
- **Account Type:** The account type chosen for this plan. Different account types have different properties. A suitable account type should be selected that will best meet guest usage requirements.
- **Quota:** The usage terms on how much or how long an On-demand users are allowed to access the network.
- **Price:** The unit price of the respective billing plan.
- **Status:** Show whether the billing plan is enabled or disabled.
- **Function:** Press **Create** button for the desired plan; an On-demand user account will be created, and then click **Printout** to print a receipt which will contain this on-demand user's information.

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Volume	1.1 Mbyte(s) of traffic volume quota	20	Enabled	<button>Create</button>

Creating an On-demand Account

Plan : Account Type

1 : Usage-time

Quota

2 min(s) of connection time quota with expiration

Username/Password Creation

System created ▾

Valid Period

After activation, the account will be expired in 1 day(s)

Total Price

1

Group

Group 1 ▾

Reference

plan1

Add a reference related to this account (for example, the customer's name)

External ID

Enter an external ID such as Library ID No.

Please confirm the information and press Create button to create an account.

SN:015042

Welcome!

Username	7862@ondemand
Password	7k84mp62
Plan : Account Type	1 : Usage-time
Quota	2 min(s) of connection time quota with expiration
Total Price	1
Reference	plan1
External ID	

ESSID : SSID0

Shared Wireless Key: None (Open System)

You have to login before 2011/05/13 14:32

The account will be expired in 1 day(s) after account activation.

Thank You!

Network operator can also choose to create ondemand accounts in batch. Simply specify the number of account to be generated and click “Create” at the bottom of the page.

On-demand Account Batch Creation					
Plan	Account Type	Quota	Price	Group	Number of Accounts
1	Usage-time	2 day(s) of connection time quota	1	Group 1	<input type="text" value="5"/>
2	Volume	50000 Mbyte(s) of traffic volume quota	1	Group 1	<input type="text"/>
3	Hotel Cut-off-time	Valid until 2:03 the following day	2	Group 1	<input type="text"/>

Success

Users have been successfully created.

The created accounts can be exported as a txt file or printed via pre-configures POS printer

7) On-demand Account List

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

On-demand Account List						
Username	Password	Remaining Quota	Status	Group	Reference	External ID
7862	7k84mp62	2 min(s)	Normal	Group 1	plan1	

- **Search:** Enter a keyword of a username, or reference, to be searched in the text filed and click this button to perform the search. All usernames, or reference, matching the keyword will be listed.
- **Username:** The login name of the account.
- **Password:** The login password of the account.
- **Remaining Quota:** The remaining time or volume, or the cut-off time until this account expires.
- **Status:** The status of the account.
 - **Normal:** the account is not currently in use and also does not exceed the quota limit.

- **Online:** the account is currently in use.
- **Expired:** the account is not valid any more, even there is remaining quota to be used.
- **Out of Quota:** the account has exceeded the quota limit.
- **Redeemed:** the account has been applied for account renewal.
- **Delete All:** This will delete all ondemand accounts at once.
- **Delete:** This will delete the users individually.

Redeem On-demand Accounts



For Time and Volume accounts, if they are almost out of quota, they can use redeem function to extend their quota. After the user has get, or buy, a new account, they just need to click the **Redeem** button in the login success page, input the new account **Name** and **Password** and then click **Enter**. This new account's quota will be extended to the original account.

But Redeem function can only redeem to same type of account, Time account must redeem with Time account; Volume account must redeem with Volume account only.

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.

» **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.

» **Note:**

Hotel Cut-off and Duration Time accounts do not support redeem function.

6.1.2. Configuring RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

Choose “**RADIUS**” from the **Authentication Database** field. The **Local VPN** option can be enabled or disabled for the entire **Authentication Database**.

Authentication Option - Server 1	
Name	<input type="text" value="Server 1"/> *
Postfix	<input type="text" value="radius"/> *
Black List	<input type="button" value="None"/> ▾
Authentication Database	<input type="button" value="RADIUS"/> ▾ <input type="button" value="Configure"/>
Group	<input type="button" value="Group 1"/> ▾
Enable Local VPN	<input type="checkbox"/>

- **Name:** Configurable text string designated as the mnemonic name of this authentication option.
- **Postfix:** Is the text string entered as a postfix in the account field for notifying the Controller which authentication database this account belongs to.
- **Black List:** System has built-in black-list profiles where specific user accounts can be listed. When selected and applied here, it tells the Controller that the accounts on the selected black list should be denied authentication.
- **Group:** The Group profile that will govern the users authenticated via this authentication option.
- **Enable Local VPN:** When checked, users authenticating with this authentication option will have a VPN tunnel established automatically between the Controller and the user’s client device.
- **Authentication Database:** Select the authentication database that will be used for account validation when an authentication request is received. Click the button of **Configure** for further configuration. The RADIUS server sets the external authentication server that houses user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the **Apply** button.

External RADIUS Server Related Settings		
802.1X Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 802.1X Settings	
Username Format	<input checked="" type="radio"/> Leave Unmodified <input type="radio"/> Complete (e.g. user1@postfix) <input type="radio"/> Only ID (e.g. user1)	
NAS Identifier	<input type="text"/>	
NAS Port Type	<input type="text" value="19"/> <small>*(Default: 19, Range: 0~35)</small>	
Accounting Delay Time	<input type="text" value="0"/> <small>*(Default: 0)</small>	
Service Type	<input type="text" value="1"/> <small>*(Default: 1, Range: 1~11)</small>	
Class-Group Mapping	<input type="button" value="Configure"/>	
DM & CoA Settings	<input type="button" value="Configure"/>	
Attributes Priority	Follow Server's Setting <input type="button" value="v"/>	
	Standard RADIUS Attributes	
	Session Timeout	<input type="text" value="240"/> Minutes <small>*(Range: 5~1440 mins)</small>
	Idle Timeout	<input type="text" value="10"/> Minutes <small>*(Range: 1~120 mins)</small>
	Acct Interim Interval	<input type="text" value="1"/> Minutes <small>*(Range: 1~120 mins, 0 is disable)</small>
	WISPr Vendor Specific Attributes	
	Redirection URL	<input type="text"/>
	Billing Class Of Service	<input type="text"/>
	Session Terminate on Billing Time	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Session Terminate Time	Never
Retransmission Settings	Number of Retries: <input type="text" value="3"/> <small>*(Default: 3)</small>	
	Timeout: <input type="text" value="6"/> <small>*(Default: 6)</small>	
Primary RADIUS Server		
Authentication Server	<input type="text" value="10.0.5.39"/> <small>*(Domain Name/IP Address)</small>	
Authentication Port	<input type="text" value="1812"/> <small>*(Default: 1812)</small>	
Authentication Secret Key	<input type="password" value="•••••"/>	
Authentication Protocol	CHAP <input type="button" value="v"/>	
Accounting Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Accounting Server	<input type="text" value="10.0.5.39"/> <small>*(Domain Name/IP Address)</small>	
Accounting Port	<input type="text" value="1813"/> <small>*(Default: 1813)</small>	
Accounting Secret Key	<input type="password" value="•••••"/>	
Secondary RADIUS Server		
Authentication Server	<input type="text"/> <small>(Domain Name/IP Address)</small>	
Authentication Port	<input type="text"/>	
Authentication Secret Key	<input type="password"/>	
Authentication Protocol	CHAP <input type="button" value="v"/>	
Accounting Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Accounting Server	<input type="text"/> <small>(Domain Name/IP Address)</small>	
Accounting Port	<input type="text"/>	
Accounting Secret Key	<input type="password"/>	

Item	Description
External RADIUS Server Related Settings	
802.1X Authentication	Enable /Disable 802.1X authentications for users authenticating through this

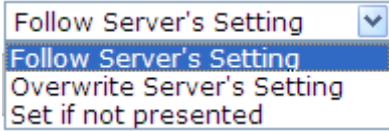
	Server. To support EAP-SIM authentication, please enable this feature and enter 802.1X Settings to configure the AP's that support associated clients to authenticate by EAP-SIM.																						
Username Format	Select the format which the user login information is sent to the external RADIUS Server. You may choose to send username in Complete (userID + Postfix), Only ID or Leave Unmodified . Please note that if Leave Unmodified option is selected, the system will send the username to Default Auth Server set in 802.1X configuration page for authentication.																						
NAS Identifier	This attribute is the string identifying the NAS originating the access request. System will send this value to the external RADIUS server, if the external RADIUS server needs this.																						
NAS Port Type	Indicates the type of physical port the network access server is using to authenticate the user. System will send this value to the external RADIUS server, if the external RADIUS server needs this.																						
Accounting Delay Time	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.)																						
Service Type	<div>A RADIUS attribute with configurable range from 1 ~ 11. Each value represents different kinds of service. The administrator can set the kind of service preferred by users and notify the RADIUS server this way.<table><tr><td>1</td><td>Login</td></tr><tr><td>2</td><td>Framed</td></tr><tr><td>3</td><td>Callback Login</td></tr><tr><td>4</td><td>Callback Framed</td></tr><tr><td>5</td><td>Outbound</td></tr><tr><td>6</td><td>Administrative</td></tr><tr><td>7</td><td>NAS Prompt</td></tr><tr><td>8</td><td>Authenticate Only</td></tr><tr><td>9</td><td>Callback NAS Prompt</td></tr><tr><td>10</td><td>Call Check</td></tr><tr><td>11</td><td>Callback Administrative</td></tr></table></div>	1	Login	2	Framed	3	Callback Login	4	Callback Framed	5	Outbound	6	Administrative	7	NAS Prompt	8	Authenticate Only	9	Callback NAS Prompt	10	Call Check	11	Callback Administrative
1	Login																						
2	Framed																						
3	Callback Login																						
4	Callback Framed																						
5	Outbound																						
6	Administrative																						
7	NAS Prompt																						
8	Authenticate Only																						
9	Callback NAS Prompt																						
10	Call Check																						
11	Callback Administrative																						
Class-Group Mapping	<div><div>This function is to assign a <i>Group</i> to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes logs into the system via the RADIUS server, each client will be mapped to an assigned Group.</div><div><div><div>RADIUS Group Mapping - Server 3</div><div><div><div><div></div></div><div><div>Enable</div></div><div><div>Disable</div></div></div><table><tr><th>No.</th><th>Class Attribute Value</th><th>Group</th><th>Remark</th></tr><tr><td>1</td><td><div>1</div></td><td><div>Group 1</div></td><td></td></tr><tr><td>2</td><td><div>2</div></td><td><div>Group 1</div></td><td></td></tr><tr><td>3</td><td><div>3</div></td><td><div>Group 1</div></td><td></td></tr></table></div></div></div></div>	No.	Class Attribute Value	Group	Remark	1	<div>1</div>	<div>Group 1</div>		2	<div>2</div>	<div>Group 1</div>		3	<div>3</div>	<div>Group 1</div>							
No.	Class Attribute Value	Group	Remark																				
1	<div>1</div>	<div>Group 1</div>																					
2	<div>2</div>	<div>Group 1</div>																					
3	<div>3</div>	<div>Group 1</div>																					
DM & CoA Settings	Under some circumstances, it may be desirable for a network																						

administrator to make changes in session characteristics without requiring to access Controller WMI to initiate change. For example, a network administrator may need to terminate a session or change the authorization attributes associated with a session. This is possible through RADIUS DM & CoA messages.

Administrator can specify the white list of devices that the Controller deem as authentic message source.

RADIUS Client Device Settings					
No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	DM & CoA	10.0.0.0	255.255.0.0 (/16)	*****	
2	Disable	192.168.0.0	255.255.0.0 (/16)	*****	
3	Roaming Out	10.0.5.39	255.255.255.255 (/32)	*****	
4	802.1X		255.255.255.255 (/32)		
	DM & CoA				
	Disable				

Devices configured here with correct shared key are allowed to issue to Controller change of authorization (CoA) messages, which affect session authorization, or disconnect messages (DM), which cause a session to be terminated immediately.

Attributes Priority	<p>The drop down selection list allows 3 options: Follow Server's Setting, Overwrite Server's Setting and Set if not presented.</p>  <p>If Follow Server's Setting is selected, system will use the RADIUS attributes set in the remote RADIUS server. If Overwrite Server's Setting is selected, system will use the RADIUS attributes set below. If Set if not presented is selected, system will use the RADIUS attribute settings below if the configured remote RADIUS server presents no attributes.</p> <p>RADIUS Standard Attributes</p> <ul style="list-style-type: none"> • Session Time Out: Forced logout once timeout period reached. • Idle Time Out: Implicitly logout when inactivity timeout period reached. • Acct Interim Interval: The time interval to send accounting updates. <p>WISPr Vendor Specific Attributes Default from the drop-down menu is to follow external Server settings. If you select to overwrite or set if not present, the following attributes will be required.</p> <ul style="list-style-type: none"> • Redirection URL: URL of Start page. • Billing Class Of Service: Text string used to indicate service used for the visitor access. • Session Terminate on Billing Time: When enabled, the session will terminate in the Billing Time set. • Session Terminate Time: Never. This means that RADIUS sessions will only terminate when a user logouts, gets kicked out, or session idled timeout. • Bandwidth Setting: It will follow the Bandwidth settings of the Group profile set for this authentication server. 							
	<ul style="list-style-type: none"> • Bandwidth Setting: The number of resends before treating this transaction as fail. • Timeout: The time in seconds to wait for reply from RADIUS server, if no reply then resend the packet. 							
	Primary / Secondary RADIUS Server							
	<table> <tr> <td>Authentication Server</td><td>Enter the domain name or IP address of your RADIUS Server.</td></tr> <tr> <td>Authentication Port</td><td>Enter the Port number used for authentication</td></tr> <tr> <td>Authentication Secret Key</td><td>Secret Key used for authentication</td></tr> <tr> <td>Authentication</td><td>Select Challenge-Handshake Authentication Protocol (CHAP) or</td></tr> </table>	Authentication Server	Enter the domain name or IP address of your RADIUS Server.	Authentication Port	Enter the Port number used for authentication	Authentication Secret Key	Secret Key used for authentication	Authentication
Authentication Server	Enter the domain name or IP address of your RADIUS Server.							
Authentication Port	Enter the Port number used for authentication							
Authentication Secret Key	Secret Key used for authentication							
Authentication	Select Challenge-Handshake Authentication Protocol (CHAP) or							

Protocol	Password Authentication Protocol (PAP).
Accounting Service	Enable / Disable RADIUS accounting
Accounting Server	Enter the Accounting Server domain name or IP address.
Accounting Port	Enter the Port number used for accounting
Accounting Secret Key	Secret Key used for accounting.

Note: The Authentication Server and Accounting Service operates in sets, which means if the Authentication Server set under Primary RADIUS Server is unavailable then the system will refer to Secondary RADIUS Server setting without referencing the Accounting service settings under Primary.

6.1.3. Configuring Local

Local is the Controller's built-in static user account database. The number of user account supported will be different for different models. Please refer to the specification details for capacity number of your WHG Controller model.

Authentication Option - radius1	
Name	radius1 *
Postfix	local *
Black List	None ▼
Authentication Database	LOCAL ▼ <button>Configure</button>
Group	Group 1 ▼

- **Name:** Configurable text string designated as the mnemonic name of this authentication option.
- **Postfix:** Is the text string entered as a postfix in the account field for notifying the Controller which authentication database this account belongs to.
- **Black List:** System has built-in black-list profiles where specific user accounts can be listed. When selected and applied here, it tells the Controller that the accounts on the selected black list should be denied authentication.
- **Group:** The Group profile that will govern the users authenticated via this authentication option.
- **Authentication Database:** Select the authentication database that will be used for account validation when an authentication request is received. Click the button **Configure** for further configuration.

Local User Database Settings	
Local User List	
Account Roaming Out	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client Device Settings	

Local User List

The link will redirect to Local User List page where all Local users on the Controller's built-in Local database will be displayed. The page has an **Upload User** button for importing a list of user account from a text file and a **Download User** button

for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a Group and applied Local VPN individually.

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

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

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

Local User List				
Username	Password	MAC Address	Applied Group	<input type="button" value="Del All"/>
			Local VPN Enabled	
			Remark	
1	1		None	Delete
			No	

Add User: Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as “**Username**”, “**Password**”, “**MAC Address**”, and “**Remark**”. Select a desired **Group** to apply to this local user account. Check to enable *Local VPN* in the **Enable Local VPN** column if you wish to establish a VPN link between the Controller and user device using this local account. Click **Apply** to complete adding the user(s). MAC address entered here means that a networking device can be bound with a local user as well. Therefore user must login to system with a networking device (PC) that has this MAC address, so this user can not login with other networking device.

Adding User(s) to the List						
No.	Username*	Password*	MAC Address (xx:xx:xx:xx:xx:xx)	Group	Remark	Enable Local VPN
1	<input type="text" value="test"/>	<input type="password" value="...."/>	<input type="text"/>	Group 1 ▾	<input type="text" value="None"/>	<input checked="" type="checkbox"/>

6.1.4. Configuring LDAP

The **Lightweight Directory Access Protocol (LDAP)** is an application protocol for reading and editing directories over an IP network.

Authentication Option - Server 4	
Name	Server 4 *
Postfix	ldap *
Black List	None
Authentication Database	LDAP <input type="button" value="Configure"/>
Group	Group 1
Enable Local VPN	<input type="checkbox"/>

- **Name:** Configurable text string designated as the mnemonic name of this authentication option.
- **Postfix:** Is the text string entered as a postfix in the account field for notifying the Controller which authentication database this account belongs to.
- **Black List:** System has built-in black-list profiles where specific user accounts can be listed. When selected and applied here, it tells the Controller that the accounts on the selected black list should be denied authentication.
- **Group:** The Group profile that will govern the users authenticated via this authentication option.
- **Enable Local VPN:** When checked, users authenticating with this authentication option will have a VPN tunnel established automatically between the Controller and the user's client device.
- **Authentication Database:** Select the authentication database that will be used for account validation when an authentication request is received. Click the button **Configure** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisk are necessary information which should be filled in. These settings will become effective immediately after clicking the **Apply** button.

Primary LDAP Server	
Server	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(e.g. 389 for LDAP, 636 for LDAPS)
Service Protocol	<input checked="" type="radio"/> LDAP <input type="radio"/> LDAPS <input type="radio"/> LDAP+StartTLS
Base DN	<input type="text"/> *(e.g. cn=users,dc=domain,dc=com)
Binding Type	User Account
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN
Secondary LDAP Server	
Server	<input type="text"/>
Port	<input type="text"/>
Service Protocol	<input checked="" type="radio"/> LDAP <input type="radio"/> LDAPS <input type="radio"/> LDAP+StartTLS
Base DN	<input type="text"/>
Binding Type	User Account
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN
Group Mapping	
Attribute-Group Mapping	Map LDAP Attributes to Group

- **Server:** The IP address of the external LDAP server.
- **Port:** The authentication port of the external LDAP server.
- **Service Protocol:** The protocol used to communicate with the external LDAP server can be LDAP, LDAPS, or LDAP+StartTLS depending on the protocol type supported on your LDAP server.
- **Base DN:** The Base DN (Distinguished Name) is the LDAP search base, telling which part of the external directory tree to search from. Think of the Base DN as the "top" of the directory for your LDAP users although it may not always be the top of the directory itself. The search base may be something equivalent

to the organization, group, or domain name (AD) of external directory.

- **Binding Type:** This specifies the binding type and search scope for LDAP authentication with 4 binding types available: User Account, Anonymous, Specified DN and Windows AD.
- **Account Attribute:** The attribute of LDAP accounts.
- **Attribute-Group Mapping:** The administrator can specify the mapping of specific LDAP attributes (name and value) to Group profiles. When enabled, users login into the network with an LDAP account will have his/her user group determined based on the LDAP attribute the account carries.

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

6.1.5. Configuring POP3

Choose “**POP3**” from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.

Authentication Option - radius2	
Name	<input type="text" value="radius2"/> *
Postfix	<input type="text" value="pop3"/> *
Black List	<input type="text" value="None"/> ▾
Authentication Database	<input type="text" value="POP3"/> ▾ <input type="button" value="Configure"/>
Group	<input type="text" value="Group 1"/> ▾
Enable Local VPN	<input type="checkbox"/>

- **Name:** Configurable text string designated as the mnemonic name of this authentication option.
- **Postfix:** Is the text string entered as a postfix in the account field for notifying the Controller which authentication database this account belongs to.
- **Black List:** System has built-in black-list profiles where specific user accounts can be listed. When selected and applied here, it tells the Controller that the accounts on the selected black list should be denied authentication.
- **Group:** The Group profile that will govern the users authenticated via this authentication option.
- **Enable Local VPN:** When checked, users authenticating with this authentication option will have a VPN tunnel established automatically between the Controller and the user's client device.
- **Authentication Database:** Select the authentication database that will be used for account validation when an authentication request is received.

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

External POP3 Server Related Settings	
Username Format	<input type="radio"/> Complete (e.g. user1@companyname.com) <input checked="" type="radio"/> Only ID (e.g. user1)
Primary POP3 Server	
Server	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(Default: 110)
SSL Connection	<input type="checkbox"/> Enable
Secondary POP3 Server	
Server	<input type="text"/>
Port	<input type="text"/>
SSL Connection	<input type="checkbox"/> Enable

- **Username Format:** When **Complete** option is checked, both the username and postfix will be transferred to the server for authentication. When **Only ID** option is checked, only the username will be transferred to the external server for authentication.
- **Server:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Connection:** The system supports POP3S. Check the check box beside to **Enable SSL Connection** to POP3.

6.1.6. Configuring NT Domain

Choose “NT Domain” from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.

Authentication Option - radius3	
Name	<input type="text" value="radius3"/> *
Postfix	<input type="text" value=""/> *
Black List	None ▾
Authentication Database	NT Domain ▾ <button>Configure</button>
Group	Group 1 ▾
Enable Local VPN	<input type="checkbox"/>

- **Name:** Configurable text string designated as the mnemonic name of this authentication option.
- **Postfix:** Is the text string entered as a postfix in the account field for notifying the Controller which authentication database this account belongs to.
- **Black List:** System has built-in black-list profiles where specific user accounts can be listed. When selected and applied here, it tells the Controller that the accounts on the selected black list should be denied authentication.
- **Group:** The Group profile that will govern the users authenticated via this authentication option.
- **Enable Local VPN:** When checked, users authenticating with this authentication option will have a VPN tunnel established automatically between the Controller and the user’s client device.
- **Authentication Database:** Select the authentication database that will be used for account validation when an authentication request is received.

Click the button **Configure** for further configuration. Enter the server IP address and enable/disable the transparent

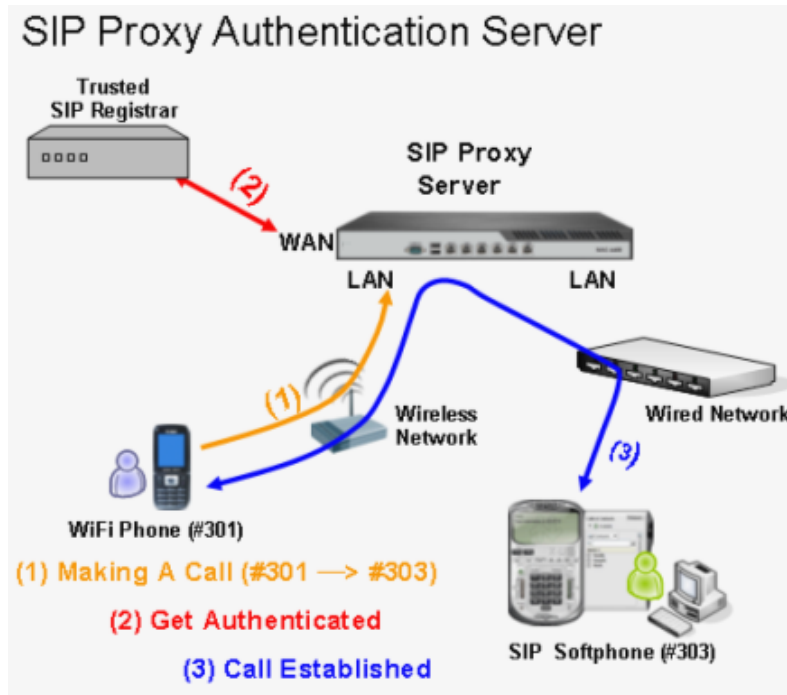
login function. These settings will become effective immediately after clicking the **Apply** button.

Domain Controller	
Server	<input type="text"/> *(IP Address)
Transparent Login	<p><input checked="" type="radio"/> Enable <input type="radio"/> Disable (Windows 2000, 2003 or above)</p> <p><input type="checkbox"/> Enable Local VPN</p> <p>(Note: When enabled, Local VPN connection will be automatically created under Transparent Login mode. For the Local VPN to work, however, it requires support from Windows Server - need to install additional logon script on Windows Server. Please refer to the User's Manual for more information.)</p>

- **Server:** The IP address of the external NT Domain Server.
- **Transparent Login:** This function refers to Windows NT Domain single sign-on. When *Transparent Login* is enabled, clients will log into the system automatically after they have logged into the NT domain, which means that clients only need to log in once.
 - **Enable Local VPN:** Check the checkbox to enable local VPN under transparent login mode. When enabled, local VPN connection will be automatically created under transparent login mode. For the local VPN to work under transparent login mode, however, it requires support from Windows Server – need to install additional logon script on Windows Server.

6.1.7. Configuring SIP

SIP (Session Initiation Protocol) is a protocol for making real-time calls over IP network. Currently, most of the SIP extensions address audio communication. Controller can act like a SIP Proxy Server that forwards end point' requests and responses. In other words, SIP Proxy server needs to log in the trusted registrar to verify identities of 2 clients. After enabling SIP proxy server, all SIP traffic pass through NAT with a selective but fixed WAN interface. In this example, client extension #301 is trying to call #303. Controller asks an external trusted SIP registrar to verify both identities. After SIP registrar responds with a YES, call is established through WHG-707.



The system provides SIP proxy for SIP clients (devices or soft clients) pass through NAT. After enable SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface. If the SIP Registrar settings in SIP client is same as the system setting, when the client try to access the SIP Registrar, system will let this client login automatically and all SIP traffic can pass through.

Configure Dynamic Domain Name Service, go to: **Users >> Authentication >> SIP.**

Authentication Server - SIP			
Trusted Registrar	IP Address		Remark
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>
Group	Group 1 ▼	Group selection applied to clients login with SIP authentication.	

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

SIP Interface Configuration

To configure Dynamic Domain Name Service, go to: **System >> Service Zones >> Service Zone Configuration.**

SIP Interface Configuration		
Enable <input type="checkbox"/>	WAN Interface	WAN1 ▼

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

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

6.1.8. Choosing Your Networks' Authentication method

For each Service Zone, network administrator can choose to enable or disable the need for authentication for that Service Zone.

Go to: Main Menu > System > Service Zones

Authentication Settings	
Authentication Required For the Zone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="radio"/> Suspend
MAC Authentication Configuration	<button>Configure</button>

Disabling the need to authenticate means that all users accessing the network via this Service Zone will not need to be authenticated before gaining access to the internet, however this way means that all users under this Service Zone will not be able to be enforced with different policies.

Authentication Settings	
Authentication Required For the Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Suspend
MAC Authentication Configuration	<button>Configure</button>

Enabling the need to authenticate means that any user accessing this Service Zone will need to be authenticated first before gaining access to the internet. The users' Group will be determined depending on which type of authentication server this user belongs to and therefore different authentication server's users in the authentication required Service Zone can be bounded with different policies as set in Service Zone – Group Mappings.

Authentication Settings	
Authentication Required For the Zone	<input type="radio"/> Enable <input type="radio"/> Disable <input checked="" type="radio"/> Suspend
MAC Authentication Configuration	<button>Configure</button>

Suspending a Service Zone's need to authenticate means that no newly connected users are allowed to access this Service Zone until it is configured back to either enabled or disabled by the network administrator.

A warning message can be customized at Main Menu > System > General page which will be displayed on the web browser of newly connected users when a Service Zone's authentication is under the Suspend status.

Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com <input checked="" type="checkbox"/> Use the name on the security certificate <small>(FQDN of this device for internal use, e.g. controller.office-name.com)</small>

The purpose of this feature is to prevent further loading to this Service Zone when network administrator needs to make changes to the Service Zone configurations. Once the configuration change is done and suspend is changed back to enable, currently online users of this service zone will be disconnected and request to re-authenticate.

Once you have enabled the need to authenticate for a Service Zone, which types of authentication servers allowed can be configured in the same page.

Authentication Options	Auth Option	Auth Database	Postfix	Default	Enable
	Server 1	LOCAL	ro	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
	On-demand User	ONDEMAND	od	<input type="radio"/>	<input checked="" type="checkbox"/>
	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>

All of the pre-configured authentication servers can be seen here. Under the “Enable” column, check the authentication servers that you wish to allow access to this service zone. In other words if an authentication server is checked here, its users can access this service zone after a successful login. One authentication server can be selected as “Default”, this means that users of this authentication server can omit the postfix during login.

6.2. Users Group

Group profiles are used to divide users based on role. A Group profile can be designated for differentiating a group of users with similar statuses e.g. Student, Staff, Guest, etc.; Network administrator can determine which Service Zones are accessible to a certain Group as well as the Policy that will govern the user. Therefore users belonging to a certain Group profile may be allowed to access many Service Zones and be govern by different policies under different Service Zone, depending on how the network administrator setup the Group – Service Zone mapping.

Configure Group settings; go to: **Users >> Group.**

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

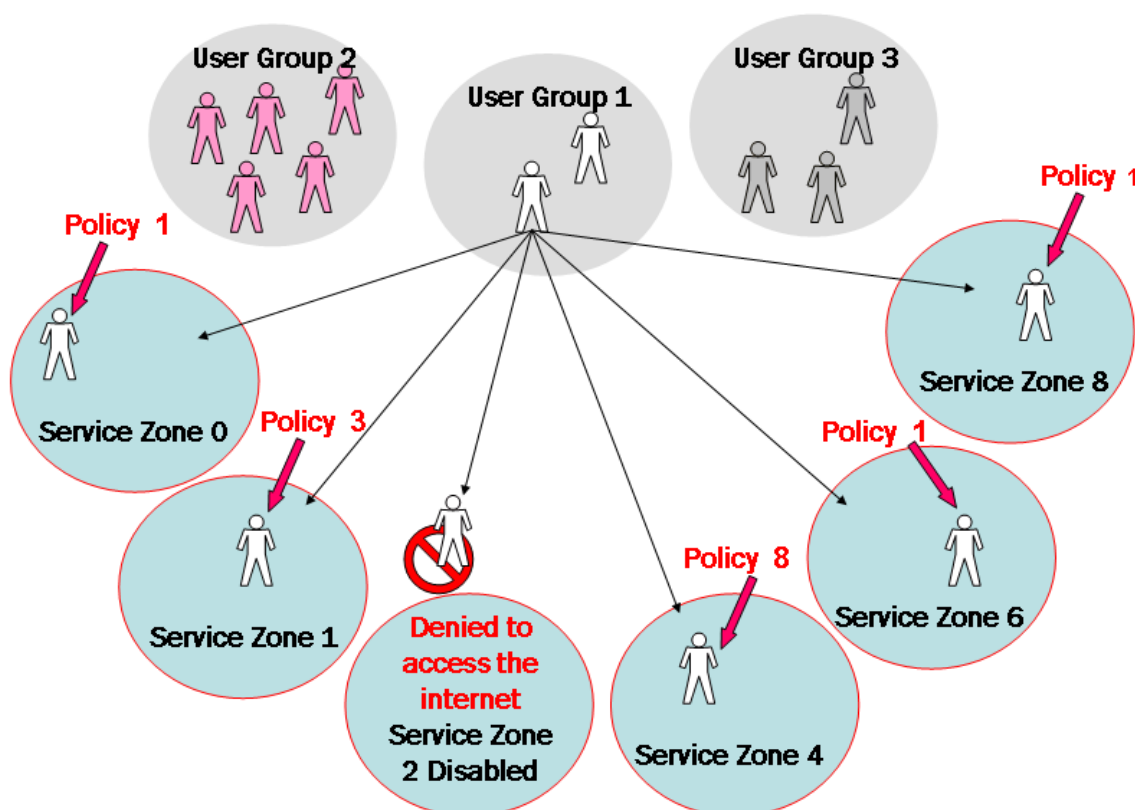
Screenshot above illustrates an example for Group 1. By checking the “Enable” check box of corresponding Service Zone, it means that users from Group 1 are allowed to access these Service Zones (allowed authentication). Policy that will be applied can also be selected here.

6.2.1. Assign users to a Group

Configure Group settings; go to: **Users >> Group**.

This section shows how to group users, how to rule each grouped user with different policy as he moves to different service zone. The following examples will help you better understand this section.

Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	Enabled	Policy	To Group Permission Configuration
Service Zone : Default	<input checked="" type="checkbox"/>	Policy 1	Default
Service Zone : SZ1	<input checked="" type="checkbox"/>	Policy 3	SZ1
Service Zone : SZ2	<input type="checkbox"/>	Policy 1	SZ2
Service Zone : SZ3	<input type="checkbox"/>	Policy 1	SZ3
Service Zone : SZ4	<input checked="" type="checkbox"/>	Policy 8	SZ4
Service Zone : SZ5	<input type="checkbox"/>	Policy 1	SZ5
Service Zone : SZ6	<input checked="" type="checkbox"/>	Policy 1	SZ6
Service Zone : SZ7	<input type="checkbox"/>	Policy 1	SZ7
Service Zone : SZ8	<input checked="" type="checkbox"/>	Policy 1	SZ8
Remote VPN	<input type="checkbox"/>	Policy 1	Remote VPN



In this example, Group 1 users are allowed to access the internet in 5 places; Service Zone 0,1,4,6, and 8. They must follow policy 1 at Service Zone 1, 6 and 8. They are ruled by Policy 3 at Service Zone 1 and by Policy 8 at Service Zone 4.

In each authentication option, you can assign a Group with each authentication option. All users login with same authentication server will belong to same Group.

Authentication Option - Server 1	
Name	<input type="text" value="Server 1"/> *
Postfix	<input type="text" value="local"/> *
Black List	<input type="text" value="None"/> ▼
Authentication Database	<input type="text" value="LOCAL"/> ▼ <input type="button" value="Configure"/>
Group	<input type="text" value="Group 1"/> ▼

But there are some exceptions:

- In Local Authentication, each user can assign to different Group one by one.
- In RADIUS Authentication, the users can assign to different Group by Class-Group Mapping.
- In LDAP Authentication, the users can assign to different Group by Attribute-Group Mapping.

6.2.2. Permission in Service Zone

Configure Group settings; go to: **User Authentication >> Group.**

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

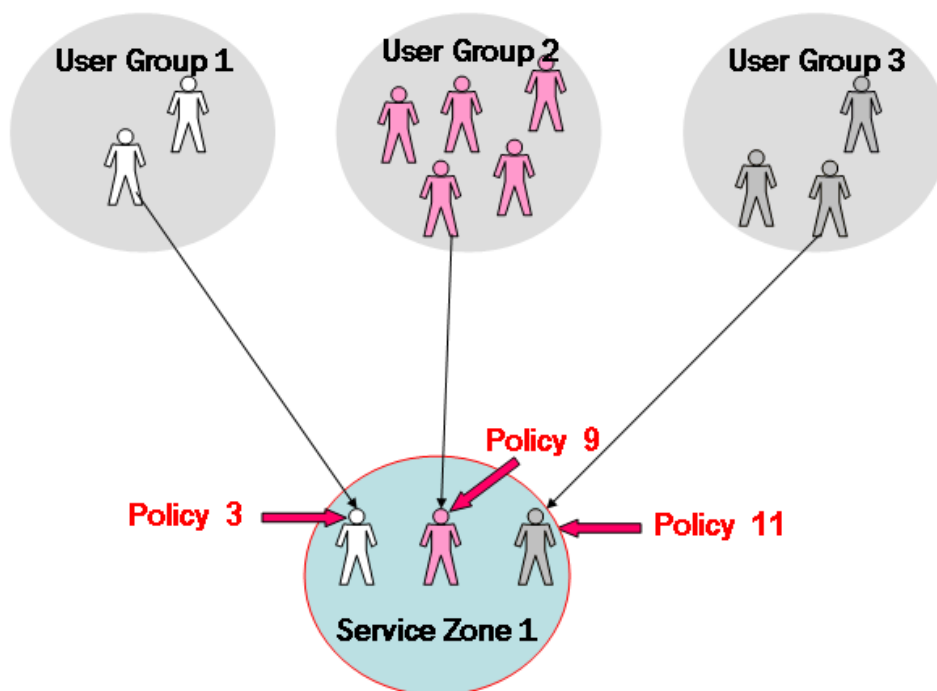
Group Configuration - Group 1			
Select Group	Group 1 <input type="button" value="v"/>		
QoS Profile	<input type="button" value="Configure"/>		
Privilege Profile	<input type="button" value="Configure"/>		
Remark	<input type="text"/>		

Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	Enabled	Policy	To Group Permission Configuration
Service Zone : Default	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	Default
Service Zone : SZ1	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ1
Service Zone : SZ2	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ2
Service Zone : SZ3	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ3
Service Zone : SZ4	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ4
Service Zone : SZ5	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ5
Service Zone : SZ6	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ6
Service Zone : SZ7	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ7
Service Zone : SZ8	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	SZ8
Remote VPN	<input checked="" type="checkbox"/>	Policy 1 <input type="button" value="v"/>	Remote VPN

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

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

Group Permission Configuration & Policy Assignment - Service Zone : Z1			
Group Option	Enabled	Policy	To Zone Permission Configuration
Group 1	<input checked="" type="checkbox"/>	Policy 3	Group 1
Group 2	<input checked="" type="checkbox"/>	Policy 9	Group 2
Group 3	<input checked="" type="checkbox"/>	Policy 11	Group 3
Group 4	<input type="checkbox"/>	Policy 4	Group 4
Group 5	<input type="checkbox"/>	Policy 5	Group 5
Group 6	<input type="checkbox"/>	Policy 6	Group 6
Group 7	<input type="checkbox"/>	Policy 7	Group 7
Group 8	<input type="checkbox"/>	Policy 8	Group 8



At Service Zone 1, Group 1 user is ruled by Policy 3. Group 2 is by Policy 9 and Group 3 is by Policy 11. Other Groups are not enabled to access Service Zone 1.

Group Permission Configuration & Policy Assignment - Service Zone : Default			
Group Option	Enabled	Policy	To Zone Permission Configuration
Group 1	<input checked="" type="checkbox"/>	Policy 1 ▾	Group 1
Group 2	<input checked="" type="checkbox"/>	Policy 2 ▾	Group 2
Group 3	<input checked="" type="checkbox"/>	Policy 3 ▾	Group 3
Group 4	<input checked="" type="checkbox"/>	Policy 4 ▾	Group 4
Group 5	<input checked="" type="checkbox"/>	Policy 5 ▾	Group 5
Group 6	<input checked="" type="checkbox"/>	Policy 6 ▾	Group 6
Group 7	<input checked="" type="checkbox"/>	Policy 7 ▾	Group 7
Group 8	<input checked="" type="checkbox"/>	Policy 8 ▾	Group 8
Group 9	<input checked="" type="checkbox"/>	Policy 9 ▾	Group 9
Group 10	<input checked="" type="checkbox"/>	Policy 10 ▾	Group 10

- **Group Option:** The name of Group options available for selection.
- **Enabled:** Select *Enabled* to allow clients of the enabled Groups to log in to this Service Zone under constraints of the selected Policies.
Check *Enabled* of each individual Group to assign it to the Service Zone listed.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing this Service Zone.
- **To Zone Permission Configuration:** Click the hyperlink in the **To Zone Permission Configuration** column to enter **Zone Permission Configuration & Policy Assignment** interface, which is based on the role of Group, to configure the relation between Group and Zone.

6.2.3. QoS Traffic Class and Bandwidth Control

Configure QoS; go to: **Users >> Group >> QoS Profile.**

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

Group 1 - Traffic Configuration	
Traffic Class	Best Effort ▼
Group Total Downlink	Unlimited ▼
Individual Maximum Downlink	0 Mbps ▼ <small>*(Unlimit: 0, Range: 1-999)</small>
Individual Request Downlink	None ▼
Group Total Uplink	Unlimited ▼
Individual Maximum Uplink	0 Mbps ▼ <small>*(Unlimit: 0, Range: 1-999)</small>
Individual Request Uplink	None ▼

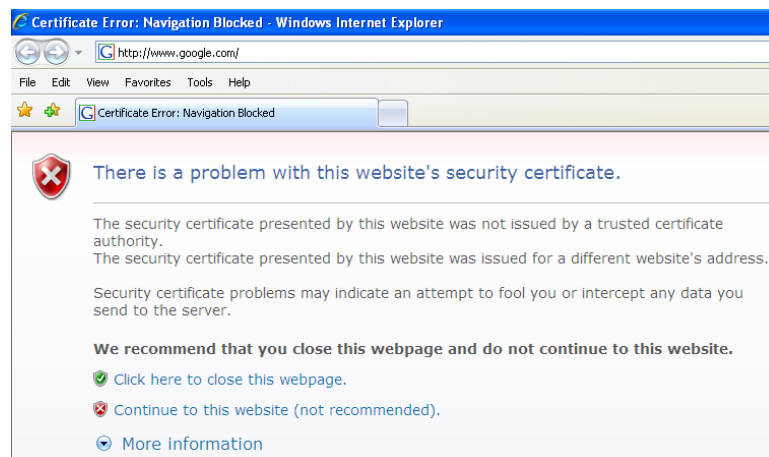
- **Traffic Class:** A Traffic Class can be chosen for a Group of users. There are four traffic classes: **Voice**, **Video**, **Best-Effort** and **Background**. **Voice** and **Video** traffic will be placed in the high priority queue. When **Best-Effort** or **Background** is selected, more bandwidth management options such as Downlink and Uplink Bandwidth will appear.
- **Group Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
- **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
- **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
- **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client belonging to this Group. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

6.3. User Login

6.3.1. An Example of User Login

Normally, users will be authenticated before they get network access through WHG Controller. This section presents the basic authentication flow for end users. Please make sure that the WHG Controller 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).
 - a) For the first time, if the WHG Controller is not using a trusted SSL certificate, there will be a “Certificate Error”, because the browser treats WHG Controller as an illegal website.



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

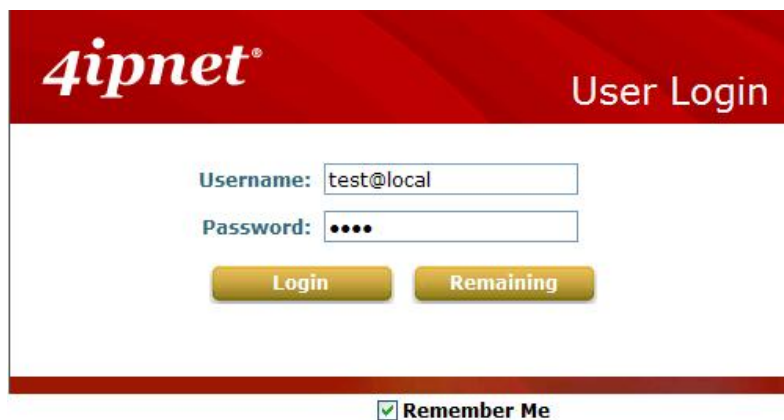


2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click **Submit** button. If the **Remember Me** check box is checked, the browser will remember this user's name and password so that he/she can just click Submit next time he/she wants to login.

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.

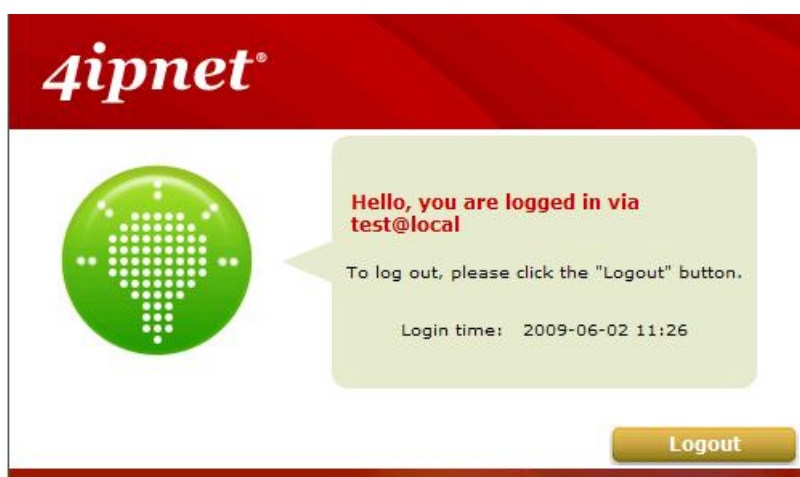
The **Remaining** button on the **User Login Page** is for on-demand users only, where they can check their

Remaining quota.



The image shows the 4ipnet User Login interface. It features a red header with the 4ipnet logo and the text "User Login". Below the header, there are two input fields: "Username:" with the value "test@local" and "Password:" with four dots. Below these fields are two buttons: "Login" and "Remaining". At the bottom of the form, there is a checkbox labeled "Remember Me" which is checked.

3. Successful! The **Login Successful** page appearing means you are connected to the network and Internet now!



The image shows the 4ipnet Login Successful page. It features a red header with the 4ipnet logo. Below the header, there is a green circular icon with a white grid pattern. To the right of the icon, there is a light green box containing the text: "Hello, you are logged in via test@local", "To log out, please click the 'Logout' button.", and "Login time: 2009-06-02 11:26". At the bottom right of the page, there is a yellow button labeled "Logout".

- **Note:** When On-demand accounts are used, the system will display more information, as shown below.



The image shows the 4ipnet Login Successful page for On-demand accounts. It features a red header with the 4ipnet logo. Below the header, there is a green circular icon with a white grid pattern. To the right of the icon, there is a light green box containing the text: "Hello, you are logged in via 3p6z@ondemand", "To log out, please click the 'Logout' button.", and "Login time: 2009-06-02 11:11". Below this box, there is a section labeled "Remaining Time:" with a timer showing "4 Hour 59 Min 51 Sec". At the bottom of the page, there are two yellow buttons: "Redeem" and "Logout".

6.3.2. Default Authentication

In each Service Zone, there are different types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. There are up to six authentication servers can be enabled, two of them constantly as Ondemand and SIP, and one of them can be set as the **Default Authentication**— so that users do not have to type in the postfix string while entering username during login.

A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap".

6.3.3. Login with Postfix

Set a postfix that is easy to relate (e.g. Local) user login with which authentication server. The acceptable characters are numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Beside the Default Authentication, all other authentication server users need to key in postfix in username during login in order for the Controller to recognize which authentication server to authenticate against.

7. Policies and Access Control

7.1. Policy

Configure Policy; go to: [Users >> Policy.](#)

WHG Controller supports multiple Policies, including one **Global Policy** and individual **Policies**. Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users.

Global Policy is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone.

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

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

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

When the type of database is **Local**, the **Group** selection function will be available to allow the administrator to assign a Group to each user one by one.

Global Policy

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

Policy Configuration - Global Policy	
Select Policy	Global <input type="button" value="v"/>
Firewall Profile	<input type="button" value="Configure"/>
Specific Route Profile	<input type="button" value="Configure"/>
Maximum Concurrent Sessions	300 <input type="button" value="v"/> (sessions per user)

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

Policy 1 ~ Policy n

Beside **Global Policy**, there are **Policy1** to **Policy n** (different models have different number of Policy), each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. The clients belonging to a Service Zone will also be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

Policy Configuration - Policy 1	
Select Policy	Policy 1 <input type="button" value="v"/>
Firewall Profile	<input type="button" value="Configure"/>
Specific Route Profile	<input type="button" value="Configure"/>
Schedule Profile	<input type="button" value="Configure"/>
Maximum Concurrent Sessions	300 <input type="button" value="v"/> (sessions per user)

- **Select Policy:** Select **Policy 1~Policy n** to set the **Firewall Profile**, **Specific Route Profile**, **Schedule Profile** and **Maximum Concurrent Sessions**.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this gateway settings, include default gateway.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

7.1.1. Firewall

Firewall Profile (Global Policy): Click **Setting** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **User Firewall Rules** to edit the rules. **Machine Firewall Rules – Input** is for editing firewall rules which will be enforced on traffics entering the WAN ports from the external network. **Machine Firewall Rules – Output** is for editing firewall rules which will be enforced on outgoing traffics from the internal network passing WAN ports. **DoS Protection** allows the administrator to select which type of attack to block by clicking the Enable checkbox.

Global Policy - Firewall Configuration	
Predefined and Custom Service Protocols	Configure
User Firewall Rules	Configure
Machine Firewall Rules - Input	Configure
Machine Firewall Rules - Output	Configure
DoS Protection	Configure

Firewall Profile (Policy 1, Policy 2, and etc.): Click **Setting** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **User Firewall Rules** to edit the rules.

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

■ Predefined Protocols

Predefined and Custom Service Protocols: There are predefined service protocols available for firewall rules editing.

Policy 1 - Service Protocols List			
No.	Name	Description	Select All
0	ALL	ALL	<input type="checkbox"/>
1	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
2	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL ICMP	ICMP; Type: Any, Code: Any	<input type="checkbox"/>
4	FTP	TCP/UDP; Destination Port: 20;21	<input type="checkbox"/>
5	HTTP	TCP/UDP; Destination Port: 80	<input type="checkbox"/>
6	HTTPS	TCP/UDP; Destination Port: 443	<input type="checkbox"/>
7	POP3	TCP; Destination Port: 110	<input type="checkbox"/>
8	SMTP	TCP; Destination Port: 25	<input type="checkbox"/>
9	DHCP	UDP; Destination Port: 67;68	<input type="checkbox"/>
10	DNS	TCP/UDP; Destination Port: 53	<input type="checkbox"/>

The administrator is able to add new custom service protocols by clicking **Add**, and delete the added protocols with **Select All** and **Delete** operations.



The Predefined Service Protocols can not be deleted.

Click **Add** to add a custom service protocol. The **Protocol Type** can be defined from a list of service by protocols (*TCP/UDP/ICMP/IP*); and then define the **Source Port** (range) and **Destination Port** (range); click **Apply** to save this protocol .

Add Service Protocol			
Name	<input type="text"/>		
Protocol Type	TCP ▾		
Source Port	<input type="text" value="1"/>	~	<input type="text" value="65535"/>
Destination Port	<input type="text" value="1"/>	~	<input type="text" value="65535"/>

If the **Protocol Type** is **ICMP**, it will need to define **Type** and **Code**.

Add Service Protocol			
Name	<input type="text"/>		
Protocol Type	ICMP ▾		
Type	<input type="text"/>	Code	<input type="text"/>

If the **Protocol Type** is **IP**, it will need to define **Protocol Number**.

Add Service Protocol	
Name	<input type="text"/>
Protocol Type	IP ▾
Protocol Number	<input type="text"/>

■ Rules

After the custom protocol is defined or just use the **Predefined Service Protocols**, you will need to enable the **Firewall Rule** to apply these protocols.

- **Firewall Rules:** Click the number of **Filter Rule No.** to edit individual rules and click **Apply** to save the settings. The rule status will show on the list. Check “**Active**” checkbox and click **Apply** to enable that rule.

This link leads to the Firewall Rules page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to **Always**, **Recurring** or **One Time**.

Policy 1 - Firewall Rules								
Create a New Rule								
No.	Active	Action	Rule Name	Source	Destination	Service	Schedule	Operation
				Source Interface	Destination Interface			
1	<input type="checkbox"/>	Block		ANY	ANY	ALL	Always	Edit Move to Insert Before Delete
				ALL	ALL			

Selecting the Filter Rule Number 1 as an example:

Policy 1 - Edit Filter Rule			
Rule Number	1		
Rule Name	<input type="text"/>		
Source		Destination	
Interface/Zone	ALL <input type="button" value="v"/>	Interface/Zone	ALL <input type="button" value="v"/>
IP Address <input type="button" value="v"/>	<input type="text" value="0.0.0.0"/>	IP Address <input type="button" value="v"/>	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0 (/0)"/> <input type="button" value="v"/>	Subnet Mask	<input type="text" value="0.0.0.0 (/0)"/> <input type="button" value="v"/>
MAC Address	<input type="text"/>		
Service Protocol	ALL <input type="button" value="v"/>		
Schedule	<input checked="" type="radio"/> Always <input type="radio"/> Recurring <input type="radio"/> One Time		
Action for Matched Packets	<input checked="" type="radio"/> Block <input type="radio"/> Pass		

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

■ Machine Firewall Rules – Input (Global Policy Only)

This configuration page is for administrators to configure firewall rules which will be enforced from the systems perspective to filter incoming traffics passing through WAN ports from external networks.

Policy MFIR - Firewall Rules								
No.	Active	Action	Rule Name	Source	Destination	Service	Schedule	Operation
				Source Interface	Destination Interface			
(Total:0) First Prev Next Last								
Create a New Rule								

■ Machine Firewall Rules – Output (Global Policy Only)

This configuration page is for administrators to configure firewall rules which will be enforced from the systems perspective to filter outgoing traffics passing through WAN ports from the internal network.

Policy MFOR - Firewall Rules								
No.	Active	Action	Rule Name	Source	Destination	Service	Schedule	Operation
				Source Interface	Destination Interface			
(Total:0) First Prev Next Last								
Create a New Rule								

■ DoS Protection (Global Policy Only)

This configuration page is for administrators to configure which types of DoS attack to block. This feature is enforced from the systems perspective to block DoS attacks coming from the external network.

DoS Protection			
Name	Remark	Coverage	Enable
Reverse Path Filter	If a packet is received on the interface which is not used to forward the traffic to the source of the packet, it will be dropped. Packets with spoofed source IP addresses will be dropped.	Machine & LAN Subnets	<input type="checkbox"/>
Prohibit Source Route	Drop packets carrying source router options.	Machine & LAN Subnets	<input type="checkbox"/>
Enable TCP SYN cookies	TCP protocol stack sends out syncookies when the syn backlog queue of a socket overflows. This is to prevent against the common "SYN Flood" attack.	Machine	<input checked="" type="checkbox"/>
Drop Broadcast ICMP	Drop all ICMP ECHO and TIMESTAMP requests via broadcast/multicast. This can prevent "Smurf" attack.	Machine	<input type="checkbox"/>
Drop fragmented ICMP Packet	Drop fragmented ICMP Packet. This can prevent "Ping of Death" attack.	Machine	<input checked="" type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Limit ICMP Requests	Drop ICMP requests if more than 20 ICMP requests received per second. This can prevent "Ping Flood" attack.	Machine	<input checked="" type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>

Validate TCP flags	Drop packets with bad TCP flags. This can prevent possible "NMAP", "Null Scan", and "Xmas" attacks.	Machine	<input checked="" type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Drop IGMP	Drop IGMP Packets.	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Drop fragmented UDP	Drop fragmented UDP packets. This can prevent Teardrop attacks.	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>

Scan Nimda	Drop packets containing the signature of computer worm "Nimda".	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Scan Code Red	Drop packets containing the signature of computer worm "Code Red".	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Port Scan Detection	If a source address sends multiple packets to different ports in a short time, Port Scan Detection engine will drop the excessive TCP or UDP packets to protect this system.	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Block Martian Address	Drop packets from WAN interface whose source address is a so-called "Martian Address" - an address that is reserved, including any address within 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, or 224.0.0.0/4.	Machine	<input type="checkbox"/>
		LAN Subnets	<input type="checkbox"/>
Block Connections from WAN	Allow connections initiated from LAN subnet, and block TCP/UDP connections initiated from Internet/WAN.	LAN Subnets	<input checked="" type="checkbox"/>

7.1.2. Routing

- **Specific Route Profile:** Click the button of **Setting** for **Specific Route Profile**, the Specific Route Profile list will appear.

7.1.2.1 Specific Route

- **Specific Route Profile:** The Specific Default Route is use to control clients to access some specific IP segment by the specified gateway.

Global Policy - Specific Routes			
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>
2	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>

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

7.1.2.2. Default Gateway

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

Policy 1 - Specific Default Route			
Enable <input type="checkbox"/>	Default Gateway: IP Address ▼ <input type="text"/>		
Policy 1 - Specific Routes			
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>
2	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>

- **Enable:** Check **Enable** box to activate this function or uncheck to inactivate it.
- **Default Gateway:** It may be **WAN1 Default Gateway**, **WAN2 Default Gateway** or to specific an **IP Address**, if you select **IP Address**, you may need to fill the IP address of the gateway.

7.1.3. Schedule

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

☒ Enable ☐ Disable

Policy 1 - Permitted Login Hours							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
01:00~01:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
02:00~02:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03:00~03:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
04:00~04:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

7.1.4. 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. Also this can be specified in the other policies to apply to the authenticated users.
- When the number of a user's sessions reaches the session limit, 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.

7.2. User Access Control

WHG Controller supports user access control per service zone, for the entire system, or per authentication server.

MAC Access Control per Service Zone

Go to Main Menu > System > Service Zones.

Each Service Zone's Wireless Settings will be applied to APs that are mapped to this service zone. There is a MAC Access Control section where the administrator can specify up to 10 MAC addresses which can be allowed, denied to access this service zone wirelessly.

Wireless Settings				
SSID	SSID1 *			
Security	Authentication	Open System <input type="checkbox"/> Enable 802.1X Authentication		
	Encryption	None		
Access Control	Status	Disable		
	User Limit	32 *(Range: from 1 to 32)		
	MAC Address	1		Disable
		2		Disable
		3		Disable
4			Disable	
5			Disable	
	6		Disable	
	7		Disable	
	8		Disable	
	9		Disable	
	10		Disable	

Access Control – Status: Disable means there is no limitation as to what MAC address are allowed or not allowed to access this service zone. Allowed means that only the MAC addresses listed are allowed to access this service zone wirelessly. Denied means that the MAC addresses listed are not allowed to access this service zone wirelessly. Each MAC entry can also be enabled or disabled on the list separately.

MAC Access Control for the entire system

Go to Main Menu > Users > Additional Control > MAC ACL.

Access Control List		Add MACs
<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Disable		
No.	MAC Address	Delete All

The administrator can enter multiple MAC address entries by clicking the Add MACs button. This MAC ACL list is enforced to the whole Controller. Allow means that only the MAC addresses listed are allowed to access the Controller's network. Deny means that the MAC addresses listed are not allowed to access the Controller's network. Disable means that this MAC ACL list is not enforced and that there is not restriction on MAC addresses on the whole system.

Black List

Go to Main Menu > Users > Black List.

Black List Settings		
Select Black List	1:Blacklist1 ▼	
Name	Blacklist1	
User	Remark	Del All

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) (Page:1/1)

[Add User\(s\)](#)

There are multiple Black List profiles available. Administrator can select one and enforce this black list on the desired authentication server. Click Add User(s) button to fill in usernames (postfix not required). When enforced on an authentication server, accounts in the black list will be denied authentication and network access.

Privilege Users

Setup the **Privilege IP Address List** and **Privilege MAC Address List**. The clients in the list can access the network without any login.

Privilege List	
IP Address List	Configure
MAC Address List	Configure
IPv6 Address List	Configure

Privilege IP

Privilege IP/IPv6 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 “**Granted Access by IP Address**”. The “**Remark**” field is not necessary but is useful to keep track. Controller allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

In addition to granting privileges to just IP addresses, administrator could also specify IP and MAC address sets in this Privilege IP Address List. It is more secure to specify both the IP and MAC address of a privileged client that requires no authentication.

Please note, the bandwidth of a client in the Privilege IP Address List will be bounded by the bandwidth limit in the configured QoS Profile. However, the bandwidth of a client in the Privilege MAC Address List will not be bounded at all.

Backup IP Privilege List

Restore IP Privilege List

Search IP

Granted Access by IP Address						Create a New Item
No.	IP Address	MAC Address	QoS Profile	Policy	Remark	Action
1	10.0.5.123		None	Global		Edit Delete

Backup IPv6 Privilege List

Restore IPv6 Privilege List

Search IPv6

Granted Access by IPv6 Address			
No.	IPv6 Address	MAC	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>



Permitting specific IP addresses to have network access rights without going through standard authentication process under service zone may cause security problems.

Privilege MAC

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 “**Granted Access by MAC Address**”. Controller allows specific 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**.

Granted Access by MAC Address		
No.	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"/>



Permitting specific MAC addresses to have network access rights without going through standard authentication process under service zone may cause security problems

7.3. Session Limit & Session Log

Session Limit

To prevent ill-behaved clients or malicious software from using up system's connection resources, administrators will have to 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 each Policy profile, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones will follow Global policies session limit.
- 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 the SYSLOG server specified in the *Email & SYSLOG*.
- 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 the network deployment to protect the network in daily operation.

Session Log

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

- The following table shows the fields of a session log record.

Field	Description
Date and Time	The date and time that the session is established
Session Type	[New]: This is the newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user; It shows "N.A." if 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. Note: Only 31 characters are available for the combination of Session Type plus Username. Please change the account name accordingly, if the name is not identifiable in the record.
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

➤ The following table shows an example of the session log data.

Jul 20 12:35:05 2009	[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
Jul 20 12:35:05 2009	[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
Jul 20 12:35:06 2009	[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
Jul 20 12:35:06 2009	[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
Jul 20 12:35:07 2009	[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
Jul 20 12:35:09 2009	[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
Jul 20 12:35:10 2009	[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

8.Users' Login and Logout

8.1. Before User Login

8.1.1. Login with SSL

Configure HTTPS; go to: **System >> General.**

HTTPS (HTTP over SSL or HTTP Secure) by means of Secure Socket Layer (SSL) or Transport Layer Security (TLS) encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

This function will provide extra security upon client's login. Enable to activate https (encryption) or disable to activate http (non encryption) login page.

General Settings for the Entire System	
System Name	<input type="text"/>
Administrator Contact Information	<input type="text"/>
Suspend Warning Message	<input type="text" value="Sorry! The service is suspended."/> *
Internal Domain Name	<input type="text" value="gateway.example.com"/> <input checked="" type="checkbox"/> Use the name on the security certificate <small>(FQDN of this device for internal use, e.g., controller.office-name.com)</small>
Disclaimer Page	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Portal URL	<input checked="" type="radio"/> Specific <input type="radio"/> Original <input type="radio"/> None <input type="text" value="http://www.google.com"/> *(e.g., http://www.example.com)
User Log Access IP Address	<input type="text"/> (e.g., 192.168.2.1)
Management IP Address List	<input type="button" value="Configure"/>
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Configure"/>
HTTPS Certificate	Default CERT <input type="button" value="v"/>
HTTPS Protected Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time	<div>System Time : 2011/03/18 19:20:57</div> <div>Time Zone : <input type="text" value="(GMT+08:00)Taipei"/> <input type="button" value="v"/></div> <div><input checked="" type="radio"/> NTP</div> <div>NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> *(e.g., tock.usno.navy.mil)</div> <div>NTP Server 2: <input type="text" value="ntp1.fau.de"/></div>

8.1.2. Internal Domain Name with Certificate

Configure Internal Domain Name; go to: **System >> General >> Internal Domain Name.**

Internal Domain Name is the domain name of the WHG CONTROLLER as seen on client machines connected under service zone. It must conform to FQDN (Fully-Qualified Domain Name) standard. A user on client machine can use this domain name to access WHG CONTROLLER instead of its IP address.

In addition, when “**Use the name on the security certificate**” option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.

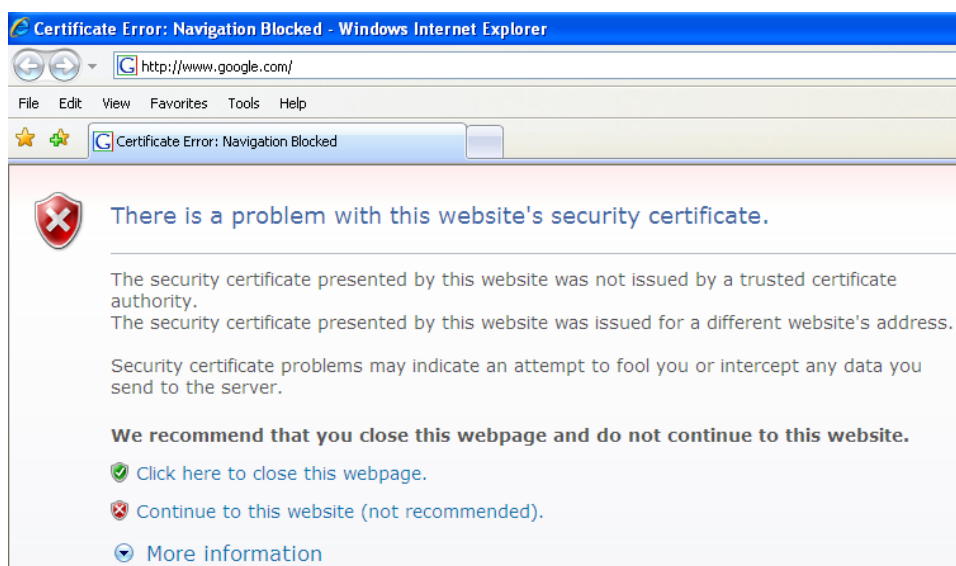
Configure Certificate; go to: **Users >> Additional Control >> Certificate Upload.**

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

After Create Root CA, please select **Upload Certificate**. Click **Browse** to select the file and upload it. Click **Apply** to complete the upload process.

Certificate Utility	
Upload Certificate ▾	
Upload Certificate	
Private Key	<input type="text"/> <input data-bbox="890 1193 975 1216" type="button" value="Browse..."/>
Certificate	<input type="text"/> <input data-bbox="890 1238 975 1261" type="button" value="Browse..."/>
Certification Path Verification	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

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



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

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

[Main Menu](#) > [Users](#) > [Additional Control](#) > [Certificate](#) > Use Default Certification

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

8.1.3. Walled Garden

Configure Walled Garden; go to: **Network >> Walled Garden.**

This function provides certain free services for users to access the websites listed here before login and authentication. Specific 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				Add Walled Garden List
No.	Active	Domain Name/IP Address	Remark	
(Total 0/40) First Prev Next Last Go to Page <div><div></div></div> Row per Page: 20 <div><div></div></div>				

8.1.4. Walled Garden AD List

Configure Walled Garden AD List; go to: **Network >> Walled Garden AD List.**

This function provides advertisement web pages for users to access free advertisement websites listed before login and authentication. Advertisement hyperlinks are displayed on the user's login page. Clients who click on it will be redirected to the listed advertisement websites.

Walled Garden Ad List				
Item	URL	Description	Topic	
1				<div>Edit</div> <div>Display <input type="checkbox"/></div>

- **Edit:** Click **Edit** to add a new item or make changes. Click **Apply**, the items will be added and shown in the list.
- **Display:** Choose **Display** to display advertisement hyperlinks on the login pages

Walled Garden Ad List Item 1	
URL	<input type="text" value="http://www.ykcafe.com"/>
Topic	<input type="text" value="YK Cafe"/>
Description	<input type="text" value="Welcome to YK Cafe!"/>

Walled Garden Ad List Item 2	
URL	<input type="text" value="http://www.google.com"/>
Topic	<input type="text" value="Google"/>
Description	<input type="text" value="No. 1 Search Engine"/>

Walled Garden Ad List Item 3	
URL	<input type="text" value="http://www.yahoo.com"/>
Topic	<input type="text" value="Yahoo!"/>
Description	<input type="text"/>



Walled Garden Ad List				
Item	URL	Description	Topic	
1	http://ykcafe.com	YK Cafe		<div>Edit</div> <div>Display <input checked="" type="checkbox"/></div>
2	http://www.google.com	Google		<div>Edit</div> <div>Display <input checked="" type="checkbox"/></div>
3	http://www.yahoo.com	Yahoo!		<div>Edit</div> <div>Display <input checked="" type="checkbox"/></div>

4ipnet[®]

User Login

Username:

user01

Password:

•••••

Login

Remaining

☐ Remember Me

- ☒ [YK Cafe](#) Welcome YK Cafe!
- ☒ [Google](#) No. 1 Search Engine
- ☒ [Yahoo!](#)

8.1.5. Mail Message

Configure Mail Message, go to: **System >> Service Zones.**

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

When enabled, the system will automatically send an email to users if they attempt to send/receive their emails using POP3 email program (for example, Microsoft Outlook) before they are authenticated. Click **Edit Mail Message** to edit the message in HTML format.

POP3 Email Message Editing - Service Zone: Default	
Email Contents in HTML	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD> <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii"> </HEAD> <BODY> <DIV> <DIV> Welcome! </DIV> <DIV> </DIV></pre>

8.2. After User Login

8.2.1. Portal Home Page

Configure Home Page Redirect; go to: **System >> General.**

Portal URL function allows the network administrator to specify whether to redirect a user's web browser to a specific webpage or not.

When "Specific" is checked, once a user logged in successfully, user's web browser will be redirected to the specified URL as set in the test box, such as *http://www.google.com*, regardless of the original homepage set in their computers.

Portal URL	<input checked="" type="radio"/> Specific <input type="radio"/> Original <input type="radio"/> None
	<input type="text" value="http://www.google.com"/> <small>*(e.g. http://www.example.com)</small>

When "Original" is selected, once a user logged in successfully, user's web browser will be redirected to the homepage URL as set in his browser configurations.

When "None" is selected, once a user logged in successfully, user's web browser will not be redirected to any URL.

8.2.2. Idle Timer

Configure Idle Timer; go to: **Users >> Additional Control.**

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

Additional Control	
User Session Control	Idle Timeout (minutes) <input type="text" value="10"/> <small>*(1-1440)</small>
	Idle Timeout Check Direction <input type="radio"/> Uplink <input checked="" type="radio"/> Uplink & Downlink
	Multiple Login <input type="checkbox"/> Enable <small>(Authentication options using On-demand and RADIUS databases will not support this function.)</small>
	Charge Traffic to/from Hosts in Walled Garden List <input type="radio"/> Enable <input checked="" type="radio"/> Disable

8.2.3. Multiple Login

Configure Idle Timer, go to: **Users >> Additional Control.**

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

Additional Control	
User Session Control	Idle Timeout (minutes) <input type="text" value="10"/> <small>*(1-1440)</small>
	Idle Timeout Check Direction <input type="radio"/> Uplink <input checked="" type="radio"/> Uplink & Downlink
	Multiple Login <input checked="" type="checkbox"/> Enable (Authentication options using On-demand and RADIUS databases will not support this function.)
	Charge Traffic to/from Hosts in Walled Garden List <input type="radio"/> Enable <input checked="" type="radio"/> Disable

8.2.4. Change Password Privilege

Configure Local Users change password privilege; go to: **Users >> Group >> Privilege.**

➤ **Privilege Profile:**

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

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



This function is not applicable for on-demand users.

8.2.5. Proxy Server

Configure Proxy Server; go to: **Network >> Proxy Server**.

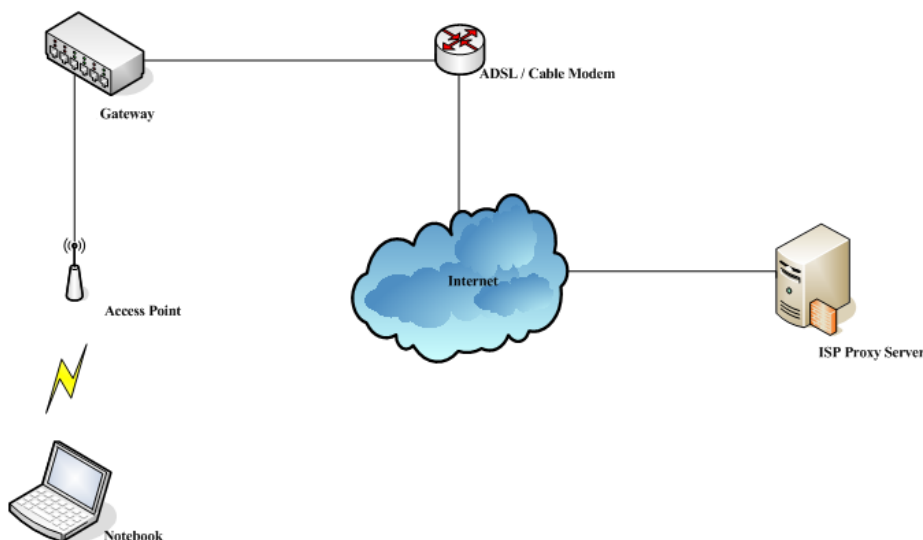
The system provides a Build-in Proxy Server and External Proxy Server function. After successful authentication, the clients' will be redirected back to the desired proxy servers.

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 WHG CONTROLLER.

Outgoing Proxy Traffic	
Proxy Server	<input type="radio"/> Enable Build-in <input checked="" type="radio"/> Disable Build-in <input type="radio"/> External

■ 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.



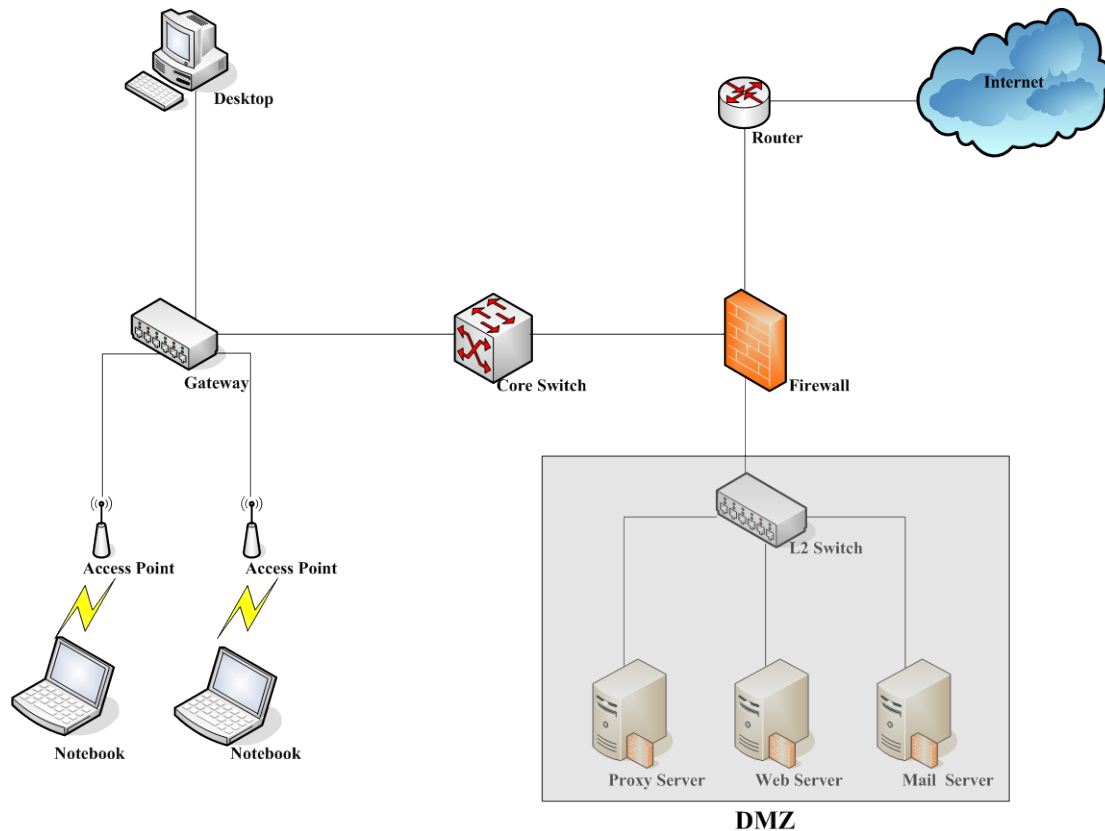
Follow the following steps to complete the proxy configuration:

- Step 1.** Log into the system by using the **admin** account.
- Step 2.** **Network >> Proxy Server >> External Proxy Servers** page.
Enable the **Built-in Proxy Server**. Click **Apply** to save the settings.

Outgoing Proxy Traffic	
Proxy Server	<input checked="" type="radio"/> Enable Build-in <input type="radio"/> Disable Build-in <input type="radio"/> External

■ 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.




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. Select **External** for Proxy Server. Add the IP address and port number of the Proxy server into External Proxy Servers setting. Click **Apply** to save the settings.


Outgoing Proxy Traffic	
Proxy Server	<input type="radio"/> Enable Build-in <input type="radio"/> Disable Build-in <input checked="" type="radio"/> External
External Proxy Server	External Proxy : <input type="text" value="10.168.1.100"/> External Proxy Port : <input type="text" value="6588"/>


9.Local Area AP Management


All of the supported APs under management of the system will be shown in this table and listed by different AP type.



System


Users


Access Points


Network


Utilities


Status

[Main Menu](#) > Access Points

Welcome to AP Management System

The AP Management System is a Web-interface management system.It is able to manage the both local area and wide area APs:

Enter Local Area AP Management

Enter Wide Area AP Management

9.1. Multiple Type of AP

Besides letting users being connected to the WHG Controller via wired Ethernet cable, you can connect AP to the WHG Controller to extent the network access by wireless. The WHG Controller can manage multiple type of AP, such as, EAP100, EAP-110, EAP-200, EAP-300, EAP700, OWL400, OWL410, OWL500 and OWL510. Almost all the settings of these Local Area APs can be configured from the WHG Controller's WMI.

This is because apart from personal or home usage, most other environment typically needs more than one AP to service a lot of clients; places like franchised hotspots, multiple offices, school campuses etc. where in many of these environments it is required to cover both indoor and outdoor areas. Therefore, it is necessary to be able to manage multiple types of APs (Indoor and Outdoor) at the same time.

View AP Overview; go to: **Access Points >>Enter Local Area AP Management >> Overview.**

In the Overview page, all of the supported AP type will be listed here.

AP Type List				
AP Type	No. of AP	OnLine	OffLine	No. of Client
EAP100	0	0	0	0
EAP110	0	0	0	0
EAP200	0	0	0	0
EAP300	0	0	0	0
EAP700	0	0	0	0
OWL400	0	0	0	0
OWL410	0	0	0	0
OWL500	0	0	0	0
OWL510	0	0	0	0

Because the WHG Controller can manage many different models of access points, the easiest way to configure a lot of APs is by AP Template. You can configure one template for each AP model, and then apply this template to many managed APs at once.

9.2. Configure AP Template

Configure AP Template; go to: **Access Points >> Enter Local Area AP Management >> Templates.**

The system supports up to three templates which include configurations of APs. The administrator can configure the setting together in the template instead of logging the AP management interface to set the configurations one by one. Select the **AP type** (if available) and one of the three available templates, and then click **Edit** to have the **Template Editing** page.

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

Input the template **Name** and **Remark** for easy reference and memorization. An easy way to configure a template is to copy the configuration of an already configured AP to the template. Select the desired AP from **Copy Setting's From** list and click apply to copy the selected AP's configuration to the template.

If copy is not desired, please select **NONE** then click the button of **Configure** to proceed with manual template configuration.

Template Editing - EAP100	
Name	TEMPLATE1 <input type="button" value="Configure"/>
Copy Settings From	None ▾
Remark	Template 1

- **Template Editing:** The administrator can set the template configuration manually or copy the configurations from a specific existing managed AP by **Copy Settings From** option. Click **Configure** button to have detailed configurations.
 - ◆ **Name:** The name shown for this particular template.
 - ◆ **Copy Settings From:** Select a pre-configured existing AP and click **Apply** to save its settings as the template settings.
 - ◆ **Remark:** The remark or additional information for this template profile.

- **Template Configuration**

To configure a template manually please click the **Configure** button.

Reset

General - EAP100: TEMPLATE1	
Subnet Mask	255.255.0.0 *
Default Gateway	192.168.1.254 *
NTP	Time Zone (GMT+08:00)Taipei,Taiwan ▼ NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Disabled ▼
SYSLOG	Disabled ▼

- **General:** In this section, revise the **Subnet Mask** and **Default Gateway** here if desired. Configure the **NTP Servers** and **Time Zone**. In addition, administrator can enable **SYSLOG** server to receive the log from AP and enable **SNMP** read/write ability.

Wireless - EAP100: TEMPLATE1	
SSID Broadcast	Enabled ▼
Band	802.11b+802.11g ▼
Data Rate	Auto ▼
Preamble	Long Only ▼
IAPP	Disabled ▼
Wireless Client Isolation	Disabled ▼
Transmit Power	Auto ▼
Wireless QoS WMM	Enabled ▼
Fragment Threshold	2346 (Default: 2346; Range: 256 ~ 2346)
RTS Threshold	2346 (Default: 2346 ; Range: 1 ~ 2346)
Beacon Interval (ms)	100 (Default: 100; Range: 100 ~ 500)

- **Wireless:**
- **SSID Broadcast:** Select this option to enable the AP's SSID to broadcast in your network. It is suggested to disable SSID broadcast feature when you have an authentication disabled network intended for private use.
 - **Band:** Depending on the AP model template you are editing there are different modes to select, **802.11a**, **802.11b**, **802.11g**, **802.11a+802.11n**, **802.11b+802.11g** and **802.11g+802.11n**.
 - **Data Rate:** The default is set to **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to allow the Access Point to automatically use the fastest rate possible.
 - **Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
 - **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association

throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.

- **Wireless Client Isolation:** The default value is **Disabled**. When “**Enabled**” is selected, all the wireless clients will be isolated each other.
- **Transmit Power:** The default is **Auto**. Select from the range or keep the default setting, **Auto**, to allow the Access Point to automatically adjust transmit power based on AP's loading.
- **Wireless QoS WMM:** Select **Enabled** will allow the packets with QoS WMM processed with higher priority.
- **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet. Set the maximum packet size here, packets larger than the configured threshold will be fragmented before transmission.
- **RTS Threshold:** Request To Send. When a packet size has reached or exceeded the configured threshold, the computer will need to send a request to send message to the AP. The computer will wait for a CTS (Clear To Send) message before sending data.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal is transmitted between the access point and the wireless network.

9.3. AP Discovery

Configure Discovery AP; go to: **Access Points >> Enter Local Area AP Management >> Discovery.**

After AP template configuration is complete, use this function to detect and scan for all of the APs connected under the managed network. Note that in **Local Area AP Management** the WHG Controller can only manage APs that are connected to its LAN ports. Therefore, the AP discovery function is for adding locally connected APs to its management list. The administrator must know the local IP addresses of the APs he/she wishes to discover. Or the alternative is to reset the AP to default setting for discovery.

Discovery Settings					
AP Type	EAP100 ▾				
Interface	Default ▾				
Admin Settings Used to Discover	<input checked="" type="radio"/> Factory Default IP Address: 192.168.1.1 Login ID: admin Password: admin <input type="radio"/> Manual				
<div>Scan Now</div>					

Background AP Discovery		
Status	Disabled	<div>Configure</div>

Discovery Results					
AP Type	IP Address	AP Name	Template	Service Zone	<div>Add</div>
	MAC Address	Password	Channel		
(Total: 0) First Prev Next Last					

- To discover AP:
 - **AP Type:** Choose the type of AP you wish to discover.
 - **Interface:** Select which interface to scan. For example if “Default” is selected, all of the APs connected under default service zone matching the selected AP type will be scanned and listed.
 - **Admin Settings Used to Discover:** Select “Factory Default” when the connected AP is under default settings. Select “Manual” and fill in the IP address range if the connected APs’ IP address has been modified.

Click the **Scan Now** button and the APs matching the configured criteria will be displayed in the **Discovery Results** list below.

- **Discovery Results:** The newly discovered APs will be listed here. When the system's Service Zone is set to Tag-based mode, service zones also can be assigned here. After clicking **Add**, the current management page is directed to AP List, where the newly added APs will show up in the AP List with a status of "configuring". It may take a couple of minutes to see that the status of the newly added AP change from "configuring" to "online" or "offline".

Discovery Results					
AP Type	IP Address	AP Name	Template	Service Zone	Add
	MAC Address	Password	Channel		
EAP700	192.168.1.1	NEWDEV-00001	TEMPLATE1 ▾	Default	<input type="checkbox"/>
	00:A7:03:14:CA:02	admin	Auto ▾		

- **AP Type:** The model type of the discovered APs.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **AP Name:** Mnemonic name of the specific AP, configurable.
- **Admin Password:** Password required for this AP, configurable.
- **Template:** Administrator can select a template profile which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.
- **Service Zone:** The item is only available for selecting service zone when **Tag-Based** mode is selected.
- **Add:** The administrator can click **Add** button to register the APs to the **List** for management.

Input the desired name and password for the AP. Select one template, preferred channel, check the Add checkbox and then click **Add** button to add it under the managed list.

When the AP is added, it will show up in the list below and be given a new IP address (depending on which Service Zone it belongs to e.g.: 192.168.10.1).

AP List						
<input type="checkbox"/>	AP Name	No. of Client	IP Address	Service Zone	Status	
			MAC Address		Channel	
<input type="checkbox"/>	NEWDEV-00001	0	192.168.10.1	Default	Configuring	▲
			00:A7:03:14:CA:02		NA	

9.3.1. AP Background Discovery

Configure AP Background Discovery; go to: **AP Management >> Enter Local Area AP Management >> Discovery.**

- **Background AP Discovery:** Click **Configure** to enter **Background AP Discovery** interface and proceed with related configuration.

Discovery Settings					
AP Type	EAP100				
Interface	Default				
Admin Settings Used to Discover	<input checked="" type="radio"/> Factory Default IP Address: 192.168.1.1 Login ID: admin Password: admin <input type="radio"/> Manual				
<div>Scan Now</div>					

Background AP Discovery		
Status	Disabled	<div>Configure</div>

Discovery Results					
AP Type	IP Address	AP Name	Template	Service Zone	<div>Add</div>
	MAC Address	Password	Channel		

The configuration is the same as **AP Discovery**. When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and **Auto Adding AP to the List** is enabled, it will be assigned an available IP from the starting IP address set in checked Service Zone profile and applied with the selected template. You can also set the channel of the AP would use.



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

9.4. Manually add AP

Add an AP Manually; go to: **Access Points >> Enter Local Area AP Management >> Adding.**

The administrator can add supported APs into the **List** table manually here. Similar to the AP added after discovery, a manually added AP will show up with a status of "configuring" in the AP List initially. The system will attempt to configure the AP with the value specified. A couple of minutes later, the AP's status will become "online" or "offline" on the AP List.

The AP can also be added manually without being online. Input the related data of the AP and select a Template. After clicking **Add**, the AP will be added to the managed list.

Adding An AP to the List	
AP Type	EAP100 ▾
AP Name	<input type="text"/> *
Admin Password	<input type="text" value="admin"/>
IP Address	<input type="text"/> *
MAC Address	<input type="text"/> *
Remark	<input type="text"/>
Service Zone	<input type="checkbox"/> Default <input type="checkbox"/> SZ7
Template Applied	TEMPLATE1 ▾
Channel	1 ▾

- **AP Type:** The model type of the AP for adding to the List.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **Remark:** Some extra information to be filled in for this AP if desired.
- **Service Zone (Tag-Based only):** This item is only shown when Tag-Based mode is selected in *System Configuration >> LAN Port Mapping*. Select the name of Service Zone such as Default, SZ7, etc. And it is only for Multi-VAP AP only.
- **Template Applied:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.

9.5. AP with Service Zone

Configure AP with Service Zone; go to: **System >> Service Zones >> Service Zone Configuration.**

- Service Zone Settings – Assigned IP Address range for AP Management**

Assigned IP Address for AP Management	
IP Range	Start IP Address : 192.168.0.1 *
	End IP Address : 192.168.0.190 *

Under port-based service zone, each service zone can designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the service zone. Under tag-based service zone, only default service zone will designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the selected service zones.

- Service Zone Settings – Managed AP in this Service Zone**

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

Managed AP(s) in this Service Zone			
AP Type	AP Name	IP Address	Status
		MAC Address	
EAP700	EAP700	192.168.10.1	Online (Enable)
		00:A7:03:14:CA:02	

- Service Zone Settings – SSID for Service Zone**

All managed APs that belong to this service zone will be set with the Service Zone's SSID.

Wireless Settings			
SSID	SSID0 *		
Security	Authentication	Open System <input type="checkbox"/> Enable 802.1X Authentication	
	Encryption	None	
Access Control	Status	Disable	
	User Limit	32 <small>*(Range: from 1 to 32)</small>	
	MAC Address	1	Disable
		2	Disable
		3	Disable
		4	Disable
	MAC Address	5	Disable
		6	Disable
		7	Disable
		8	Disable
	MAC Address	9	Disable
		10	Disable

- **Service Zone Settings – Access Control for Service Zone**

All managed APs (VAP) that belong to this service zone have same ACL table. When the status is **Allowed**, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP; on the other hand, when the status is **Denied**, the clients whose MAC addresses are listed in the list will be denied to connect to the AP. When **Disabled** is selected, any clients can connect to the AP. The default is **Disabled**.

Wireless Settings									
SSID	SSID0 *								
Security	Authentication	Open System <input type="checkbox"/> Enable 802.1X Authentication							
	Encryption	None							
Access Control	Status	Disable							
	User Limit	32 *(Range: from 1 to 32)							
	MAC Address	1		Disable	2		Disable		
		3		Disable	4		Disable		
5			Disable	6		Disable			
7			Disable	8		Disable			
9			Disable	10		Disable			

- **User Limit:** Limit the number of users connected to an AP managed under this Service Zone. *Not all AP types support this option.*

9.6. AP Security

Configure AP Security; go to: **System >> Service Zones.**

Wireless Settings				
SSID	SSID0 *			
Security	Authentication	Open System <input type="button" value="v"/> <input type="checkbox"/> Enable 802.1X Authentication		
	Encryption	None <input type="button" value="v"/>		
Access Control	Status	Disable <input type="button" value="v"/>		
	User Limit	32 *(Range: from 1 to 32)		
	MAC Address	1	<input type="text"/>	Disable <input type="button" value="v"/>
		2	<input type="text"/>	Disable <input type="button" value="v"/>
3		<input type="text"/>	Disable <input type="button" value="v"/>	
4		<input type="text"/>	Disable <input type="button" value="v"/>	
5		<input type="text"/>	Disable <input type="button" value="v"/>	
6	<input type="text"/>	Disable <input type="button" value="v"/>		
7	<input type="text"/>	Disable <input type="button" value="v"/>		
8	<input type="text"/>	Disable <input type="button" value="v"/>		
9	<input type="text"/>	Disable <input type="button" value="v"/>		
10	<input type="text"/>	Disable <input type="button" value="v"/>		

- **Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.
- **Authentication:** Including **Open System**, **Share Key**, **WPA**, **WPA2** or **WPA/WPA2 Mixed**.
- **Encryption:**
 - **WEP:** When **Authentication** is **Open System** or **Share Key**, **WEP** will be enabled.
 - **WPA:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.
 - **WPA2:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.
 - **WPA/WPA2 Mixed:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.

9.7. Change managed AP settings

Configure AP settings in AP List; go to: **Access Points >> Enter Local Area AP Management >> List.**

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

AP Type





EAP700

List

AP Name

Search

AP List

	AP Name	No. of Client	IP Address	Service Zone	Status
			MAC Address		Channel
	EAP700-Tony	0	192.168.10.1	Default	Configuring
			00:A7:03:14:CA:02		4
	EAP700-1	0	192.168.1.232	Default	Offline
			12:34:56:78:32:12		NA
	EAP700-2	0	192.168.10.32	Default	Offline
			12:34:56:72:32:41		NA

Reboot

Enable

Disable

Delete

Apply Template

(Total: 3)

- **AP Name**

Click **AP Name** and enter the interface about related settings. There are four kinds of settings, **General Settings**, **LAN Interface Setting** and **Wireless Interface Setting**. Click the hyperlink to proceed with the configuration of that category.

General Settings		
General	AP Name	EAP700-0
	Firmware	1.10.01
LAN Interface Settings		
LAN	IP Address	192.168.10.1
	Gateway	192.168.1.254
Wireless Interface Settings		
Wireless LAN	Channel	Auto
	Data Rate	Auto

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

General Settings	
Name	EAP700-0 *
Admin Password	•••••
NTP	Time Zone (GMT+08:00)Taipei,Taiwan NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Disabled ▾
SYSLOG	Disabled ▾
Remark	
Firmware	1.10.01

- **LAN Setting:** Click the link to enter the **LAN Setting** interface. Administrator can revise the AP's LAN IP settings including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN	
IP Address	192.168.10.1 *
Subnet Mask	255.255.0.0 *
Default Gateway	192.168.1.254 *
Primary DNS	192.168.1.254 *
Secondary DNS	

- **Wireless LAN:** Click the link to enter the **Wireless** interface.

Wireless	
SSID Broadcast	Enabled ▾
Channel	Auto ▾
Band	802.11b+802.11g ▾
Data Rate	Auto ▾
Fragment Threshold	2346 <small>(Default: 2346; Range: from 256 to 2346)</small>
RTS Threshold	2346 <small>(Default: 2346; Range: from 1 to 2346)</small>
Beacon Interval (ms)	100 <small>(Default:100 ; Range: from 100 to 500)</small>
Preamble	Long Only ▾
Transmit Power	Highest ▾
Wireless QoS WMM	Enabled ▾
Wireless Client Isolation	Disabled ▾
IAPP	Disabled ▾

- **Status**

After clicking the hyperlink in the **Status** column, there are two areas of information shown: **AP Status Summary** and **AP Status Details**.

AP Status Summary includes **AP Name**, **AP Type**, **LAN Interface MAC address**, **Wireless Interface MAC address**, **Report Time**, **SSID**, and **Number of Associated Clients**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Associated Client Status** and **Local Log Status**.

AP Status Summary	
AP Name	EAP700-0
AP Type	EAP700
LAN Interface MAC Address	00:A7:03:14:CA:02
Wireless Interface MAC Address	00:A7:03:14:CA:03
Report Time	2010-09-13 11:14:08
SSID	SSID0 (Service Zone: Default)
Number of Associated Clients	0

AP Status Details
System
LAN Interface
Wireless Interface
Associated Clients
Local Log Status

9.8. AP Operations from AP List

Configure AP List; go to: **Access Points >> Enter Local Area AP Management >> List.**

9.8.1. Reboot, Enable, Disable and Delete the AP

Select any AP by checking the checkbox and then click the button below to **Reboot**, **Enable**, **Disable**, **Delete**, **Apply Template** and **Apply Service Zone** (Tag-Based) the selected AP if desired.

AP Type

EAP700

List

AP Name

Search

AP List					
<input type="checkbox"/>	AP Name	No. of Client	IP Address	Service Zone	Status
			MAC Address		Channel
<input type="checkbox"/>	EAP700-0	0	192.168.10.1	Default	Online (Enabled)
			00:A7:03:14:CA:02		4
<input type="checkbox"/>	EAP700-1	0	192.168.1.232	Default	Offline
			12:34:56:78:32:12		NA
<input type="checkbox"/>	EAP700-2	0	192.168.10.32	Default	Offline
			12:34:56:72:32:41		NA

Reboot

Enable

Disable

Delete

Apply Template

(Total: 3)

9.8.2. Apply Template

Select any AP by check the checkbox and then click **Apply Template**; select one template to apply to the AP.

TEMPLATE1 ▾

Apply

Cancel

Template: TEMPLATE1	
Band	802.11b+802.11g
Subnet Mask	255.255.254.0
Gateway	192.168.1.254

Note: If the Band of the template cannot match current Channel, the Channel will be changed to "Auto."

9.8.3. Apply Service Zone (Tag-Based Only)

Select any AP by the check the checkbox and then click **Apply Service Zone** to select which Service Zones this AP associates to. For example, if **SZ3** and **SZ5** are selected for this AP, then these two Service Zones will be available under this AP. This AP will have two VAPs with two SSIDs according to two Service Zones for clients to associate. If a user connected to one SSID (for example, SSID3) of this AP and wishing to access the Internet, then this user must log into Service Zones (SZ3) first.

Service Zone				
<input type="checkbox"/>	ID	Name	SSID	WLAN Encryption
<input type="checkbox"/>	0	Default	SSID0	None
<input type="checkbox"/>	3	SZ3	SSID3	None
<input type="checkbox"/>	5	SZ5	SSID5	None

Check the checkbox to select the available Service Zones from the list. Click **Apply** to finish the settings.



1. This function only support in **Tag-Base** mode.
2. Not all AP types support this feature, only Multi-VAP-AP can Apply Service Zone in **Tag-Based** mode.

9.9. Firmware management and upgrade

Configure Firmware management; go to: **Access Points >> Enter Local Area AP Management >> Firmware.**

The system supports the firmware management of APs to upload new firmware, delete the existing firmware, and download the firmware to managed APs. Note that the AP's firmware version must be one that has been integrated.

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

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

List				
File Name	AP Type	Version	Size	Actions
Checksum				
4ipnet_EAP300_2.10.00-EN-E_1.24-1.4225.rom	EAP300	2.10	4174016	Download
c18aeda4652996191867fadb92dd5a5a				Delete

Configure Firmware upgrade; go to: **Access Points >> Enter Local Area AP Management >> Upgrade.**

- **List:** The uploaded firmware will be listed here.
- **File Name:** The name of the AP firmware has been uploaded.
- **Checksum:** The automatically detected security identification of the firmware.
- **AP Type:** The AP type of the firmware.
- **Version:** The version of the firmware.
- **Size:** The file size of the firmware.
- **Download:** Click **Download** to save the selected firmware to a local disk.
- **Delete:** Click **Delete** to delete the selected firmware from the system.

AP Upgrade: Select the APs which need to be upgraded and select the upgrade version of firmware, and click **Upgrade** to upgrade firmware.

AP Type

List					
Name	Type	Version	Last Upgraded Time	Next Version	Selection
EAP700-0	EAP700	1.10.01	N/A	<input type="text" value="1.10"/>	<input checked="" type="checkbox"/>

9.10. WDS Management

Configure WDS management; go to: **Access Points >> Enter Local Area AP Management >> WDS Management.**

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

Default Settings for Newly Added WDS Tree				
Security	WEP 152bits	Channel	56	Edit

WDS Status			
WDS Tree	Security	Channel	Edit
Refresh Interval	10 seconds <input type="button" value="v"/>		
No WDS operation has been done.			

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

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

9.11. Rogue AP Detection

Configure Rogue AP Detection; go to: **Access Points >> Enter Local Area AP Management >> Rogue AP Detection.**

It is designed to detect the non-managed or possibly malicious AP in the deployed environment. It takes the managed APs as sensors to find out the non-managed AP even if the AP uses the same SSID with managed AP's. It shows the AP's BSSID, ESSID, Type, Channel, Encryption, and found time.

General Configuration		
Interval	Disabled	Edit

Sensor List Configuration		
Sensors	0/1	Edit

Trusted AP Configuration		
Status	0/40	Edit

ESSID

Search

Rogue AP List							
<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
Add to Trusted AP List		Delete					

1. Setup the Detection Interval

Configure Detection Interval; go to: **Access Points >>Rogue AP Detection >>General Configuration.**

General Configuration	
Detection Interval	<input type="text" value="5"/> <small>*(0 ~ 999, 0:Disable)</small>

Input a **Detection Interval**, if you input "0", it will "Disable" this function, and system will not enable the Rogue AP Detection function.

2. Let the managed AP be the sensor

Configure Rogue AP Sensor; go to: **Access Points >>Rogue AP Detection >>Sensor List Configuration.**

Before setup the AP sensor, you must discovery the APs and apply template first.

► **Note:** For more detail of AP Management, please refer to the section of **Managing Wireless Network.**

Basically, all of the managed AP can become a Rogue AP sensor, but some earlier version AP will not support this function, they will list in the **Sensor List**, but they are not available for selection, so the **Sensor List** will list all of the managed AP. Select the APs and click **Apply**.

AP Type

Sensor List				
<input type="checkbox"/>	Name	MAC Address	IP Address	Log
<input checked="" type="checkbox"/>	yes-00151	00:1F:D4:00:0D:13	192.168.0.151	View

3. Add the non-managed AP to the Trust List

Configure Trust AP List; go to: **Access Points >>Rogue AP Detection >>Trusted AP Configuration.**

After the AP detection is finished. All of the non-managed AP will show in the List.

Rogue AP List							
<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
<input type="checkbox"/>	1	00:03:7F:0C:82:F4	A600-1	AP	6	NONE	2009/06/18 11:09:21
<input type="checkbox"/>	2	00:1F:D4:00:0D:14	CPE100-APTEST	AP	6	WEP	2009/06/18 11:09:21
<input type="checkbox"/>	3	0A:11:A3:08:09:56	Cip-AP	AP	6	NONE	2009/06/18 11:09:21
<input type="checkbox"/>	4	06:11:A3:08:09:56	Cip-Cherry	AP	6	WPA	2009/06/18 11:09:21
<input type="checkbox"/>	5	0E:11:A3:08:09:56	Cip-psk	AP	6	WPA	2009/06/18 11:09:21
<input type="checkbox"/>	6	00:11:A3:08:09:56	Cip-wep	AP	6	WEP	2009/06/18 11:09:21
<input type="checkbox"/>	7	00:06:19:00:AB:D3	EAP100-1	AP	6	NONE	2009/06/18 11:09:21
<input type="checkbox"/>	8	06:06:19:00:AB:D3	EAP100-tag1	AP	6	NONE	2009/06/18 11:09:21
<input type="button" value="Add to Trusted AP List"/> <input type="button" value="Delete"/>							

If there are some APs that are trusted by administrator, or these APs are just temporary usage. So you can add these APs to the Trust List, and then system will ignore these APs and will not show in the **Rogue AP List** again. Also you can check which AP had added to trust list by the **Trusted AP List**.

Trusted AP List		
NO	BSSID	Remark
1	<input type="text" value="0A:11:A3:08:09:56"/>	<input type="text" value="Cip-AP"/>
2	<input type="text" value="0E:11:A3:08:09:56"/>	<input type="text" value="Cip-psk"/>
3	<input type="text" value="00:11:A3:08:09:56"/>	<input type="text" value="Cip-wep"/>
4	<input type="text" value="06:11:A3:08:09:56"/>	<input type="text" value="Cip-Cherry"/>
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"/>
11	<input type="text"/>	<input type="text"/>

9.12. AP Load Balancing

Configure AP Load Balancing; go to: **Access Points >> Enter Local Area AP Management >> AP Load Balancing.**

It is a function to prevent managed APs from overloading. When the system detects the occurrence of APs' associated-client numbers exceeding a predefined threshold at circumstances other APs in the same group are still below the threshold, the balancing function will be activated to decrease the overloading APs' transmit power and increase other available APs' transmit power; this will let other available APs have more chance to be associated. The system can divide the managed APs into groups; define the group threshold, and a time interval which will trigger the AP load balancing.

General Configuration							
Interval	Disabled					Edit	

Group Configuration		
Status	0/3	Edit

AP Type [List](#)

Device List							
<input type="checkbox"/>	Group	Device Name	MAC Address	IP Address	Power Level	Loading	Log

Add to

AP Load Balancing Page

General Configuration	
Interval	<input type="text"/> <small>*(0 ~ 999, 0:Disable)</small>

Editing General Configuration Page

Group Configuration		
Group	Status	Loading Threshold
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

Editing Group Configuration Page

1. Setup the Interval

Configure Interval; go to: **Access Points >>AP Load Balancing.**

General Configuration		
Interval	1 minutes	Edit

Group Configuration		
Status	1/3	Edit

AP Type EAP100 List

Device List							
<input type="checkbox"/>	Group	Device Name	MAC Address	IP Address	Power Level	Loading	Log

Go to: **Access Points >>AP Load Balancing >> Configuration.**

Input an **Interval**, if you input “0”, it means “Disabled”, and system will not enable the AP Load Balancing function.

General Configuration	
Interval	<input type="text" value="1"/> <small>*(0 ~ 999, 0:Disable)</small>

2. Configure the Loading of Threshold of each Group

Configure Group Configuration; go to: **Access Points >>AP Load Balancing >>Group Configuration.**

Group Configuration		
Group	Status	Loading Threshold
1	Enabled	15
2	Disabled	15
3	Disabled	15

You can choose the Loading Threshold of each group. Also you can disable the AP group, if the group is disabled; this group of AP will not enable the Load Balancing function.

3. Add the AP to the Group

Configure AP to the Group; go to: **Access Points >>AP Load Balancing >>Device List.**

Device List							
<input type="checkbox"/>	Group	Device Name	MAC Address	IP Address	Power Level	Loading	Log
<input checked="" type="checkbox"/>	1	NEWDEV-00154	00:1F:D4:00:0C:CD	192.168.0.2	Highest	Offline	View
<input type="checkbox"/>	None	auto101	00:02:00:00:00:65	192.168.0.101	Highest	Offline	View
<input type="checkbox"/>	None	auto102	00:02:00:00:00:66	192.168.0.102	Highest	Offline	View
<input type="checkbox"/>	None	auto103	00:02:00:00:00:67	192.168.0.103	Highest	Offline	View
<input type="checkbox"/>	None	auto104	00:02:00:00:00:68	192.168.0.104	Highest	Offline	View
<input type="checkbox"/>	None	auto105	00:02:00:00:00:69	192.168.0.105	Highest	Offline	View
<input type="checkbox"/>	None	auto106	00:02:00:00:00:6A	192.168.0.106	Highest	Offline	View
<input type="checkbox"/>	None	auto107	00:02:00:00:00:6B	192.168.0.107	Highest	Offline	View
<input type="checkbox"/>	None	auto108	00:02:00:00:00:6C	192.168.0.108	Highest	Offline	View
<input type="checkbox"/>	None	auto109	00:02:00:00:00:6D	192.168.0.109	Highest	Offline	View

Add to None

None
Group 1
Group 2
Group 3

Apply
Cancel

Before setup the AP Load Balancing, you must discovery the APs and apply template first.

►► **Note:** For more detail of AP Management, please refer to the section of **Managing Wireless Network**.

All of the managed AP can join to any of the Load Balancing Group, so the **Device List** will list all of the managed AP. Select the APs, chose a **Group** and click **Apply**. The APs will join into this group.

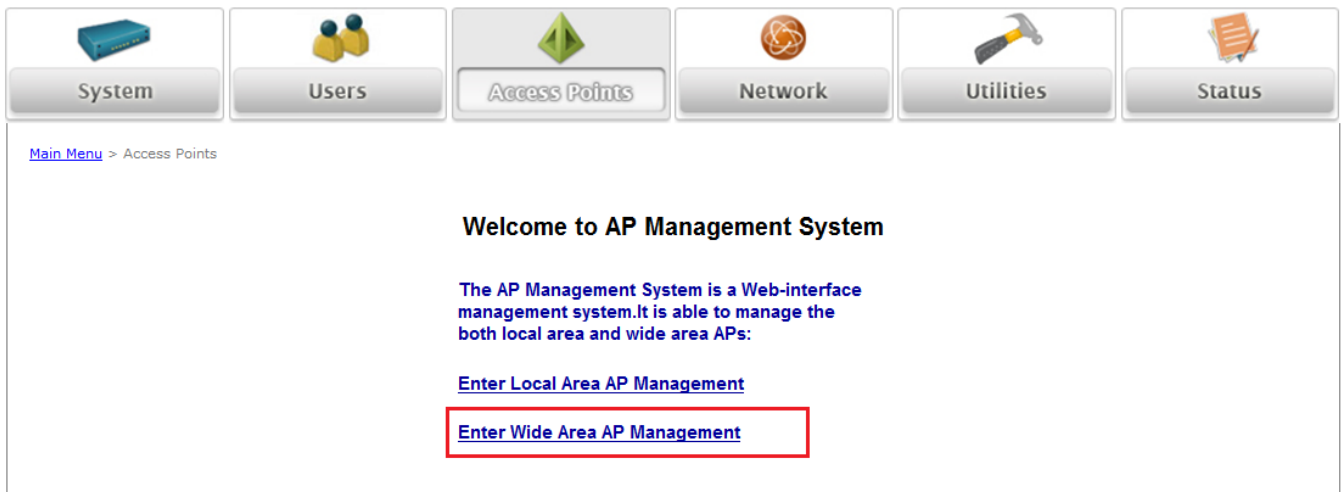
If the overloading is happened, you can check the Power Level from this List. It will record the changing process, such as, “Highest to High”; “Low to Medium”.

►► **Note:** It is strongly recommended that don't choose different type of AP to create the Load Balance Group.

10. Wide Area AP Management

The WHG Controller supports the planning and monitoring of Access Points deployed over complicated network structures such as the internet. Integrated with Google Map API, Wide Area AP Management provides intuitive graphical tools for mapping APs at various physical locations and keeping track of these devices.

Under Wide Area AP management, you can choose to simply monitor AP's status via SNMP or logically incorporate LevelOne APs into the WHG Controllers managed network via tunnels. AP models supported for Wide Area AP management include OWL800, EAP-200, EAP-110, EAP-300 and 3rd party AP. Please note that different WHG models may support different LevelOne AP models, please refer to datasheet for AP models supported.



10.1. AP Discovery

Discover connected APs; go to: **Access Points >> Enter Wide Area AP Management >> Discovery.**

With the Discovery feature, administrator can scan for APs regardless of their physical location as long as their IP address can be reached. After the discovery process, newly found AP's will be listed under **Device Results** allowing administrators to add it to the managed AP **List**.

Discovery AP			
Device Type	OWL800 ▾		
Admin Settings Used to Discover	Start IP Address	<input type="text"/>	*
	End IP Address	<input type="text"/>	
	Login ID	<input type="text" value="admin"/>	*
	Password	<input type="text" value="admin"/>	*
<input type="button" value="Discover"/>			

Device Results				
Device Type	IP Address	Device Name	SNMP Community	<input type="button" value="Add"/> <input type="button" value="Delete"/>

- **Start / End IP address:** Administrator need to specify the IP address range for AP discovery, and the specified IP address can be external or internal network IP addresses. This is useful when scanning for multiple devices connected to the managed network. APs with an IP address that is not within the specified range will not be listed after discovery.
- **Login ID / Password:** Fill in the Login ID and Password of the target AP's management interface, this will allow the administrator to remotely configure the AP's SNMP community.
- **Discover:** When the administrator tries to discover a new AP, select the **Device Type**. Second, enter the current IP range of the APs, **Login ID** and **Password**. Then click **Discover** button. If the new AP has been discovered, it will appear in the following Discovery Results list.
- **Device Results:** The discovery new APs will be listed here. The administrator can click **Add** to register the APs to the List for management.

When the discovery process is complete, the APs found will be listed under **Device Results** table. Here the administrator can specify the individual APs **Device Name** and SNMP **Community** string. Click the Add button and the discovered APs will be added into **List**.

10.2. Manually add AP

Add an individual Access Points to the managed list; go to: **Access Points >> Enter Wide Area AP Management**

>> Adding.

Besides **Discovery** feature that can search and list multiple APs for adding to the management list, **Adding** page allows administrator to directly add a single Access Point to the management list. Simply configure the devices IP address, name and login credentials, set a SNMP community string and click the **Add** button.

Add an AP	
Device Type	OWL800 ▾
Device IP	<input type="text"/> *
Device Name	<input type="text"/> *
Login ID	<input type="text" value="admin"/> *
Password	<input type="text" value="admin"/> *
SNMP Community	<input type="text" value="public"/> *

- **Device Type:** The device type of Wide Area APs.
- **Device IP:** The IP address of the AP to add to the management list.
- **Device Name:** The mnemonic name given to this AP device.
- **Login ID:** The Device's management interface login name.
- **Password:** The Device's management interface login password.
- **SNMP Community:** The SNMP Read Community string used for status access.

10.3. Manage AP Lists

Manage AP lists; go to: **Access Points >> Enter Wide Area AP Management >> List.**

When an EAP-200 is discovered or added to the AP list, it can be logically deployed into the WHG Controller's managed network regardless of its physical location by tunnels.

Initially when an AP has been successfully added to the List, it's "**Tunnel Status**" will show a red light indicating that no tunnel is established and that this AP is only being monitored via SNMP.

If you wish to create a tunnel between this AP and the WHG Controller, click the **Edit** button to proceed with necessary configurations.

AP List									
Type				All					
Status				All					
Tunnel				None					
<input type="checkbox"/>	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web	AP Attribute	CAPWAP	
1	<input type="checkbox"/> EAP300	EAP300-10_0_5_150	10.0.5.150 00:1F:D6:67:93:00	Online 1	<div><div></div><div>Edit</div></div>	System Overview <div></div> <div>Goto</div>	<div>Edit</div>	N/A	
2	<input type="checkbox"/> EAP300	EAP300-10_0_5_91	10.0.5.91 00:1F:D4:77:66:55	Online 0	<div><div></div><div>Edit</div></div>	System Overview <div></div> <div>Goto</div>	<div>Edit</div>	N/A	

In the AP's tunnel configuration page, check "**Enable**", set a numerical authentications key between WHG Controller and AP. Click **Apply** to create tunnel.

EAP300-10_0_5_150: Tunnel Configuration	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Key	<input type="text" value="88"/>

EAP300-10_0_5_150: VAP Status			
Profile Name	ESSID	VLAN ID	Mapped Service Zone
VAP-1	EAP300-1	None	Default ▼

A new window will automatically open and display the tunnel settings on the AP side which is passed from the WHG Controller. Click the "**Reboot**" link to apply and activate the settings.

Once the AP has completed the reboot process, the tunnel will be in effect as shown in the APs "**Status >> Overview**" page.

LAN Interface

MAC Address

00:1F:D4:00:75:EF

IP Address

10.0.4.72

Subnet Mask

255.255.0.0

Gateway

10.0.1.1

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:75:F1	EAP200-1	None	0

GRE Tunnel

Status

Active (Last RTT: 0.001194 s...

Remote IP

10.0.5.199

Key

12345

AP's tunnel settings can be checked at **"System >> Management"** page.

Trap :

☒ Disable
 ☐ Enable

Server IP :

System Log :

☒ Disable
 ☐ Enable

SYSLOG Server IP :

192.168.1.254

Server Port :

514

SYSLOG Level :

Error

GRE Tunnel :

☐ Disable
 ☒ Enable

Remote IP :

10.0.5.199

Key :

12345

On the WHG Controller side, the AP's Tunnel status will show green light indicating an active tunnel has been set up between WHG Controller and AP.

Now the administrator can click **"Edit"** and re-enter the Tunnel Status page to assign a Service Zone to this tunnel managed AP. **VAP status** will display all the enabled VAP on the remote EAP-200 with their respective ESSID and VLAN ID. An enabled Service Zone can be applied to each VAP entry and users associated to ESSID of this VAP will be governed by the applied service zone as if under the WHG Controller's managed internal network.

demo: Tunnel Configuration

Status

☒ Enable
 ☐ Disable

Key

12345

Apply

Cancel

demo: VAP Status

Profile Name	ESSID	VLAN ID	Mapped Service Zone
VAP-1	A210-change1	None	Default
VAP-2	A210-change2	1001	Default
VAP-3	A210-change3	1002	Default

10.4. Manage Third Party AP

Add a third party AP; go to: **Access Points >> Enter Wide Area AP Management >> List.**

Add third party AP by selecting THIRDPAP from Device Type. Add to AP List manually by specifying third party AP's IP address, Name, and VLAN ID. Click **Add** to finish adding and check lists to List icon.

Add an AP	
Device Type	3rd Party AP ▾
Device IP	192.168.1.1 *
Device Name	3rdAP001 *
VLAN ID	1 ▾ *

Add

Check and Manage List of third Party AP; go to: **Access Points >> Enter Wide Area AP Management >> List.**

Manage this third party AP from the Type Lists. Edit its AP Attribute and Administration from the column.

Go to Map icon. The added third party AP could be placed on Google Map feature and all map function. Create graphical reports for data traffics passing through this third party AP. Configure third party AP to maps; go to:

Access Points >> Enter Wide Area AP Management >> Map.

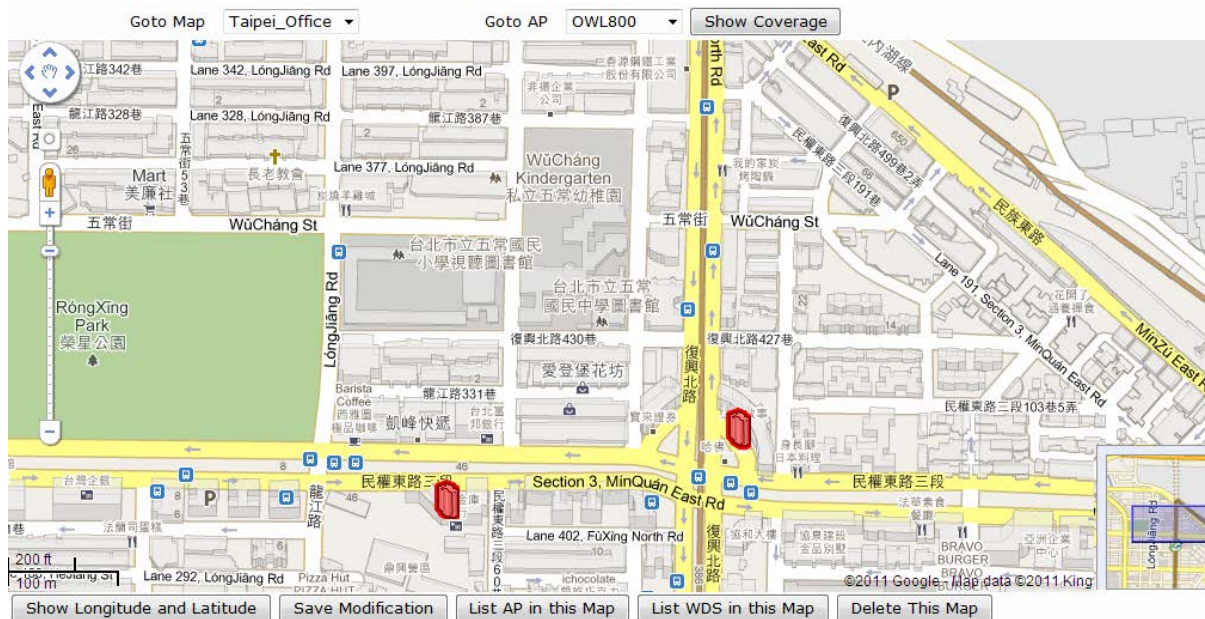
AP List								
Type		All ▾						
Status		All ▾						
Map		None ▾						
Tunnel		None ▾						
	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web	AP Attribute	CAPWAP
1	<input type="checkbox"/> 3rd Party AP	3rdAP001	192.168.1.1 N/A	Online <u>0</u>	N/A	Home Page ▾ <input type="button" value="Goto"/>	<input type="button" value="Edit"/>	N/A

10.5. Map

Configure maps; go to: **Access Points >> Enter Wide Area AP Management >> Map.**

The Map tab page is implemented with Google Map API version2 which allows administrators to view at a glance the whereabouts of all of the AP's under Wide Area AP Management. This feature is helpful when it comes to network planning and management.

Once the administrator has added APs to the managed list, then these APs can be tagged or marked on the Google Map API to show its' geographical location, as shown below:



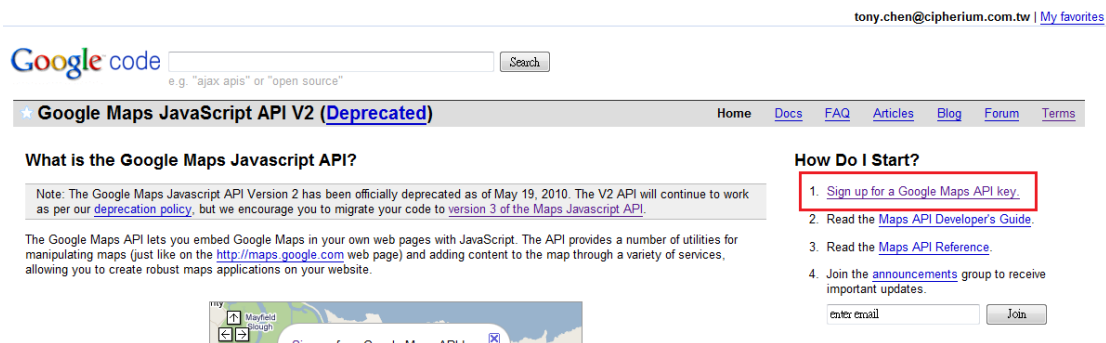
Procedure to create a Map:

- Step 1:** Get a Public IP Address from your ISP and configure this address to WAN interface.
- Step 2:** Apply for a Google Maps Registration key.
- Step 3:** Click **Add a New Map** button on the Map page. Configure Map Name and registration key.
- Step 4:** Discover APs and Add these AP to managed List.
- Step 5:** From the List page, add some APs to the created Map.

The necessary steps required to configure your map with AP information are described in the subsequent sections.

10.5.1. Register key from Google

Before configuring your maps, you will need to register the WHG Controller's IP address at Google Maps and get a key from Google. Go to <http://code.google.com/intl/en/apis/maps/documentation/javascript/v2/> or search for "Google Map API", to enter the **Google code** page.



Click on "Sign up for a Google Maps API key".

1. Your relationship with Google.

1.1 Use of the Service is Subject to these Terms. Your use of any of the Google Maps/Google Earth APIs (referred to in this document as the "Maps API(s)" or the "Service") is subject to the terms of a legal agreement between you and Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States ("Google"). This legal agreement is referred to as the "Terms".

1.2 The Terms include Google's Legal Notices and Privacy Policy.

☒ I have read and agree with the terms and conditions ([printable version](#))

My web site URL: Controller's WAN IP address

Tip: Signing up a key for <http://yourdomain.com> is usually the best practice, as it will work for all subdomains and directories. See this [FAQ](#) for more information.

Click the terms and condition check box and fill in your WHG Controller's WAN IP address.

Google will generate an API key for your WHG Controller.

Thank You for Signing Up for a Google Maps API Key!

Your key is:

Note: for more information on the API key system, consult <http://code.google.com/apis/maps/faq.html#keysystem>.

How you use your key depends on what Maps API product or service you use. Your key is valid for use within the entire family of Google Maps API solutions. The following examples show how to use your key within the Maps API product family.

JavaScript Maps API Example

Within the JavaScript Maps API, place the key within the script tag when you load the API:

```
...
// Note: you will need to replace the sensor parameter below with either an explicit true or false value.
<script src="http://maps.google.com/maps?file=api&v=2&sensor=true_or_false&key=ABQIAAAkf_mMpRETFZUaDr5paUTBTQNSXw9wit7VEiW-QmsIzRiVcN7BTEWPFVn
...

```

See [Loading the Maps API](#) in the JavaScript Maps API documentation for more information.

10.5.2. Create a Map

Now, return to the **Map** tab page in WHG Controller's WMI and Scroll down to the bottom of the page, click on the **Add a New Map** button.

Add a New Map

Distance Calculation

From :

To :

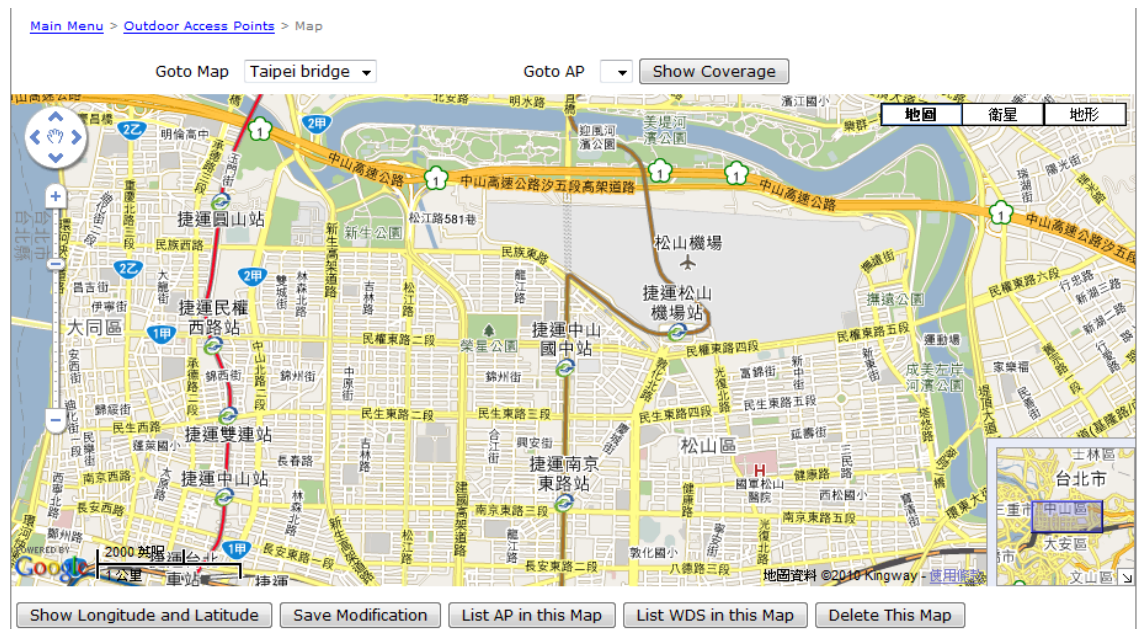
Address :

Address :

Result :

MAP Configuration	
Map Name	Taipei bridge*
Latitude	25.062554*
Longitude	121.54477*
Google Maps Registration Key.	ABQIAAAkf_mMpRETPZUXaDrSpaUTBTQNSXw9wit7VEiW-QmsIzRiVcN7*
Zoom Level	14*
Map Type	Normal*

An editing page will open for configuration, please fill in a **Map Name** for this map and its geographical location as defined by **Longitude** and **Latitude**, remember to also fill in the **Key** issued by Google. Finally choose the **Zoom Level** and **Map Type** and click the **Save** button.



The above screenshot is an example showing Taipei City with Map Name as Taipei Bridge, Zoom Level of 14 and Normal Map Type.

10.5.3. Marking APs on your Map

If you have several APs deployed and listed in **List** under Wide Area AP Management, their geographical location can be marked on a particular map.


Firstly, go to the **List** tab page and click on the **Edit** button of the AP's that you wish to mark in the map. In the AP configuration page, set the coordinates (**Latitude** and **Longitude**) of this AP and the radius of signal coverage.

Device : EAP200_Ext	
Device Name	EAP200_Ext *
SNMP Community	public *modify snmp setting will reboot the AP
Latitude	25.062636 *-85 ~ 85
Longitude	121.544688 *-180 ~ 180
Remark	
Radius of Coverage	0 x3 meters
Link 1	Name: IP Camera Description: The security camaera connected to this AP URL: http://10.3.24.234

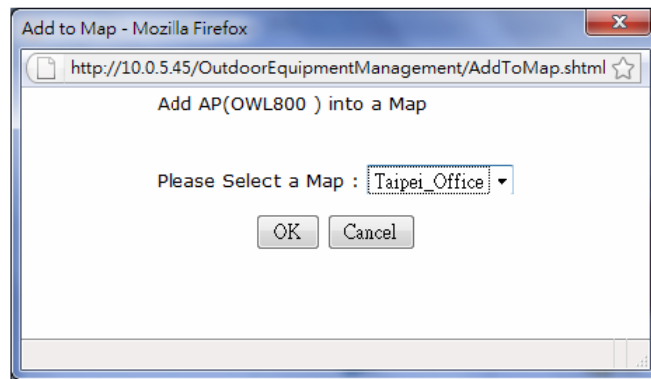
Fill in the coordinates where you wish to mark this particular AP. **Link 1 ~ Link 3** is for configuring a http link that will show up in the dialogue box on the map for referencing additional information related to this AP, for instance the IP address of a IP surveillance camera connected to this AP or the URL of the Venue Website where this AP is deployed.

Administrator can upload customized thumbnail image shown in the map. After configuring all the necessary settings and uploading your images, click **Save** button and return to AP **List** page.

Check the AP's that you wish to mark in the map and click the "**Add to Map**" button, choose the name of the map on which you wish to mark these APs and click **OK** button.

AP List							
<input type="checkbox"/>	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web Event Log	AP Attribute
<input checked="" type="checkbox"/>	EAP200	EAP200_Ext	10.0.4.72 00:1F:D4:00:75:EF	Online u	 <input type="button" value="Edit"/>	<input type="button" value="Goto"/>	<input type="button" value="Edit"/>





The selected APs will show up as marker images on the map at the physical coordinates configured, as shown below.



You can click on the AP icon to see the dialogue box for additional information or links that you have configured. Click the **more info** link for information on **AP status**, **Client List**, **WDS List** and **Links** related to this AP.





Goto Map Taipei_Bridge Goto AP EAP200_Ext Show Coverage

AP Detail Status

AP Name: EAP200_Ext
AP Status: Online
#of Clients: 0
[less info..](#)

[AP Statistic](#) [AP Status](#) [Client List](#) [WDS List](#) [Link](#)

IP Camera - [The security camera connected to this AP](#)

地圖資料 ©2010 Kingway - 使用條款

Show Longitude and Latitude Save Modification List AP in this Map List WDS in this Map Delete This Map

AP status, **Client List** and **WDS List** information listed are collected from the remote AP via SNMP.

10.5.4. Operations from Map page

Goto Map Goto AP

- **Goto Map:** When you have configured multiple map profiles, this function allows switching between different maps.
- **Goto AP:** This function is for administrator to select an AP on the list, and the map will shift to show the selected AP in the center of the map.
- **Show Coverage:** This button once pressed will display the signal coverage of all the APs on the map according the coverage radius set in each AP's profile under **List** tab page.

- **Show Longitude and Latitude:** This function when pressed will display in a pop up window the longitude and latitude of the map's current center point.
- **Save Modification:** This function is for saving the changes made to the map and overwriting the maps profile attributes. For instance if you have altered or panned the original map, clicking this button will save the changes made.
- **List AP in this Map:** Clicking this button will open a new page on your browser redirecting to the **List** tab page for displaying a list of APs in the Map.
- **List WDS in this Map:** Clicking this button will open a new page on your browser redirecting to the **WDS List** tab page for displaying a list of WDS links in the Map.
- **Delete this Map:** Delete the current map profile.
- **Add a New Map:** Click to add a new map profile.
- **Edit this Map:** Click to modify the current map's attribute settings.
- **Customize Image:** Administrator can upload desired images for each AP model that will be used as AP markers on the MAP.

10.6. AP Operations from AP List

Perform operations on managed APs; go to: **Access Points >> Enter Wide Area AP Management >> List.**

After adding APs to the managed List, the List page provides some operations for managing the listed AP's.

(Total 1) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page Row per Page

AP List									
Type		All							
Status		All							
Tunnel		None							
<input type="checkbox"/>	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web	AP Attribute	CAPWAP	
1	<input type="checkbox"/> EAP110	EAP110-10_0_5_224	192.168.2.123 00:1F:D5:30:40:70	Offline 0	Edit	System Overview Goto	Edit	N/A	

(Total 1) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page Row per Page

[Delete](#)
[Add to Map](#)
[Backup Config](#)
[Restore Config](#)
[Upgrade](#)

- **Goto:** The WHG Controller cannot directly configure Wide Area AP's settings remotely. However, the Goto button is a convenient link for accessing the remote AP's WMI.

Please note that the **Goto** button will only become active when the listed AP's status is Online.

AP List							
<input type="checkbox"/>	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web	AP Attribute
<input type="checkbox"/>	EAP200	EAP200_Ext	10.0.4.72 00:1F:D4:00:75:EF	Online 0	Edit	<div> Event Log System Overview VAP Overview WDS Link Overview System Upgrade Reboot WDS Link Status Associated Clients Event Log </div>	Edit
<input type="checkbox"/>	OWL800	OWL800_annex	10.3.2.123	Un-Sync 0	N/A		Edit

[Delete](#)
[Add to Map](#)
[Backup Config](#)
[Restore Config](#)
[Upgrade](#)

The drop down list on the column header is for specifying which WMI page to go to.

- **Edit (AP Attribute):** Click this button to enter the AP's attribute editing page where administrator can specify the Device Name and SNMP community. If the AP is to be marked on a map, this page also allows administrator to configure the geographical location, coverage, related links and customize marker or icon images that will be displayed on the map.
- **Edit (Tunnel Status):** Only applicable to EAP-200 APs. Click this button to setup a secure tunnel between the WHG Controller and the listed EAP-200. Once the tunnel has been established, the AP can be seen as logically connected under the WHG Controllers managed network and can be applied a Service Zone.
- **Delete:** Remove the checked AP from the List.
- **Add to Map:** Clicking this button will open a popup window. Administrator can Mark the selected APs on the Map chosen from the drop down list. If no map profile has been configured, there will be no available map to choose in the drop down list.
- **Backup Config:** Clicking this button will open a popup window where administrator can backup the chosen AP's configuration settings into a .db file store in the WHG Controller's memory. The Backup up files are listed under Backup Config tab page for download or deletion.
- **Restore Config:** Clicking this button will open a popup window where administrator can restore the

chosen AP's configuration settings using a .db file store locally in administrator PC or in the WHG Controller's memory.

- **Upgrade:** Clicking this button will open a popup window where administrator can upgrade the chosen AP's firmware using a firmware file store locally in administrator PC or in the WHG Controller's memory (under **Firmware** tab page).

10.7. WDS List

View the WDS link information established between APs in Wide Area AP Management; go to [Access Points >>](#)

[Enter Wide Area AP Management >> WDS List.](#)

WDS List										
Peer AP	Band	Channel	Security	TX Power	Link Speed	SNR	TX Bytes	TX Packets	STP	STATUS
EAP300-10_0_5_150	ng	1	WEP	17 dBm	129M	68	10175524	14752	Forwarding	Active
00:1F:D4:77:66:56									Disabled	
EAP300-10_0_5_91		1	WEP		129M	66	3283	76	Forwarding	Active
00:1F:D6:67:93:01									Disabled	

The WDS link if established between APs listed in **List** will be listed here with related information such as the Band and Channel of the link, Security settings if any and the Transmit Power, Byte, Packets etc.

10.8. Backup Config

View previously saved backup files for Wide Area APs; go to: **Access Points >> Enter Wide Area AP**

Management >> Backup Config.

Backed up Config files can be used to restore an AP's settings in **List**. When administrator backups an AP's configuration settings, all the backup files are listed at the **Backup Config** tab page and can be downloaded to a local storage device or deleted from WHG Controller's memory.

Backup Config					
Device Type	Version	Size	Backup Time	File Name	Action
EAP200	1.50.00	35367	2010/12/15 11:32:44	EAP200_ext_20101211	Download
					Delete

10.9. Firmware management and upgrade

Upload or view the details of previously uploaded firmware for upgrading APs; go to: **Access Points >> Enter Wide Area AP Management >> Firmware.**

The WHG Controller can store AP’s firmware in its’ built-in memory. Under the **Firmware** tab page administrator can upload new AP firmware to the WHG Controller’s memory allowing for easy remote AP upgrade and restore operations from the AP **List** page. The AP firmware listed under this page can be downloaded or deleted from WHG Controller memory if desired.

Firmware

File Name

Browse...

Upload

Firmware List				
File Name	Device Type	Version	Size	Actions

10.10.CAPWAP

Enable CAPWAP auto-discovery feature for supported AP's; go to: **Access Points >> Enter Wide Area AP**

Management >> CAPWAP. CAPWAP is a standard interoperable protocol that enables a WHG Controller to manage a collection of wireless access points.

CAPWAP Settings				
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Restore Configuration	EAP200	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		▼
	EAP300	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		▼
Template	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
	VAP	CAPWAP	GRE Tunnel	Service Zone
	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	map to SZ1 ▼
	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ2 ▼
	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ3 ▼
	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ4 ▼
	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ5 ▼
	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ6 ▼
	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ7 ▼
	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	map to SZ8 ▼
Certificate	DEFAULT ▼			

- **Status:** The configuration status of CAPWAP function. Click **Enable** to open the Access WHG Controller to allow CAPWAP supported AP's to automatically add to the managed AP List.
- **Restore Configuration:** Currently EAP-200 and EAP-300 are the AP models that support the CAPWAP feature. Once an AP is added to the list and is manually configured, its configuration profile can be backed up in the AC memory and will be selectable in the drop down menu. When a configuration profile is selected here, whenever an AP of this model is automatically discovered and added to the managed List, that AP will be configured with the configuration profile selected here.
- **Template:** This configuration item allows the administrator to specify which of the VAP profiles on the AP are allowed DTF (Distributed Traffic Forwarding) once it is discovered and managed by the AC. It enables the administrator to statically assign which VAPs are to be tunneled back to AC and what SZ they service, unassigned VAPs will service by DTF where the client traffic will not be tunneled back to AC, but directly to the internet instead.
- **Certificate:** This configuration item allows the administrator to select which of the certificates will be used during CAPWAP negotiation between AC and AP. If the certificate selected is invalid, the negotiation will be unsuccessful and the AP will not be automatically added in the managed List.
- **WHG Access Controller IP List:** The AC can statically designate other CAPWAP supported ACs as backup AC for CAPWAP APs in case it can no longer provide service. The No. designates the priority of these backup ACs to the AP, in the event that the original AC is down, the AP will first attempt to join the No. 1 backup AC and so on.

11. Networking Features of a Gateway

11.1. DMZ

Configure DMZ; go to: **Network >> NAT >> DMZ (Demilitarized Zone)**.

The system supports specific 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 specific 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	Remark
<input type="checkbox"/>		WAN1	<input type="text"/>	<input type="text"/>

Static Assignments				
No.	External IP Address	External Interface	Internal IP Address	Remark
1	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>

11.2. Virtual Server

Configure Virtual Server; go to: **Network >> NAT >> Public Accessible Server.**

This function allows the administrator to set virtual servers, 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						
No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	<input type="text"/>

11.3. Client Mobility

Configure IP Plug and Play; go to: **Network >> Client Mobility**.

WHG CONTROLLER supports IP PNP function: users can login and access network with any IP address setting.

Client Mobility	
IP PNP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Cross Gateway Roaming	Configure

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

- **IP PNP:** When IP PNP is enabled, a PC with a static IP address can still access the network even the system enables built-in DHCP server. No TCP/IP reconfiguration is needed.
- **Cross Gateway Roaming:** Configure this gateway to **Master** or **Slave**. In **Master** mode, you may also need to input the **Slave IP** and **Secret Key**. In **Slave** Mode, input **Master IP** and **Key**.
 - **Master Node:** While configure Master Node, one master could active up to 15 Slave node setting.

Cross Gateway Roaming	
Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Master Node <input type="radio"/> Slave Node
Status	Node List

Slave Nodes Setting				
No.	Active	Remote IP Address*	Secret Key*	Remark
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **Slave Node:** While configure Slave Node, enter its master node setting.

Cross Gateway Roaming	
Mode	<input type="radio"/> Disable <input type="radio"/> Master Node <input checked="" type="radio"/> Slave Node
Status	Node List

Master Node Setting	
Remote IP Address	<input type="text"/> *
Secret Key	<input type="text"/> *
Remark	<input type="text"/>

11.4. DNS Cache

Configure DNS Cache; go to: **Network >> DNS Cache.**

The administrator could statically assign Domain Name to IP mappings for all clients connected to the WHG Controller's LAN network. This feature can be used to redirect clients to preferred IP address for certain Domain Names.

DNS Cache Setting		
DNS Time-to-Live	<input type="text" value="120"/>	seconds *(0~604800, i.e. up to 7 days)
DNS Cache		
No.	IP Address	Domain Name
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"/>

11.5. Dynamic Domain Name Service

Configure Dynamic Domain Name Service; go to: **Network >> DDNS.**

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. WHG CONTROLLER supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access WHG Controller'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"/> Enable <input checked="" type="radio"/> Disable
Provider	DynDNS.org(Dynamic) ▼
Host Name	<input type="text"/> *
Username/E-mail	<input type="text"/> *
Password/Key	<input type="text"/> *

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



Note:

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

11.6. Port and IP Forwarding

Configure Port and IP Redirect; go to: **Network >> NAT >> Port and IP Forwarding.**

This function allows the administrator to set specific 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 Forwarding						
No.	Destination		Translated to Destination		Type	Remark
	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	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

11.7. Dynamic Route

Configure Dynamic Route; go to: **Network >> Dynamic Route.**

The function supports three dynamic routing protocols: RIP, OSPF and IS-IS.

Dynamic Route Settings	
RIP	<button>Configure</button>
OSPF	<button>Configure</button>
ISIS	<button>Configure</button>

- **RIP Configuration:** It is a dynamic routing protocol used in local and wide area networks. You can configure each interface to be Passive, supportive version and authentication.

RIP Configuration				
Enable RIP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Basic Configuration				
	Status	Passive	Version	AUTH
WAN1	Enabled	<input type="checkbox"/>	both ▼	none ▼
WAN2	Disabled	<input type="checkbox"/>	both ▼	none ▼
Default	Enabled	<input type="checkbox"/>	both ▼	none ▼
SZ1	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ2	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ3	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ4	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ5	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ6	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ7	Disabled	<input type="checkbox"/>	both ▼	none ▼
SZ8	Disabled	<input type="checkbox"/>	both ▼	none ▼
Advanced Options				
Advertise i am default gateway	<input type="checkbox"/>			
Advertise global policy route	<input type="checkbox"/>			
Redistribute OSPF	<input type="checkbox"/>			
RIP Timer	Update timer:	<input type="text" value="30"/>	* (30~600 seconds)	
	Time out timer:	<input type="text" value="180"/>	* (30~600 seconds)	
	Garbage collect timer:	<input type="text" value="120"/>	* (30~600 seconds)	

- Passive: RIP packets will not be sent from network interfaces that are checked as Passive.
- Version: Select the RIP version for this interface, RIPv1 uses broadcast to deliver RIP packets, RIPv2 uses Multicast to deliver RIP packets, both uses broadcast and multicast.
- AUTH: AUTH: Allows the authenticating of RIP neighbors. The authentication method "none" means that no authentication is used for RIP and it is the default method. The two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication.
- Advertise I am Default Gateway: Inform neighboring nodes that this controller is the default gateway.
- Advertise Global Policy Route: Inform neighboring nodes the Global Policy route on this controller.
- Redistribute OSPF: Check this option to enable using RIP to distribute routing information acquired via OSPF.
- RIP Timer:
 - ◆ Update timer: Specify the time in seconds when the system will request for immediate update in

routing information.

- ◆ **Timeout Timer:** Routes are only kept in the routing table for a limited amount of time. A special *Timeout* timer is started whenever a route is installed in the routing table. Whenever the router receives another *RIP Response* with information about that route, the route is considered “refreshed” and its *Timeout* timer is reset. When this timer expires, the route is marked as invalid.
- ◆ **Garbage Collection Timer:** Specify the time in seconds before erasing invalid route from the routing table.

- **OSPF Configuration:** It is an adaptive routing protocol for Internet Protocol (IP) networks. You can configure each interface Area, Stub and authentication.

OSPF Configuration				
Enable OSPF	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Basic Configuration				
Interface	Status	Area	Stub	AUTH
WAN1	Enabled	<input type="text"/>	<input type="checkbox"/>	none ▾
WAN2	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
Default	Enabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ1	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ2	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ3	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ4	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ5	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ6	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ7	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
SZ8	Disabled	<input type="text"/>	<input type="checkbox"/>	none ▾
Advanced Options				
Advertise i am default gateway		<input type="checkbox"/>		
Advertise global policy route		<input type="checkbox"/>		
Redistribute RIP		<input type="checkbox"/>		

- **Area:** An Area is a set of networks and hosts within a routing domain that have been administratively grouped together. Area 0, known as the *backbone area*, resides at the top level of the hierarchy and provides connectivity to the non-backbone areas (numbered 1, 2).
- **Stub Area:** Are areas through which or into which AS external advertisements are not flooded.
- **AUTH:** Allows the authenticating of OSPF neighbors. The authentication method "none" means that no authentication is used for OSPF and it is the default method. With MD5 authentication, enter the MD5 password, the password does not pass over the network.
- **Advertise I am Default Gateway:** Inform neighboring nodes that this controller is the default gateway.
- **Advertise Global Policy Route:** Inform neighboring nodes the Global Policy route on this controller.
- **Redistribute RIP:** Check this option to enable using OSPF to distribute routing information acquired via RIP.

- **ISIS Configuration:** It is a routing protocol designed to move information efficiently within a computer network,

a group of physically connected computers or similar devices. You can configure each interface Circuit Type to Level 1 or Level 2.

IS-IS Configuration		
Enable IS-IS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Basic Configuration		
Net ID	<input type="text"/>	
Router Level	<input type="button" value="Level 1"/>	
Interface	Status	Circuit Type
WAN1	Enabled	<input type="button" value="Level 1"/>
WAN2	Disabled	<input type="button" value="Level 1"/>
Default	Enabled	<input type="button" value="Level 1"/>
SZ1	Disabled	<input type="button" value="Level 1"/>
SZ2	Disabled	<input type="button" value="Level 1"/>
SZ3	Disabled	<input type="button" value="Level 1"/>
SZ4	Disabled	<input type="button" value="Level 1"/>
SZ5	Disabled	<input type="button" value="Level 1"/>
SZ6	Disabled	<input type="button" value="Level 1"/>
SZ7	Disabled	<input type="button" value="Level 1"/>
SZ8	Disabled	<input type="button" value="Level 1"/>

- Net ID: It is the ISO address Network Entity Title (NET). The NET is used just like an IP address to uniquely identify a router on the inter-network.
- Circuit Type: Level 1 systems route within an area; when the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other routing domains. The level type of each network interface can be assigned.

12. System Management and Utilities

12.1. System Time

Configure System Time; go to: **System >> General.**

12.1.1. NTP

NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT).

Time	System Time : 2010/06/02 18:21:16	
	Time Zone :	
	<div>(GMT+08:00)Taipei</div>	
	<input checked="" type="radio"/> NTP	
	NTP Server	1: <div>tock.usno.navy.mil</div> <small>*(e.g. tock.usno.navy.mil)</small>
	NTP Server	2: <div>ntp1.fau.de</div>
	NTP Server	3: <div>clock.cuhk.edu.hk</div>
	NTP Server	4: <div>ntp1.pads.ufrj.br</div>
	NTP Server	5: <div>ntp1.cs.mu.OZ.AU</div>
	<input type="radio"/> Manually set up	

12.1.2. Manual Settings

The time can also be manually configured by selecting **Manually set up** and then entering the date and time in these fields.

Time	System Time : 2010/06/02 18:21:16
	Time Zone :
	(GMT+08:00)Taipei
	<input type="radio"/> NTP
	<input checked="" type="radio"/> Manually set up
	-- Year -- Month -- Day
	-- Hour -- Minute -- Second

12.2. Management IP

Configure Management IP; go to: **System >> General.**

Only PCs within this IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, the user can access the web management page.

Management IP Address List					
No.	Active	IP Address/Segment	No.	Active	IP Address/Segment
1	<input type="checkbox"/>	0.0.0.0/0.0.0.0	2	<input type="checkbox"/>	
3	<input type="checkbox"/>		4	<input type="checkbox"/>	
5	<input type="checkbox"/>		6	<input type="checkbox"/>	

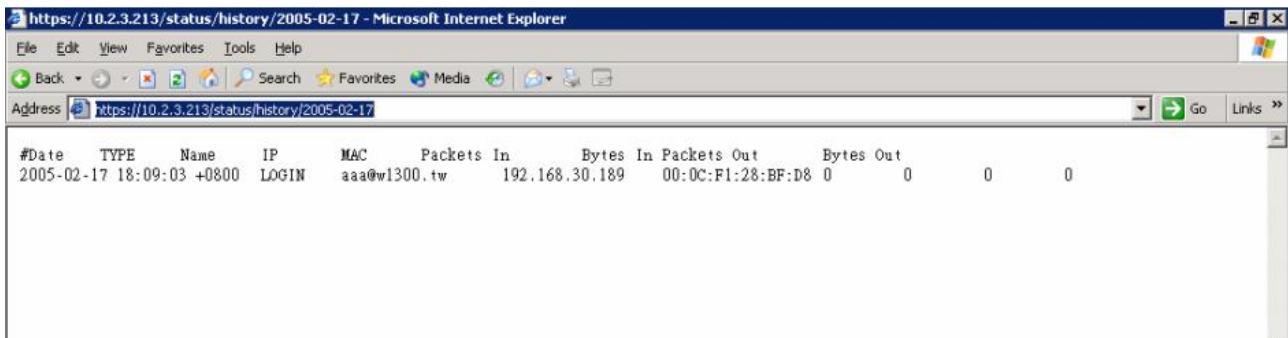
The default value is "0.0.0.0/0.0.0.0". It means that the WMI can be accessed by any IP address, for security consideration; please change this value before the system provides service.

12.3. Access History IP

Configure Access History IP; go to: **System >> General**.

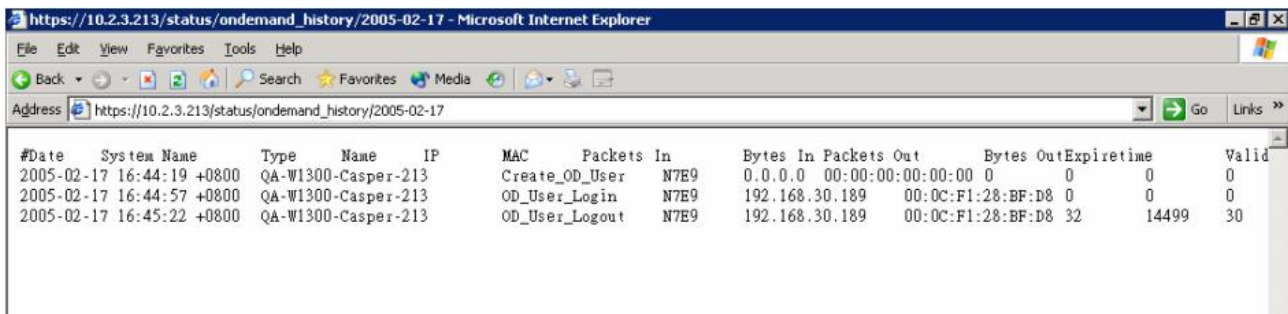
Specify an IP address of the administrator's computer or a billing system to get billing history information of WHG CONTROLLER with the predefined URLs. The file name format is "yyyy-mm-dd". An example is provided as follows:

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



#Date	TYPE	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out
2005-02-17 18:09:03 +0800	LOGIN			aaa@w1300.tw	192.168.30.189	00:0C:F1:28:BF:D8	0	0

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



#Date	System Name	Type	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Expiretime	Valid
2005-02-17 16:44:19 +0800	QA-W1300-Casper-213	Create_OD_User			N7E9	0.0.0.0	00:00:00:00:00:00	0	0	0	0
2005-02-17 16:44:57 +0800	QA-W1300-Casper-213	OD_User_Login			N7E9	192.168.30.189	00:0C:F1:28:BF:D8	0	0	0	0
2005-02-17 16:45:22 +0800	QA-W1300-Casper-213	OD_User_Logout			N7E9	192.168.30.189	00:0C:F1:28:BF:D8	32	14499	30	30

12.4. SNMP

Configure SNMP; go to: **System >> General.**

If this function is enabled, the SNMP Management IP and the Community can be assigned to access the **SNMP Configuration List** of the system.

SNMP Configuration List		
Item	Manager IP Address	Community
1	<input type="text" value="192.168.1.54"/>	<input type="text" value="public"/>
2	<input type="text" value="192.168.1.214"/>	<input type="text" value="public"/>

12.5. Change Password

Configure Change Password; go to: **Utilities >> Password Change**.

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 WHG CONTROLLER.

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.

►► **Note:** Only login with **admin** can change password.

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

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

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

12.6. Backup / Restore and Reset to Factory Default

Configure Backup / Restore and Reset to Factory Default; go to: **Utilities >> Backup & Restore.**

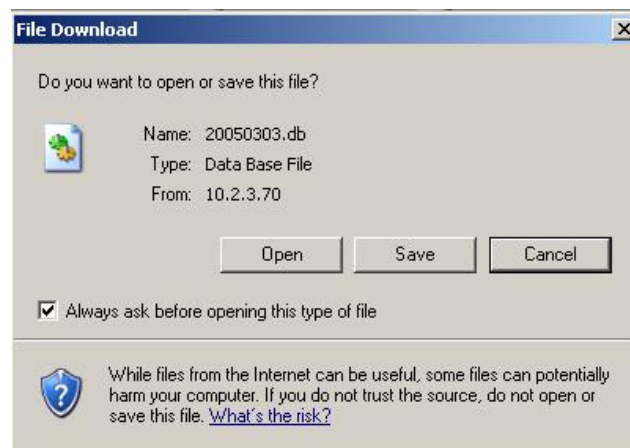
This function is used to backup/restore the WHG CONTROLLER settings. Also, WHG CONTROLLER can be restored to the factory default settings here.

Backup System Settings	
<div>Backup</div>	

Restore System Settings	
File Name	<input type="text"/> <div>Browse...</div>
<input type="checkbox"/> Keep WAN1 setting and Management IP Address List.	
<div>Restore</div>	

Reset to the Factory Default
<div>Reset</div>

- **Backup System Settings:** Click **Backup** to create a .db database backup file and save it on disk.



- **Restore System Settings:** Click **Browse** to search for a .db database backup file created by WHG CONTROLLER and click **Restore** to restore to the same settings at the time when the backup file was saved. The option of "Keep WAN1 setting and Management IP Address List" can be selected to retain WAN1 setting for remote access.
- **Reset to Factory Default:** Click **Reset** to load the factory default settings of WHG CONTROLLER.

12.7. Firmware Upgrade

Configure Firmware Upgrade; go to: **Utilities >> System 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.

FTP firmware upgrade is also an option, enter the FTP server IP address, FTP server port, and the FTP account name and password, and lastly specify the complete firmware filename stored on the FTP server that will be used to upgrade the system.

System Firmware Upgrade											
Current Version	5.00.00										
File Name	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Apply"/>										
Upgrade by FTP	<table><tbody><tr><td>Server IP</td><td><input type="text"/></td></tr><tr><td>Server Port</td><td><input type="text"/></td></tr><tr><td>Username</td><td><input type="text"/></td></tr><tr><td>Password</td><td><input type="password"/></td></tr><tr><td>File Name</td><td><input type="text"/></td></tr></tbody></table> <input type="button" value="Apply"/>	Server IP	<input type="text"/>	Server Port	<input type="text"/>	Username	<input type="text"/>	Password	<input type="password"/>	File Name	<input type="text"/>
Server IP	<input type="text"/>										
Server Port	<input type="text"/>										
Username	<input type="text"/>										
Password	<input type="password"/>										
File Name	<input type="text"/>										

Note: For better maintenance, 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.

12.8. Restart

Configure Restart; go to: **Utilities >> Restart.**

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

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



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

12.9. Network Utility

Configure Network Utility; go to: **Utilities >> Network Utilities.**

The system provides some network utilities to help administrators manage the network easily.

Network Utilities	
Wake-on-LAN	<input type="text"/> (MAC, e.g. XX:XX:XX:XX:XX:XX) <input type="button" value="Wake Up"/>
IPv4	Ping <input type="text"/> (IP/Domain Name) <input type="button" value="Ping"/>
	Trace Route <input type="text"/> (IP/Domain Name) <input type="button" value="Start"/> <input type="button" value="Stop"/>
	ARPing <input type="text"/> (IP/Domain Name) Interface <input type="text" value="WAN1"/> <input type="button" value="ARPing"/>
	ARP Table <input type="button" value="Show"/>
IPv6	Ping6 <input type="text"/> (IP/Domain Name) <input type="button" value="Ping6"/>
	Trace Route 6 <input type="text"/> (IP/Domain Name) <input type="button" value="Start"/> <input type="button" value="Stop"/>
	Neighbor Discovery <input type="text"/> (IP/Domain Name) Interface <input type="text" value="WAN1"/> <input type="button" value="Discovery"/>
	Neighbor Cache <input type="button" value="Show"/>
Sniff	<p>Usage:</p> <p>The Sniff tool is for the administrator to capture packets from the selected "Interface" The "Packet" count field is for telling how many packets to capture. If the information of link layer is to be displayed, check the "Link Layer" box. If the packet information is to be displayed in hexadecimal format, check the "Hex" box.</p> <p>To further filter the types of packets, please enter the filtering "Expression" below following the syntax of Linux tcpdump command. Example 1, to capture only TCP related packets occurring at port 23, type "tcp port 23" Example 2, to capture only ARP related packets, type in "arp" Example 3, to capture only ICMP related packets, type in "icmp"</p> <p>Interface <input type="text" value="WAN1"/> Packet <input type="text" value="1000"/> (1 - 1000) <input type="checkbox"/> Link Layer <input type="checkbox"/> Hex</p> <p>Expression <input type="text"/></p> <p><input type="button" value="Capture"/> <input type="button" value="Stop"/></p>
Status	
Result	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

Item	Description
Wake-on-LAN	It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled in its BIOS and it is connect to any service zone. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
IPv4	<ul style="list-style-type: none"> ▪ Ping: It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not. ▪ 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. ▪ ARPing: Allows the administrator to send ARP request for a specific IP address or domain name. ▪ ARP Table: It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).
IPv6	<ul style="list-style-type: none"> ▪ Ping: It allows administrator to detect a device using IPv6 address or Host domain name to see if it is alive or not. ▪ Trace Route 6: It allows administrator to find out the real path of packets from the gateway to a destination using IPv6 address or Host domain name. ▪ Neighbor Discovery: The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name. ▪ Neighbor Cache: a node manages the information about its neighbors in the Neighbor Cache. This feature allows the administrator to view the information stored on system's neighbor cache.
Sniff	With this feature the administrator can listen for packets from selected Interfaces. The administrator can further filter the types of packets to capture by using tcpdump commands under the Expression field.
Status	When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
Result	The operation result is displayed here.

12.10.Certificate

Configure Certificate Utility; go to: **Utility >> Certificate.**

AC can issue certificates to APs that it manages in its private network. Administrator can sign certificates issues by the system's root CA and load these certificates to managed APs. These APs will be used in verifying the identity and authenticity of CAPWAP discovery requests between AP and AC.

Certificate Utility				
Create Root CA ▾				
Certificate Signed Information				
Common Name	<input type="text"/> *			
Email Address	<input type="text"/>			
Country Name	<input type="text"/>			
State or Province Name	<input type="text"/>			
Locality Name	<input type="text"/>			
Organization Name	<input type="text"/>			
Organization Unit Name	<input type="text"/>			
Key Type	RSA ▾			
Key Length	512 ▾			

Certificate Information				
CERT Name	Subject	Issuer	Valid Date	Download Delete
My Root CA/Default Certificate				
Root CA	N/A	N/A	N/A	<input type="button" value="Get CERT"/> <input type="button" value="Delete"/>
Default Certificate	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com	2020/08/13 10:36:37	<input type="button" value="Get Key"/> <input type="button" value="Get CERT"/>
My Issue Certificate				
N/A	N/A	N/A	N/A	<input type="button" value="Get Key"/> <input type="button" value="Get CERT"/> <input type="button" value="Delete"/>
Trust CA				
N/A	N/A	N/A	N/A	<input type="button" value="Get CERT"/> <input type="button" value="Delete"/>

- **Get CERT:** Download Certificate,
- **Get Key:** Download Key.

- **Create System's Root CA**

Administrator can create a root CA for private use. The created root CA certificate can be downloaded and used to sign certificates generated by the system.

Certificate Utility	
Create Root CA ▾	
Certificate Signed Information	
Common Name	4ipnet.com *
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	RSA ▾
Key Length	512 ▾
<div>Apply</div> <div>Clear</div>	

The created root CA will be displayed in the table below.

Certificate Information				
CERT Name	Subject	Issuer	Valid Date	Download Delete
My Root CA/Default Certificate				
Root CA	CN=4ipnet.com	CN=4ipnet.com	2021/03/18 15:17:07	<div>Get CERT</div> <div>Delete</div>
Default Certificate	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com	2020/08/13 10:36:37	<div>Get Key</div> <div>Get CERT</div>

- **Signing Certificates with System Root CA**

When a root CA has been created, the **Create Root CA** option in the drop down list will become **Signed by Root CA**. Certificate information entered and Applied will be used to generate an issued certificate from root CA.

Certificate Utility	
Signed by Root CA ▾	
Certificate Signed Information	
Common Name	EAP.com *
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	RSA ▾
Key Length	512 ▾
<div>Apply</div> <div>Clear</div>	

The generated certificate will be listed in the **My Issue Certificate** table. Certificate and key can be downloaded with **Get Cert, Get key** button.

My Issue Certificate				
CERT1	CN=EAP.com	CN=4ipnet.com	2021/03/18 15:20:20	<div>Get Key</div> <div>Get CERT</div> <div>Delete</div>

- **Uploading Certificate or Trusted CA**

Apart from self signed certificate and system's root CA, administrators can also upload other certificates signed by other CA entities or Trusted CAs into the system.

Select **Upload Certificate** to browse and upload a selected Certificate and Key into the System.

Certificate Utility	
Upload Certificate ▾	
Upload Certificate	
Private Key	<input type="text"/> Browse...
Certificate	<input type="text"/> Browse...
Certification Path Verification	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Select **Upload Trust CA** to browse and upload a trusted CA certificate into the System.

Certificate Utility	
Upload Trust CA ▾	
Upload Trust CA	
Certificate	<input type="text"/> 瀏覽...
<div>Apply</div> <div>Clear</div>	

12.11.Administrator Account

Configure operator accounts; go to: **Utilities >> Administrator Account.**

WHG Controller has three kinds of permanent management account: **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

Admin: The administrator can access all configuration pages of WHG Controller and has all modification and access privilege.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under **User Authentication** to manage the user account, it does not have the 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**

►► **Note:**

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

Besides permanent Administrator, Manager, and Operator accounts, different operator accounts can be created with different levels of authority and access for managing the Service Zones and APs they are in charge of.

Generate Admin Account	
Name	<input type="text"/> *
Password	<input type="password"/> *
Confirm Password	<input type="password"/> *
Group	Super Group <input type="button" value="Configure"/>

Admin List						
Name	Password	IP	MAC	Group	Status	<input type="button" value="Delete All"/>
admin	*	10.0.5.228	00:26:2D:85:35:2E	Super Group	/Utilities/MlaUser.shtml	

• Create Admin Account

Different operator accounts and their password can be specified here. **Group** here are authorization profiles that will be applied to this operator account, each Group profile can specify which SZ this account can access and the Maps that this operator can access.

Generate Admin Account	
Name	NY_office *
Password	● *
Confirm Password	● *
Group	<div> <div>Super Group ▼</div> <div> <div>Super Group</div> <div>Group 1</div> <div>Group 2</div> <div>Group 3</div> <div>Group 4</div> </div> </div> <input type="button" value="Configure"/>

Administrator can enter the desired user account name and password, select an authorization Group profile and **Apply**. The created operator account, password, group and status will be shown in the Admin List below.

Generate Admin Account	
Name	<input type="text"/> *
Password	<input type="password"/> *
Confirm Password	<input type="password"/> *
Group	Super Group <input type="button" value="Configure"/>

Admin List						
Name	Password	IP	MAC	Group	Status	<input type="button" value="Delete All"/>
NY_office	1	NA	NA	Group 1	logoff	Delete
LA_Office	2	NA	NA	Group 2	logoff	Delete
EU_office	3	NA	NA	Group 3	logoff	Delete
admin	*	10.0.5.228	00:26:2D:85:35:2E	Super Group	/Utilities/MlaUser.shtml	

- **Configure operator Group profile**

Group allowed SZ and Map can be configured here.

Select Group	
Super Group ▼	

Setting Permission	
Service Zone	<input checked="" type="checkbox"/> SZ0 <input checked="" type="checkbox"/> SZ1 <input checked="" type="checkbox"/> SZ2 <input checked="" type="checkbox"/> SZ3 <input checked="" type="checkbox"/> SZ4 <input checked="" type="checkbox"/> SZ5 <input checked="" type="checkbox"/> SZ6 <input checked="" type="checkbox"/> SZ7 <input checked="" type="checkbox"/> SZ8
MAP	<input checked="" type="checkbox"/> Overview <input checked="" type="checkbox"/> NY_office <input checked="" type="checkbox"/> EU_Office <input checked="" type="checkbox"/> Osaka_office

In this configuration page, administrator can specify which Service Zone and Map are allowed to be accessed by the operator that belongs to this Group. This feature allows the administrator to create multi-level privilege accounts with flexibility to meet the deployment and management needs.

When an operator logs into the system with a created account, he will only be able to access the Service Zone profiles checked in the Group profile he belongs to and he can only see the Map and only the APs marked on the checked Maps in the managed AP list.

12.12. Monitor IP

Configure Monitoring 3rd Party IP; go to: **Network >> Monitor IP.**

WHG CONTROLLER will send out a packet periodically to monitor the connection status of the IP addresses on the list. On each monitored item with a WEB server running, administrators may add a link for the easy access by entering the IP, select the **Protocol** to *http* or *https* and then click **Create**. After clicking **Create** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the **Delete** button to remove the setting.

Monitor IP List				
No.	Protocol	IP Address	Hyperlink	Remark
1	<input type="text" value="http"/>	<input type="text"/>	<input type="button" value="Create"/>	<input type="text"/>
2	<input type="text" value="http"/>	<input type="text"/>	<input type="button" value="Create"/>	<input type="text"/>
3	<input type="text" value="http"/>	<input type="text"/>	<input type="button" value="Create"/>	<input type="text"/>

Monitoring 3rd Party AP, go to: **Network >> Monitor IP.**

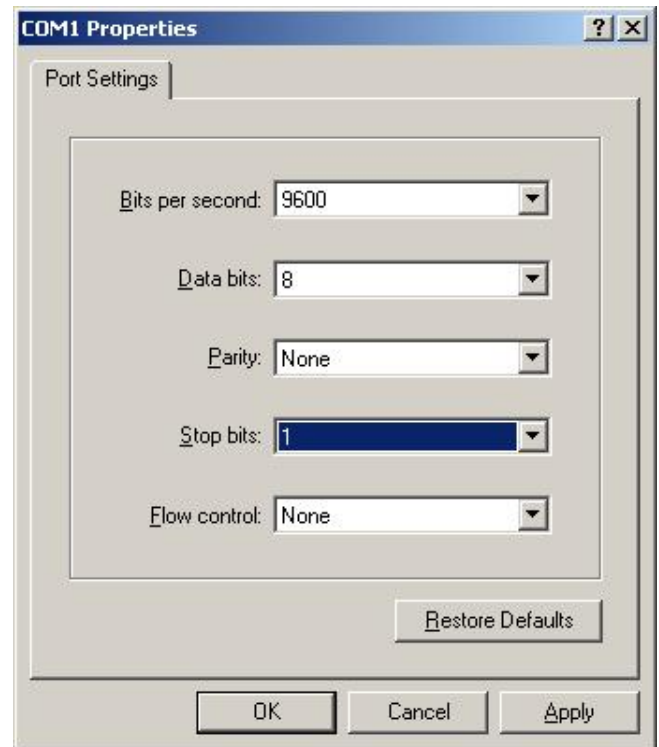
If you are using 3rd party AP, you can use Monitor IP function to monitor the AP connection status. Because WHG CONTROLLER can not manage these APs, Monitor IP is a better way to monitor the AP connection status. WHG CONTROLLER will send out a packet periodically to monitor the connection status of the 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 Now** to check the current status of all the monitored IP. The system supports monitoring on 200 IP addresses listed in the “**Monitor IP List**”.

12.13.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 WHG CONTROLLER, 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, None, 1, None**.



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 WHG CONTROLLER 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.

```

Please select functions:
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x      Utility      Utilities for network debugging      x
x      Password     Change admin password                    x
x      Reset        Reload factory default                x
x      Restart      Restart                          x
x
x

```


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 WHG CONTROLLER Admin username and password after logging in the system for the first time.

- **Reload factory default**

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

- **Restart WHG CONTROLLER**

Choosing this option will restart WHG CONTROLLER.

13. System Status and Reports

13.1. View the Status

This section includes **System Status**, **Interface Status**, **Hardware**, **Routing Table**, **Online Users**, **Session List**, **User Logs**, **Logs**, **DHCP Lease**, and **E-mail & Syslog** to provide system status information and online user status.

Status	
System	Display current settings of the system.
Interface	Display the current settings of all network interfaces.
Hardware	Display current CPU and memory usage.
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.
Online Users	Display the information of the online users. Content of the information includes Username, IP Address, MAC Address, Packet Count (In/Out), Byte Count (In/Out) and idle time. Administrator can remove the online user via clicking the Logout button in each record.
Session List	Display the information of the current sessions of all clients; include login clients and privilege clients.
User Logs	Display detailed user access records on daily basis. History record of up to 3 days is kept in the system.
Logs	Display system syslog messages.
DHCP Lease	Display the information of DHCP Lease status.
Report & Notification	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.

13.1.1. System Status

View System Status; go to: **Status >> System.**

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

System Setting Overview		
Firmware Version		
Build		
System Name		WHG
Portal URL		http://www.google.com
SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2010/06/18 17:18:28 +0800
User Session Control	Idle Time Out	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:

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

13.1.2. Interface Status

View Interface Status; go to: [Status >> Interface.](#)

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **SZ Default**, **SZ1 ~ SZ8**.

Network Interface																							
Select Interface	WAN1																						
WAN1	Mode	STATIC																					
	MAC Address	00:90:0B:18:58:41																					
	IP Address	10.0.4.72																					
	Subnet Mask	255.255.0.0																					
	IPv6 Address																						
	IPv6 Prefix																						
Traffic summary	<div><div><div>today</div><div>rx 2.09 MiB tx 3.53 MiB = 5.62 MiB 1.34 kbit/s</div><div></div></div><div><div>08/27/10</div><div>rx 967.01 MiB tx 148.91 MiB = 1.09 GiB 105.81 kbit/s</div><div></div></div><div><div>all time</div><div>rx 969.11 MiB tx 152.43 MiB = 1.10 GiB since 08/27/10</div><div></div></div><div><div>Aug '10</div><div>rx 969.11 MiB tx 152.43 MiB = 1.10 GiB 3.62 kbit/s</div><div></div></div><div><div>09:33 unStat / Teemu Toivola</div></div></div>																						
Traffic of the day	<table><thead><tr><th>day</th><th>rx</th><th>tx</th><th>total</th><th>avg. rate</th></tr></thead><tbody><tr><td>08/27/10</td><td>967.01 MiB</td><td>148.91 MiB</td><td>1.09 GiB</td><td>105.81 kbit/s</td></tr><tr><td>08/30/10</td><td>2.09 MiB</td><td>3.53 MiB</td><td>5.62 MiB</td><td>1.34 kbit/s</td></tr><tr><td>estimated</td><td>5 MiB</td><td>7 MiB</td><td>12 MiB</td><td></td></tr></tbody></table> <div>09:33 unStat / Teemu Toivola</div>			day	rx	tx	total	avg. rate	08/27/10	967.01 MiB	148.91 MiB	1.09 GiB	105.81 kbit/s	08/30/10	2.09 MiB	3.53 MiB	5.62 MiB	1.34 kbit/s	estimated	5 MiB	7 MiB	12 MiB	
day	rx	tx	total	avg. rate																			
08/27/10	967.01 MiB	148.91 MiB	1.09 GiB	105.81 kbit/s																			
08/30/10	2.09 MiB	3.53 MiB	5.62 MiB	1.34 kbit/s																			
estimated	5 MiB	7 MiB	12 MiB																				
Traffic of the Month	<table><thead><tr><th>month</th><th>rx</th><th>tx</th><th>total</th><th>avg. rate</th></tr></thead><tbody><tr><td>Aug '10</td><td>969.11 MiB</td><td>152.43 MiB</td><td>1.10 GiB</td><td>3.62 kbit/s</td></tr><tr><td>estimated</td><td>1.00 GiB</td><td>160 MiB</td><td>1.15 GiB</td><td></td></tr></tbody></table> <div>09:33 unStat / Teemu Toivola</div>			month	rx	tx	total	avg. rate	Aug '10	969.11 MiB	152.43 MiB	1.10 GiB	3.62 kbit/s	estimated	1.00 GiB	160 MiB	1.15 GiB						
month	rx	tx	total	avg. rate																			
Aug '10	969.11 MiB	152.43 MiB	1.10 GiB	3.62 kbit/s																			
estimated	1.00 GiB	160 MiB	1.15 GiB																				
Traffic of the top 10	<table><thead><tr><th>#</th><th>day</th><th>rx</th><th>tx</th><th>total</th><th>avg. rate</th></tr></thead><tbody><tr><td>1</td><td>08/27/10</td><td>967.01 MiB</td><td>148.91 MiB</td><td>1.09 GiB</td><td>105.81 kbit/s</td></tr></tbody></table> <div>09:33 unStat / Teemu Toivola</div>			#	day	rx	tx	total	avg. rate	1	08/27/10	967.01 MiB	148.91 MiB	1.09 GiB	105.81 kbit/s								
#	day	rx	tx	total	avg. rate																		
1	08/27/10	967.01 MiB	148.91 MiB	1.09 GiB	105.81 kbit/s																		

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

Item		Description
Select Interface		From the drop-down menu, administrators can select which interface status to display.
WAN1	Mode	Operating mode of this interface.
	MAC Address	The MAC address of the WAN2 port.
	IP Address	The IPv4 address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
	IPv6 Address	The IPv6 address of the chosen interface
	IPv6 Prefix	The prefix of IPv6 address
Traffic Summary		Displays daily, monthly and all time graphical summary of the TX and Rx rate for this interface.
Traffic of the day		Displays traffic information of the day in a table.
Traffic of the month		Displays traffic information of the in a table.
Traffic of the top 10		Shows the top 10 traffic of the day records.
Service Zone – Default, SZ1~SZ8	Mode	The operation mode of the default SZ.
	MAC Address	The MAC address of the default SZ.
	IP Address	The IP address of the default SZ.
	Subnet Mask	The Subnet Mask of the default SZ.
Service Zone – DHCP Server (Default, SZ1~SZ8)	Status	Enable/disable stands for status of the DHCP server in Default Service Zone
	WINS IP Address	The WINS server IP on DHCP server. N/A means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.


13.1.3. HW

View Hardware Status; go to: **Status >> HW.**

This tab page displays the system's hardware usage information.

Hardware Information	
CPU	0.00%
Memory	11.71%
Disk Usage	5.98%

Refresh

Refresh Disable 

13.1.4. Routing Table

View Routing Table; go to: **Status >> Routing Table >> IPv4/IPv6 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
•			
•			
•			
Global Policy			
Destination	Subnet Mask	Gateway	Interface
Interface			
Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Default
192.168.11.0	255.255.255.0	0.0.0.0	SZ1
10.0.0.0	255.255.0.0	0.0.0.0	WAN1
System			
Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	10.0.1.1	WAN1

IPv4 Routing Table

System			
Destination	Prefix	Gateway	Interface

IPv6 Routing Table

- **Policy 1~n:** Shows the information of the individual Policy from 1 to n.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
 - **Destination:** The destination IP address of the device.
 - **Subnet Mask:** The Subnet Mask IP address of the port.
 - **Gateway:** The Gateway IP address of the port.
 - **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

13.1.5. Online Users

View Online Users, go to: [Status >> Online Users](#).

In this page, all online users' information is displayed. Administrators can force out a specific online user by clicking the hyperlink of **Kick Out** and check the user access AP status by clicking the hyperlink of the AP name for **Access From**. Click **Refresh** is to update the current users list or you can select the time interval for automatic refresh from the drop-down box in the lower right corner of this page.

Online Users List							
No.	Username		Pkts In/Out	SZ / VLAN	Auth. Method	Online (Sec.)	Access From
	IP Address	MAC Address	Bytes In/Out	Group / Policy	Auth. Database	Idle (Sec.)	Kick Out
(Total:0) First Prev Next Last							
<div>Refresh</div>							
Refresh <div>Disable</div>							

Item	Description
Username	The user account name.
IP Address	The IP address of this user.
MAC Address	The MAC address of this user.
Pkts In / Out	Number of packets received / sent by this user
Bytes In / Out	Number of Bytes received / sent by this user.
SZ / VLAN	Service Zone and VLAN which this user is associated to.
Group / Policy	The Group and Policy this user is applied to.
Auth. Method	The authentication method used by this user.
Auth. Database	The database used to authenticate this user.
Online (Sec.)	The number of seconds since user successfully login.
Idle (Sec.)	The time period of which the user showed no network activity.
Access From	The name of the managed AP which the user is connected to.
Kick Out	Administrators can forcefully logout a user here.

13.1.6. Non-Login Users

View Non-Login Users; go to: [Status >> Non-Login Users](#).

This page shows users that have acquired an IP address from the system's DHCP server but have not yet been authenticated. This feature is designed for administrators to keep track of systems resources from being exhausted. The list shows the client's **MAC Address**, **IP Address** and associated **VLAN ID**, **Service Zone** as well as **Associated AP** if the client uses wireless connection.

Non-Login Users List				
MAC Address	IP Address	VLAN ID	Service Zone	Associated AP
<div>Refresh</div> <div>Refresh Disable ▼</div>				

13.1.7. Session List

View Session List; go to: **Status >> Session List.**

This page allows the administrator to inspect sessions currently established between a client and the system. Each result displays the IP and Port values of the Source and Destination. You may define the filter conditions and display only the results you desire.

Filter				
Protocol	Source IP	Port	Destination IP	Port
All				

Apply Filter

Display Mode: ALL

(Total 21) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page 1

Row per Page: 20

Session List							
No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	tcp	10.29.3.137	2657	10.0.5.233	80	TIME_WAIT	67
2	tcp	10.29.3.137	2658	10.0.5.233	80	TIME_WAIT	68
3	tcp	10.29.3.137	2653	10.0.5.233	80	TIME_WAIT	36
4	tcp	10.29.3.137	2647	10.0.5.233	80	SYN_RECV	21
5	tcp	10.29.3.137	2652	10.0.5.233	80	TIME_WAIT	36
6	tcp	10.29.3.137	2659	10.0.5.233	80	TIME_WAIT	68
7	tcp	10.29.3.137	2661	10.0.5.233	80	TIME_WAIT	68
8	tcp	10.29.3.137	2663	10.0.5.233	80	TIME_WAIT	68
9	tcp	10.29.3.137	2654	10.0.5.233	80	TIME_WAIT	36
10	udp	10.0.5.196	137	10.0.255.255	137	UNREPLIED	10
11	tcp	10.29.3.137	2651	10.0.5.233	80	TIME_WAIT	36
12	tcp	10.29.3.137	2648	10.0.5.233	80	TIME_WAIT	36
13	tcp	10.29.3.137	2656	10.0.5.233	80	SYN_RECV	50
14	udp	10.0.5.233	32773	168.95.1.1	53	ASSURED	127
15	tcp	10.29.3.137	2662	10.0.5.233	80	TIME_WAIT	68
16	tcp	10.29.3.137	2660	10.0.5.233	80	TIME_WAIT	68
17	tcp	10.29.3.137	2664	10.0.5.233	80	ESTABLISHED	7199
18	tcp	10.29.3.137	2655	10.0.5.233	80	TIME_WAIT	64
19	tcp	10.29.3.137	2650	10.0.5.233	80	TIME_WAIT	36
20	tcp	10.29.3.137	2646	10.0.5.233	80	TIME_WAIT	36

(Total 21) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page 1

Row per Page: 20

13.1.8. User Logs

View Traffic History, go to: [Status >> Users Log.](#)

This page is used to check the traffic history of WHG CONTROLLER. 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.

Users Log		
Date		Size (Byte)
2010-06-07		70
2010-06-06		70
2010-06-05		70
On-demand Users Log		
Date		Size (Byte)
2010-06-07		125
2010-06-06		125
2010-06-05		125
Roaming Out User Log		
Date		Size (Byte)
2010-06-07		106
2010-06-06		106
2010-06-05		106
Roaming In User Log		
Date		Size (Byte)
2010-06-07		112
2010-06-06		112
2010-06-05		112
SIP Call Usage Log		
Date		Call Count
2010-06-07		0
2010-06-06		0
2010-06-05		0
Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2010-06	0	Download



Since the history is saved in the system for limited time frame, please manually copy and save the traffic history information for backup purpose.

If the **Receiver E-mail Address(es)** has been entered under the **Notification Configuration** page, the system will automatically send out the history information to that specified email address.

- Users Log**

All activities occur on the system within the nearest 72 hours are recorded; in date and time order. As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out** and **Bytes Out** of the user activities.

Users Log 2010-06-07								
Date	Type	Name	IP	IPv6	MAC	Pkts In	Bytes In	Bytes Out

- **On-demand User Log**

As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **1st Login Expiration Time**, **Account Valid Through** and **Remark**, of user activities.

On-demand Users Log 2010-06-07													
Date	System Name	Type	Name	IP	IPv6	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	activationtime	1st Login Expiration Time	Account Valid Through

- **Roaming Out User Log**

As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming Out User Log 2010-06-07													
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Roaming In User Log**

As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In User Log 2010-06-07														
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **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)

13.1.9. Local User Monthly Network Usage

View Local User Monthly Network Usage; go to: **Status >> User Logs**.

- **Monthly Network Usage of Local User**

The system keeps a cumulated record of the traffic data generated by each Local 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					

- **Username:** Username of the local user account.
 - **Connection Time Usage:** The total time used by the user.
 - **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
 - **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.
- **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
2010-06	1	Download

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

13.1.10. Logs

View Logs; please go to: [Status >> Logs.](#)

Logs	
System Log	Show
Web Log	Show
UAMD Log	Show
CAPWAP Log	Show
RADIUS Server Log	Show
WMI Configuration Log	Show

This page displays the system's local log information since system boot up. Administrators can examine the log entries of various events. However, since all these information are stored on volatile memory, they will be lost during a restart/reboot operation. Therefore if the log information needs to be documented, the administrator will need to make back up manually.

- **System Log:** This page displays system related logs for event tracing.
- **Web Log:** This page shows which of the web pages have been accessed on the Controllers built-in web server.
- **UAMD Log:** Displays the UAM related information output from the UAM daemon.
- **CAPWAP Log:** This page shows the CAPWAP message communicated between the Controller and CAPWAP enabled APs.
- **RADIUS Server Log:** This page displays the RADIUS messages that passes through the controller.
- **WMI Configuration Log:** This page shows the account, and IP of the person that has made changes to Controllers WMI configurations.

13.1.11. DHCP Lease

View DHCP Lease; go to: **Status >> DHCP Lease.**

The DHCP IP lease statistics can be viewed after clicking on **Show** Statistics List in this page.

- **Statistics of offered list**

Valid lease counts of the **Last 10 Minutes**, **Hours** and **Days** are shown here. The header 1 ~ 10 are unit multiplier, for instance the number under column 2 indicates the lease count in the last 20 minutes/hours/days, the number under column 3 indicated the lease count in the last 30 minutes/hours/days and so on.


- **Statistics of expired list**

IP leased to clients that have expired in the **Last 10 Minutes**, **Hours** and **Days** are shown here. The header 1 ~ 10 are unit multiplier, for instance the number under column 2 indicates the expired count in the last 20 minutes/hours/days, the number under column 3 indicated the expired count in the last 30 minutes/hours/days and so on.

Statistics of offered list										
	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	2	22	3	1	0	0	1	2	2
Last 10 Days	51	0	0	0	0	0	0	0	0	0

Statistics of expired list										
	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	1	0	0	0	0	0	2	1
Last 10 Days	10	0	0	0	0	0	0	0	0	0

Refresh

Refresh Disable 

- **DHCP Lease List**

Valid IP addresses issued from the DHCP Server and related information of the client using this IP address is displayed here.

DHCP Logs	
Statistics List	Show
DHCP Lease Log	Show

DHCP Lease List					
No.	IP Address	MAC Address	Host Name	Vlan	Lease Expires
1	192.168.1.4	00:40:96:a1:af:dd	x30-ac42	0	2011/03/19 17:13:49
2	192.168.1.41	00:1d:73:3b:73:3e	AC109-NB	0	2011/03/19 18:32:35
3	192.168.1.76	cc:08:e0:04:80:cf	*	0	2011/03/19 19:01:04

13.2. Notification

Configure Notification; go to: **Status >> Report & Notification**.

WHG CONTROLLER can automatically send various kinds of user and/or system related reports to configured E-mail addresses, SYSLOG Servers, or FTP Server.

Report and Notification	
SMTP Settings	Configure
SYSLOG Settings	Configure
FTP Settings	Configure
Notification Settings	Configure
System Report	Show

- **SMTP Settings:** Allows the configuration of 5 recipient E-mail addresses and necessary mail server settings where various user related logs will be sent to.
- **SYSLOG Settings:** Allows the configuration of two external SYSLOG servers where selected users logs as well as system logs will be sent to.
- **FTP Settings:** Allows the configuration of an external FTP Server where selected users logs as well as system logs will be sent to.
- **Notification Settings:** Provides an overview of all the available user and system logs for selection. Selected logs can be sent to the chosen location (E-mail, SYSLOG, FTP) on customizable time intervals.
- **System Report:** Provides a graphical display of system status and resources usage based on selected time intervals.

13.2.1. SMTP Settings

SMTP Settings	
Receiver E-mail Address 1	<input type="text"/>
Receiver E-mail Address 2	<input type="text"/>
Receiver E-mail Address 3	<input type="text"/>
Receiver E-mail Address 4	<input type="text"/>
Receiver E-mail Address 5	<input type="text"/>
Sender E-mail Address	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Auth Method	None ▾

- **Receiver E-mail Address (1 ~ 5):** Up to 5 E-mail addresses can be set up here to receive notifications.
- **Sender E-mail Address:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **SMTP Server:** Enter the IP address of the sender's SMTP server.
- **SMTP 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.

13.2.2. SYSLOG Settings

SYSLOG Settings			
SYSLOG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
SYSLOG Destinations	SYSLOG Server 1	IP Address: <input type="text"/>	Port: <input type="text"/>
	SYSLOG Server 2	IP Address: <input type="text"/>	Port: <input type="text"/>

- **SYSLOG Destinations:** Up to two external SYSLOG servers may be configured, please enter the IP address and port number of the external SYSLOG server.
- **System Log:** This controls the enabling/disabling of the SYSLOG logging feature. When enabled, the selected logs from “Notification Settings” will be sent to the SYSLOG server configured above. However, when disabled, no logs will be sent to the SYSLOG server configured above.

13.2.3. FTP Settings

FTP Settings	
FTP Destination	IP Address: <input type="text"/> Port: <input type="text"/>
	Anonymous <input type="radio"/> Yes <input checked="" type="radio"/> No
	Username <input type="text"/>
	Password <input type="text"/>
	FTP Setting Test <input type="button" value="Send Test Log"/>

➤ **FTP Destination:** Specify the IP address and port number of your FTP server. If your FTP needs authentication, enter the Username and Password. The “Send Test Log” radio button can be used to send a test log for testing your current FTP destination settings.

13.2.4. Notification Settings

This configuration page allows the selection of log types to send, either to preconfigured E-mail, SYSLOG Servers or FTP Server based on the chosen time Interval.

Notification Settings									
	Receiver E-mail Address(es)					Detail / Test	SYSLOG	FTP	Interval
	1	2	3	4	5				
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾
Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
On-demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Report <input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associate Client <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail <input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report	
Hardware Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
HTTP Web Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
DHCP Server Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
DHCP Lease Log	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	1 Hour ▾
System Report <input type="checkbox"/> CPU Loading <input type="checkbox"/> CPU Temperature <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail <input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report	

■ Sending Logs to E-mail

The following log types can be sent to E-mail addresses configured in “SMTP Settings”: Monitor IP Report, Users Log, On-demand Users Log, Session Log. The numbers 1 to 5 represents the corresponding E-mail address configured in “SMTP Settings”, click the desired E-mail address profile (1 ~ 5) and select the time interval for sending report or log.

Notification Settings									
	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾
Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
On-demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Report <input type="checkbox"/> CPU Loading									

- **Detail:** Clicking this radio button allows the configuration of the E-mail subject for the corresponding log.
- **Send:** Clicking this radio button sends a test log to the selected E-mail address.

■ Sending Logs to SYSLOG

The following log types can be sent to external SYSLOG servers configured in “SYSLOG Settings”: Users Log, On-demand Users Log, Session Log, Hardware Log, HTTP Web Log, and DHCP Server Log. Click the desired log type and select the time interval for sending log.

Notification Settings									
	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾
Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
On-demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Report <input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associate Client <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic									
	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
Hardware Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
HTTP Web Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
DHCP Server Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
DHCP Lease Log	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	1 Hour ▾

- **Detail:** Clicking this radio button allows the configuration SYSLOG attributes such as Tag, Severity and Facility which will be assigned to the corresponding log to meet the filtering requirements on the SYSLOG Server.

Note: The “System Log” option needs to be enabled under SYSLOG Settings in order to send the selected logs to the configured SYSLOG Servers.

SYSLOG Settings			
SYSLOG Destinations	SYSLOG Server 1	IP Address: 10.23.1.101	Port: 514
	SYSLOG Server 2	IP Address:	Port:
System Log	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		

■ Sending Logs to FTP

The following log types can be sent to external FTP servers configured in “FTP Settings”: Users Log, On-demand Users Log, Session Log, HTTP Web Log, DHCP Lease Log, and System Report. Click the desired log type and select the time interval for sending log.

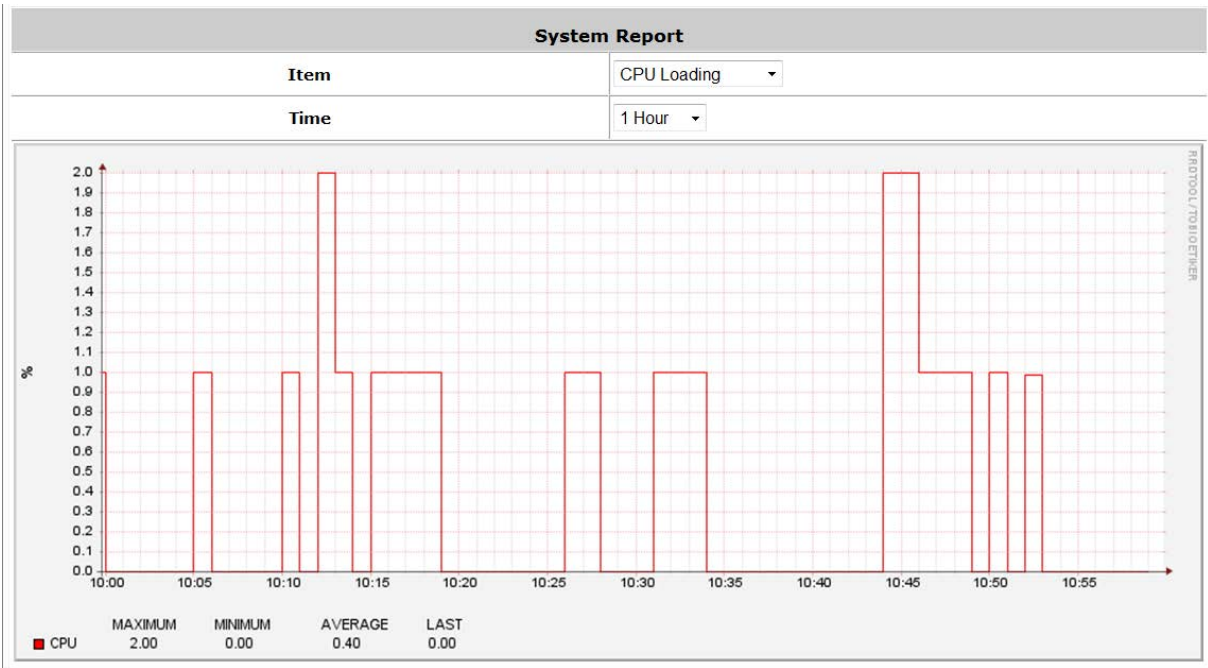
Notification Settings									
	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾
Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
On-demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detail / Send	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Wide Area AP Report <input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associate Client <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
Hardware Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
HTTP Web Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/> Detail	1 Hour ▾
DHCP Server Log	N/A						<input type="checkbox"/> Detail	<input type="checkbox"/>	N/A
DHCP Lease Log	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	1 Hour ▾
System Report <input type="checkbox"/> CPU Loading <input type="checkbox"/> CPU Temperature <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query	N/A						<input type="checkbox"/>	<input type="checkbox"/> Detail	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report

Detail: Clicking this radio button allows the specification of the FTP server folder where the logs sent will be stored on the FTP server.

Note: The outputted log files to the FTP server will be named according to the format **\$Topic_ExtraDesc_SystemName_Date_Time.txt**. For example: HTTPWebLog_GW1_2010-10-15_0800.txt

13.2.5. System Report

The function provides the graphical statistics information of CPU Loading, CPU Temperature, Memory Usage and etc. This page displays system status and resource usages in a plotted graph. It can show the total DHCP Lease number of all Service Zone and each Service Zone.



- **Item:** Select the type of report you wish to see. Available report types are: CPU Loading, CPU Temperature, Memory Usage, Network Traffic, Online User, Successful Login, Session, DHCP Lease, and DNS Query.
- **Time:** For selecting the time scale of the displayed graph. The reports can be displayed on hourly, daily, weekly, monthly or yearly basis.

14. Virtual Private Network (VPN)

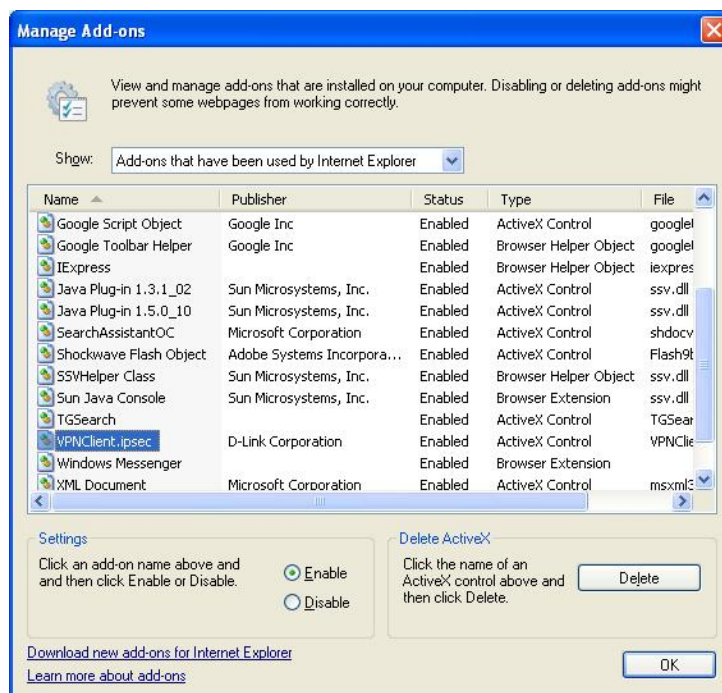
14.1. Local VPN

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 WHG CONTROLLER with Local VPN, 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 WHG CONTROLLER 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 WHG CONTROLLER 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.

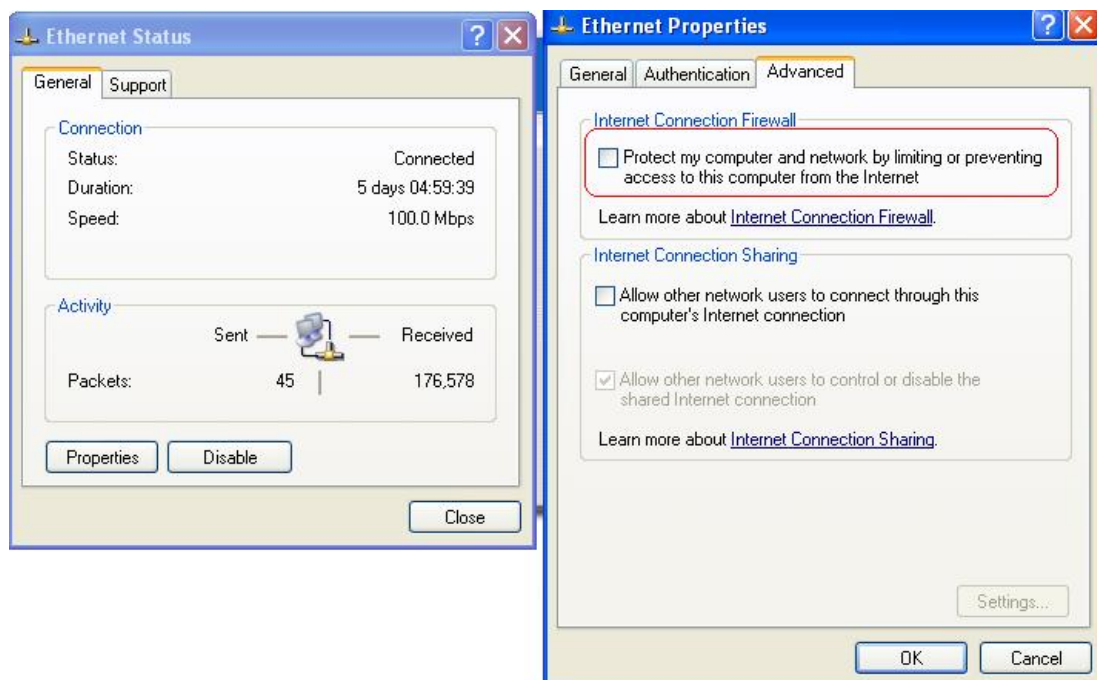
• Limitations

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

- 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.
- Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.
- 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.
- 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**

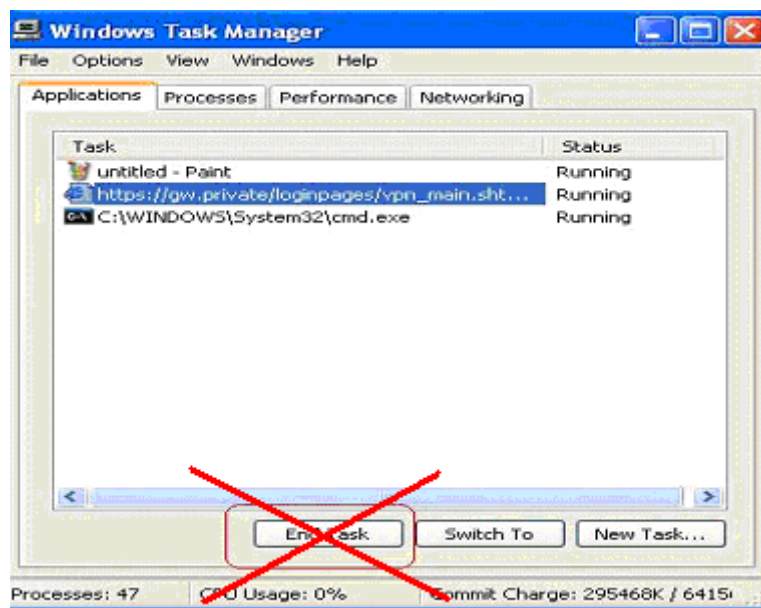
The ActiveX component for IPSec VPN is running in parallel with the web page of "Login Success". To ensure that the built-in IPSec VPN tunnel is always alive, unless clients decide to close the session and to disconnect from WHG CONTROLLER, **the following conditions or behaviors, which may cause the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

14.2. Remote VPN

Configure Remote VPN; go to: **Network >> VPN >> Remote VPN.**

WHG CONTROLLER support **Remote VPN** for user login to system from remote area. After the user is login to system from the outside network of WAN, the user will feel that it is look like login to WHG CONTROLLER under the service zone locally. They also can be applied Policy and are controlled by system to access the network.

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 100 connections.)</small>				
SIP Configuration	Enable <input type="checkbox"/> WAN Interface: WAN1				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enable
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Group Permission Configuration	<input type="button" value="Configure"/>				
Applied Policy to Remote Client	<input type="text" value="Policy 1"/>				
Remote VPN Login Page	<input type="button" value="Configure"/>				

All settings are look like the settings in Service Zone. It also can setup the **SIP WAN Interface**, **Authentication Options**, **Group Permission**, **Applied Policy** and customizable Login Page.

After Remote VPN is enabled, when you browse the home page with the WAN IP, you will get the Remote VPN login page, input the enabled authentication options username and password, then you will login success to system.



After Remote VPN is enabled, the default home page will be the Remote VPN login page. If you want to access the WMI of WHG CONTROLLER, please input "login.shtml" after the WAN IP. For example, it may be: "http://192.168.X.X/login.shtml"

14.3. Site-to-Site VPN

Configure Site-to-Site VPN; go to: **Network >> VPN >> Site-to-Site VPN.**

WHG CONTROLLER support **Site-to-Site VPN** for more than 2 WHG CONTROLLER create VPN tunnel to each other over the WAN network. For example, if there are 2 WHG CONTROLLER, you can create a VPN tunnel to let a subnet of one WHG CONTROLLER to access the subnet of another WHG CONTROLLER.

Remote Site Configuration					
Name	IP Address	Pre-shared Key	Edit	Delete	
<button>Add A Remote Site</button>					

Local Site Configuration					
Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Edit	Delete
<button>Add A Local Site</button>					

First, you need to add a Remote Site with remote subnet.

Remote VPN Gateway	
Name	<input type="text"/>
IP Address	<input type="text"/>
Authentication Method	Pre-shared Key ▾
Pre-shared Key	<input type="text"/>
Phase1 Proposal	Encryption <input type="text" value="AES256"/> ▾ Authentication <input type="text" value="SHA-1"/> ▾
Diffie-Hellman Group	<input type="checkbox"/> Group 1 <input type="checkbox"/> Group 2 <input type="checkbox"/> Group 5
IKE Life Time	<input type="text" value="8"/> <input type="text" value="h"/> ▾ (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)
Dead Peer Detection	DPD Delay: <input type="text" value="10"/> (second) DPD Timeout: <input type="text" value="15"/> (second)

Remote Subnet		
No.	Network	Mask
1	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/> ▾



The IPsec settings in both sites must be same.

And then create a Local Site with subnet for mapping to the remote site.

Local Site Information	
Local Interface	WAN1
Remote VPN Gateway	<div> <div></div> <div>Edit Host</div> <div>Add a New Host</div> </div>
Local Host/Subnet	<input checked="" type="radio"/> Host <input type="radio"/> Subnet
Remote Host/Subnet	
Phase2 Proposal	Encryption AES256 Authentication SHA-1
Key's Life Time	24 h (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)
Rekey	<input type="checkbox"/> Enable Rekey Rekey Margin: 9 m (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)
Perfect Forward Secrecy	<input checked="" type="checkbox"/> Enable PFS PFS Group Group 2

Such as “192.168.11.0/24” of WHG CONTROLLER_A >> “192.168.111.0/24” of WHG CONTROLLER_B, after the tunnel is created, the users within these two subnets can reach each other.



You can create more than one VPN tunnel, but the IP segment mapping can not be overlap that same IP segment has more than one routing rule.

15. Customization of Portal Pages

15.1. Customizable Pages

Configure Customizable Pages; go to: **System >> Service Zones.**

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

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

Click the button of **Configure**, the setup page will appear.

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

Custom Pages	Disclaimer Page	Configure
	Login Page	Configure
	Port Location Mapping Free Login Page	Configure
	Port Location Mapping Charge Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Failed Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure
	Logout Failed Page	Configure

Now, let us discuss two examples: **Login Page** and **Logout Page**

15.2. Loading a Customized Login Page

■ *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.

• *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
This is the default login page for users. You could click Preview to preview the default login page.
Preview

• *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	<input type="text" value="CC0000"/> Select (RGB values in hex mode)
Color for Title Text	<input type="text" value="FFFFFF"/> Select (RGB values in hex mode)
Color for Page Background	<input type="text" value="FFFFFF"/> Select (RGB values in hex mode)
Color for Page Text	<input type="text" value="000000"/> Select (RGB values in hex mode)
Title	<input type="text" value="User Login Page"/>
Welcome	<input type="text" value="Welcome To User Login Page"/>
Information	<input type="text" value="Please Enter Your Name and Password to Sign In"/>
Username	<input type="text" value="Username"/>
Password	<input type="text" value="Password"/>
Submit	<input type="text" value="Submit"/>
Cancel	<input type="text" value="Clear"/>
Remaining	<input type="text" value="Remaining"/>
Copyright	<input type="text" value="Copyright (c)"/>
Remember Me	<input type="text" value="Remember Me"/>
Logo Image File	<input type="button" value="Preview and Edit the Image File"/>
Background Image File	<input type="button" value="Preview and Edit the Image File"/>
<input type="button" value="Preview"/>	

- Custom Pages >> Login Page >> **Uploaded Page**

Choose Uploaded Page and upload a login page to the built-in HTTP server.

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

Existing Image Files:	
<p>Total Capacity: 512 K Now Used: 0 K</p>	

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

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.

15.3. Using an External Login Page

- *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>
```

15.4. Load a Customized Logout Page

- *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.

Logout 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"/> <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"/>	
Preview	

►► **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>
```

15.5. How External Page Operates

Choose **External Page** if you desire to use an external web page for your custom pages. Simply enter the URL of your external webpage, click **Preview** button to check if it is reachable, take a look at how your external webpage will be displayed, then click **Apply** button.

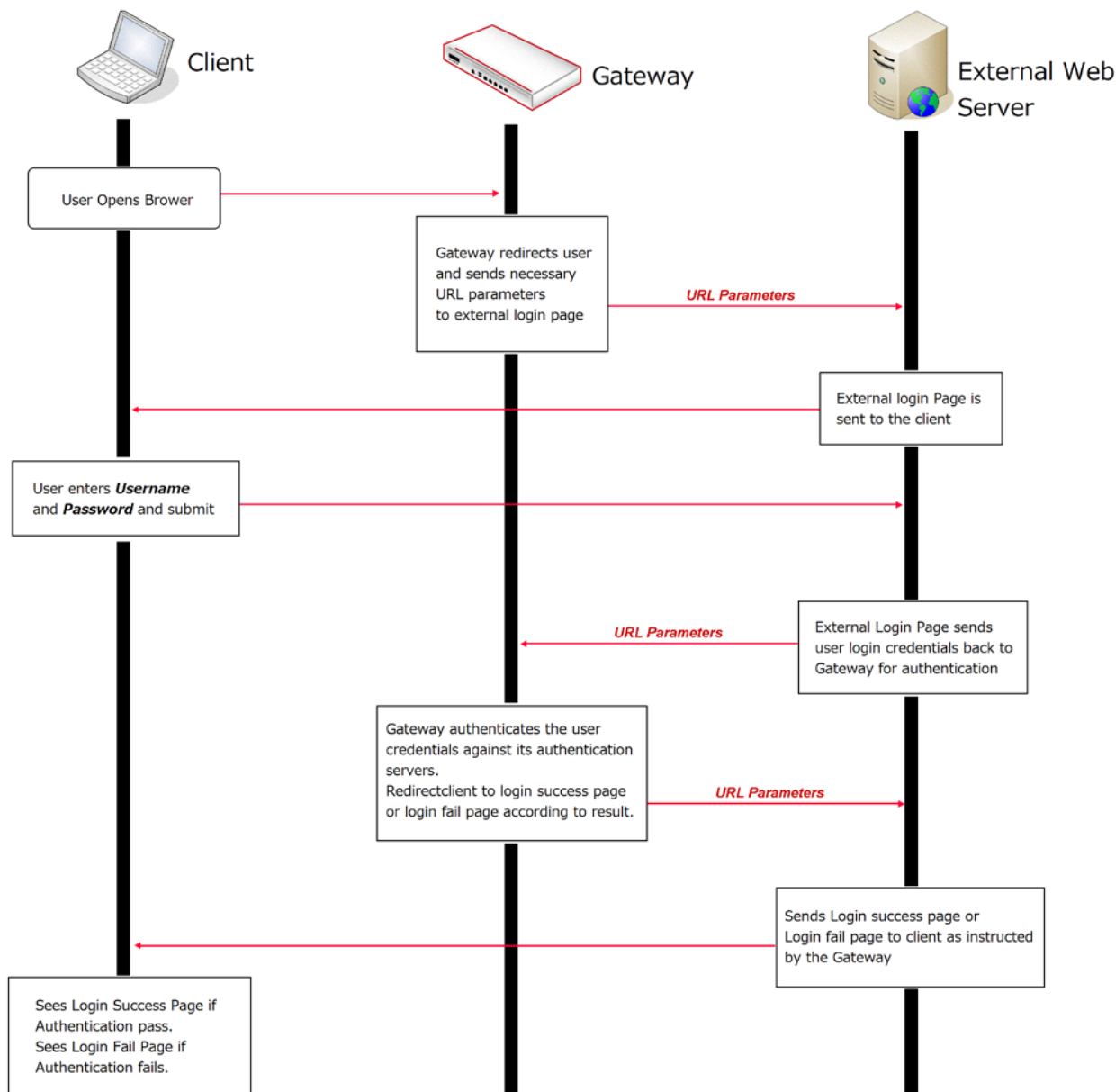
Login Page Selection for Users - Service Zone: SZ1	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL	<input type="text" value="http://192.168.1.1/ExternalPage/login.html"/>
<input type="button" value="Preview"/>	

Main Menu>System>Service Zone>Service Zone Configuration>Login Page

When a user connects to this Service Zone, opens a web browser and attempts to access the internet, the system will redirect the user to the external login page configured. Gateway while redirecting users to the external web page will also send URL parameters required for the operation, for instance user authentication. Therefore, each self-defined external pages (*Login*, *Logout*, *Login Success*, *Logout Success*, etc.) requires codes to handle **URL parameters** to and from the Gateway. A simple example is illustrated below for Login Page, please refer to **External Login Page Parameters** for URL parameter relating to other pages such as *Login Success Page* ... and etc. Therefore it is important that your external pages are designed by someone with good knowledge of URL parameter utilization.

Diagram below explains how External Page operates using user login flow as illustration:



The URL parameters sent by the Gateway to the external login page are as follows:

Field	Value	Description
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user want to get remaining quota.
vlanid	Integer (1 ~ 4094)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
umac	MAC format (separated by ':')	Client MAC address
session	String	Encrypted session information, include: client IP address, MAC address, date, and return URL.

You will need to parse the required parameters in your html code. The following HTML code segment is an example of parsing *loginurl* parameter with a self define javascript function:

```

<FORM action="" method="post" name="form">
<script language="Javascript">
form.action = getVarFromURL(window.location.href, 'loginurl');
</script>
<INPUT type="text" name="myusername" size="25">
<INPUT type="password" name="mypassword" size="25">
<INPUT name="button_submit" type="submit" value="Enter">
<INPUT name="button_clear" type="button" value="Clear">
</FORM>

```

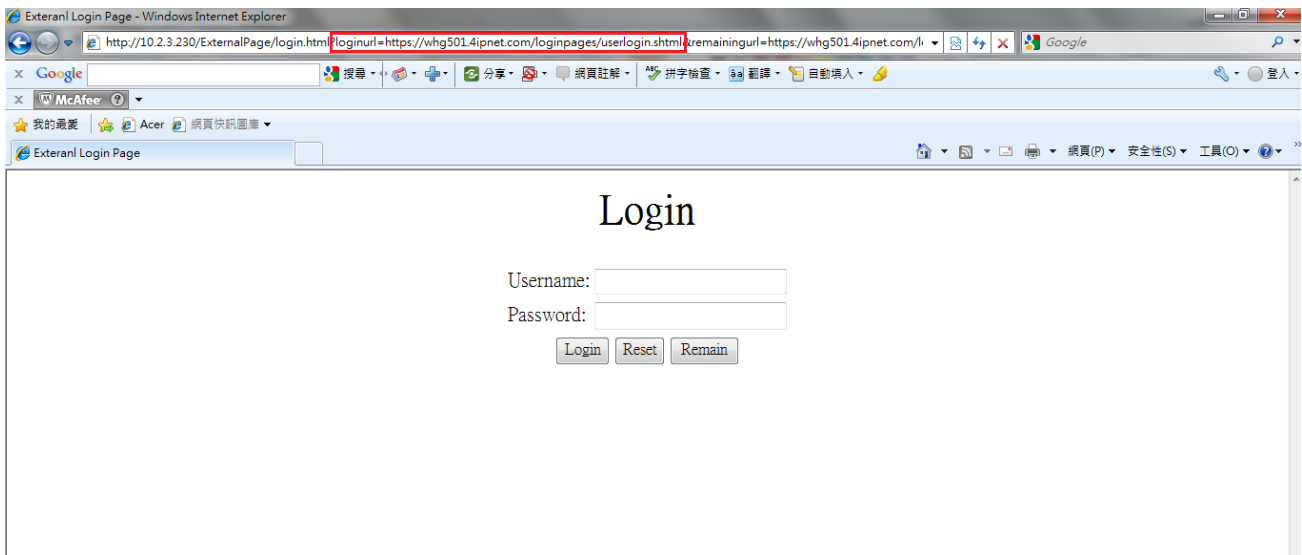
The following shows the corresponding self-defined javascript function used to parse the *loginurl* parameter:

```

function getVarFromURL(url, name) {
    if(name == "" || url == "") { return ""; }
    name = name.replace(/\[/|\]|"|"').replace(/\[/|\]|"|"');
    var regObj = new RegExp("[\?&]" + name + "=(^&#)*");
    var result = regObj.exec(url);
    if(result == null) { return ""; }
    else { return decodeURIComponent(result[1]); }
}

```

An external page example that the user will see upon launching a browser, highlighted in red you can see the URL parameters sent from the system:



▪ URL Variables from Gateway

This section displays all the URL parameters that are sent from the Gateway to the various external pages.

- **External Login Page:**

Variables:

Field	Value	Description
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user want to get remaining quota.
vlanid	Integer (1 ~ 4094)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
umac	MAC format (separated by ':')	Client MAC address
session	String	Encrypted session information, include: client IP address, MAC address, date, and return URL.

- **External Login Successful Page:**

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name
Umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	RADIUS user session length (Only available for RADIUS user)
byteamount	Integer (Bytes)	RADIUS user volume limit (Only available for RADIUS user)
idletimeout	Integer (Sec.)	Idle timeout
acct-interim-interval	Integer (Sec.)	RADIUS accounting interim update interval (Only available for RADIUS user)
logouturl	String (URL encoded)	The URL which shall be submitted when user want to logout.

Change_passwd_url	String (URL encoded)	The URL which shall be submitted when user want to change password. (Only available for LOCAL user)
ondemand_creation_url	String (URL encoded)	The URL which shall be submitted when user want to create on-demand user. (Only available for LOCAL user)
Vlanid	Integer (1~4094)	VLAN ID
Gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
Sz	Integer	Service Zone ID
Group	Integer	Group index
Policy	Integer	Policy index
max_uplink	Integer (b/s)	Maximum up-link rate
max_downlink	Integer (b/s)	Maximum down-link rate
Req_uplink	Integer (b/s)	Minimum up-link rate
Req_downlink	Integer (b/s)	Minimum down-link rate
next_page	String	Client redirection URL
CLASS	String	RADIUS CLASS attribute (Only available for RADIUS user)
WISPR-SESSION-TERMINATE-TIME	String, format: YYYY-MM-DDThh:mm:ssTZD	WISPr Session-Terminate-Time attribute (Only available for RADIUS user)
WISPR-SESSION-TERMINATE-END-OF-DAY	Integer (0/1)	WISPr Session-Terminate-End-Of-Day attribute, 0 or 1 to indicate termination rule. (Only available for RADIUS user)
WISPR-BILLING-CLASS-OF-SERVICE	String	WISPr Billing-Class-Of-Service attribute (Only available for RADIUS user)
WISPR-LOCATION-ID	String	WISPr Location-ID attribute (Only available for RADIUS user)
WISPR-LOCATION-NAME	String	WISPr Location-Name attribute

(Only available for RADIUS user)

WISPR-BILLING-TIME	String, format: HH:MM	WISPr Billing-Time attribute (Only available for RADIUS user)
session	String	Encrypted session information

- **External Error Page:**

Variables:

Field	Value	Description
msg	String, includes: The system is busy. Please try again later. Cannot find session related information. Please enable the Cookie in the browser setting or open a website to get a Cookie. Invalid IP address. Please check the IP address and try again. Invalid MAC address. Please check the MAC address and try again. Sorry, your account is not usable, because the authentication option is currently disabled. Please contact your network administrator. Sorry, your account is not usable, because the authentication option (associated with the postfix) is not found. Please contact your network administrator. Sorry, you are not allowed to log in, because your account is currently on the Black List. Sorry, you are not allowed to log in,	Error message

because it is currently not the service hour for your account.

You have already logged in.

Sorry, there is a system problem checking the information of your account (XXX).
Please contact your network administrator.

Invalid username or password.
Please check your username and password and try again.

Cannot identify the policy for your account.
Please contact your network administrator.

User of this device (the MAC address) is not allowed to use this account.
Please contact your network administrator.

Sorry, the external authentication server is currently unreachable.
Please contact your network administrator.

Sorry, you are not allowed to create a remote VPN connection.

Vlanid	Integer (1~4094)	VLAN ID
Gwip	IP format	Gateway activated IP address

- **External Logout Successful Page:**

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Vlanid	Integer (1~4094)	VLAN ID
Gwip	IP format	Gateway activated IP address

- **External On-demand login successful page:**

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name
Umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	On-demand user's quota of time type
byteamount	Integer (byte)	On-demand user's quota of volume type
idletimeout	Integer (Sec.)	Idle timeout
logouturl	String (URL encoded)	Logout URL
redeemurl	String (URL encoded)	Redeem URL
Vlanid	Integer (1~4094)	VLAN ID
Gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
Sz	Integer	Service Zone ID
Group	Integer	Group index
Policy	Integer	Policy index
next_page	String	Client redirection URL
max_uplink	Integer (b/s)	Maximum up-link rate
max_downlink	Integer (b/s)	Maximum down-link rate
Req_uplink	Integer (b/s)	Minimum up-link rate
Req_downlink	Integer (b/s)	Minimum down-link rate
session	String	Encrypted session information

- **External Logout Fail Page:**

Variables:

Field	Value	Description
Uid	String	User ID
Gwip	IP format	Gateway activated WAN IP address
Vlanid	Integer (1~4094)	VLAN ID

1.URL Variables to Gateway

This section presents the parameters that need to be sent back to the Gateway for the various external pages. **Path:** is the URL destination; **Input:** the parameters required to send back; **Output:** the feedback from system.

- **User Login:**

Path:

(LAN IP address or Internal Domain Name) /loginpages/userlogin.shtml

Input:

Field	Required	Value	Description
myusername	Required	String	User ID
mypassword	Required	String	User password
session	Optional	String	Encoded string which contains some information of this session, default is taken from cookie.

Output:

No output, redirect user to login successful page.

- **User Logout:**

Path:

(LAN IP address or Internal Domain Name) /loginpages/logoff.shtml

Input:

Field	Required	Value	Description
Uid	Optional	String	User ID, default is taken from cookie
session	Optional	String	Encoded string which contains some information of this session, default is taken from cookie

Output:

No output, redirect user to logout successful page.

- **Remaining quota (Credit balance):**

Path:

(LAN IP address or Internal Domain Name) /loginpages/reminder.shtml

Input:

Field	Required	Value	Description
myusername	Required	String	User name
mypassword	Required	String	Password
ret_url	Optional	String (URL encoded)	Returned URL, default is pop_reminder.shtml
command	Optional	String	getValue: If command is set to "getValue", the return URL would be ignored, and the page would only print out the available quota.

Output:

If command is set to "getValue", the output is simply "value".(secs. or bytes according to user type)

If command is not set and there is no ret_url is presented, client would be redirected to pop_reminder.shtml page, which shows remaining quota in our UI style. If ret_url is presented, client would be redirected to ret_url, and gateway would add these four variables in URL.

Field	Value	Description
msg	String, including: Sorry, this feature is available for on-demand user only. Sorry, this username: XXX is not found. Sorry, this username: XXX is out of quota. Sorry, this username: XXX is expired. Sorry, this username: XXX is redeemed.	Error messages
Value	Integer (Sec. Or Byte) or error no. -1: Account not found.	Remaining quota, if user is time type, the value is remaining seconds, if user is volume type, the value remaining bytes.

-2: Out of quota.

-3: Expired.

-4: Redeemed.

Uname	String	User name
Type	String, includes:	On-demand user billing type

TIME: Time type

DATA: Volume type

CUTOFF: Cut-off type

- **Change password (Local User):**

Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/user_change_password.shtml](#)

Input:

Field	Required	Value	Description
Save	Required	1 (have to be 1)	
Opw	Required	String	Old password
Npw	Required	String	New password
Npwc	Required	String	Confirmed new password
ret_url	Required	String (URL encoded)	Return URL

Output:

Client would be redirected to ret_url and gateway would add result in ret_url which indicates the result of changing password.

Field	Value	Description
Result	String, including:	Result and error messages
	Change password successfully	
	User password is incorrect	
	Invalid password format	

- **Redeem (On-demand user):**

Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/redeemuserlogin.shtml](#)

Input:

Field	Required	Value	Description
Uid	Optional	String	Current user ID (If not presented, user name stored in cookie is the default value)
upassword	Optional	String	Current user password (If not presented, password stored in cookie is the default value)
myusername	Required	String	Redeem user ID
mypassword	Required	String	Redeem user password
ret_url	Optional	String (URL encoded)	Return URL, login successful page is the default value

Output:

If no ret_url is presented, client would be redirected to login successful page, and in addition, a JavaScript window would pop-up and show the result. If ret_url is presented, client would be redirected to ret_url and gateway would add an additional variable rmsg to indicate redeem procedure result.

Field	Value	Description
rmsg	String, including: Redeem process completed. Original user name can not be found from the database. Redeem user name can not be found from the database. Original user password is incorrect. Redeem user password is incorrect. Original user type and ondemand user type do not match. Original user has not login.	Result and error messages

Redeem user login already.

Had been redeemed before.

User run out of quota.

Maximum allowable time is exceeded.

Maximum allowable memory space is exceeded.

Wrong postfix please check it.

This account is expired.

- **On-demand account creation (Local User)**

Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/UserAuthentication/OnDemandRecept.shtml](#)

Input:

Field	Required	Value	Description
buttonNo	Required	Integer (1~10)	Billing Plan No.
random	Optional	Integer	A random number, this number is to prevent quick-click issue in IE 6.0.
ret_url	Optional	String (URL encoded)	Return URL.

Output:

If no ret_url is presented, the client would be redirected to a ticket page in our UI style. If ret_url is presented, client would be redirected to ret_url and receive the result containing created on-demand account information.

Field	Value	Description
Result	String, the format is: (separated by ',')	If ret_url is presented, the client would be redirected to ret_url page and carry the result valuable.
	username,	expiretime is account expiration
	password,	time which is a Linux time stamp,
	expiretime,	and duration is account duration
	usage,	time and the unit is 'day', serial

price,
duration,
serial number

number is account s/n.

15.6. Disclaimer Page

Configure Disclaimer Page; go to: **System >> Service Zone >> Service Zone Configuration >> Disclaimer Page.**
Before the configuration of the Disclaimer Page, **Disclaimer Page** must be enabled first; click on **Enable Disclaimer Page** to redirect to General Settings: **System >> General >> Disclaimer Page.**

Note: Please Enable [Disclaimer Page](#)



General Settings for the Entire System	
System Name	<input type="text"/>
Administrator Contact Information	<input type="text"/>
Suspend Warning Message	<input type="text" value="Sorry! The service is suspended."/> *
Internal Domain Name	<input type="text" value="gateway.example.com"/> <input checked="" type="checkbox"/> Use the name on the security certificate <small>(FQDN of this device for internal use, e.g. controller.office-name.com)</small>
Disclaimer Page	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Go to: **System >> Service Zone >> Service Zone Configuration >> Disclaimer Page.**

Disclaimer Pages >> Login Page

The administrator can use the default disclaimer page or get the customized 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.

- Custom Pages >> Disclaimer Page >> **Default Page**
Select the type of Disclaimer Page to use the default page.

Disclaimer Page Type	
<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: SZ1
This is the default disclaimer page for users. You could click Preview to preview the default disclaimer page.
Preview



Authentication Required

Welcome to broadband Internet access service!

Before you proceed, please acknowledge that:

- (1) There may be interruptions to the service due to technical reasons beyond our control.
- (2) We are not responsible for the accuracy and appropriateness of the information or material contained on

16. Payment Gateways

16.1. Payments via Authorize.Net

Configure Payments via Authorize.Net; go to: **User >> Authentication >> On-demand User >> External Payment Gateway >> Authorize.Net.**

Before setting up “Authorize.Net”, it is required that the merchant owners have a valid Authorize.Net account.

➤ Authorize.Net Payment Page Configuration

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

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

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

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

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

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

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

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

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

Service Disclaimer Content	
<div> <div>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.</div> <div> <div></div> <div></div> <div></div> </div> </div>	

Choose Billing Plan for Authorize.Net Payment Page				
Plan	Enable/Disable		Quota	Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	1.1 Mbyte(s) of traffic volume quota	20
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	9 hr(s) 59 min(s) of connection time quota with expiration	57
3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

Client's Purchasing Record	
Starting Invoice Number	<div> <div>Hotspot</div> <div>-</div> <div>0000000</div> </div> <div>* <input type="checkbox"/> Change the Number</div>
Description (Item Name)	<div>Internet Access</div> <div>*</div>
E-mail Header	<div>Enjoy Online!</div> <div>*</div>

- **Service Disclaimer Content**
- View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.
- **Choose Billing Plan for Authorize.Net Payment Page**
- These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.
- **Client's Purchasing Record**
- **Starting Invoice Number:** An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.
- **Description (Item Name):** This is the item information to describe the product (for example, Internet Access).
- **Email Header:** Enter the information that should appear in the header of the invoice.

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

Authorize.Net Payment Page Fields Configuration		
No.	Displayed Text	Required
<input checked="" type="checkbox"/> Credit Card Number	Credit Card Number *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Credit Card Expiration Date	Credit Card Expiration Date *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> First Name	First Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Last Name	Last Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Type	Card Type * <input checked="" type="checkbox"/> Visa <input checked="" type="checkbox"/> American Express <input checked="" type="checkbox"/> Master Card <input checked="" type="checkbox"/> Discover	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Code	Card Code *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> E-mail	E-mail *	<input type="checkbox"/>
<input type="checkbox"/> Customer ID	Room Number *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Company	Company *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Address	Address *	<input type="checkbox"/>
<input checked="" type="checkbox"/> City	City *	<input type="checkbox"/>
<input checked="" type="checkbox"/> State	State *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Zip	Zip *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Country	Country *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Phone	Phone *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Fax	Fax *	<input type="checkbox"/>

*Displayed text fields must be filled.

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

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

- **Item:** Check the box to show this item on the customer's payment interface.
- **Displayed Text:** Enter what needs to be shown for this field.
- **Required:** Check the box to indicate this item as a required field.
- **Credit Card Number:** Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.
- **Credit Card Expiration Date:** Month and year expiration date of the credit card. This should be entered in the format of MMY. For example, an expiration date of July September 2009 should be entered as 0709.
- **Card Type:** This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.
- **Card Code:** The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).
- **E-mail:** An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.
- **Customer ID:** This is an internal identifier for a customer that may be associated with the billing

information of a transaction. This field may contain any format of information.

- **First Name:** The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.
- **Last Name:** The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.
- **Company:** The name of the company associated with the billing or shipping information entered on a given transaction.
- **Address:** The address entered either in the billing or shipping information of a given transaction.
- **City:** The city is associated with either the billing address or shipping address of a transaction.
- **State:** A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.
- **Zip:** The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.
- **Country:** The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.
- **Phone:** A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.
- **Fax:** A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

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

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

16.2. Payments via PayPal

Configure Payments via PayPal; go to: **User >> Authentication >> On-demand User >> External Payment Gateway >> PayPal.**

Before setting up “PayPal”, it is required that the hotspot owners have a valid PayPal “Business Account”. After opening a PayPal Business Account, the hotspot owners should find the “**Identity Token**” of this PayPal account to continue “PayPal Payment Page Configuration”.

➤ External Payment Gateway / PayPal Payment Page Configuration

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

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

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

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

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

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

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

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

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

Choose Billing Plan for PayPal Payment Page			
Plan	Enable/Disable	Quota	Price
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	1.1 Mbyte(s) of traffic volume quota	20
2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	9 hr(s) 59 min(s) of connection time quota with expiration	57
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

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

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

➤ **Client's Purchasing Record / PayPal Payment Page Remark Content**

Client's Purchasing Record	
Starting Invoice Number	Hotspot 00000000 * <input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

PayPal Payment Page Remark Content
<div> <div>(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,</div> </div>

Client's Purchasing Record:

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

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

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

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

16.3. Payments via SecurePay

Configure Payments via SecurePay; go to: **User >> Authentication >> On-demand Users >> External Payment Gateway >> SecurePay.**

Before setting up “SecurePay”, it is required that the hotspot owners have a valid SecurePay “Merchant Account” from its official website.

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

SecurePay Payment Page Configuration	
Merchant ID	<input type="text"/> *
Merchant Password	<input type="text"/> *
Payment Gateway URL	<input type="text" value="https://www.securepay.com.au/xmlapi/payment"/> *
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <div>Trusted CA Management</div>
Currency	<input type="text" value="AUD (Australian Dollar)"/> *

Service Disclaimer Content	
<div>We may collect and store the following personal information: physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.</div>	

Choose Billing Plan for SecurePay Payment Page			
Plan	Enable/Disable	Quota	Price
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	1.1 Mbyte(s) of traffic volume quota	20
2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	9 hr(s) 59 min(s) of connection time quota with expiration	57
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

SecurePay Payment Page Remark Content	
<div>You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.</div>	

➤ Payment Page Configuration

Merchant ID: The ID that is associated with the Business Account.

Password: This is the key used by Secure Pay to validate all the transactions.

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

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

Pay.

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

➤ **Service Disclaimer Content**

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

➤ **SecurePay Payment Page Billing Configuration**

These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

➤ **SecurePay Payment Page Remark Content**

The message content will be displayed as a special notice to end customers.

16.4. Payments via WorldPay

Configure Payments via WorldPay; go to: **User >> Authentication >> On-demand Users >> External Payment Gateway >> WorldPay.**

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

WorldPay Payment Page Configuration	
Installation ID	<input type="text"/> *
Payment Gateway URL	<input type="text" value="https://select.wp3.rbsworldpay.com/wcc/purchase"/> *
Currency	<input type="text" value="GBP (Pound Sterling)"/> *

Service Disclaimer Content	
<div><div>We may collect and store the following personal information: physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.</div><div><div></div><div></div><div></div></div></div> *	

Choose Billing Plan for WorldPay Payment Page				
Plan	Enable/Disable		Quota	Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

WorldPay Payment Page Remark Content	
<div><div>You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.</div><div><div></div><div></div><div></div></div></div>	

➤ WorldPay Payment Page Configuration

Installation ID: The ID of the associated Merchant Account.

Payment Gateway URL: The default website of posting all transaction data.

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

➤ Service Disclaimer Content

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

➤ WorldPay Payment Page Billing Configuration

These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

➤ WorldPay Payment Page Remark Content

The message content will be displayed as a special notice to end customers.

Before setting up “WorldPay”, it is required that the hotspot owners have a valid WorldPay “Merchant Account” from its official website: RBS WorldPay: Merchant Services & Payment Processing, going to ***rbsworldpay.com >> support center >> account login.***

STEP①. Log in to the Merchant Interface.











- Login url: www.rbsworldpay.com/support/index.php?page=login&c=WW
- Select Business Gateway - Formerly WorldPay
- Click [Merchant Interface](#)
- Username: user2009
- Password: user2009

STEP②. Select Installations from the left hand navigation

STEP③. Choose an installation and select the Integration Setup button for the specific environment.

- Installation ID: 239xxx



223643 (Select Junior - 01server)		
232449 (Select Junior - Raja Dasgupta)		
237397 (Select Junior)		
237398 (Select Junior - Ivis Group)		
212370 (Select Junior - SAI GLOBAL)		
213296 (Select Junior)		
214432 (Select Junior)		
215568 (Select Junior - Stof)		
215910 (Select Junior)		
219440 (Select Junior - Unearthed)		
239341 (Select Junior - futurepay)		
239805 (Select Junior - Neton)		
239 — (Select Junior - System)		
210071 (Select Junior - KNOG)		
210158 (Select Junior - Chris)		
222948 (Select Junior - innopacific)		

STEP④. Check the Enable Payment Response checkbox.

STEP⑤. Enter the Payment Response URL.

- URL : <wpdisplay item=MC_callback>

STEP⑥. Check the Enable the Shopper Response.

RBS WorldPay - Installation Administration

Installations

Profile

Financial Status

Command Batch

Risk Management

User Management

User Profile

Dispute Management

Reports

Data current up to: 12/Oct/02:14:00
Merchant: MERCHANT18TAH1

Switch to Production

Copyright © RBS plc 2009

To other actions

Installation ID: 239TEST

Administration Code: TEST

Company Name: TEST
www.invest.com

Environment

Description: System

Customer description (for payment pages)

Integration type: Select Junior(60)

Use 3D Secure Authentication? true

Use MasterCard SPA? true

Store-builder used: Default

store-builder: if other - please specify

Payment Response URL: <wpdisplay item=MC_callback>

Payment Response enabled? ☒

Enable Recurring Payment Response ☐

Enable the Shopper Response ☒

Suspension of Payment Response ☐

Payment Response failure count: 0

Payment Response failure email address

Attach HTTP(s) Payment Message to the failure email? ☒

Enable whitelisting? ☒

Merchant receipt email address (if set, overrides value at Merchant Code level)

Info servlet password: Confirm: Use default

Payment Response password: Confirm: Use default

MVS secret for transactions: Confirm: Use

STEP⑦. Select the Save Changes button

STEP⑧. Input Installation ID and Payment Gateway URL in gateway UI.

- Installation ID: 2009test
- URL : <https://select.wp3.rbsworldpay.com/wcc/purchase>

External Payment Gateway

☐ Authorize.Net ☐ PayPal ☐ SecurePay ☒ WorldPay ☐ Disable

WorldPay Payment Page Configuration

Installation ID: 239--- *

Payment Gateway URL: <https://select.wp3.rbsworldpay.com/wcc/purchase> *

Currency: GBP (Pound Sterling) *

Note: The WAN IP of gateway must be real IP.

17. Additional Applications

17.1. Upload / Download Local Users Accounts

Configure Upload / Download Local Users Accounts; go to: **User >> Authentication >> Option >>Local >> Local User List.**

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

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

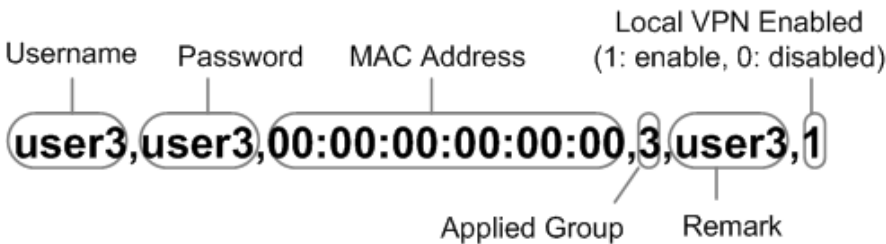
Upload User from File

File Name

Browse...

Upload

When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, and then, try again.



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

Download User to File					
Username	Password	MAC Address	Applied Group		
			Local VPN Enabled		
			Remark		
			1		
test	1234		None		

17.2. Backup / Restore and Upload New On-demand Users Accounts

Configure Backup / Restore On-demand Users Accounts; go to: **Users >> Authentication >> On-demand User >> On-demand Account List.**

- **Backup Current Accounts:** Use this function to create a .txt file with all current user account information and then save it on disk.
- **Restore Accounts:** After the current user accounts have backup, you can restore all these accounts to another system. Click **Restore Accounts** to enter the **Restore On-demand User Account** interface. Click the **Browse** button to select the text file for restore the user accounts, and then click **Submit** to complete the restore process.

On-demand Account List							
Username	Password	Remaining Quota	Status	Group	Reference	External ID	Delete All
8y86	em5nc2n2	1 day(s) 1 hr(s) 1 min(s)	Expired	Group 24			Delete

17.3. Account Roaming Out

Configure Notification; go to: **Users >> Authentication >> Local >> Configure.**

In sometime, WHG Controller's built in Local database can act as a RADIUS server for Roaming Out from other system. The Local User database will act as the RADIUS user database.

- **Account Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled; the link of this function will be available to define the authorized device with IP address, Subnet Mask, and Secret Key.

Local User Database Settings	
Local User List	
Account Roaming Out	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client Device Settings	

802.1X Auth Setting	
Default Auth Server	<input type="text" value="Disable"/> (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings					
No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	192.168.1.7	255.255.255.255 (/32)	
2	802.1X	192.168.1.8	255.255.255.255 (/32)	string1
3	DM & CoA		255.255.255.255 (/32)		

Click the hyperlink **Roaming Out & 802.1x Client Device Settings** to enter the **Roaming Out & 802.1x Client Device Settings** interface. Choose **Roaming Out** and key in the Roaming Out client's IP address and network mask and then click **Apply** to complete the settings.

In the other system, such as another WHG Controller, setup it's RADIUS server to this WHG Controller with same postfix, then the local user in this WHG Controller can login success from another WHG Controller by RADIUS authentication.

17.4. Seamless Cross Gateway Roaming

Configure Notification; go to: **Network >> Client Mobility >> Cross Gateway Roaming.**

Client Mobility	
IP PNP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Cross Gateway Roaming	<input type="button" value="Configure"/>

WHG Controllers supports seamless inter-Controller roaming with up to 15 other Controllers in a star like topology. The Master Node means that this Controller will be at the center of the roaming cluster, and its users can roam with all the Slave nodes.

The Slave Node are Controllers that are connected to the Master node (Master AP), their users can only roam with the Master node.

Cross Gateway Roaming	
Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Master Node <input type="radio"/> Slave Node
Status	<input type="button" value="Node List"/>

Master Node

Master node can roam with many slave nodes. Contains 15 entries where network administrator can specify the slave nodes that will perform roaming with this master node. Fill in the IP address and common secret key. Check the “Active” check box and apply to enable roaming tunnel between the master node and slave node.

Cross Gateway Roaming	
Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Master Node <input type="radio"/> Slave Node
Status	<input type="button" value="Node List"/>

Slave Nodes Setting				
No.	Active	Remote IP Address*	Secret Key*	Remark
1	<input checked="" type="checkbox"/>	<input type="text" value="10.0.5.143"/>	<input type="text" value="123123"/>	<input type="text" value="additional info"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Slave Node

Slave node can only roam with the master node. Fill in master node's IP address and common shared secret to establish roaming tunnel between the master node and slave node.

Cross Gateway Roaming	
Mode	<input type="radio"/> Disable <input type="radio"/> Master Node <input checked="" type="radio"/> Slave Node
Status	<button>Node List</button>

Master Node Setting	
Remote IP Address	<input type="text" value="10.7.21.233"/> *
Secret Key	<input type="text" value="123123"/> *
Remark	<input type="text"/>

Appendix A. Certificate Settings for IE6 and IE7

▪ Certificate setting for the company with Certificate Authority

➤ Background information

Any website or high-value Web Applications will require a client to access their websites via Secure Sockets Layer (SSL). The browser will automatically ask for a public SSL certificate from the website and check if it is valid. The public SSL Certificate consists of the public key and identity information which can be signed by any established certificate authority (e.g. VeriSign). The certificate authority guarantees that the public key belongs to the named entity. Usually, website's security certificate may encounter problem only if the security certificate presented to the browser has not been signed by any certificate authority which can be trusted.

As long as the SSL function is enabled in the WHG CONTROLLER, there must be a public SSL certificate signed by an established certificate authority. To avoid the error message in the browser, a company should have its own Certificate Authority (CA). The IT department must therefore install the SSL certificate for each normal user when deploying the WHG CONTROLLER.

➤ Secure Certificate setting for both IE6 and IE7

For the company with its own Certificate Authority (CA), the certificate of the company should be trusted by all his employees' computers, and the certificate should be delivered through a trusted media. For example, the MIS staff should install the CA certificate in each computer. The company CA will issue a certificate for the WHG CONTROLLER and export it to the WHG CONTROLLER.

Note: *If the WHG CONTROLLER is installed in a company, the administrator can create a certificate using software instead of purchasing a public trusted certificate.*

▪ Certificate setting for the company without Certificate Authority

For a company that does not have its own Certificate Authority (CA), the administrators should first apply for a trusted certificate, or create one by using certificate software. Second, the administrators should use some

trusted media to install this certificate (as trusted CA) in each employee's computer, and in the meantime export this certificate to the WHG CONTROLLER.

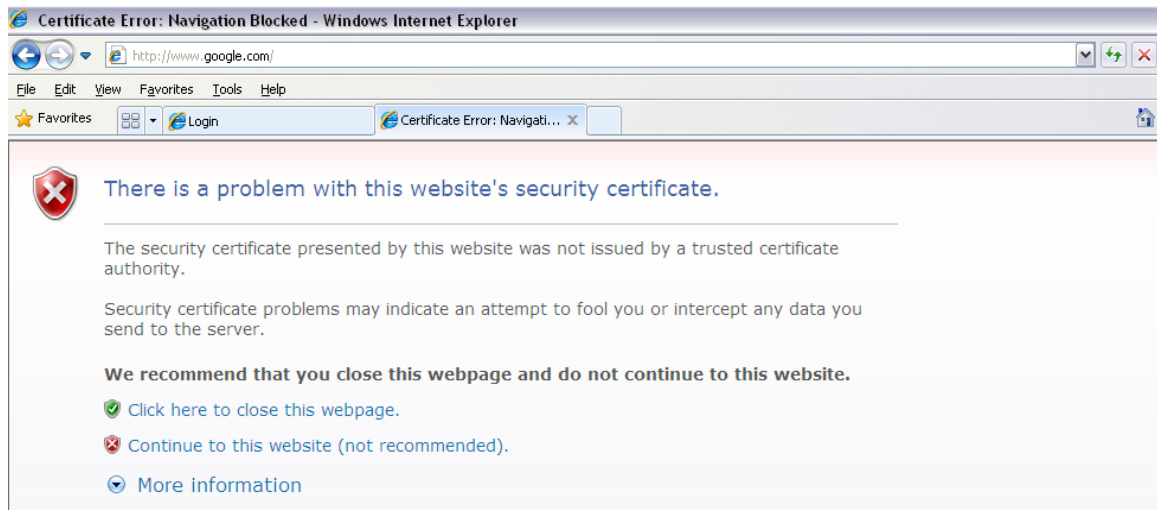
In some circumstance, the company without Certificate Authority may follow the steps stated below to avoid error message. When in the LAN environment of the office instead of a wireless environment, administrators may already have recognized certificates in the system which the CA must be verified as secured.

■ Certificate setting for Internet Explorer 7

For IE7, regarding certificate issues caused by certificate publisher not being trusted by IE7, the following steps may be taken to provide a workaround or to bypass the issue.

- (1) Open the IE7 browser, and you will be redirected to the default login page. If the certificate is not trusted, the following page will appear.

Click **“Continue to this website”**.

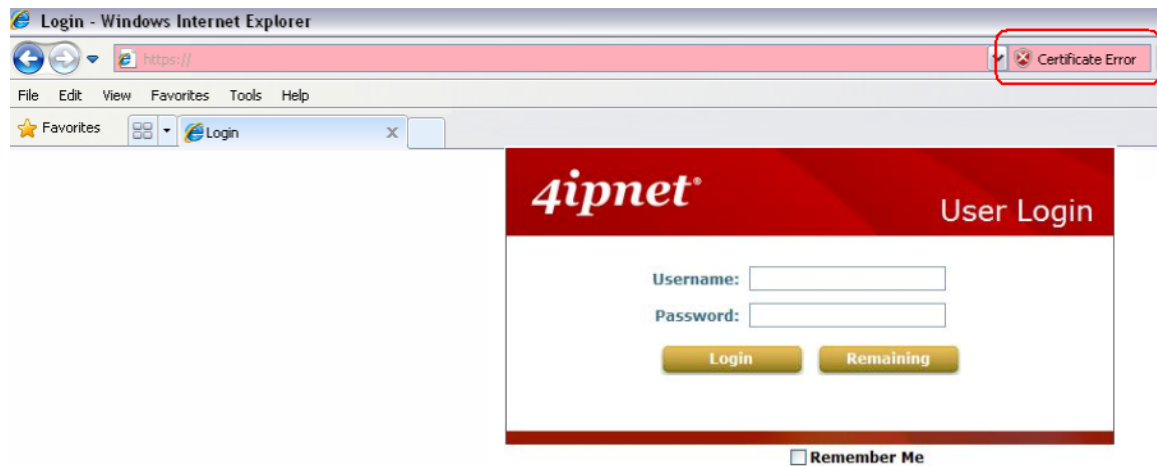


- (2) The default User Login Page will appear and the users can then login normally.

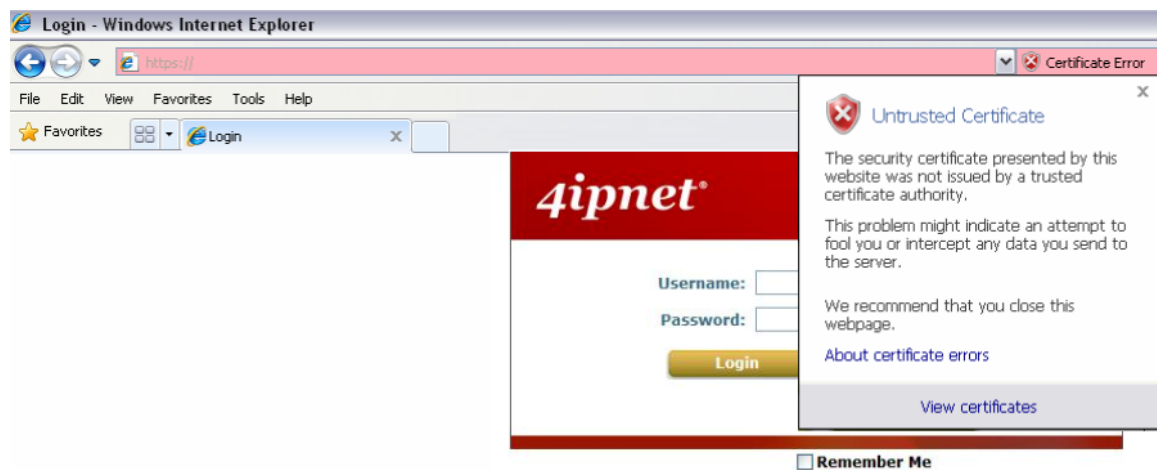


For installing a trusted certificate to solve the IE7 certificate issue, please follow the instructions stated below.

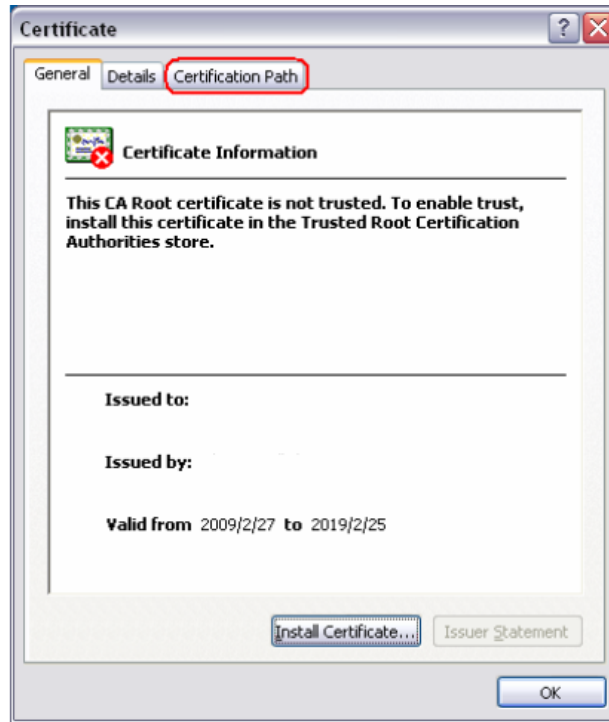
- (1) When the User Login page appears, click **“Certificate Error”** at the top.



- (2) Click **“View Certificate”**.



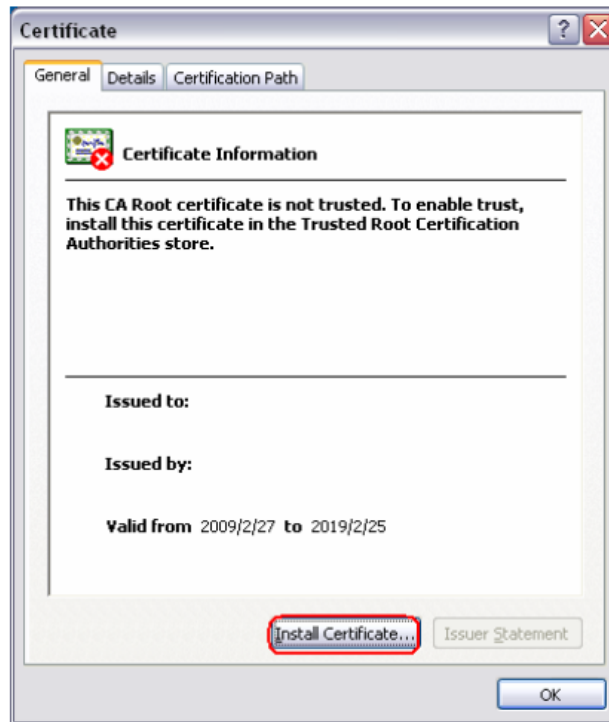
- (3) Click **“Certification path”**.



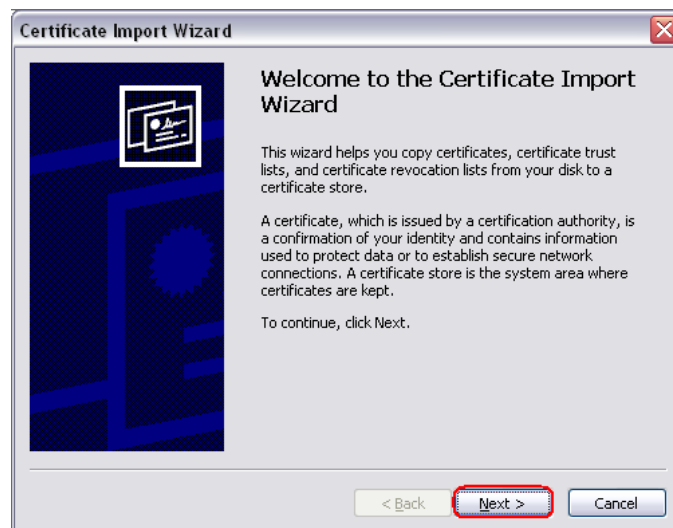
(4) Select root certification, and then click **“View Certificate”**.



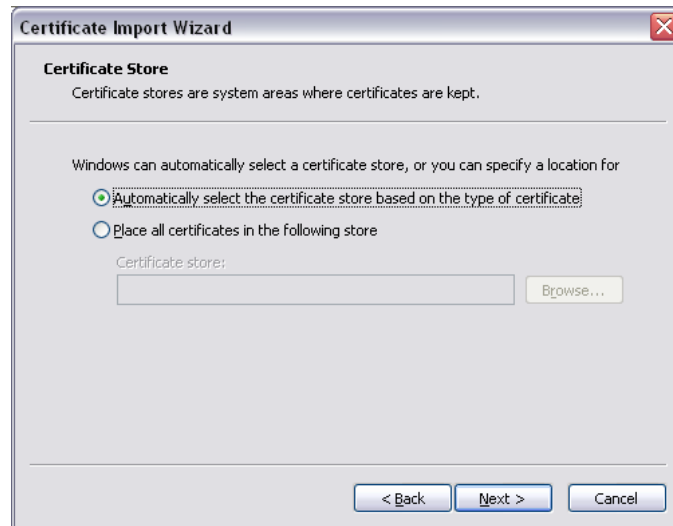
(5) Click **“Install Certificate”**.



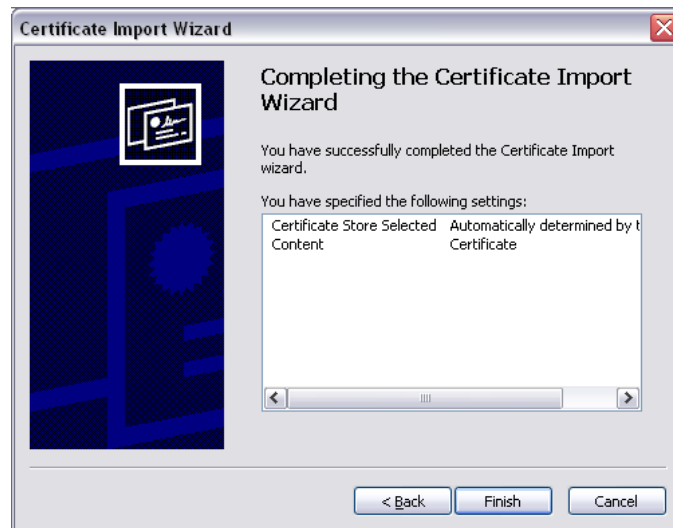
(6) Click ***“Next”***.



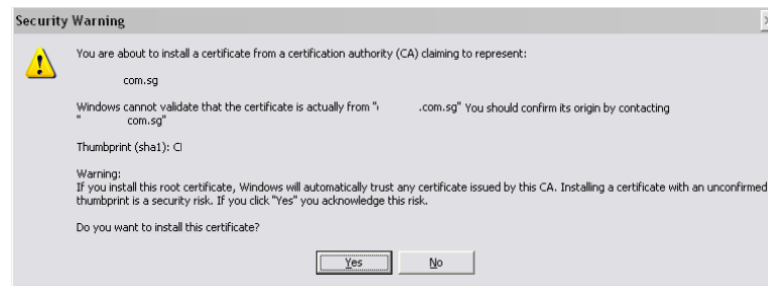
(7) Select ***“Automatically select the certificate store based on the type of certificate”***, and then click ***“Next”***.



(8) Click ***Finish***.



(9) Click **“Yes”**.



(10) Click **“OK”**.



(11) Launch a new IE7 browser. The certificate is now trusted via IE7 according to the key symbol shown at top next to the address field.



■ Certificate setting for Internet Explorer 6

For issues relating to IE6 certificate error, the following information provides the step to take when the certificate publisher is not trusted by IE6.

- (1) Open an IE6 browser, the Security Alert message will be appeared if the certificate is not trusted. Click **“Yes”** to proceed.



- (2) The User Login Page will appear.



- (3) The user can now login normally.

Appendix B. Network Configuration on PC & User Login

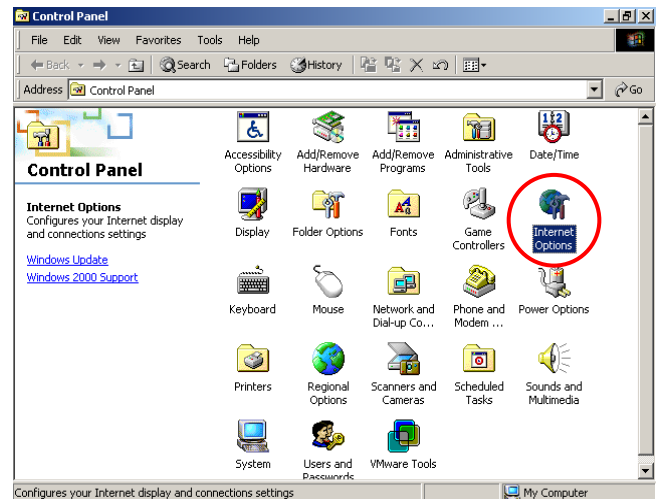
■ Network Configuration on PC

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

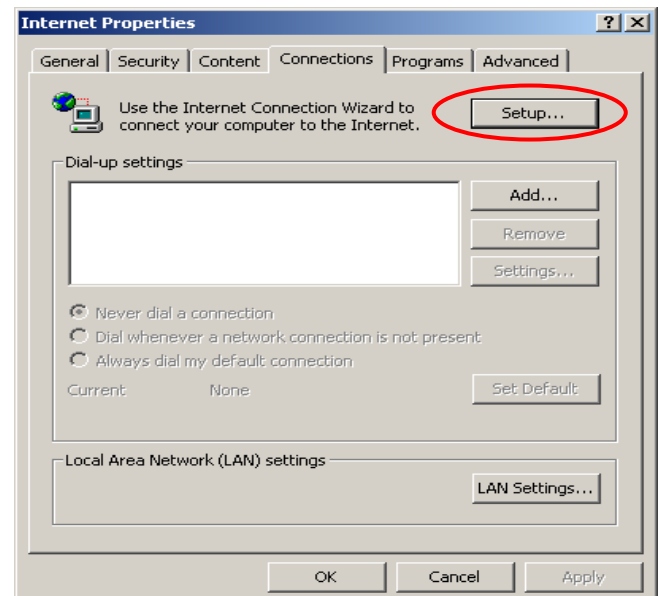
- **Internet Connection Setup**

- **Windows 9x/2000**

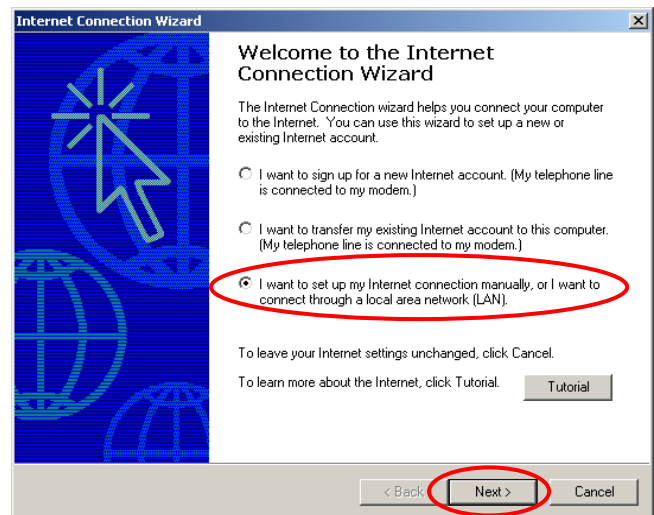
- 1) Choose **Start >> Control Panel >> Internet Options**.



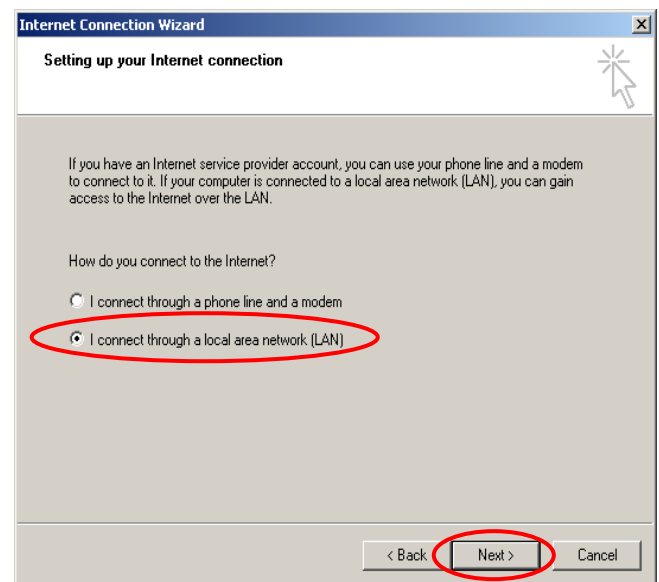
- 2) Choose the **Connections** tab, and then click **Setup**.



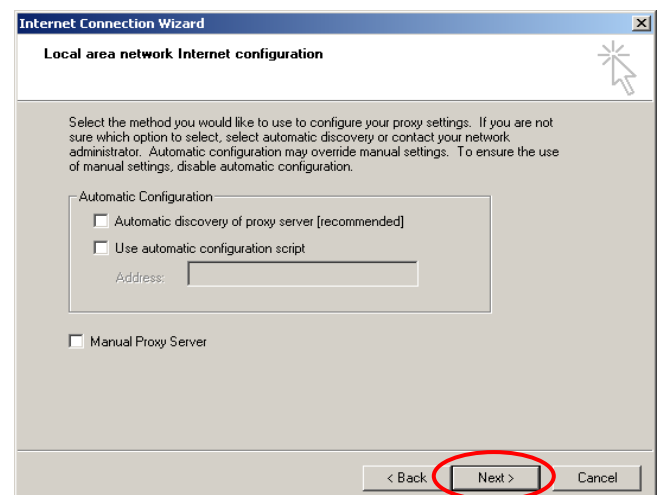
- 3) Choose “I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)”, and then click **Next**.



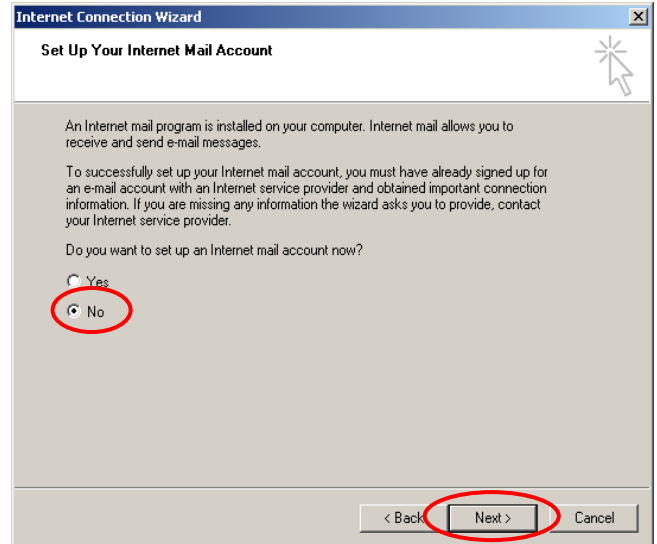
- 4) Choose “I connect through a local area network (LAN)” and then click **Next**.



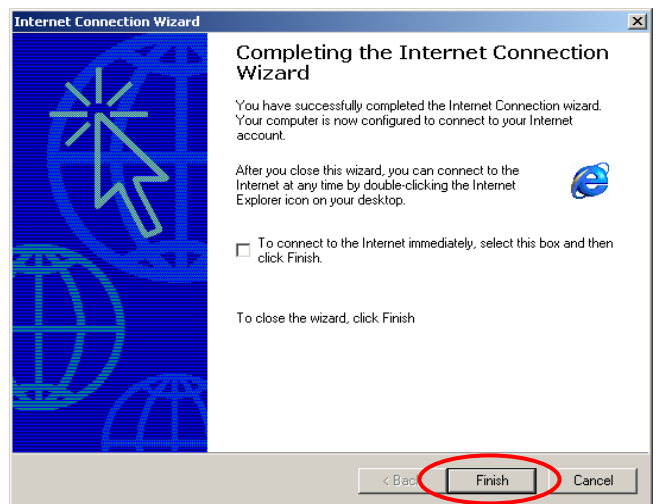
- 5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click **Next**.



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

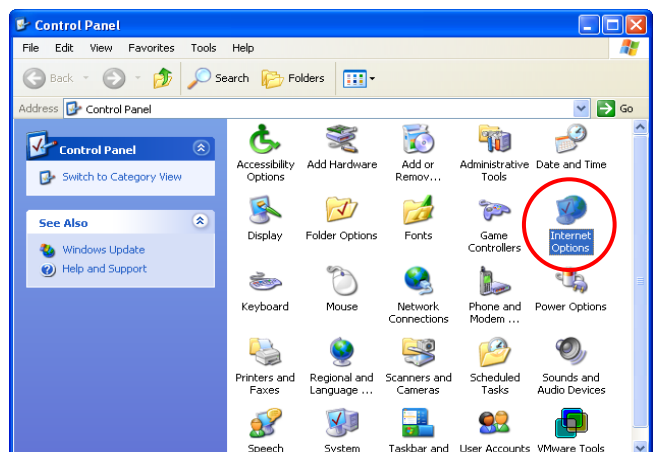


- 7) Finally, click **Finish** to exit the **Internet Connection Wizard**. Now, the set up is completed.

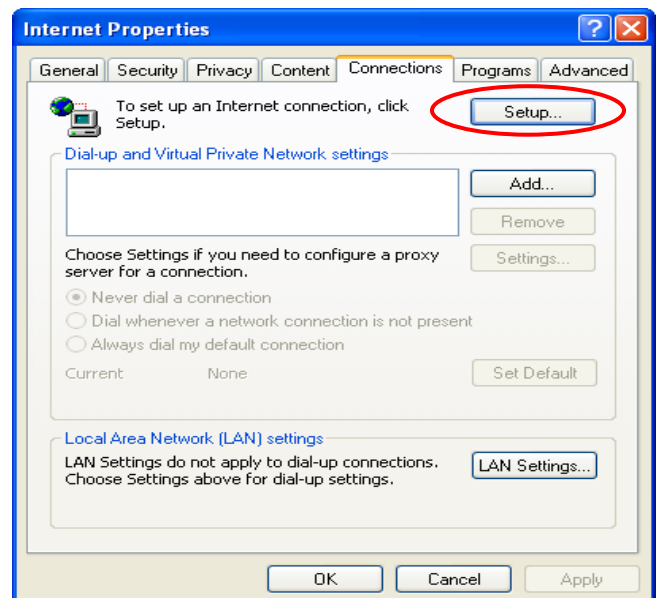


■ Windows XP

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



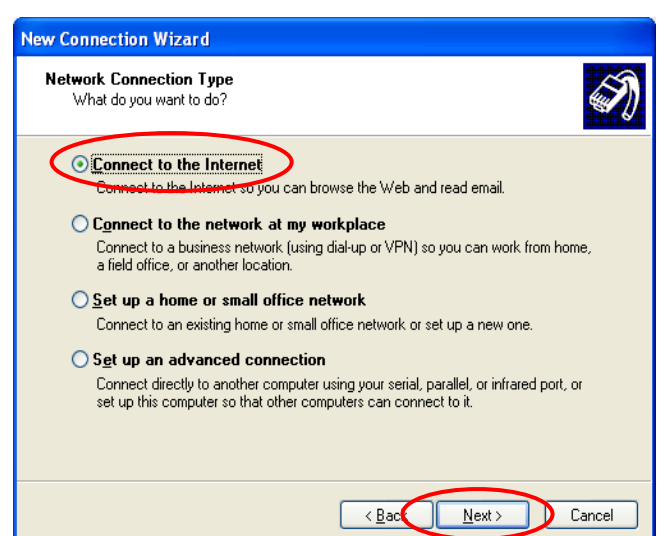
- 2) Choose the **Connections** tab, and then click **Setup**.



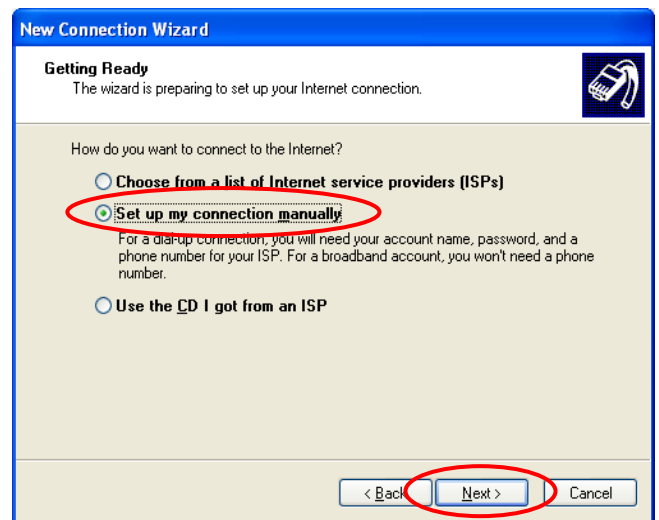
- 3) When the **Welcome to the New Connection Wizard** window appears, click **Next**.



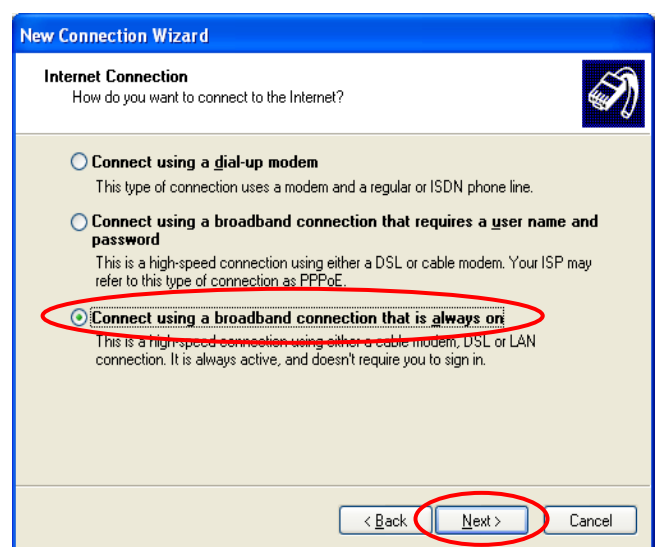
- 4) Choose **“Connect to the Internet”** and then click **Next**.



- 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.



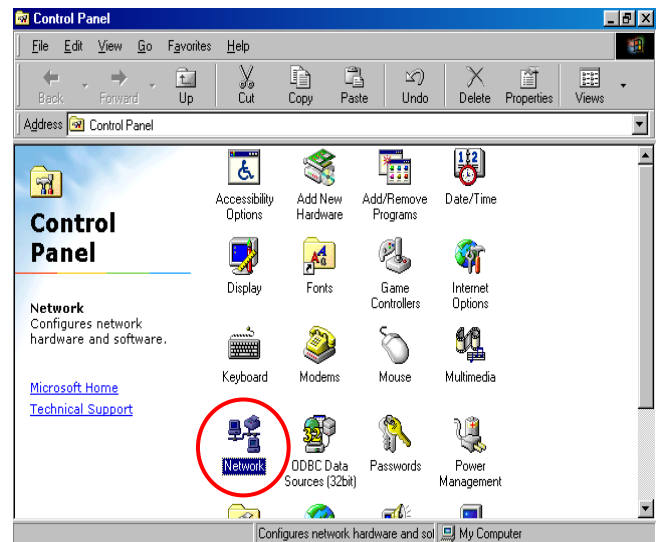
- **TCP/IP Network Setup**

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, WHG CONTROLLER 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**”.

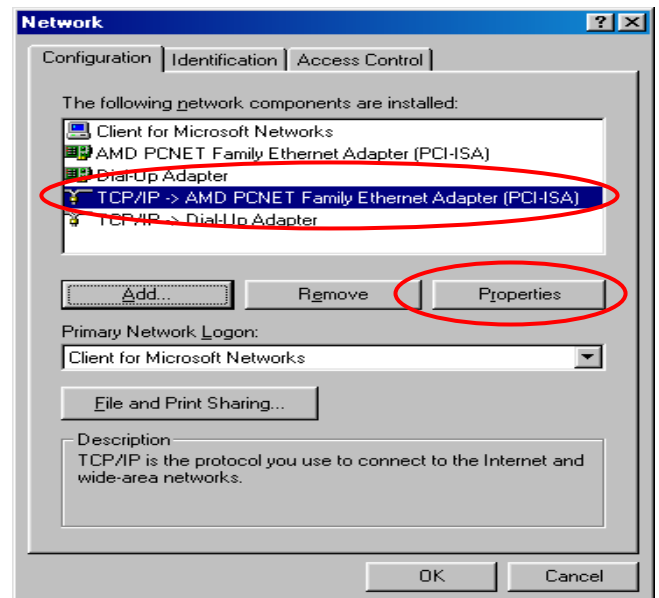
If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

- **Check the TCP/IP Setup of Window 9x/ME**

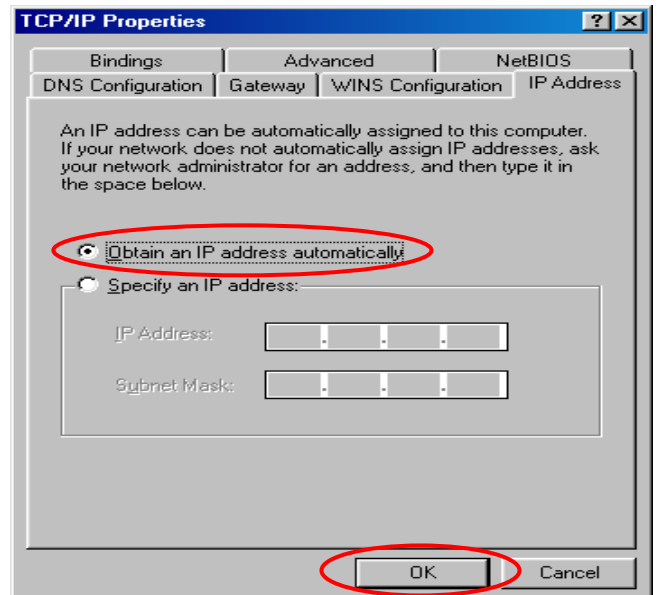
- 1) Choose **Start >> Control Panel >> Network**.



- 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 WHG CONTROLLER.

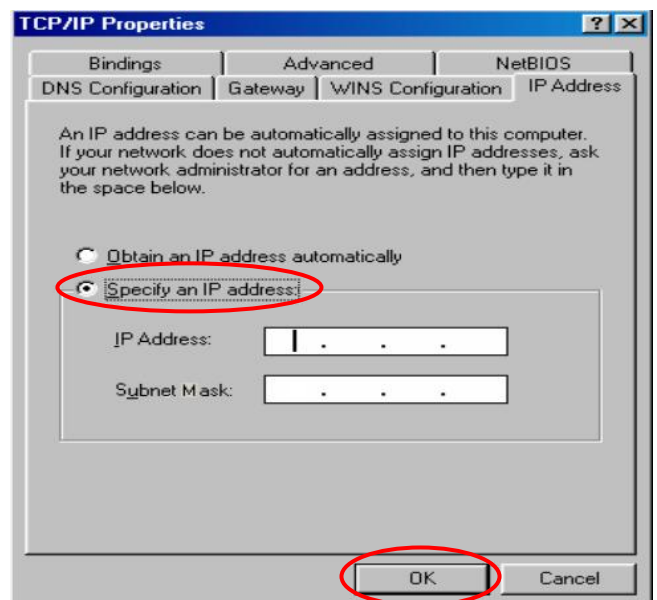


- 4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG CONTROLLER.

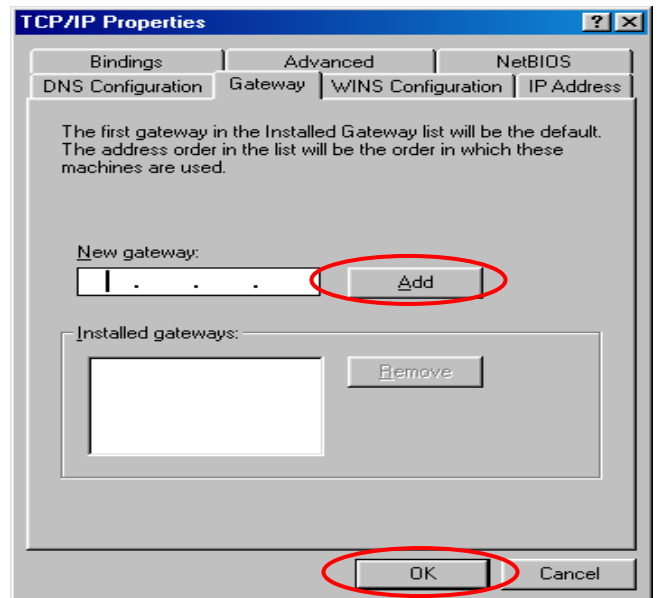


If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

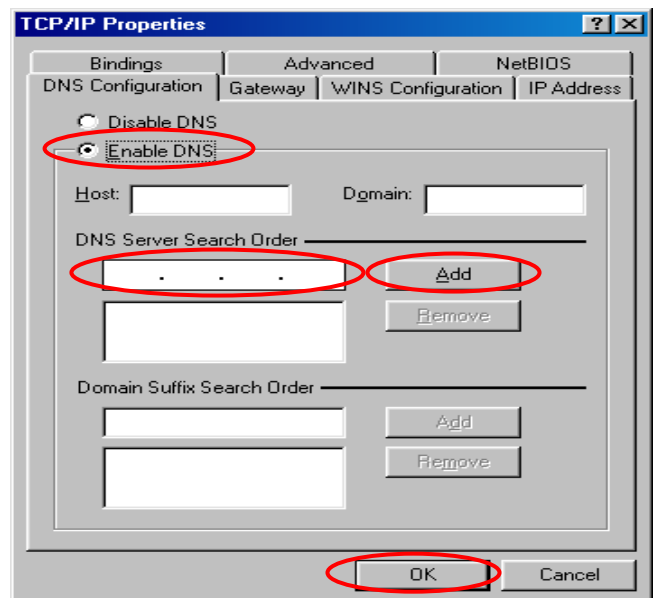
- 4.1) Click on the **IP Address** tab and choose “**Specify an IP address**”. Enter the *IP Address*, *Subnet Mask* and then click **OK**.



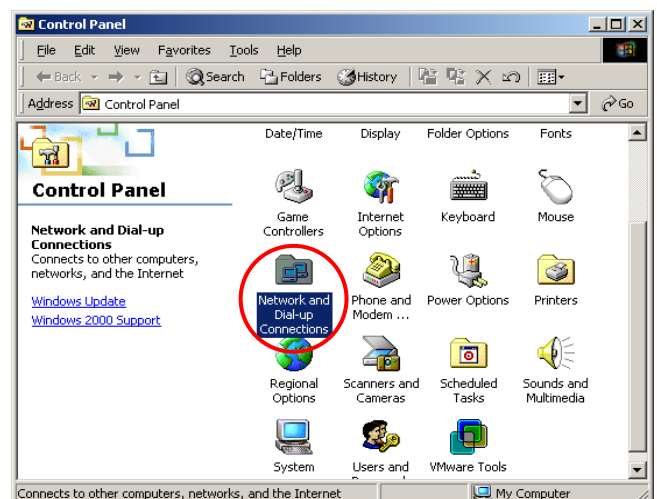
- 4.2) Click on the **Gateway** tab. Enter the gateway address of WHG CONTROLLER in the “**New gateway**” field and click **Add**. Then, click **OK**.



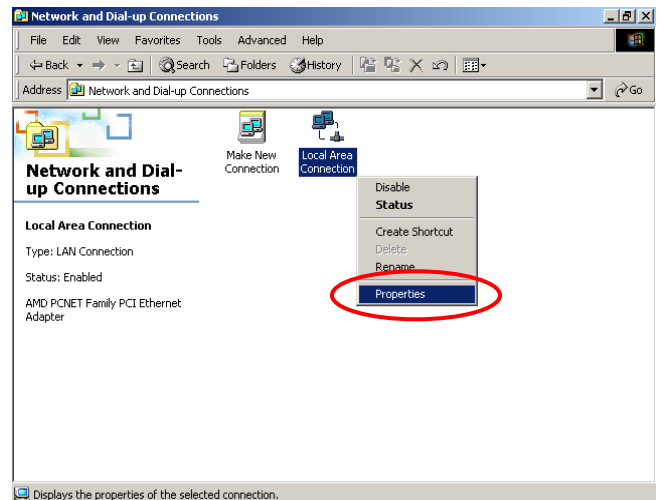
- 4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select “**Enable DNS**” and enter *DNS Server address*. Click **Add**, and then click **OK** to complete the configuration.



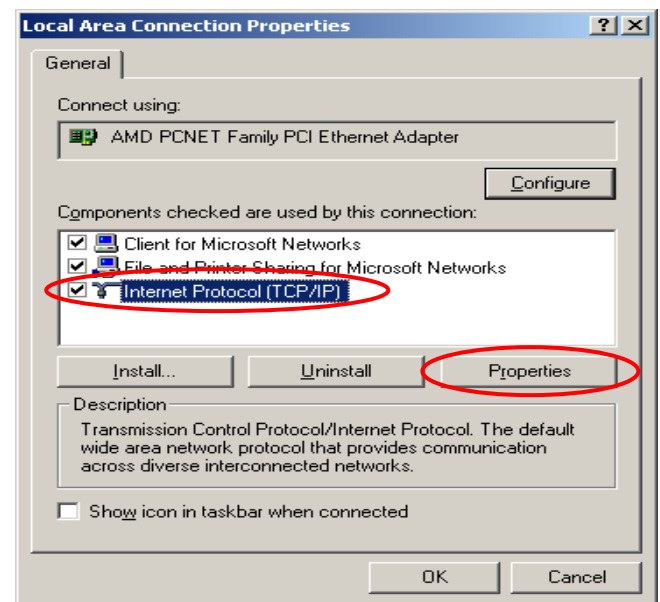
- **Check the TCP/IP Setup of Window 2000**
 - 1) Select **Start >> Control Panel >> Network and Dial-up Connections**.



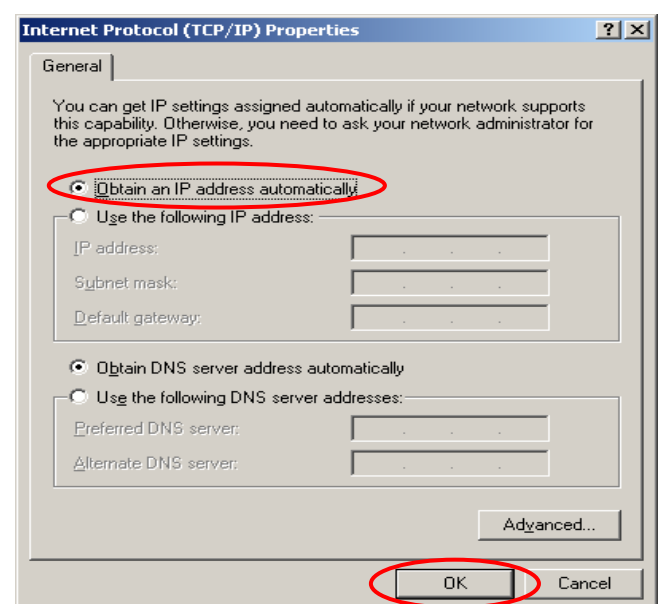
- 2) Right click on the **Local Area Connection** icon and select **“Properties”**.



- 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 WHG CONTROLLER.

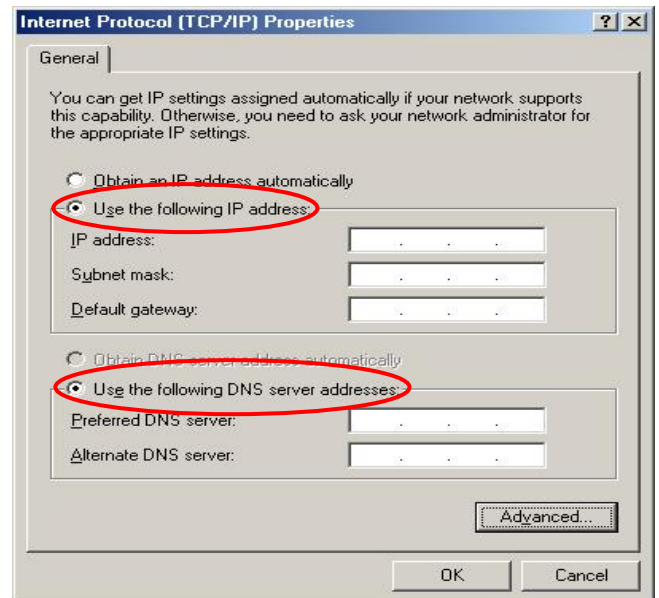


- 5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG CONTROLLER.

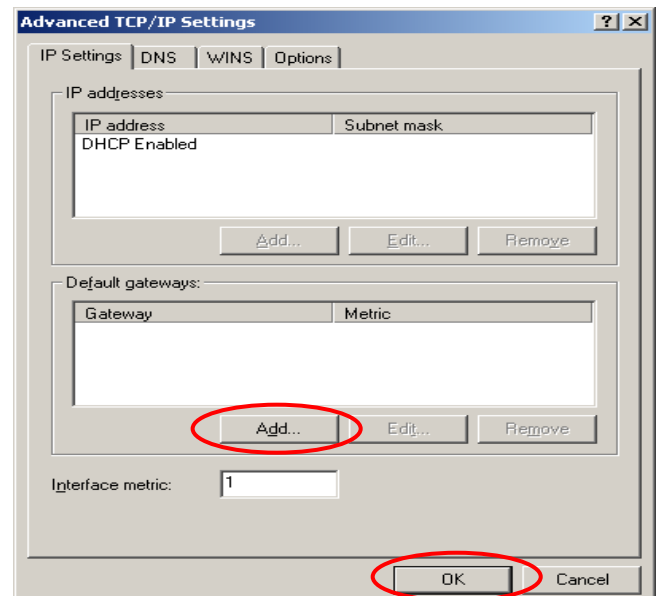


If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

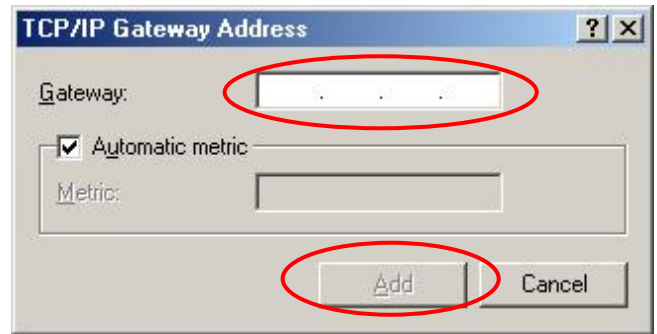
- 5.1) Choose “**Use the following IP address**” and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select “**Using the following DNS server addresses**” and enter the *DNS Server address*. Then, click **OK**.
- 5.2) Click **Advanced** to enter the **Advanced TCP/IP Settings**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

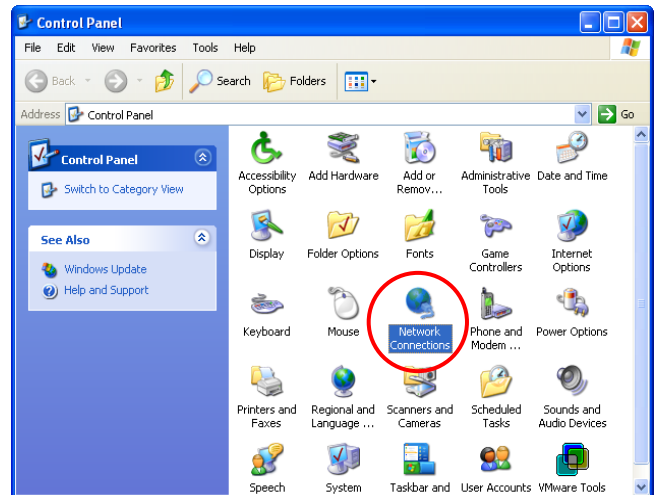


- 5.4) Enter the gateway address of WHG CONTROLLER in the “**Gateway**” field, and then click **Add**. After back to the **IP Settings** tab, click **OK** to complete the configuration.

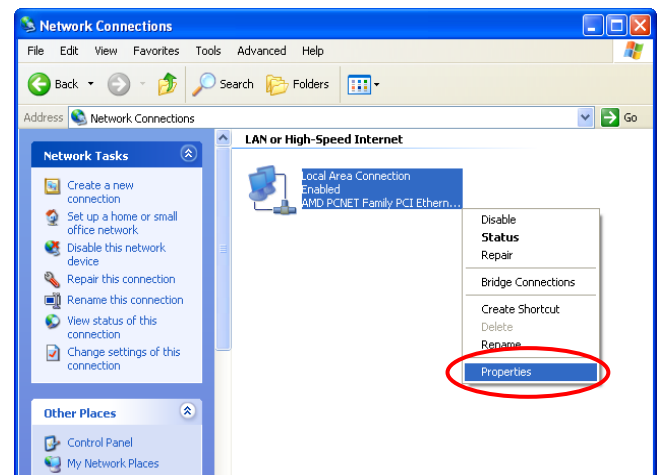


▪ **Check the TCP/IP Setup of Window XP**

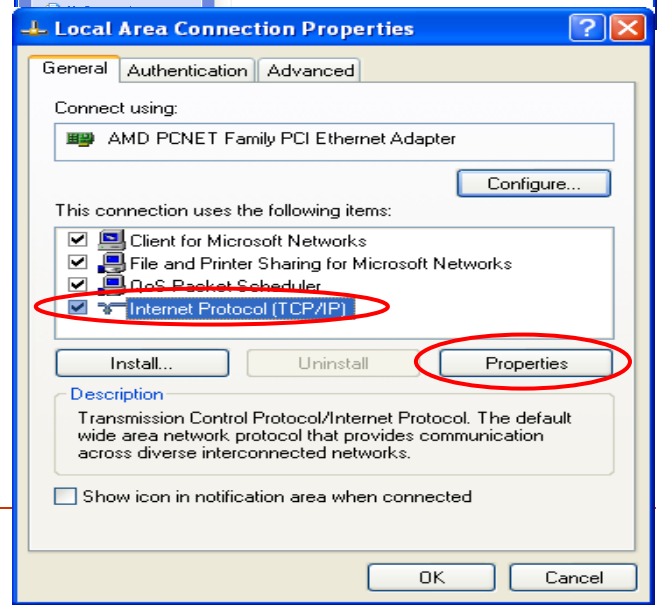
- 1) Select **Start >> Control Panel >> Network Connection**.



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

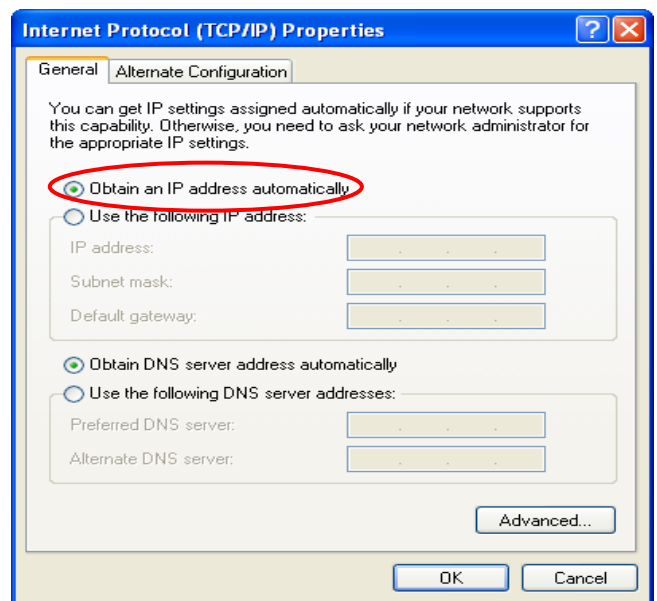


- 3) Click on the **General** tab and choose “**Internet Protocol (TCP/IP)**”, and then click **Properties**.



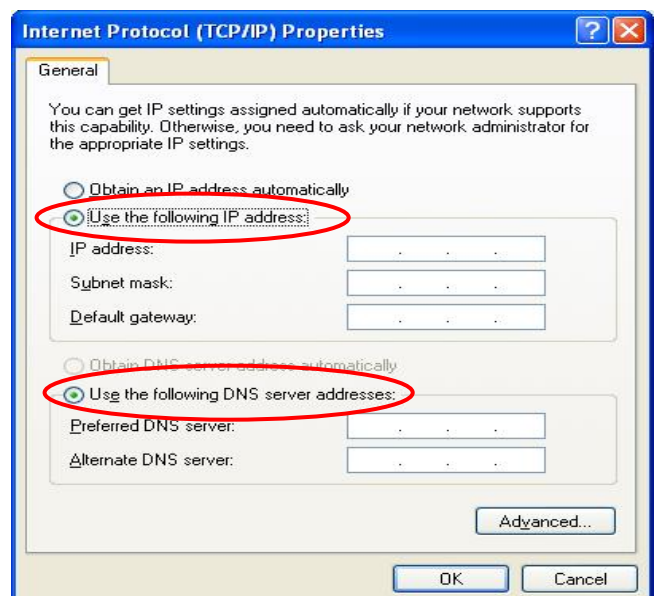
Now, you can choose to use DHCP or a specific IP address.

- 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 WHG CONTROLLER.
- 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 WHG CONTROLLER.

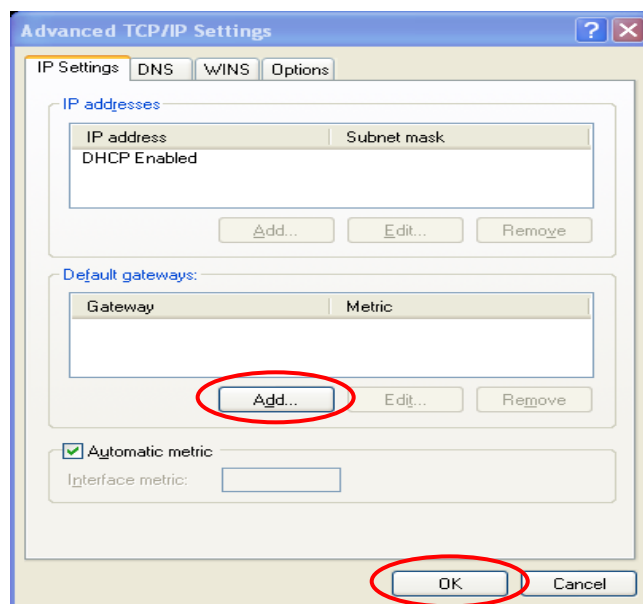


If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

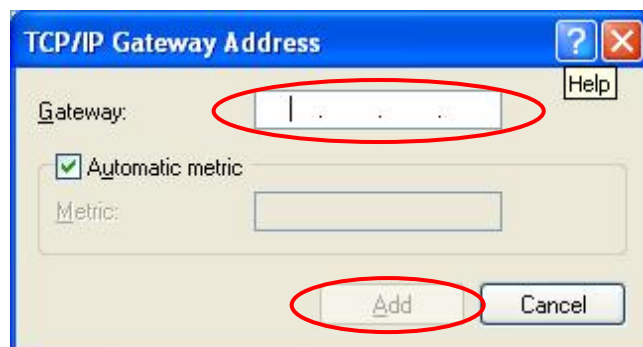
- 5.1) Choose **“Use the following IP address”** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **“Using the following DNS server addresses”** and enter the *DNS Server address*. Then, click **OK**.
- 5.2) Click **Advanced** to enter the **Advanced TCP/IP Settings** 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 WHG CONTROLLER in the “**Gateway**” field, and then click **Add**. After back to the **IP Settings** tab, click **OK** to finish the configuration.



Appendix C. Policy Priority

■ Global Policy, Service Zone Policy, Authentication Policy and User Policy

WHG Controller supports multiple Policies, including one **Global Policy** and multiple individual **Policy** which can be assigned and bound to **Group**. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone. On the other hand, **Service Zone** also has a **Default Policy**. For some authentication, such as Local, RADIUS and LDP, user can assign to different Group individually. The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. So one user may be applied different policy at the same time. Which policy is actually applied to this user?

The Policy Priority must be:

User Policy >> Authentication Policy >> Service Zone Policy >> Global Policy

Now, let us discuss different user policy type:

- For Local, RADIUS and LDAP, if these users are assigned to different Group individually, these users can be assigned to their Group. For example, a Local user, user01, is assigned to Group1 and the Local Authentication is assigned to Group2. If Group1 in Service Zone1 can be applied Policy1. Then user01 login to Service Zone1 will get Policy1. This is a common case for users that can assign Group individually.
- For Local, RADIUS and LDAP, if these users do not assigned any Group individually, so they are same as other authentication server users that they can not assign to Group individually. For example, a POP3 user, pop01, the POP3 Authentication is assigned to Group1. If Group1 in Service Zone1 can be applied Policy1. Then pop01 login to Service Zone1 will get Policy1. This is another common case for users that can assign Group by authentication server.
- If Authentication server also do not assign to a Group, then the user will applied the Service Zone Default Policy. For example, a Local user, user01, is assigned to Group *None* and the Local Authentication is also assigned to Group *None*. If the Default Policy of Service Zone1 is applied Policy1. Then user01 login to Service Zone1 will get Policy1.
- If the Default Service Zone Policy is *None*. Authentication server does not assign to a Group and user Group is *None* too. For example, a Local user, user01, is assigned to Group *None* and the Local Authentication is also assigned to Group *None*. If the Default Policy of Service Zone1 is *None*. Then user01 login to Service Zone1 will apply the Global Policy.

So, the Global Policy has the lowest policy priority; on the other hand, the User Policy will be the highest one.

Appendix D. RADIUS Accounting

This section is trying to organize the basic configuration with RADIUS server to work with VSA. The aim is trying to control the maximum usage (upload; download or upload + download traffic) of clients in each session.

This **VSA** will send from RADIUS server to gateway along with an **Access-Accept** packet. In other words, when the external RADIUS server accepts the request, it will not only reply with an **Access-Accept** and it will also carry a maximum value in bytes that each user is allowed to transfer. This value may be the maximum upload traffic; download traffic or the summation of each user's download plus upload traffic in bytes. Gateway will check this value every minute, if the user is reached this value, gateway will stop the session of this user and send a "Stop" to RADIUS server.

1. Description

This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. It MUST not affect the operation of the RADIUS protocol.

The standard **Attribute Type** of VSA is "26". Also we need to know the "**Vendor ID**", in this example; the **Vendor ID** of LevelOne is "31932". There must have other attribute to define the amount of traffic with "**Attribute Number**" and "**Attribute Value**":

Attribute Name	Attribute Number	Attribute Value
LevelOne-Byte-Amount	10	To be defined by administrator for different user group
LevelOne-MaxByteIn	11	To be defined by administrator for different user group
LevelOne-MaxByteOut	12	To be defined by administrator for different user group
LevelOne-Byte-Amount-4GB	20	To be defined by administrator for different user group
LevelOne-MaxByteIn-4GB	21	To be defined by administrator for different user group
LevelOne-MaxByteOut-4GB	22	To be defined by administrator for different user group

If the amount of traffic is larger than 4 GB, then the attribute of "XXXX-4GB" is for the carry. For example, if the amount is 5 GB, you must set "LevelOne-Byte-Amount = 1048576" and "LevelOne-Byte-Amount-4GB = 1".

On the other hand, if administrator fills in all attributes, it means that if any condition is reached, the user will be kicked out from system. For example, if administrator set "LevelOne-Byte-Amount = 1048576"; "LevelOne-MaxByteIn = 1048576" and "LevelOne-MaxByteOut = 1048576". It means that whatever the downlink or uplink or total traffic exceeded the limit, the user will be kicked out from system.

2. VSA configuration in RADIUS server (IAS Server)

This section will guide you through a VSA configuration in your external RADIUS server. Before getting start, please access your external RADIUS server's desktop directly or remotely from other PC.

Step 1

Assume there are already have **users** in RADIUS Server

Assume there are already have **Groups** and assigned **users** to belong these **Groups** in RADIUS Server

Assume there are already have **Policies** and assigned **Groups** to belong these **Policies** in RADIUS Server

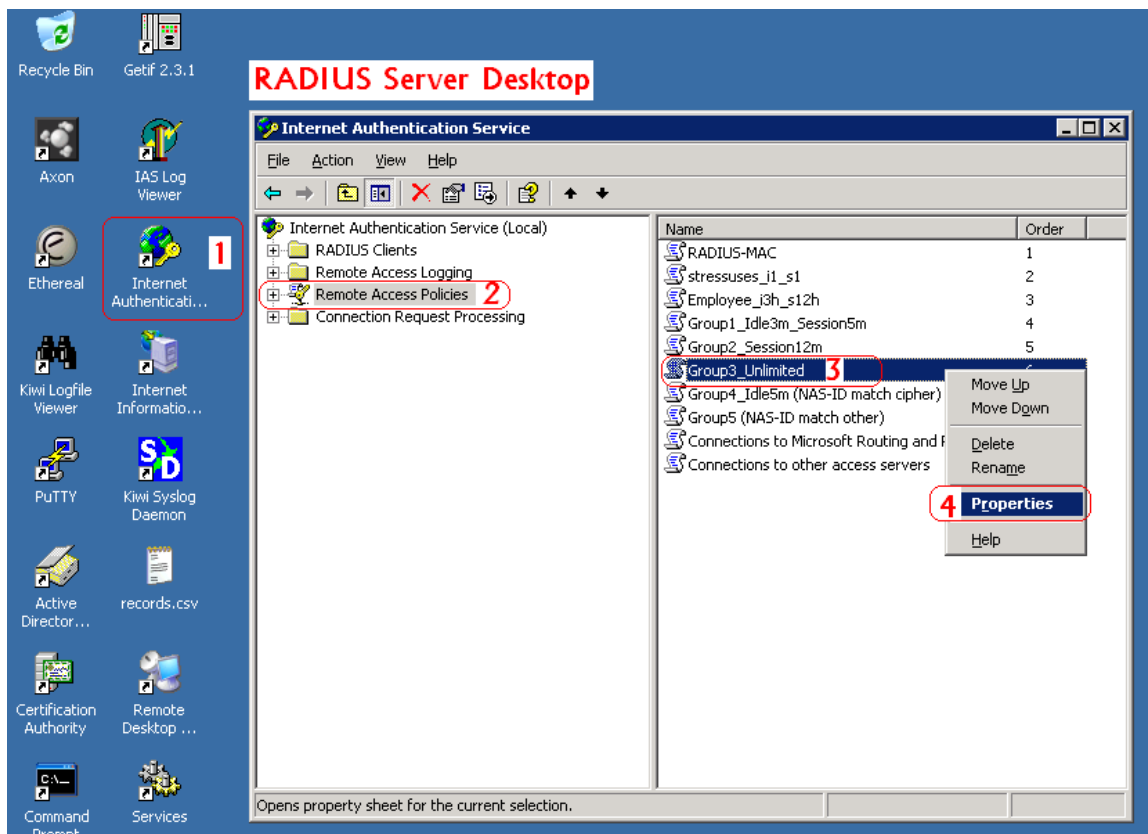
Step 2

Run "Internet Authentication Service"

Open "Remote Access Policies"

Select a **Policy**

Right click and scroll down to its properties page



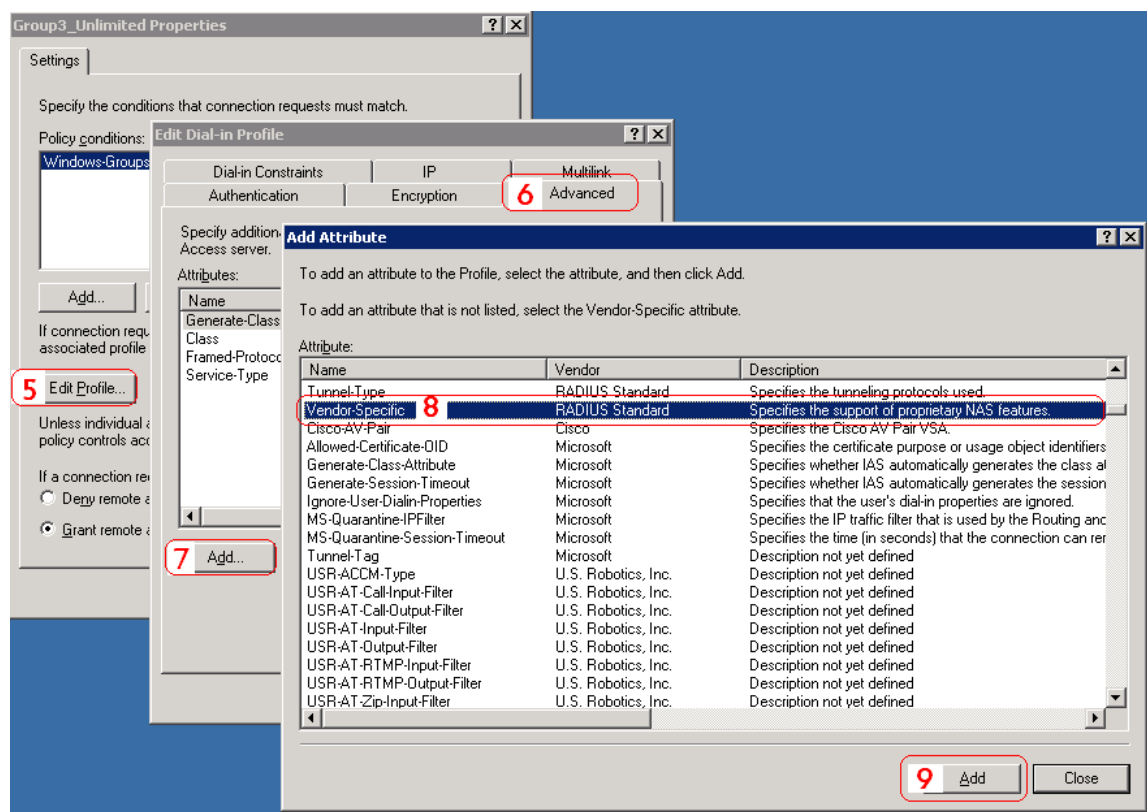
Step 3

Edit Profile

Select the **Advanced** Tag

Add a new attribute

Add a new **Vendor-specific** attribute



Step 4

Add a new attribute under **Vendor-specific**

Set "Vendor Code = 31932"

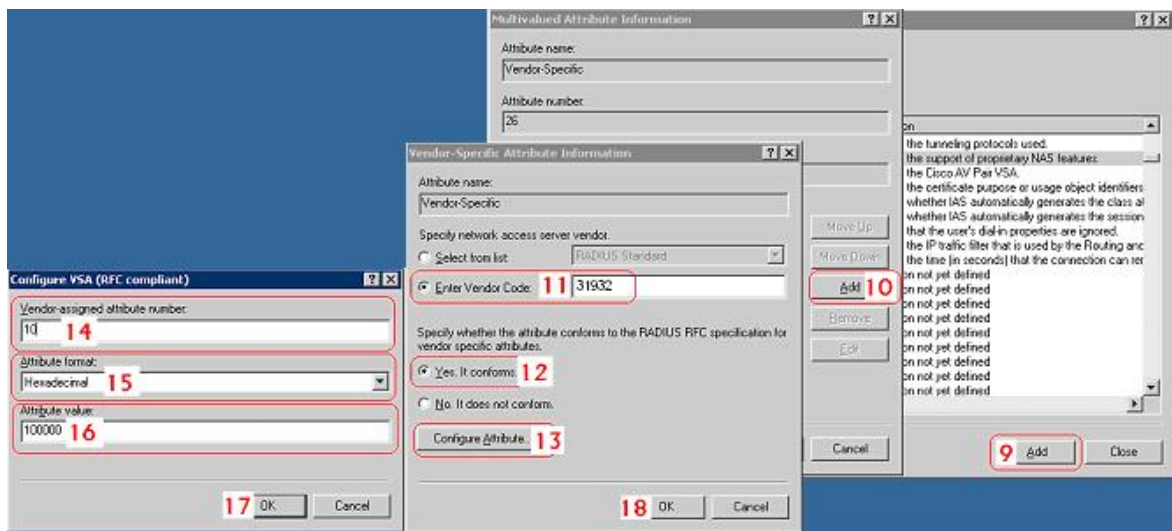
Set it conforms to the RADIUS RFC

Configure Attribute

Set "Vendor-assigned attribute number = 10"

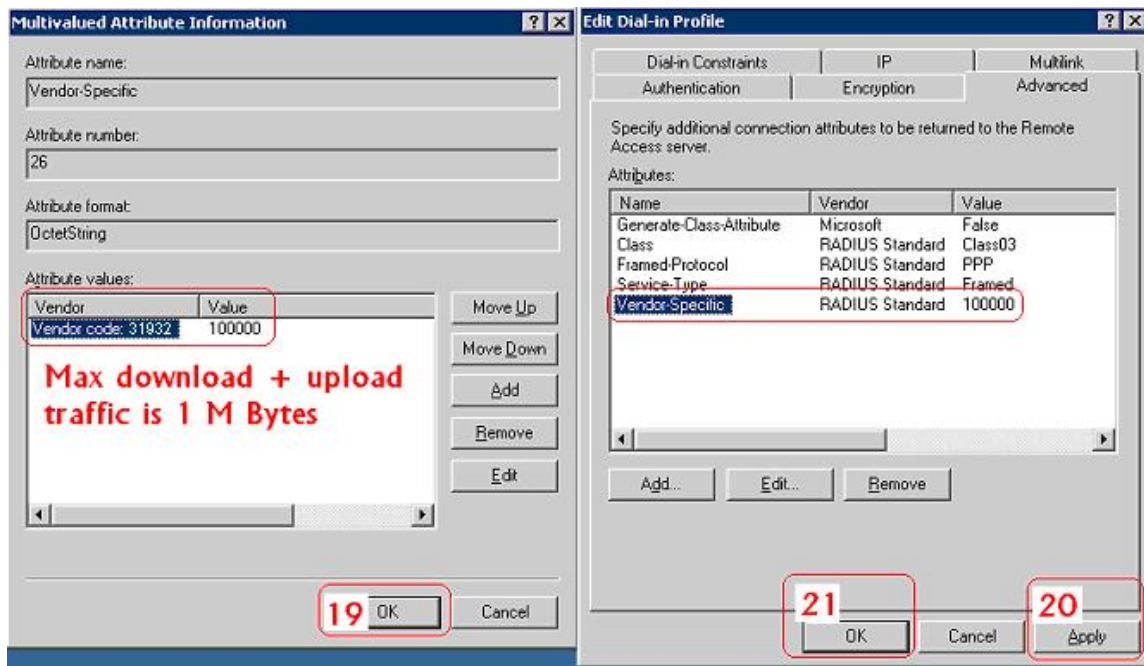
Set "Attribute format = Hexadecimal"

Set "Attribute Value = 1000000"



Step 5

Confirm the **Vendor-specific Attribute** has been added success

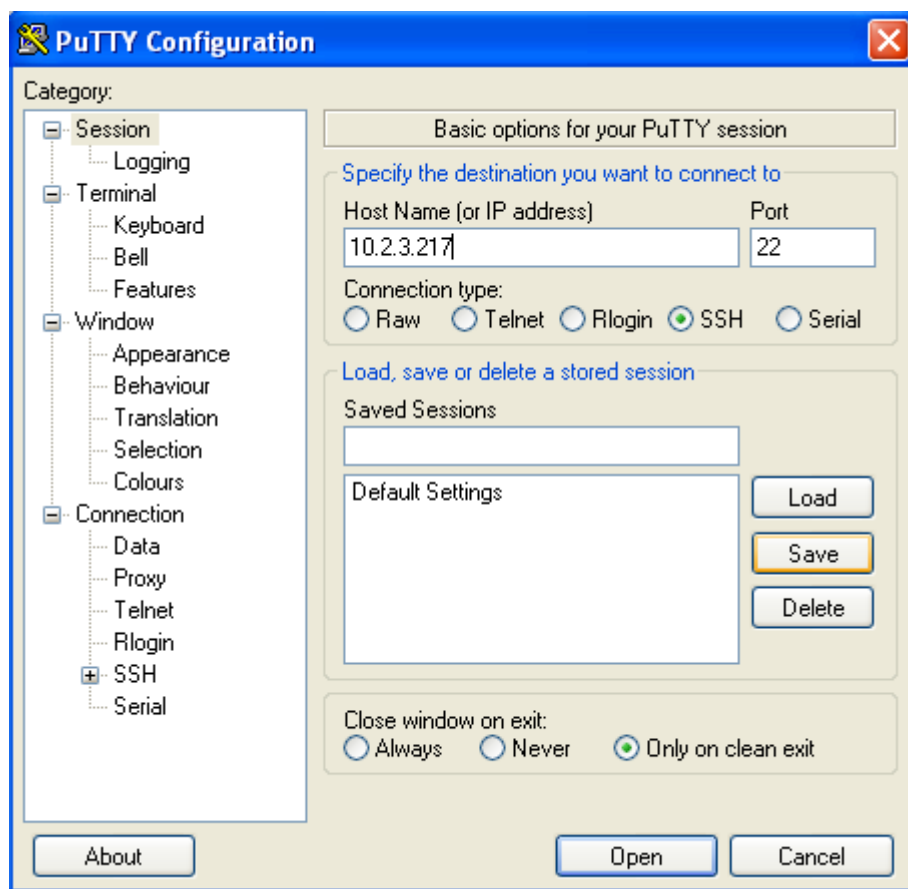


Step 6

Follow the same steps to create other **Vendor-specific Attribute** as you need.

3. VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through a **VSA** configuration using the operating system “Fedora” FreeRADIUS version 1.0.5. Before getting start, open the shell of RADIUS server, for example, use *PuTTY* to access the Linux Host:



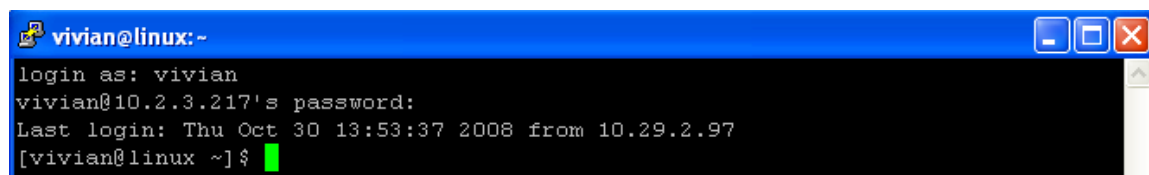
Step 1

Assume there are already have users in RADIUS Server

Assume there are already have **Groups** and assigned **users** to belong these **Groups** in RADIUS Server

Step 2

Login the Linux Host of the RADIUS server.



Step 3

Create a file “dictionary.LevelOne” under the “freeradius” folder.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary.4ipnet
```

Step 4

Edit and save the content of the file “dictionary.LevelOne” as the following:

```

VENDOR          4ipnet          31932

#
#      Standard attribute
#
ATTRIBUTE        4ipnet-Byte-Amount          10      interger 4ipnet

```

Administrator also can add other attributes as the table stated in Section 2 with same format.

```

VENDOR          4ipnet          31932

#
#      Standard attribute
#
ATTRIBUTE        4ipnet-Byte-Amount          10      interger 4ipnet
ATTRIBUTE        4ipnet-MaxByteIn            11      interger 4ipnet
ATTRIBUTE        4ipnet-MaxByteIn            12      interger 4ipnet
ATTRIBUTE        4ipnet-Byte-Amount-4GB      20      interger 4ipnet
ATTRIBUTE        4ipnet-MaxByteIn-4GB        21      interger 4ipnet
ATTRIBUTE        4ipnet-MaxByteIn-4GB        22      interger 4ipnet

```

Step 5

Edit the file “dictionary” under the folder “freeradius”.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary
```

Step 6

Include “dictionary.LevelOne” in the dictionary of RADIUS server. Insert it in an incremental position that easy to find it again.

```

$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.4ipnet
$INCLUDE dictionary.cisco
#
# This is the same as the altiga dictionary.
#
#$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000
$INCLUDE dictionary.cisco.bbsm
$INCLUDE dictionary.colubris
$INCLUDE dictionary.erx
$INCLUDE dictionary.extreme

```

Step 7

Open the “radius” database.

```
[vivian@linux ~]$ mysql -u root -p radius
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 98 to server version: 5.0.27

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> █
```

Step 8

Insert **VSA** into RADIUS respond. In this example, the maximum download and upload in bytes for **group03 users** is 1MBytes.

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
VALUES ('group03',4ipnet-Byte-Amount,':','=','1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

Step 9

Restart RADIUS to get your settings activated.

```
[vivian@linux ~] # /etc/init.d/radiusd restart
Stopping RADIUS server: [ OK ]
Starting RADIUS server: Thu Oct 30 14:26:41 2008 : Info: Starting - reading conf
figuration files ... [ OK ]
```

Appendix E. VLAN Port Location Mapping and PMS Middleware

This section introduces the Port Location Mapping feature. This feature is designed for creating multiple VLAN divisions (as if they were separate LAN ports) under a Service Zone and mapping these VLANs to different locations individually. This feature can be utilized to provide separate VLAN to separate clients in MTU/MDU deployments where a VLAN switch is deployed under the gateway to provide VLAN connection to individual rooms.

The Port Location Mapping feature is also commonly used in hospitality venues to manage the internet service for their guest rooms and public areas. In addition it can operate in conjunction with third party hospitality applications and has been tested with the Net Retriever middleware which provides seamless integration between the gateway and the popular High Speed Internet Access (HSIA) hardware and Front Office System (FOS) software.

Each Port Location Mapping entry can be configured to provide charged (single or multiple user), free or blocked internet service at the location corresponding to the entry's VLAN Tag. Please note that for charged service to work, it is required that least one or more On-demand Billing Plans are created, allowing the user to choose a desired plan to pay for their internet access.

►► Note:

For more detail of On-demand Billing Plan configuration, please refer to the section of **On-demand Users**.

1. Enabling Port Location Mapping

The Port Location Mapping feature allows each Service Zone to own multiple VLANs (as if each VLAN is a port) in order to identify where the clients are coming from.

Before the configuration of the PMS Middleware or adding VLANs to a Service Zone, the Port Mapping feature must be enabled first; go to: **System >>Port Location Mapping**.

Note: Please enable [Port Location Mapping Status](#) and restart the system for Middleware configuration.



Port Location Mapping Configuration	
Port Location Mapping Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Port Location Mapping Setup	Configure

2. Port Location Mapping

Configure Port Location Mapping; go to: **System >>Port Location Mapping>> Configure.**

Create Batch	
From	LAN1 ▾
Port Type	Free ▾
Service Zone	Default ▾
VLAN ID Start	<input type="text"/> *
Number of VLAN	<input type="text"/> *
Start Room NUM / Location ID	<input type="text"/> *
Room NUM / Location ID Prefix	<input type="text"/>
Room NUM / Location ID Postfix	<input type="text"/>

Change All Port Type	
Port Type	Free ▾
Service Zone	Default ▾

Create One	
From	LAN1 ▾
Port Type	Free ▾
Service Zone	Default ▾
VLAN ID	<input type="text"/> * (1 ~ 4094)
Room Number / Location ID	<input type="text"/> *
Room Description / Location Name	<input type="text"/>

Administrator could use Port Location Mapping feature to map a location (such as a hotel room) to a VLAN port of VLAN switch or a DSLAM device. Each Room is mapped to a VLAN Tag. And each Room can be assign to different Service Zone to get different policy. Furthermore, according to your application, you can configure the different rooms to different Port Type: **Single User**, **Multiple User**, **Free** or **Block**.

- **Free**, this port type means the user can access internet in this room without any charge.
- If you do not want to provide any internet access right in the rooms, you may change the Port type of the rooms to **Block**. If the user opens a browser and tries to access internet, it will pop up a Blocking message to notify the user.
- **Single User** port type is used mainly for hospitality application to charge a single user. If the user opens a browser and tries to access internet, a page with disclaimer and billing plan options will be displayed. User can select the desired plan and click confirm button to purchase an account. The account cost will be sent to the PMS and added to the hotel bill via the configured middleware. The room with this port type only allows one user at most to access the network within the room.

- **Multiple User** is the port type used for rooms with many users for example dormitory applications. If the user opens a browser and tries to access internet, a user login page without billing plan options will be displayed. The user needs to buy accounts from the front dorm office in order to login. The room with this port type allows more than one user to access the network within the room.

Now, let us begin to configure the Port Mapping. There are three main groups of operations that can be performed in this configuration page: **Create Batch**, **Change All Port Type** and **Create One**.

You can create the Room Mapping by batch processing if you wish to create a contiguous VLAN Tag and Room number.

➤ **Port Location Mapping Setup – Create Batch**

Create Batch	
From	LAN1 ▾
Port Type	Single User ▾
Service Zone	Default ▾
VLAN ID Start	100 *
Number of VLAN	25 *
Start Room NUM / Location ID	001 *
Room NUM / Location ID Prefix	R
Room NUM / Location ID Postfix	

- **From:** Set the Physical LAN port on the gateway to provide Port Location Mapping Service.
- **Port Type:** The default state of the rooms, it may be: Free, Block, Single User, Multiple User.
- **Service Zone:** The service zone profile used to provide internet service to the corresponding room or location.
- **VLAN ID Start:** The starting VLAN ID.
- **Number of VLAN:** The total number of VLAN.
- **Start Room Number / Location ID:** The start room number.
- **Room NUM / Location ID Prefix:** The prefix of room number.
- **Room NUM / Location ID Postfix:** The postfix of room number.

After you have created the VLAN Tag and Room number mapping, you can change the **Port Type** for all entries in a particular Service Zone.

➤ **Port Location Mapping Setup – Change All Port Type**

Change All Port Type	
Port Type	Free ▾
Service Zone	Default ▾

Port Type: The Port Type that will be applied to all of the mapping entries, it may be: Free, Block, Single User, Multiple User.

Service Zone: Select to change the Port Type of which Service Zone.

If you want to create the Room Mapping with noncontiguous VLAN Tag and Room number, then you can create them individually.

➤ **Port Location Mapping Setup – Create One**

Create One	
From	LAN1 ▾
Port Type	Free ▾
Service Zone	Default ▾
VLAN ID	<input type="text"/> * (1 ~ 4094)
Room Number / Location ID	<input type="text"/> *
Room Description / Location Name	<input type="text"/>

From: Set the Physical LAN port on the gateway to provide Port Location Mapping Service.

Port Type: The default state of the rooms, it may be: Free, Block, Single User, Multiple User.

Service Zone: The service zone profile used to provide internet service to this room.

VLAN ID: The VLAN ID to be designated to this room.

Room Number / Location ID: The room number mapping to this VLAN ID.

Room Description / Location Name: Additional reference or remark information of this room.



The VLAN Tags configured in Port Location Mapping must not conflict with any of the VLAN Tags that has been assigned to each Service Zone.

When you have finished creating Port Location Mapping profiles, go back to the Port Location Mapping page, the **Port Location Mapping List** displays all the profile entries with information such as its' *VLAN ID*, *Room Num/Location ID*, *Port Type* and *Service Zone*.

3. PMS Middleware (For hospitality application)

Now, let us begin to configure the PMS Middleware (Net Retriever) connection:

Configure Middleware Connection Setup; go to: **Users >>Middleware >>Connection Setup.**

➤ **Middleware Configuration**

Middleware Configuration	
Connection Setup	Configure
Event Log	View

- ◆ **Event Log:** Record all the Middleware Event Log.

➤ **Middleware Connection Setup**



Connection Setup	
Secret	<input type="text" value="12345"/>
Interface Port	<input type="text" value="8324"/> *
Middleware ID (MI ID)	<input type="text"/> *(1 ~ 9999)
Access Controller ID (AC ID)	<input type="text"/> *(1 ~ 9999)
Link Test Interval	<input type="text" value="60"/> *(60~600 seconds)

- ◆ **Connection Setup:** Enter the Secret, Interface Port, MI ID, AC ID, and Link Test Interval for Middleware connection.
- ◆ **Secret:** The secret key between **Guest Service Device** and **PMS Middleware** for challenge and response (MD5 Hash) to test the authenticity of the link. It should contain one or more lowercase letters, uppercase letters, numbers and symbols. It also should be between 8 ~ 16 characters.
- ◆ **Interface Port:** The port used by Net Retriever, the default is “8324”.
- ◆ **MI ID:** The ID of the **Middleware**.
- ◆ **AC ID:** The ID of the Access WHG Controller (the gateway).
- ◆ **Link Test Interval:** The time interval for the gateway to perform Link Test, the default is “300” seconds.

Now, the PMS Middleware connection is finished in the **Access WHG Controller** side. In the **PMS Middleware** (Net Retriever) side, it has to know the *IP address* of **Access WHG Controller**, *Secret Key*, *AC ID* and *MD ID* configured in Middleware Connection Setup in order for the two interfaces to communicate to each other.

4. Check or modify the Port Location Mapping profile

If you want to check the room mapping information or you want to change any setting of the room mapping. To configure Port Location Mapping List, go to: **System >> Port Location Mapping**.

The **Port Location Mapping List** displays all the profile entries with information such as its' *VLAN ID*, *Room Num/Location ID*, *Port Type* and *Service Zone*. Clicking the **Delete** link can erase an individual Port Location Mapping profile. Clicking **Delete All** button will erase all of the Port Location Mapping profiles.

Port Location Mapping List						
	VLAN ID	Room Num/ Location ID	Room Description/ Location Name	Port Type	Service Zone	<input type="button" value="Delete All"/>
	100	R001		Single User	Default	Delete
	101	R002		Single User	Default	Delete
	102	R003		Single User	Default	Delete
	103	R004		Single User	Default	Delete
	104	R005		Single User	Default	Delete
	105	R006		Single User	Default	Delete
	106	R007		Single User	Default	Delete
	107	R008		Single User	Default	Delete
	108	R009		Single User	Default	Delete
	109	R010		Single User	Default	Delete

The Search field allows administrator to search for mapping entries according to VLAN ID, Room Num/Location ID or Service Zone. Click the **VLAN ID** link to enter the **Port Mapping Profile** page for that entry. You can change the **Port Type** or **Service Zone** of this room. You also can check the present user account information.

Port Mapping Profile	
VLAN ID	101
Room Number	101
Port Type	Free
Room Description	<input type="text"/>
Service Zone	SZ7
Room Available	
User Name / Password	feh9 / 8sk7g282
Plan Type	TIME
Plan Quota	5 hr(s)
Remaining Quota	5 hr(s)
User Account Status	Online
Reference	roomN-101

5. Accessing Internet from a room

After planning your VLAN network and completing all the Port Location Mapping settings, you should verify whether the configurations are working properly. According to the Port Type set, when a user tries to access the internet from a VLAN mapped room, the pages or messages displayed are as follows:

- When a user tries to access internet from a “**Single User**” room, the browser will show the Login page with a list of available plans and service agreement. The Service Agreement body can be configured at the applied Service Zone's Custom Pages settings. User may chose a billing plan, click the Confirm button and the system

will display the generated account name and password. If you already have a user account, you can click the “**here**” link to login with the user account that you possess.

Welcome to Broadband Internet Service

Please choose from the following service selection

Plan	Price
<input checked="" type="radio"/> 2 hr(s) of connection time quota with expiration	20
<input type="radio"/> 3 min(s) of connection time quota with expiration	99
<input type="radio"/> Valid until 7:08 the following day	0.24
<input type="radio"/> 7 hr(s) of connection time quota with expiration	21
<input type="radio"/> Valid until 00:00 the following day	350

Service Agreement

Please kindly note that there will be no refund once connectivity is confirmed.

Please click CONFIRM to accept the usage charge or CANCEL to exit.

The selected service charge will be posted directly into your guest folio.

CONFIRM

CANCEL

If you already have an user account, please click [here](#) to login.



4ipnet®



Hello, you are logged in via 8m7m@ondemand password:a3259zed

To log out, please click the "Logout" button.

Login time: 2010-09-09 16:13

Remaining Time:

1

Hour

59

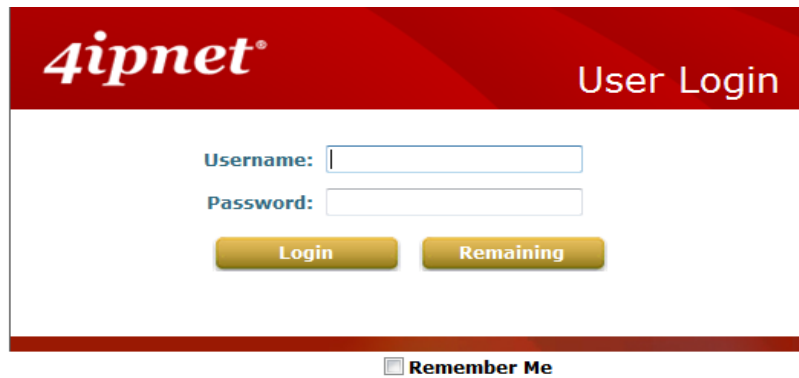
Min

53

Sec

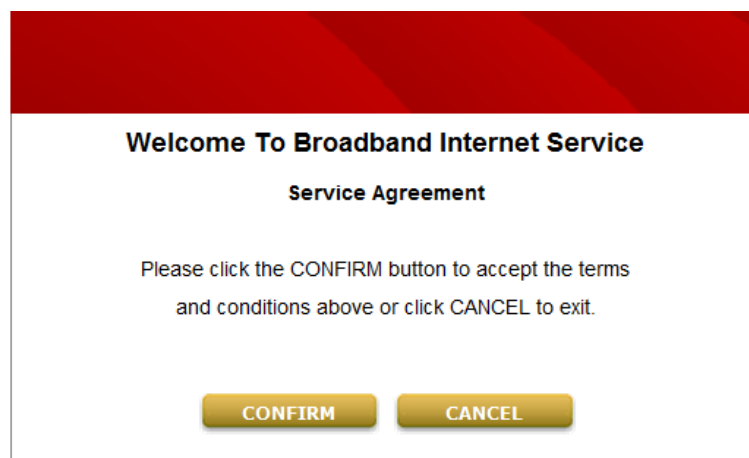
Logout

- When a user tries to access internet from a “**Multiple User**” room, the browser will show the Login page without billing plans options to select. The User will need to buy accounts from the front desk or reception to login.



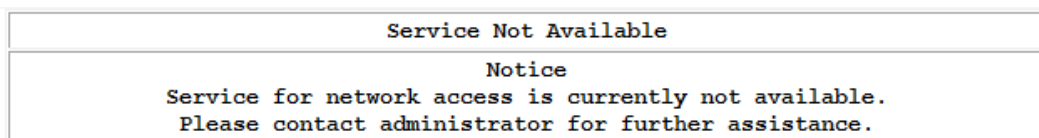
The image shows the 4ipnet User Login interface. It features a red header with the 4ipnet logo on the left and 'User Login' on the right. Below the header, there are two input fields: 'Username:' and 'Password:'. Underneath these fields are two yellow buttons: 'Login' and 'Remaining'. At the bottom of the form, there is a checkbox labeled 'Remember Me'.

- When a user tries to access internet from a “**Free**” room, the browser will show service agreement page, simply by clicking CONFIRM and the user can access the internet. The Service Agreement body can be configured at the applied Service Zone’s Custom Pages settings.



The image shows a service agreement page with a red header. The main content area has a white background and contains the following text: 'Welcome To Broadband Internet Service', 'Service Agreement', and 'Please click the CONFIRM button to accept the terms and conditions above or click CANCEL to exit.' At the bottom, there are two yellow buttons: 'CONFIRM' and 'CANCEL'.

- When a user tries to access internet from a “**Block**” room, the browser will show service unavailable page.



The image shows a service unavailable page with a white background and a thin border. The text on the page reads: 'Service Not Available', 'Notice', 'Service for network access is currently not available.', and 'Please contact administrator for further assistance.'

6. View the Event Login

After the user select a billing plan and buy it to access Internet. You can check the Middleware Event Log for information relating to users that have purchased accounts from VLAN mapped rooms.

To View Net Retriever Event Log, go to: **Users >>Middleware >>Event Log**

Authentication	Black List	Group	Policy	Additional Control	Middleware
Main Menu > Users > Middleware Configuration > Middleware Event Log					
Middleware Event Log					
Date			Size (Byte)		
2010-09-09			116		



Net Retriever Billing Log 2010-09-09							
Room	Cost	Date	Time	Duration	Description	Name	Bytes Used
10	20	20100909	161353	000000	Room number: 10, plan: 1, username: 8n7n@ondemand, password: a3259zed, price: 20	N/A	0

P/N: VWHG50020110601