

User's Manual

HSG200 v1.10

Table of Contents

1	<i>Before You Start.....</i>	1
1.1	Preface.....	1
1.2	Document Conventions.....	1
1.3	Package Checklist.....	2
2	<i>System Overview and Getting Started.....</i>	3
2.1	Introduction of HSG200.....	3
2.2	System Concept.....	3
2.3	Hardware Descriptions.....	5
2.4	System Requirement.....	8
2.5	Installation Steps.....	8
2.6	Access Web Management Interface.....	10
3	<i>Combine HSG200 to the Network.....</i>	12
3.1	Network Requirement.....	12
3.2	Configure WAN Port.....	12
3.2.1	Static IP.....	13
3.2.2	Dynamic.....	13
3.2.3	PPPoE.....	13
3.3	Internet Connection Detection.....	15
3.4	WAN Bandwidth Control.....	16
3.5	What is Zone.....	17
3.5.1	Port Role Assignment.....	18
3.5.2	Planning Your Internet Network.....	19
3.5.3	Configure Zone Network.....	20
4	<i>Let Your Network to Be a Wireless Network.....</i>	22
4.1	System Wireless General Settings.....	22
4.2	Zone Wireless Settings.....	24
4.3	Zone Wireless Security.....	27
4.4	Wireless Layer 2 firewall.....	29
4.4.1	Generic Firewall Rules.....	29
4.4.2	Predefined and Custom Service Protocols.....	35
4.4.3	Advanced.....	36
5	<i>Who Can Access the Network.....</i>	37
5.1	Type of Users.....	37
5.1.1	Local.....	38
5.1.2	RADIUS.....	41
5.1.3	On-Demand Users.....	43
5.2	User Login.....	51
5.2.1	Default Authentication.....	51

5.2.2	Login with Postfix	51
5.2.3	An Example of User Login	52
6	<i>Restrain the Users</i>	54
6.1	Black List	54
6.2	MAC Address Control	56
6.3	Policy	57
6.3.1	Firewall	59
6.3.2	Routing	62
6.3.3	Schedule	64
6.3.4	QoS Profile	65
6.3.5	Session Limit	66
7	<i>Access Network without Authentication</i>	67
7.1	DMZ	67
7.2	Virtual Server	68
7.3	Privilege List	69
7.3.1	Privilege IP	70
7.3.2	Privilege MAC	71
7.4	Disable Authentication in Public Zone	72
8	<i>User Login and Logout</i>	73
8.1	Before User Login	73
8.1.1	Login with SSL	73
8.1.2	Internal Domain Name with Certificate	74
8.1.3	Walled Garden	76
8.1.4	Walled Garden AD List	77
8.2	After User Login	78
8.2.1	Portal URL after successful login	78
8.2.2	Idle Timer	79
8.2.3	Multiple Login	80
9	<i>Networking Features of a Gateway</i>	81
9.1	IP Plug and Play	81
9.2	Dynamic Domain Name Service (DDNS)	82
9.3	Port and IP Redirect	83
10	<i>System Management and Utilities</i>	84
10.1	System Time	84
10.2	Management IP	85
10.3	User Log Access IP Address	86
10.4	SNMP	87
10.5	Three-Level Administration	88
10.6	Change Password	90
10.7	Backup / Restore and Reset to Factory	92





10.8	Firmware Upgrade	93
10.9	Restart.....	94
10.10	Network Utility	95
10.10.1	Wake-on-LAN.....	95
10.10.2	Ping	95
10.10.3	Trace Route	96
10.10.4	Show ARP Table.....	96
10.11	Monitor IP Link.....	97
10.12	Console Interface.....	98
11	<i>System Status and Reports.....</i>	101
11.1	View the Status	101
11.1.1	System Status.....	101
11.1.2	Interface Status.....	103
11.1.3	Routing Table	105
11.1.4	Current Users.....	106
11.1.5	User Log.....	107
11.1.6	Local User Monthly Network.....	109
11.2	Notification	110
11.2.1	E-Mail.....	111
11.2.2	SYSLOG	112
11.2.3	FTP	113
11.2.4	Event Log	115
12	<i>Advanced Applications.....</i>	116
12.1	Upload/Download Local Users Accounts	116
12.2	RADIUS Advanced Settings.....	118
12.3	Roaming Out.....	119
12.4	Customizable Pages	120
<i>Appendix A. Network Configuration on PC & User Login.....</i>		122
<i>Appendix B. Policy Priority.....</i>		135
<i>Appendix C. WDS Management</i>		136
<i>Appendix D. RADIUS Accounting.....</i>		137
<i>Appendix E. On-demand Account types & Billing Plan.....</i>		146
<i>Appendix F. External Payment Gateways.....</i>		156

1 Before You Start

1.1 Preface

This manual is for WLAN service providers or network administrators to set up a network environment using the HSG200 system. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	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.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	The red asterisk indicates that information in this field is compulsory.

1.3 Package Checklist

The standard package of HSG200 includes:

- HSG200 x 1
- CD-ROM (with User's Manual and QIG) x 1
- Quick Installation Guide (QIG) x 1
- Console Cable x 1
- Ethernet Cable x 1
- Power Adapter (DC 12V) x 1
- Rubber Antenna x 2
- Mounting Kit x 1
- Ground Cable x 1

Caution:

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

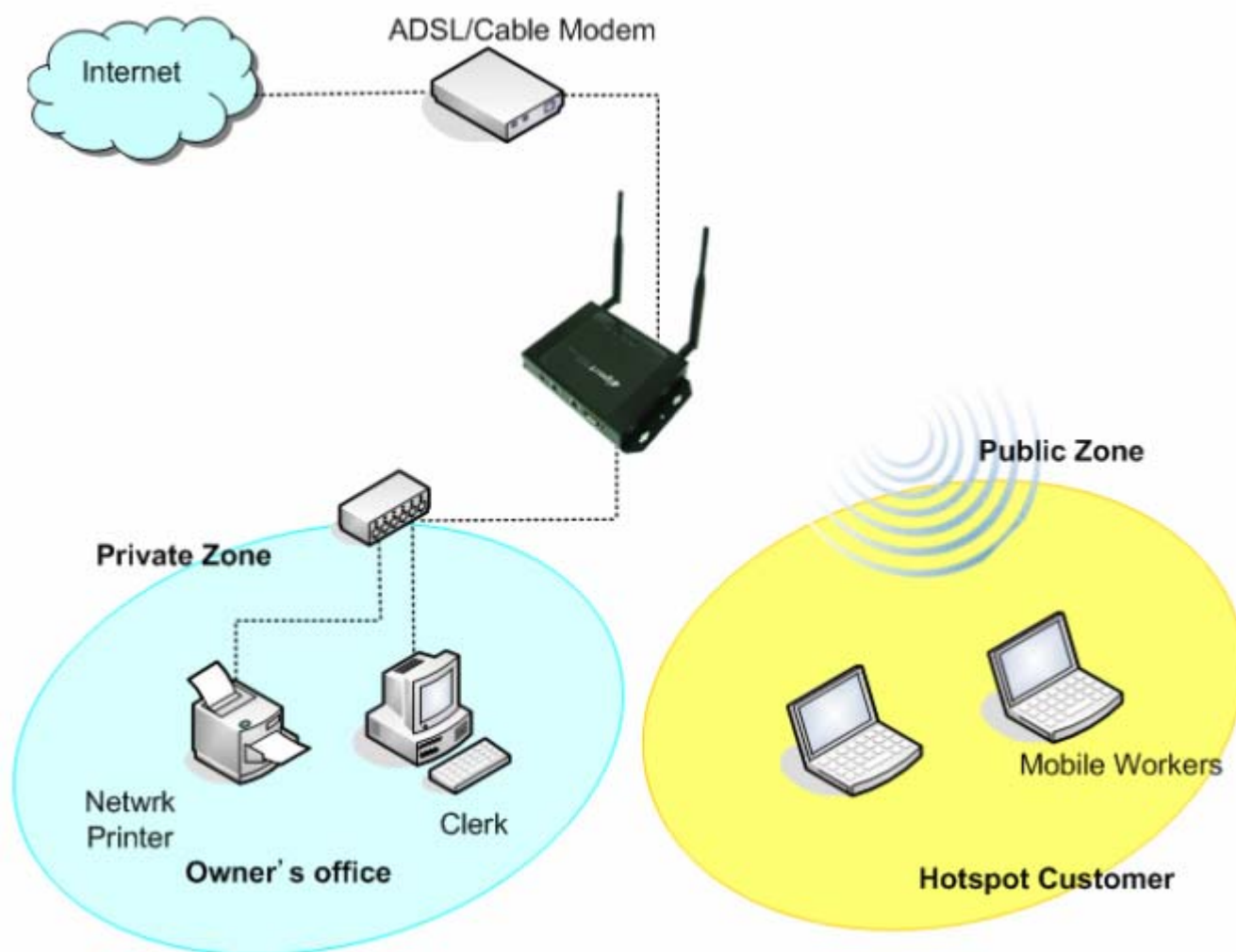
2 *System Overview and Getting Started*

2.1 Introduction of HSG200

The **HSG200** is the most economical and feature rich **Wireless Hotspot Gateway**, targeting mini-size stores that want to provide small, single-point wireless Internet access service. HSG200 is a perfect choice for beginners to run hotspot businesses. It does not cost much compared to buying a pile of equipments, nor does it take the skills of an expert to glue multiple applications out of multiple freeware. Feature-packed for hotspot operation, HSG200 comes with **built-in 802.11 n/b/g MIMO access point, web server and web pages for clients to login, easy logo-loading for branding a hotspot store, simple user/visitor account management tool, payment plans, multiple credit card gateways, traffic logs, IP sharing** and etc. HSG200 also brings in an extra advantage - the wall-mountable, dust-proof (IP50) metal housing.

2.2 System Concept

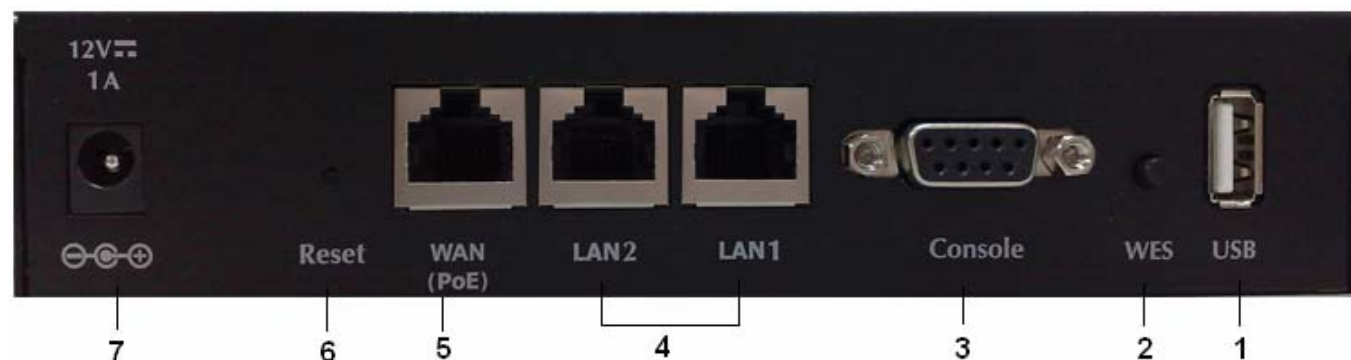
HSG200 is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external RADIUS database server. Featured with user authentication and integrated with external payment gateway, HSG200 allows users to easily pay the fee and enjoy the Internet service using credit cards through a variety of payment gateways including Authorize.Net, PayPal, SecurePay, and WorldPay. Furthermore, HSG200 introduces the concept of Zones – Private Zone and Public Zone, each with its own definable access control profiles. Private Zone means clients are not required to be authenticated before using the network service. On the other hand, clients in Public Zone are required to get authentication before using the network service. This is very useful for hotspot owners seeking to deploy wireless network service for clients and manage the network as well. The following diagram is an example of HSG200 set to manage the Internet and network access services at a hotspot venue.



【 Example: A typical Hotspot network 】

2.3 Hardware Descriptions

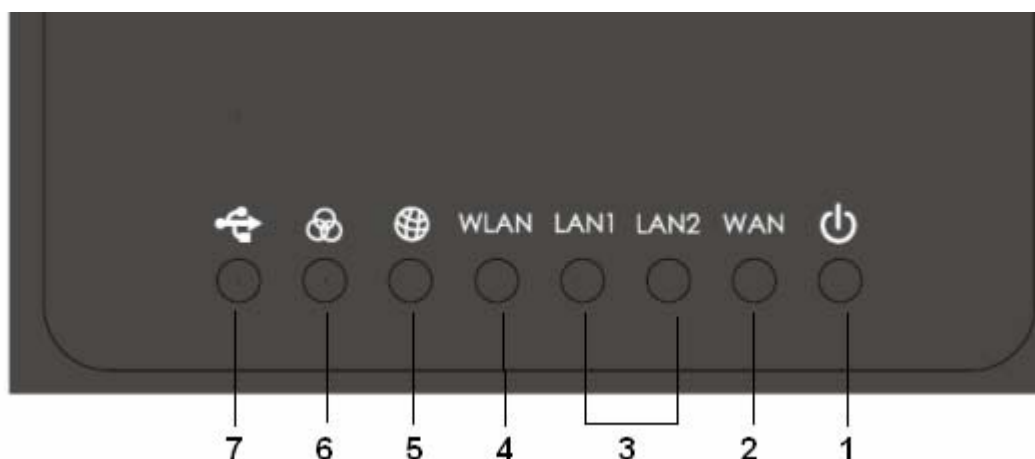
Front Panel



1	USB	For future usage only.
2	WES	Press to start running WES (WDS Easy Setup) process.
3	Console	Attach the RS-232 console cable here, for management use only.
4	LAN1/LAN2	Attach Ethernet cables here for connecting to the wired local network. LAN1 maps to Private Zone and requires no user authentication, LAN2 maps to Public Zone and by default requires user authentication.
5	WAN (PoE)	Attach the wired external network here. This port supports Power over Ethernet (PoE) for flexible installation.
6	Reset	This is hardware reset button. Press once to restart the system.
7	Power Socket (12VDC/1A)	For connecting to external power supply via the power adapter.

Rear Panel

1	Antenna Connector	Attach antennas here. HSG200 supports 1 RF interface with 2 SMA connectors.
2		

Top LED Panel


1		LED ON indicates power on; OFF indicates power off.															
2		LED ON indicates WAN connection; OFF indicates no connection; BLINKING indicates transmitting data.															
3		LED ON indicates LAN1/LAN2 connection; OFF indicates no connection; BLINKING indicates transmitting data.															
4		LED ON indicates wireless ready.															
5		LED ON indicates outbound internet connection is alive; LED OFF indicates that outbound internet connection is down. The detection interval is 1 minute; hence it reflects the connection status within the last minute.															
6		<p>For indicating WES status during WES setup:</p> <table border="1"> <thead> <tr> <th></th><th>Master</th><th>Slave</th></tr> </thead> <tbody> <tr> <td>WES Start</td><td>LED BLINKING SLOWLY</td><td>LED BLINKING QUICKLY</td></tr> <tr> <td>WES Negotiate</td><td>LED BLINKING SLOWLY</td><td>LED BLINKING QUICKLY</td></tr> <tr> <td>WES Fail (Negotiate Timeout)</td><td>LED OFF</td><td>LED OFF</td></tr> <tr> <td>WES Success</td><td>LED ON for over 5 seconds</td><td>LED ON for over 5 seconds (after Master displays WES Success)</td></tr> </tbody> </table>		Master	Slave	WES Start	LED BLINKING SLOWLY	LED BLINKING QUICKLY	WES Negotiate	LED BLINKING SLOWLY	LED BLINKING QUICKLY	WES Fail (Negotiate Timeout)	LED OFF	LED OFF	WES Success	LED ON for over 5 seconds	LED ON for over 5 seconds (after Master displays WES Success)
	Master	Slave															
WES Start	LED BLINKING SLOWLY	LED BLINKING QUICKLY															
WES Negotiate	LED BLINKING SLOWLY	LED BLINKING QUICKLY															
WES Fail (Negotiate Timeout)	LED OFF	LED OFF															
WES Success	LED ON for over 5 seconds	LED ON for over 5 seconds (after Master displays WES Success)															
7		For future usage only.															

2.4 System Requirement

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

2.5 Installation Steps

Please follow the steps below to install HSG200:

Please follow the steps mentioned below to install the hardware of HSG200:

1. Place the HSG200 at a best location.

The best location for HSG200 is usually at the center of your wireless network.

2. There are two ways to supply power over to HSG200.

(a) Connect the **DC power adapter** to the HSG200 power socket on the front panel.

(b) HSG200 is capable of receiving DC current via its WAN PoE port. Connect an IEEE 802.3af-compliant PSE device, e.g. a PoE-switch, to the WAN port of HSG200 with the Ethernet cable.

3. Connect HSG200 to your outbound network device.

Connect one end of the **Ethernet cable** to the WAN port of HSG200 on the front panel. Depending on the type of internet service provided by your ISP, connect the other end of the cable to the ATU-Router of an ADSL, a cable modem, a switch or a hub. The WAN LED indicator should be ON to indicate a proper connection.

4. Connect HSG200 to your network device.

Connect one end of the **Ethernet cable** to the LAN1 port of HSG200 on the front panel. Connect the other end of the cable to a PC for configuring the system. The LAN1 LED indicator should be ON to indicate a proper connection.

Note:

HSG200 has two virtual zones **Private** and **Public** which are mapped to LAN1(192.168.1.254) and LAN2(192.168.11.254) respectively.

Now, the hardware installation is completed.

Caution:

Please only use the power adapter supplied with the HSG200 package. Using a different power adapter may damage this system.

Caution:

To double verify the wired connection between HSG200 and your switch/router/hub, please check the LED status indication of these network devices.

2.6 Access Web Management Interface

HSG200 supports Web Management Interface (WMI) configuration. Upon the completion of hardware installation, HSG200 can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox.

Default LAN interface IP address:

LAN1 (192.168.1.254) is mapped to Private Zone with no authentication required for users.

LAN2 (192.168.11.254) is mapped to Public Zone, by default authentication is required for users.

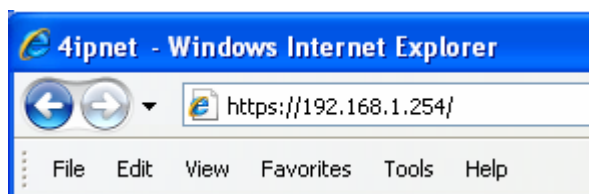
Note: The instructions below are illustrated with the administrator PC connected to LAN1.

To access the web management interface, connect a PC to **LAN1 Port**, and then launch a browser.

Make sure you have set DHCP in TCP/IP of your PC to "Obtain an IP address automatically".

The default gateway IP address is the default gateway IP address of Private Zone: "192.168.1.254".

Next, enter the gateway IP address of HSG200 at the address field. The default gateway IP address of **LAN1 Port** is "**https://192.168.1.254**" ("**https**" is used for a secured connection).



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



After a successful login, a "Home" page with four main buttons will appear on the screen.



For the first time, if HSG200 is not using a **trusted SSL certificate**, there will be a **“Certificate Error”**, because the browser treats HSG200 as an illegal website. Please press **“Continue to this website”** to continue.

Caution:

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

3 Combine HSG200 to the Network

3.1 Network Requirement

In the general network environment, the main role of HSG200 is a gateway that manages all the network access from internal network to Internet. Thus, the first step is to prepare an Internet connection from your ISP (Internet Service Provider) and connect it to the WAN port of HSG200.

3.2 Configure WAN Port

There are 3 connection types for the WAN Port: **Static**, **Dynamic** and **PPPoE**. These connection types are enough to support most ISP.

Now, let us discuss how to configure WAN port. Go to: **System >> WAN Configuration**.

WAN Configuration	
WAN	<input type="radio"/> Static (Use the following IP settings) <input checked="" type="radio"/> Dynamic (IP settings assigned automatically) Renew <input type="radio"/> PPPoE

The parameters related to each connection method are described in the following page.

3.2.1 Static IP

Static: Manually specifying the IP address of the WAN Port. The fields with red asterisks are mandatory.

- **IP Address:** The IP address of the WAN port.
- **Subnet Mask:** The subnet mask of the WAN port.
- **Default Gateway:** The gateway of the WAN port.
- **Preferred DNS Server:** The primary DNS Server of the system.
- **Alternate DNS Server:** The substitute DNS Server of the system. This is an optional field.

WAN Configuration	
WAN	<input checked="" type="radio"/> Static (Use the following IP settings)
	IP Address: <input type="text"/> *
	Subnet Mask: <input type="text"/> *
	Default Gateway: <input type="text"/> *
	Preferred DNS Server: <input type="text"/> *
	Alternate DNS Server: <input type="text"/>
	<input type="radio"/> Dynamic (IP settings assigned automatically) <input type="radio"/> PPPoE

3.2.2 Dynamic

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

WAN Configuration	
WAN	<input type="radio"/> Static (Use the following IP settings)
	<input checked="" type="radio"/> Dynamic (IP settings assigned automatically) <input type="button" value="Renew"/>
	<input type="radio"/> PPPoE

3.2.3 PPPoE

PPPoE: When selecting PPPoE to connect to the network, please set the **"Username"**, **"Password"**, **"MTU"** and **"Clamp MSS"**. There is a **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.

WAN Configuration	
WAN	<input type="radio"/> Static (Use the following IP settings)
	<input type="radio"/> Dynamic (IP settings assigned automatically)
	<input checked="" type="radio"/> PPPoE
	Username: <input type="text"/> *
	Password: <input type="text"/> *
	MTU: <input type="text" value="1492"/> bytes *(Range:1000~1492)
	Clamp MSS: <input type="text" value="1400"/> bytes *(Range:980~1400)
	Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable

3.3 Internet Connection Detection

Configure Internet Connection Detection, go to: **System >> WAN Traffic**.

WAN Traffic	
Available Bandwidth on WAN Interface	Uplink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small> Downlink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small>
Internet Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Target for detecting Internet connection: IP/Domain Name: <input type="text" value="www.google.com"/> * IP/Domain Name: <input type="text"/> IP/Domain Name: <input type="text"/> When Internet connection is down, the system will display the message as: <input type="text" value="Sorry! The network outbound service is temporari"/> *

- **Internet Connection Detection:** When enabled, system will try to access these IP/Domain addresses, if system can reach these IP/Domain address, it means that the outbound Internet connection is in normal state. On the other hand, there is a text box available for the administrator to enter a reminding message. This reminding message will appear on clients' screens when Internet connection is down.

3.4 WAN Bandwidth Control

Configure WAN Bandwidth Control, go to: **System >> WAN Traffic**.

WAN Traffic	
Available Bandwidth on WAN Interface	Uplink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small>
	Downlink: <input type="text" value="100000"/> Kbps <small>*(Range: 10-100000)</small>
Internet Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Target for detecting Internet connection:
	IP/Domain Name: <input type="text" value="www.google.com"/> *
	IP/Domain Name: <input type="text"/>
	IP/Domain Name: <input type="text"/>
	When Internet connection is down, the system will display the message as:
	<input type="text" value="Sorry! The network outbound service is temporari"/> *

The feature gives administrators control over the entire system's traffic though the WAN interface. These parameters set here should not exceed the real bandwidth coming from your ISP. For example, if your xDSL is 8Mbps/640Kbps, you may input these two values here.

Available Bandwidth on WAN Interface:

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

3.5 What is Zone

Configure Zone, go to: **System >> Zone Configuration**.

A *Zone* is a logical network area that covers wired or wireless networks, or both of them. By associating to a unique ESSID of a Zone, wireless network is divided into different logical zones. Clients attempting to access the resources within a Zone will be controlled based on the access control profile of that Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc.

There are two Zones that can be utilized by HSG200 – Private Zone and Public Zone, as shown in the table below. Private Zone means clients are not required to be authenticated before using the network service. On the other hand, clients in Public Zone are required to get authentication before using the network service.

Zone Settings				
Name	ESSID	Wireless Security	Default Authen Option	Details
Private	HSG200-1	None	N/A	Configure
Public	HSG200-2	None	On-demand User	Configure

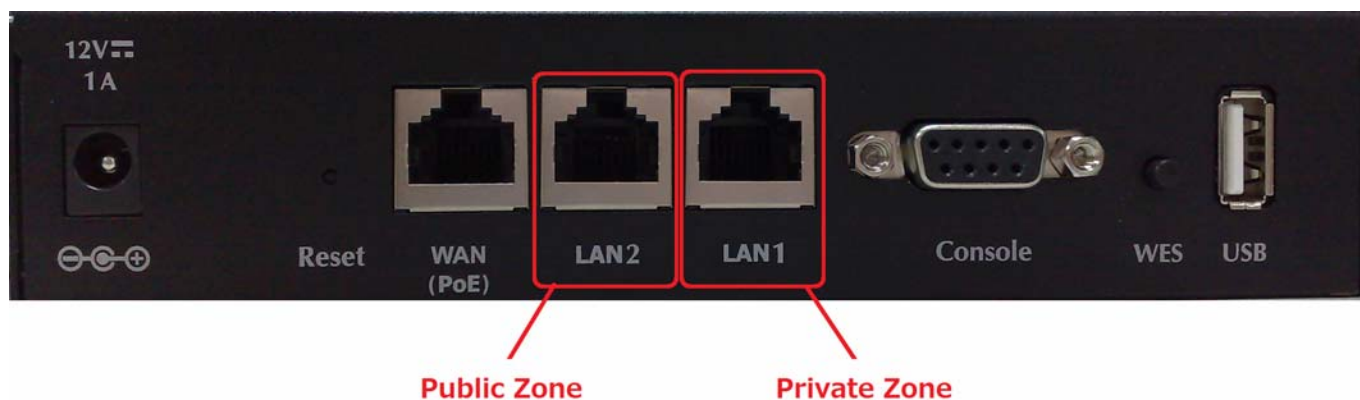
- **Name:** Mnemonic name of the Zone.
- **ESSID:** The SSID that is associated with the Zone.
- **Wireless Security:** Data encryption method for wireless networks within the Zone.
- **Default Authen Option:** Default authentication method/server that is used within the Zone.
- **Details:** Configurable, detailed settings for each Zone.

Click **Configure** button to configure each Zone: **Basic Settings**, **Authentication Settings (Public Zone only)**, **Wireless Settings**, and **WDS Settings (Public Zone only)**.

3.5.1 Port Role Assignment

HSG200 supports two zones, Private and Public. In the Private Zone, authentication is not required to access the network via wired and wireless. In the Public Zone, by default, Authentication Required is enabled by default, so clients are required to get authenticated successfully before surfing the Internet.

The Zone and Port mappings are shown below, LAN1 and LAN2 maps to Private Zone and Public Zone respectively.

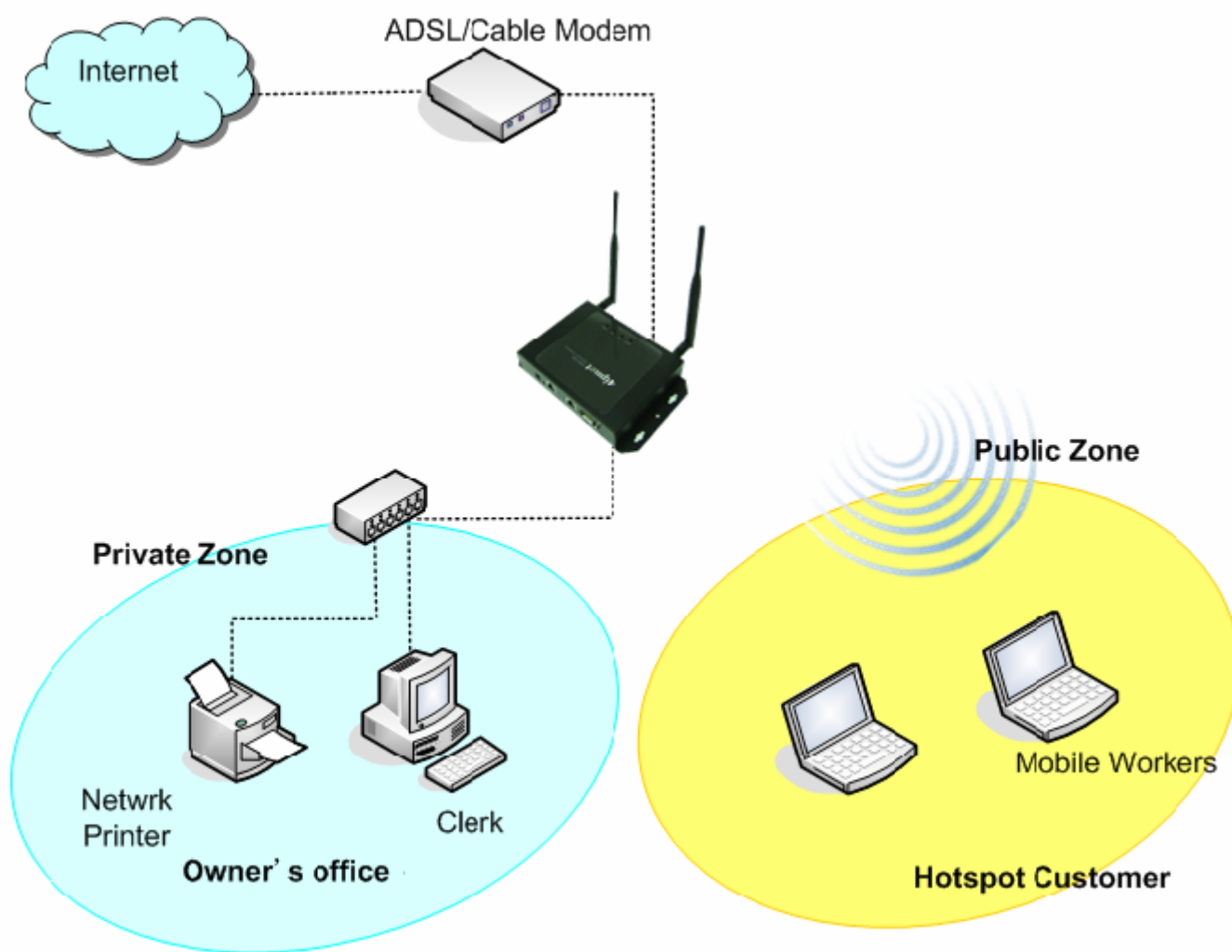


Note:

System's WMI can also be accessed via WAN port as long as the administrator uses an IP address listed in **Management IP Address List** setting. If both WAN and LAN ports are unable to reach WMI, please use console interface to resolve this issue.

3.5.2 Planning Your Internet Network

HSG200 supports two zones, Private and Public. In the Private Zone, authentication is not required to access the internet via wired and wireless. In Public Zone, by default Authentication Required is enabled, so clients are required to get authenticated successfully before surfing the Internet. Administrator can access the Web Management Interface (WMI) of HSG200 through the wired LAN port. Waiters or waitresses can send orders back to the electrical menu system via wireless hand set devices.



3.5.3 Configure Zone Network

Configure Zone network; go to: **System >> Zone Configuration**. Click the button **Configure** of Private zone for further configuration. The parameter descriptions of Basic Settings for Private Zone and Public Zone are the same. The wireless settings under each zone will be covered in the next section.

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

➤ **Network Interface:**

- **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen, this zone runs in Router mode.
- **IP Address:** The IP Address of this zone.
- **Subnet Mask:** The subnet Mask of this zone.

➤ **DHCP Server:** Related information needed on setting up the DHCP Server is listed here.

Please note that when "Enable DHCP Relay" is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this zone.

- **Start IP Address / End IP Address:** A range of IP addresses that the built-in DHCP server will assign to clients.
Note: please change the Management IP Address List accordingly (at *System >> General >> Management IP Address List*) to permit the administrator to access the HSG200 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 Zone.
- **Alternate DNS Server:** The substitute DNS server that is used by this Zone.

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

4 Let Your Network to Be a Wireless Network

4.1 System Wireless General Settings

Configure System's Wireless General Settings, go to: **System >> Zone Configuration**.

Wireless General Settings	
Band	802.11g+802.11n ▼
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Short Guard Interval	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel Width	20 MHz ▼
Channel	1 ▼
Max Transmit Rate	Auto ▼
Transmit Power	Auto ▼
DTIM Period	1 (1-255ms)
ACK Timeout	100 (0-255ms)

Wireless General Settings:

- **Band:** There are 4 modes to select, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps), **802.11b+g**, and **802.11g+n**.
- **Short Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select **Enable** for **Short Preamble** or **Disable** for **Long Preamble**.
- **Short Guard Interval (802.11g+n only):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. With 802.11n, short guard interval is half of what it is used to be to increase throughput. Select *Enable* to use Short Guard Interval or *Disable* to use normal Guard Interval.
- **Channel Width (802.11g+n only):** For 802.11n, double channel bandwidth to 40 MHz is supported to enhance throughput.
- **Channel:** Select the appropriate channel from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default *Auto*.
- **Max Transmit Rate:** The default is **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 make the Access Point automatically use the fastest rate possible.
- **Transmit Power:** Select from the range, or keep the default setting or to make the Access

Point use different transmit power as you wish.

- **DTIM Period:** Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will let the wireless client save energy more, but the throughput will be growing worse.
- **ACK Timeout:** The time interval for waiting the “**ACK**nowledgement frame”. If the ACK is not received within that timeout period then the packet will be re-transmitted. Higher ACK Timeout will decrease the packet lost, but the throughput will be growing worse.

4.2 Zone Wireless Settings

Each zone has its own VAP and corresponds to one SSID. In Private zone, it's VAP1 and the SSID is hidden, so public users cannot scan this SSID in the air, for privilege users who already know this SSID, they can manually associate to the SSID of Private zone. On the other hand, the SSID of VAP2 under Public zone by default is enabled with SSID Broadcast feature, allowing public users to scan this SSID in the air.

After wireless general settings are done, use the parameters in Wireless Settings under zone configuration to fine tune the wireless network under Private and Public Zone.

To configure Private Zone's Wireless Settings, go to: **System >> Zone Configuration**, click **Configure** of Private zone

Wireless Settings : VAP 1	
Basic	VAP Status : <input checked="" type="radio"/> Enable <input type="radio"/> Disable ESSID : <input type="text" value="HSG200-1"/> *
Security	Security Type : <input type="text" value="None"/>
Advanced	Beacon Interval : <input type="text" value="100"/> (25-500ms) RTS Threshold : <input type="text" value="2346"/> (1-2346) Fragment Threshold : <input type="text" value="2346"/> (256-2346) Station Isolation : <input type="radio"/> Enable <input checked="" type="radio"/> Disable WMM : <input type="radio"/> Enable <input checked="" type="radio"/> Disable

➤ Wireless Settings: VAP1 (Wireless Settings Private Zone)

- **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID for VAP1 under Private Zone or use default "HSG200-1", the ESSID of Private Zone will not be broadcasted and internal staff will need to associate to Private Zone's VAP1 manually.
- **Security:** Configure the wireless network under Private Zone with security encryption to prevent unauthorized wireless association if necessary. The encryption standards supported are WEP and WPA-PSK.
- **Advanced:** The parameters in advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP.

RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with EAP200 or in areas where the clients are far apart and can detect only EAP200 but not each other.

Fragment Threshold: Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from each other and can only communicate with the system.

WMM: The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

Normally we use VAP2, the VAP under Public Zone to provide wireless service to public clients in a hotspot environment. To configure Public Zone's Wireless Settings, go to: **System >> Zone Configuration**, click **Configure** of Public zone

Wireless Settings : VAP 2	
Basic	VAP Status : <input checked="" type="radio"/> Enable <input type="radio"/> Disable ESSID : <input type="text" value="HSG200-2"/> *
Security	Security Type : <input type="text" value="None"/>
Advanced	Beacon Interval : <input type="text" value="100"/> (25-500ms) RTS Threshold : <input type="text" value="2346"/> (1-2346) Fragment Threshold : <input type="text" value="2346"/> (256-2346) Broadcast SSID : <input checked="" type="radio"/> Enable <input type="radio"/> Disable Station Isolation : <input type="radio"/> Enable <input checked="" type="radio"/> Disable WMM : <input type="radio"/> Enable <input checked="" type="radio"/> Disable

➤ **Wireless Settings: VAP2 (Wireless Settings for Public Zone)**

- **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID for VAP2 under Private Zone or use default "HSG200-2", the ESSID of Private Zone will be broadcasted in default settings to allow it to be scanned in the air.
- **Security:** Configure the wireless network under Public Zone with security encryption to prevent unauthorized wireless association if necessary. The encryption standards supported are WEP, 802.1X, WPA-PSK and WPA-RADIUS.
- **Advanced:** The parameters in advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP.

RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with EAP200 or in areas where the clients are far apart and can detect only EAP200 but not each other.

Fragment Threshold: Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

Broadcast SSID: Enable to broadcast VAP2's SSID in the air, Disable to hide VAP's SSID so that it cannot be scanned.

Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from each other and can only communicate with the system.

WMM: The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

4.3 Zone Wireless Security

Configure Zone Wireless Security, go to: **System >> Zone Configuration**, click **Configure** of Private zone or click **Configure** of Public zone.

After the above configurations are finish, setup the wireless security is very important to protect your wireless network.

Wireless Settings : VAP 1	
Basic	VAP Status : <input checked="" type="radio"/> Enable <input type="radio"/> Disable ESSID : <input type="text"/> *
Security	Security Type : <div>None</div> Beacon Interval : <input type="text" value="100"/> <div>500ms</div> RTS Threshold : <input type="text" value="2346"/> (1-2346)

Wireless Settings : VAP 2	
Basic	VAP Status : <input checked="" type="radio"/> Enable <input type="radio"/> Disable ESSID : <input type="text"/> *
Security	Security Type : <div>None</div> Beacon Interval : <input type="text" value="100"/> <div>500ms</div> RTS Threshold : <input type="text" value="2346"/> (1-2346) Fragment Threshold : <input type="text" value="2346"/> (256-2346)

Security:

For each zones, administrators can set up the wireless security profile, it include **WEP**, **802.1x** (for **Public Zone** only), **WPA-PSK** or **WPA-RADIUS** (for **Public Zone** only).

- **WEP:**
 - **802.11 Authentication:** Select from **Open System** or **Shared Key**.
 - **WEP Key Length:** Select from **64-bit**, **128-bit**, **152-bit** key length.
 - **WEP Key Format:** Select from **ASCII** or **Hex** format for the WEP key.
 - **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
 - **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
- **802.1X:**
 - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
 - **WEP Key Length:** Select from **64-bit** or **128-bit** key length.
 - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in second.
- **WPA-PSK:**
 - **Cipher Suite:** Select an encryption method from **TKIP (WPA)**, **AES (WPA)**, **TKIP (WAP2)**, **AES (WAP2)**, or **Mixed**.
 - **Pre-shared Key / Passphrase:** Enter the key value for the pre-shared key or passphrase.
 - **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.
- **WPA-RADIUS:** Same as **802.1X**, when it is selected, it is combined with **TKIP**, **AES** or **Mixed** mode.

- **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

4.4 Wireless Layer 2 firewall

The system provides an additional security feature, Layer2 Firewall, in addition to standard wireless security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffics, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured in Policies, this extra security feature will assist to mitigate possible security breach. This section provides information in the following functions: **Generic Firewall Rules**, **Predefined and Custom Service Protocols** and **Advanced**.

4.4.1 Generic Firewall Rules

You can choose to enable or disable the wireless Generic Firewall. This section provides an overview of firewall rules for the system's wireless interface; 6 default rules with up to a total 20 firewall rules are available for configuration.

NAT Privilege Monitor IP Walled Garden Walled Garden Ad List DDNS Client Mobility Layer 2 Firewall

Generic Firewall

☒ Enable ☐ Disable

Firewall Rules

No.	Active	Action	Rule Name	Ether Type	Remark	Operation
1	<input checked="" type="checkbox"/>	Block	CDP and VTP	IEEE 802.3		Edit Move to Insert Before Delete
2	<input checked="" type="checkbox"/>	Block	STP	IEEE 802.3		Edit Move to Insert Before Delete
3	<input checked="" type="checkbox"/>	Block	GARP	IEEE 802.3		Edit Move to Insert Before Delete
4	<input checked="" type="checkbox"/>	Block	RIP	IPv4		Edit Move to Insert Before Delete
5	<input checked="" type="checkbox"/>	Block	HSRP	IPv4		Edit Move to Insert Before Delete
6	<input checked="" type="checkbox"/>	Block	OSPF	IPv4		Edit Move to Insert Before Delete
7	<input type="checkbox"/>	Block	rule 7	ANY		Edit Move to Insert Before Delete
8	<input type="checkbox"/>	Block	rule 8	ANY		Edit Move to Insert Before Delete
9	<input type="checkbox"/>	Block	rule 9	ANY		Edit Move to Insert Before Delete
10	<input type="checkbox"/>	Block	rule 10	ANY		Edit Move to Insert Before Delete

(Total:10) [First](#) [Prev](#) [Next](#) [Last](#)

From the overview table, each rule is designated with the following field;

- **No.:** The numbering will decide the priority to let system carry out the available firewall rules in the tables.
- **Active:** Checking this field will mark the rule as active which means this rule will be enforced.
- **Action:** **Block** denotes a block rule; **PASS** denotes a pass rule.
- **Name:** This is the denominated name of the rule.
- **EtherType:** It denotes the type of traffics subject to this rule.
- **Remark:** It shows the additional reference information of this rule.
- **Operation:** 4 actions are available; **Edit** denotes to edit the rule details, **Move to** denotes to move the rule to a specified rule number, **Insert Before** denotes to insert a rule before the current rule, and **Delete** denotes to delete the rule.

>> **To edit a specific rule,**

Edit in **Operation** column of firewall rules will lead to the following page for detail configuration.

From this page, the rule can be edited from an existing rule for revision.

NAT
Privilege
Monitor IP
Walled Garden
Walled Garden Ad List
DDNS
Client Mobility
Layer 2 Firewall

Edit Filter Rule			
Rule Number		8	
Rule Name		rule 8	
Action for Matched Packets		<input type="radio"/> Pass <input checked="" type="radio"/> Block	
Rule Remark			

Link Layer Configuration			
Ether Type	All		
Interface	<input checked="" type="radio"/> From <input type="radio"/> To VAP2		
Source		Destination	
MAC Address		MAC Address	
MAC Mask		MAC Mask	

- **Rule Number:** The numbering of this specific rule will decide its priority among available firewall rules in the list.
- **Rule name:** The rule name can be denominated here.
- **Action for Matched Packets:** The rule can be chosen to be **Block** or **Pass** packets that match the rule criteria.
- **Rule Remark:** The additional reference note of this rule can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics subject to this rule.
- **Interface:** For specifying the traffic direction (To or From VAP2) subjected to this rule.

- **IPv4 Service** (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP** (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.
- **SNAP Type** (when EtherType is **IEEE802.3**): The field can be used to indicate the type of encapsulated traffics.
- **VLAN ID** (when EtherType is **VLAN**): The VLAN ID is provided to associate with certain VLAN-tagging traffics.
- **VLAN Priority** (when EtherType is **VLAN**): It denotes the priority level with associated VLAN traffics.
- **VLAN Type** (when EtherType is **VLAN**): It can be used to indicate the type of encapsulated traffics.
- **Opcode** (when EtherType is **ARP/RARP**): This list can be used to specify the ARP Opcode in ARP header.
- **Source**: MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).
- **Destination**: MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).

When the configurations are made; please click **Apply** to let the firewall rule take effort.

>>To insert a specific rule,

Insert Before in **Operation** column of firewall list will lead to the following page for detail configuration with rule ID for the rule currently being inserted.

NAT	Privilege	Monitor IP	Walled Garden	Walled Garden Ad List	DDNS	Client Mobility	Layer 2 Firewall
-----	-----------	------------	---------------	-----------------------	------	-----------------	------------------

Edit Filter Rule	
Rule Number	9
Rule Name	default rule
Action for Matched Packets	<input type="radio"/> Pass <input checked="" type="radio"/> Block
Rule Remark	

Link Layer Configuration	
Ether Type	All
Interface	<input checked="" type="radio"/> From <input type="radio"/> To VAP2
Source	
MAC Address	
MAC Mask	
Destination	
MAC Address	
MAC Mask	

>> *To move a specific rule,*

Move to in **Operation** column of firewall rules will lead to the following page for reordering confirmation. Click **OK** to save the changes made.

Move to No. 5

OK Cancel

Please make sure all desired rules are checked as Active and applied in overview page.

NAT Privilege Monitor IP Walled Garden Walled Garden Ad List DDNS Client Mobility **Layer 2 Firewall**

Gereric Firewall

☒ Enable ☐ Disable

Firewall Rules

No.	Active	Action	Rule Name	Ether Type	Remark	Operation
1	<input checked="" type="checkbox"/>	Block	CDP and VTP	IEEE 802.3		Edit Move to Insert Before Delete
2	<input checked="" type="checkbox"/>	Block	STP	IEEE 802.3		Edit Move to Insert Before Delete
3	<input checked="" type="checkbox"/>	Block	GARP	IEEE 802.3		Edit Move to Insert Before Delete
4	<input checked="" type="checkbox"/>	Block	RIP	IPv4		Edit Move to Insert Before Delete
5	<input checked="" type="checkbox"/>	Block	HSRP	IPv4		Edit Move to Insert Before Delete
6	<input checked="" type="checkbox"/>	Block	OSPF	IPv4		Edit Move to Insert Before Delete
7	<input checked="" type="checkbox"/>	Block	rule 7	ANY		Edit Move to Insert Before Delete
8	<input type="checkbox"/>	Block	rule 8	ARP		Edit Move to Insert Before Delete
9	<input type="checkbox"/>	Block	default rule	ANY		Edit Move to Insert Before Delete
10	<input type="checkbox"/>	Block	rule 9	ANY		Edit Move to Insert Before Delete

(Total:10) [First](#) [Prev](#) [Next](#) [Last](#)

Apply

Cancel

4.4.2 Predefined and Custom Service Protocols

The administrator can add or delete firewall service protocols here; the services in this list will become available drop-down options to choose from in firewall rule (when EtherType is IPv4).

The first 27 entries are default services and the administrator can add any extra desired services.

The 27 default firewall services cannot be deleted but can be disabled.

NAT
Privilege
Monitor IP
Walled Garden
Walled Garden Ad List
DDNS
Client Mobility
Layer 2 Firewall

Service Protocols List			
No.	Name	Description	Select All
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL ICMP	ICMP	<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"/>

Add
Delete

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

4.4.3 Advanced

Advanced Firewall Settings can be enabled to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of system.

The screenshot shows the 'Layer 2 Firewall' configuration page. At the top, there are tabs for NAT, Privilege, Monitor IP, Walled Garden, Walled Garden Ad List, DDNS, Client Mobility, and Layer 2 Firewall. The 'Advanced' section is active, showing 'Enable' selected for the main firewall settings. Below this, the 'Advanced Firewall Settings' section is expanded, showing two main categories: 'DHCP Snooping' and 'ARP Inspection'. Under 'DHCP Snooping', 'Enable' is selected, and there is a 'Trust DHCP List' with a 'Configure' button. Under 'ARP Inspection', 'Enable' is selected, and there are three sub-options: 'Force DHCP' (set to 'Disable'), 'Broadcast' (set to 'Disable'), and 'Static List' with a 'Configure' button. At the bottom of the settings area are 'Apply' and 'Cancel' buttons.

- **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the **Trust DHCP List** (IP/MAC) can be used to specify legitimate DHCP servers to prevent rouge DHCP server.
- **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing.
 - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, therefore any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static List**.
 - **Broadcast** can be enabled to let other AP (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
 - **Static List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears in the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

If any settings are made, please click **Apply** to save the configuration before leaving this page.

5 Who Can Access the Network

5.1 Type of Users

Configure Users, go to: **Users >> Authentication**.

This section is for administrators to pre-configure authentication servers for the entire system. Concurrently up to three servers can be selected and pre-configured for static user authentication, one server uses built-in LOCAL database while the other two servers use external RADIUS database. In addition, another server called On-demand can be configured for temporary user authentication.

Authentication Settings					
Auth Database	Auth Server Name	Postfix	Policy	Black List	Configure
LOCAL	<input type="text" value="Server 1"/>	<input type="text" value="local"/>	Policy 1 ▾	None ▾	<input type="button" value="Configure"/>
RADIUS	<input type="text" value="Server 2"/>	<input type="text" value="radius1"/>	Policy 2 ▾	None ▾	<input type="button" value="Configure"/>
RADIUS	<input type="text" value="Server 3"/>	<input type="text" value="radius2"/>	Policy 3 ▾	None ▾	<input type="button" value="Configure"/>
ONDEMAND	<input type="text" value="On-demand User"/>	<input type="text" value="ondemand"/>	Policy 4 ▾	None ▾	<input type="button" value="Configure"/>

- **Auth Database:** There are four different authentication options in HSG200 that use databases: **LOCAL**, **RADIUS1**, **RADIUS2** and **ONDEMAND**.
- **Auth Server Name:** Set a name for the authentication databases by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_), space and dot (.) only. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.
- **Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated against the LOCAL authentication database.
- **Policy:** Select one Policy from the drop-down list box for this specific authentication option.
- **Black List:** There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop-down menu and this black list will be applied to this specific authentication option.
- **Configure:** Click **Configure** button to enter the specific authentication page. For example, if you want to edit the *Local* authentication database, please click **Configure** button of **Local**.

5.1.1 Local

Click the button **Configure** of **Local** for further configuration.

Local User Database Settings	
Local User List	
Account Roaming Out	<input type="radio"/> Enable <input checked="" 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.)

- **Local User List:** It let the administrator to view, add or delete local user account. The **Upload User** button is for importing a list of user account from a text file. The **Download User** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account.

Local User List					
Username	Password	MAC Address	Applied Policy	Remark	<input type="button" value="Del All"/>
user2	user2		Policy1		Delete
user3	user3		None		Delete
user1	user1		Policy4		Delete

(Total: 3/500) [First](#) [Prev](#) [Next](#) [Last](#)

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 **Policy** to classify local users. Click **Apply** to complete adding the user(s). MAC address of a networking device can be bound with a local user as well. It means this user must login to system with a networking device (PC) that has the corresponding MAC address, so this user can not login with other networking devices.

Adding User(s) to the List					
No.	Username*	Password*	MAC Address (xx:xx:xx:xx:xx:xx)	Policy	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>

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

Local User List					
Username	Password	MAC Address	Applied Policy	Remark	<input type="button" value="Del All"/>
user1	user1		Policy4		Delete

(Total: 1/500) [First](#) [Prev](#) [Next](#) [Last](#)

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

- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account in **Local User List** 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 Policy* (optional) and *Remark* (optional). Click **Apply** to complete the modification.

Editing Existing User Data	
Username	<input type="text" value="user01"/> *
Password	<input type="text" value="user01"/> *
MAC Address	<input type="text"/>
Applied Policy	Policy 1 ▼
Remark	<input type="text"/>

5.1.2 RADIUS

There are two RADIUS authentication database for configuration. Click the button **Configure** of any one of **RADIUS** servers for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not mandatory). 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 type="radio"/> Enable <input checked="" type="radio"/> Disable
Username Format	<input type="radio"/> Complete (e.g. user1@companyname.com) <input checked="" type="radio"/> Only ID (e.g. user1)
NAS Identifier	<input type="text"/>
NAS Port Type	<input type="text" value="19"/> *(Default 19, Range: 0~35)
Class-Policy Mapping	<input type="button" value="Edit Class-Policy Mapping"/>
Primary RADIUS Server	
Server	<input type="text"/> *(Domain Name/IP Address)
Authentication Port	<input type="text"/> *(Default: 1812)
Accounting Port	<input type="text"/> *(Default: 1813)
Secret Key	<input type="text"/> *
Accounting Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Authentication Protocol	CHAP <input type="button" value="v"/>
Secondary RADIUS Server	
Server	<input type="text"/> (Domain Name/IP Address)
Authentication Port	<input type="text"/>
Accounting Port	<input type="text"/>
Secret Key	<input type="text"/>
Accounting Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

➤ External RADIUS Related Settings

- **802.1X Authentication:** Enable /Disable 802.1X authentications for users authenticating through this Server.
- **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.
- **Class-Policy Mapping:** This function is to assign a Policy 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 Policy.

RADIUS Policy Mapping - Server 2				
<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
No.	Class Attribute Value	policyName	Remark	
1	<input type="text" value="GP1"/>	<input type="text" value="Policy 1"/>	<input type="text"/>	
2	<input type="text" value="GP2"/>	<input type="text" value="Policy 2"/>	<input type="text"/>	
3	<input type="text" value="GP3"/>	<input type="text" value="Policy 3"/>	<input type="text"/>	
4	<input type="text"/>	<input type="text" value="Policy 1"/>	<input type="text"/>	
5	<input type="text"/>	<input type="text" value="Policy 1"/>	<input type="text"/>	

➤ Primary / Secondary RADIUS Server

- **Server:** Enter the domain name or IP address of your RADIUS Server.
- **Authentication Port:** Enter the Port number used for authentication.
- **Accounting Port:** Enter the Port number used for accounting.
- **Secret Key:** Secret Key used for authentication.
- **Accounting Service:** Enable / Disable RADIUS accounting.
- **Authentication Protocol:** Select Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

5.1.3 On-Demand Users

On-demand User Server Configuration: The administrator can 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	WLAN ESSID	HSG200-2
	Wireless Key	
	Currency	<input checked="" type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> <small>(Input other desired currency, e.g. AU)</small>
	Remaining Reminder	time: <input type="radio"/> Enable <input checked="" type="radio"/> Disable Volume: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Sync Interval	<input checked="" type="radio"/> 10min(s) <input type="radio"/> 15min(s) <input type="radio"/> 20min(s)
Ticket Customization		Configure
Billing Plans Terminal Server		Configure 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.

- **WLAN ESSID:** It will show the ESSID of Public Zone.
- **Wireless Key:** It will show the wireless key that was configured in Public Zone settings.
- **Currency:** Select the desired currency unit for charged internet access.
- **Remaining Reminder:** Enable it and input the count-down minute, system will remind users that their quota will run out soon when their quota reaches this time. The remaining message will not show up if the Remaining Reminder time is configured longer than the quota of billing plans.
- **Sync Interval:** Select the desired interval for on-demand user quota update. The quota information, i.e. remaining time or remaining quota displayed on the on-demand user login success page will be refreshed according to the time interval configured here.

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 checked="" type="radio"/> None <input type="radio"/> Uploaded Image <input type="button" value="Edit"/>
Number of Tickets	<input checked="" type="radio"/> 1 <input type="radio"/> 2

- **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:** There are 3 receipt footers supported by the system. The entered content will be printed on the receipt. These footers are optional.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose none. Click **Edit** 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.
- **Number of Tickets:** Enable this function to print duplicate receipts. Another Remark field will appear when the Number of Ticket is selected to 2 and the content will appear at the bottom of the 2nd duplicate receipt.
- **Preview:** Click **Preview** button, the ticket will be shown including the information of username and password with the selected background. You can also print the ticket here.

3) Billing Plans

Administrators can configure several billing plans. Click **Edit** button to enter the page of **Editing Billing Plan**. Configure billing plans with desired account type, expiration date, price, etc. Click **Apply** to save the plan. Go back to the screen of **Billing Plans**, check the **Enable** checkbox or click **Select all** button, and then click **Apply**, the plan(s) will be activated.

Billing Plans					
Plan	Account Type	Quota	Price	Enable	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	<input checked="" type="checkbox"/>	Edit
2	Usage-time	11 min(s) connection time quota	1	<input checked="" type="checkbox"/>	Edit
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	<input checked="" type="checkbox"/>	Edit
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	<input checked="" type="checkbox"/>	Edit
5	N/A			<input type="checkbox"/>	Edit
6	N/A			<input type="checkbox"/>	Edit
7	N/A			<input type="checkbox"/>	Edit
8	N/A			<input type="checkbox"/>	Edit
9	N/A			<input type="checkbox"/>	Edit
0	N/A			<input type="checkbox"/>	Edit

- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan, based on which it defines how the account can be used including Usage-time, Volume, Hotel Cut-off and Duration-time.
- **Quota:** The limit on how On-demand users are allowed to access the network.
- **Price:** The unit price charged for buying an account from this billing plan.
- **Enable:** Check the checkbox to activate the plan.
- **Function:** Click the button **Edit** to add one billing plan. For detailed information regarding on-demand accounts and billing plan configuration, please refer to **Appendix E, On-demand Account types & Billing Plan**.

4) External Payment Gateway

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

The options are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** or **Disable**. For detailed parameter descriptions please refer to **Appendix F, External Payment Gateways**.

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

5) Terminal Server

Terminal Server 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 process. Enter the device IP into server IP field.

Terminal Server Configuration				
Item	Server IP	Port	Location	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

6) On-demand Account Creation

After at least one billing plan is enabled, the administrator can generate single on-demand user accounts here. Click this to enter the On-demand Account Creation page. Click on the **Create** button of the desired plan to create an on-demand account. The username and password of to be created on-demand account is configurable. Select **Manual created** in Username/Password Creation and then administrator can enter desired username and password for the on-demand account. In addition, an External ID such as student's school ID can be entered together with account creation.

After the account is created, you can click **Printout** to print a receipt which will contain the on-demand user's information, including the username and password to a network printer.

Moreover, you can click **Send to POS** to print a receipt by a POS device.

Note:

If no Billing plan is enabled, accounts cannot be created by clicking **Create** button. Please go back to Billing Plans to activate 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	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	<button>Create</button>
2	Usage-time	11 min(s) connection time quota	1	Enabled	<button>Create</button>
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	<button>Create</button>
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	<button>Create</button>
5	N/A	N/A	N/A	Disabled	<button>Create</button>
6	N/A	N/A	N/A	Disabled	<button>Create</button>
7	N/A	N/A	N/A	Disabled	<button>Create</button>
8	N/A	N/A	N/A	Disabled	<button>Create</button>
9	N/A	N/A	N/A	Disabled	<button>Create</button>
0	N/A	N/A	N/A	Disabled	<button>Create</button>

- **Plan:** The number of a specific plan.
- **Account Type:** Show account type of the plan in Usage-time. Duration-time or Hotel Cut-off.
- **Quota:** The total time amount or period on how On-demand users are allowed to access the

network. For Time users, it is the total time. For Volume users, it is the total amount of traffic.

- **Price:** For each plan, this is the unit price charged for an account.
- **Status:** Show the status in enabled or disabled.
- **Function:** Press **Create** button for the desired plan; and Creating an On-demand Account will appear for creation.

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create



Creating an On-demand Account	
Plan : Account Type	2 : Usage-time
Quota	11 min(s) connection time quota
Username/Password Creation	System created ▾
Account Activation	First time login must be done within 1 hour(s)
Total Price	1
Reference	<input type="text" value="this is a ref"/> <small>Add a reference related to this account (for example, the customer's name)</small>
External ID	<input type="text"/> <small>Enter an external ID such as Library ID No.</small>
Please confirm the information and press Create button to create an account.	

Create

Cancel

7) On-demand Account Batch Creation

After at least one billing plan is enabled, the administrator can generate multiple on-demand user accounts at once with batch creation. Click **Create** button to enter the On-demand Account Batch Creation. Enter the desired number of accounts of enabled plans to create a batch of on-demand accounts together. The Number of Accounts field of disabled plans will not be able to enter any number. The sum of all Number of Accounts will be constrained and will not accept a number over the available account limits in database. Click **Create** button to start batch creation. Next page will show Success or Failed message to indicate the batch creation status. Once creation is successful, all created accounts can be exported to a text file for extended usage. Moreover, you can click **Send to POS** to print a receipt to a POS device via Serial or Ethernet network. Please notice that it takes time if you create lots of on-demand accounts by batch creation.

On-demand Account Batch Creation				
Plan	Account Type	Quota	Price	Number of Accounts
1	Usage-time	15 min(s) connection time quota with expiration	10.91	<input type="text"/>
2	Usage-time	11 min(s) connection time quota	1	<input type="text"/>
3	Hotel Cut-off	Valid until 12:00 the following day	5	<input type="text"/>
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	<input type="text"/>
5	N/A			<input type="text"/>
6	N/A			<input type="text"/>
7	N/A			<input type="text"/>
8	N/A			<input type="text"/>
9	N/A			<input type="text"/>
0	N/A			<input type="text"/>

- **Plan:** The number of a specific plan.
- **Account Type:** Show account type of the plan in Usage-time, Duration-time or Hotel Cut-off.
- **Quota:** The total time amount, interval or traffic volume on how On-demand users are allowed to access the network.
- **Price:** For each plan, this is the unit price charged for an account.
- **Number of Accounts:** The desired number of accounts to be created from the plan.

8) On-demand Account List

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

On-demand Account List						
Username	Password	Remaining Quota	Status	External ID	Reference	<input type="button" value="Delete All"/>
7k3t	g3x5fum4	11 min(s)	Normal		New York branch	Delete
gc29	6ey68m44	Until 2010/06/16-12:30	Normal		Boston Branch	Delete

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

- **Search:** Enter a keyword of a username, External ID, or reference, to be searched in the text filed and click this button to perform the search. All usernames, External ID, 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 that the account can

continue to use to access the network.

- **Status:** The status of the account.
 - **Normal:** the account is not currently in use and has not exceeded the quota limit.
 - **Online:** the account is currently in use.
 - **Expired:** the account is not valid any more, even if there is remaining quota left.
 - **Out of Quota:** the account has exceeded the quota limit.
 - **Redeemed:** the account has been applied for account renewal.
- **External ID:** This is an additional information field for combined with a unique account only, for example the customer's name or social security number etc.
- **Reference:** Any other additional information, for example venue where the account is generated etc.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

9) Redeem On-demand Accounts



For Usage-time accounts, when the remaining quota is insufficient or if they are almost out of quota, they can use redeem function to extend their quota. After the user has got, or bought a new account, they just need to click the **Redeem** button in the login success page to enter Redeem Page, input the new account **Username** and **Password** and then click **Submit**. This new account's quota will be extended to the original account. However, Redeem function can only be used to with same billing type accounts only, i.e. Volume accounts can only be redeemed with another Volume account and so on.

The image shows a web interface for redeeming. At the top, there is a red header bar with the '4ipnet' logo on the left and the word 'Redeem' on the right. Below the header, the page has a white background. In the center, it says 'Welcome to Redeem Page' in a bold, orange-brown font. Underneath this, in a smaller grey font, it says 'Please enter the username and password to Redeem.' There are two input fields: 'Username:' followed by a white text box, and 'Password:' followed by a white text box. Below these fields are two yellow buttons with black text: 'Enter' and 'Cancel'.**Note:**

The maximum quota is 365dys 23hrs 59mins 59secs" even after redeem. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

Note:

Duration-time and Hotel Cut-off type do not support redeem function.

5.2 User Login

5.2.1 Default Authentication

There are different types of authentication database (LOCAL, RADIUS and ONDEMAND) that are supported by the system. Only Public Zone can set authentication.

A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. Bob@local or Tim@radius1 etc.) when multiple options are concurrently in use. One of the authentication options can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "local" is the postfix of the default option, then user with username Bob can login as "Bob" without having to type in "Bob@local".

Authentication Settings					
Authentication Required For the Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Authentication Options	Auth Server	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	RADIUS	radius1	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	RADIUS	radius2	<input type="radio"/>	<input checked="" type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>

5.2.2 Login with Postfix

For each authentication option, set a postfix that is easy to distinguish (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.

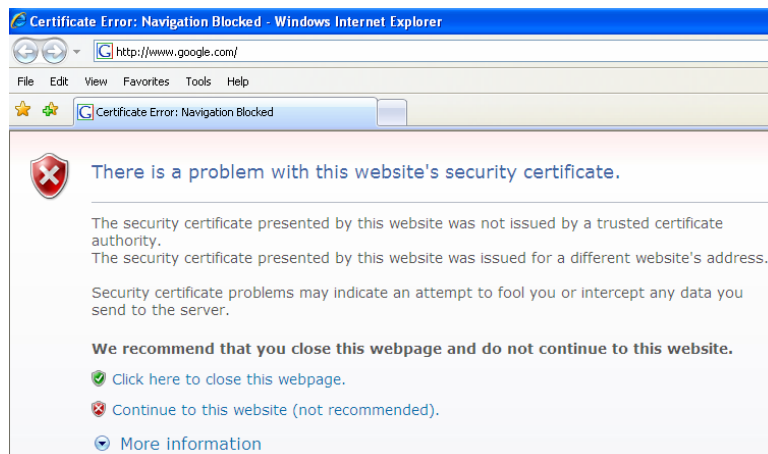
Beside the Default Authentication, all other authentication server users logging into to system, the username must contain the postfix to identify the authentication option this user belongs to.

Authentication Settings					
Auth Database	Auth Server Name	Postfix	Policy	Black List	Configure
LOCAL	<input type="text" value="Server 1"/>	<input type="text" value="local"/>	Policy 1 ▾	None ▾	<input type="button" value="Configure"/>
RADIUS	<input type="text" value="Server 2"/>	<input type="text" value="radius1"/>	Policy 2 ▾	None ▾	<input type="button" value="Configure"/>
RADIUS	<input type="text" value="Server 3"/>	<input type="text" value="radius2"/>	Policy 3 ▾	None ▾	<input type="button" value="Configure"/>
ONDEMAND	<input type="text" value="On-demand User"/>	<input type="text" value="ondemand"/>	Policy 4 ▾	None ▾	<input type="button" value="Configure"/>

5.2.3 An Example of User Login

Normally, users will be authenticated before they get network access through HSG200. This section presents the basic authentication flow for end users. Please make sure that the HSG200 is configured properly and network related settings are done.

1. Connect a client PC to Public Zone of HSG200. 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 HSG200 is not using a trusted SSL certificate, there will be a "Certificate Error", because the browser treats HSG200 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 store the username and password on the current computer in order to automatically login to the system at the next login. Then, click the **Submit** button.

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



The screenshot 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 yellow buttons: "Login" and "Remaining". At the bottom of the form, there is a checkbox labeled "Remember Me" which is checked.

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



The screenshot shows the 4ipnet Login Success 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 speech bubble containing the text: "Hello, you are logged in via test@local". Below the speech bubble, there is a line of text: "To log out, please click the 'Logout' button." and another line of text: "Login time: 2009-06-02 11:26". At the bottom right of the page, there is a yellow button labeled "Logout".

6 Restrain the Users

6.1 Black List

Configure Black List, go to: **Users >> Black List**.

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

Black List Settings		
Select Black List	1:Blacklist1 ▼	
Name	Blacklist1	
Username	Remark	Delete
(Total:0) First Prev Next Last		
Add User(s)		

- **Select Black List:** There are 5 black list profiles available for utilization.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User(s):** Click the **Add User(s)** button to add users to the selected black list.

Adding User(s) to Blacklist1		
No.	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

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

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

Black List Settings		
Select Black List	1:Blacklist1 ▾	
Name	Blacklist1	
Username	Remark	Delete
blackuser		<input checked="" type="checkbox"/>

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

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

After the Black List editing is completed. You can select the Black List in each Authentication Server to let it to become effective.

Authentication Settings					
Auth Database	Auth Server Name	Postfix	Policy	Black List	Configure
LOCAL	Server 1	local	Policy 1 ▾	None ▾	Configure
RADIUS	Server 2	radius1	Policy 2 ▾	None ▾	Configure
RADIUS	Server 3	radius2	Policy 3 ▾	None ▾	Configure
ONDEMAND	On-demand User	ondemand	Policy 4 ▾	None ▾ 1:Blacklist1 2:Blacklist2 3:Blacklist3 4:Blacklist4 5:Blacklist5	Configure

[Apply](#) [Cancel](#)

6.2 MAC Address Control

Configure MAC Address Control, go to: **Users >> Additional Control**.

Additional Control	
User Session Control	Idle Timeout (minutes): <input type="text" value="10"/> *(1-1440) Multiple Login <input type="checkbox"/> (Authentication option using On-demand database will not support this function.)
Built-in RADIUS Server Settings	Session Timeout (minutes): <input type="text" value="120"/> *(5-1440) Idle Timeout (minutes): <input type="text" value="10"/> *(1-120) Interim Update (minutes): <input type="text" value="5"/> *(1-120)
Upload File	Certificate Upload
MAC ACL	Edit (Control list to manage which client devices are allowed to access the login page)
SMTP Port Forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

MAC ACL: With this function, only the users with their MAC addresses in this list can login to HSG200. There are 40 users maximum allowed in this MAC address list. User authentication is still required for these users. Click **Edit** to enter the **MAC Address Control** list. Fill in these MAC addresses, select **Enable**, and then click **Apply**.

Access Control List			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
No.	MAC Address	No.	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

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

Caution:

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

6.3 Policy

Configure Policy, go to: **Users >> Policy**.

HSG200 supports multiple Policies, including one **Global Policy** and 5 individual **Policy**.

Global Policy is the system's universal policy and applied to all clients unless they are bounded by another policy. Individual Policy can be defined and applied to different authentication server. The client login with this authentication server will be bound by the corresponding Policy, if for an authentication server no policy is applied, its users will be governed by the Global Policy.

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

Global Policy

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

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

- **Select Policy:** Select the desired policy profile to configure.
- **Firewall Profile:** Global policy and policy 1 ~ 5 all have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client belonging to this group.

Policy 1 ~ Policy 5

Beside **Global Policy**, **Policy1** to **Policy5**, each consists of access control profiles that can be configured respectively and applied to a certain authentication server or user.

Policy Configuration - Policy 1	
Select Policy	Policy 1 ▼
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Maximum Concurrent Sessions	500 ▼ (sessions per user)

- **Select Policy:** Select the desired policy profile to configure.
- **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 a desired IP address can be defined in a policy. When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied with this policy are only allowed to login the system at the time which is checked in Schedule profile settings.
- **QoS Profile:** QoS profile defines the traffic class for the users governed by this Policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client belonging to this group.

6.3.1 Firewall

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

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

1) 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
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP; Type: Any, Code: Any	<input type="checkbox"/>
5	FTP	TCP/UDP; Destination Port: 20;21	<input type="checkbox"/>
6	HTTP	TCP/UDP; Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP; Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP; Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP; Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP; Destination Port: 67;68	<input type="checkbox"/>
			<input type="button" value="Add"/> <input type="button" value="Delete"/>
(Total: 27) First Prev Next Last			

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

Caution:

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"/>

2) Firewall 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.

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

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

Selecting the Filter Rule Number 1 as an example:

Policy 1 - Edit Filter Rule			
Rule Number	1		
Rule Name	<input type="text"/>		
Source		Destination	
Interface/Zone	ALL ▾	Interface/Zone	ALL ▾
IP Address ▾	<input type="text" value="0.0.0.0"/>	IP Address ▾	<input type="text" value="0.0.0.0"/>
Subnet Mask	0.0.0.0 (/0) ▾	Subnet Mask	0.0.0.0 (/0) ▾
MAC Address	<input type="text"/>		
Service Protocol	ALL ▾		
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**, **WAN**, **Public** and **Private** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Name filtering is supported but Domain Host 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:** These 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.

6.3.2 Routing

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

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"/>
3	<input type="text"/>	255.255.255.255 (/32) ▾	<input type="text"/>
4	<input type="text"/>	255.255.255.255 (/32) ▾	<input type="text"/>

Policy 1 - Specific Default Route			
Enable <input type="checkbox"/> 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"/>
3	<input type="text"/>	255.255.255.255 (/32) ▾	<input type="text"/>
4	<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 have just been 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.

2) Default Gateway

- **Default Gateway:** The default gateway of 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"/> IP Address: <input type="text"/>

- **Enable:** Check **Enable** box to activate this function or uncheck to inactivate it.
- **Default Gateway IP Address:** You may need to fill the IP address of the default gateway.

6.3.3 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"/>

6.3.4 QoS Profile

For certain applications or users that need stable bandwidth or traffic priority, Policy 1 to 5 allows defining the QoS profile for the users governed by this Policy.

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

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

6.3.5 Session Limit

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

Policy Configuration - Policy 1	
Select Policy	Policy 1 ▼
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Maximum Concurrent Sessions	500 ▼ (sessions per user)

- The maximum number of concurrent sessions including 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 (a choice of Unlimited, 10, 25, 50, 100, 200, 350 and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a SYSLOG server.
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

7 Access Network without Authentication

7.1 DMZ

Configure DMZ, go to: **Network >> Network Address Translation >> DMZ (Demilitarized Zone)**.

The screenshot shows the 'Network Address Translation' configuration page. The 'DMZ (Demilitarized Zone)' tab is selected and highlighted with a red box. Other tabs include NAT, Privilege, Monitor IP, Walled Garden, Walled Garden Ad List, DDNS, and Client Mobility. Below the tabs, there are links for 'Public Accessible Server' and 'Port and IP Redirect'.

There are 20 sets of static Internal IP Address and External IP Address available. Enter **Internal** and **External** IP Address as a set. After the setup, accessing the External IP address listed in DMZ will be mapped to accessing the corresponding Internal IP Address. These settings will become effective immediately after clicking the **Apply** button. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN) that will change dynamically if WAN Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN interface.

Automatic WAN IP Assignment		
Enable	External IP Address	Internal IP Address
<input type="checkbox"/>	10.2.3.70	<input type="text"/>

DMZ (Demilitarized Zone)		
Item	External IP Address	Internal IP Address
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"/>

7.2 Virtual Server

Configure Virtual Server, go to: **Network >> Network Address Translation >> Public Accessible Server**.

NAT
Privilege
Monitor IP
Walled Garden
Walled Garden Ad List
DDNS
Client Mobility

Network Address Translation

[DMZ \(Demilitarized Zone\)](#)

[Public Accessible Server](#)

[Port and IP Redirect](#)

This function allows the administrator to set 20 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. Select **"TCP"** or **"UDP"** for the service's type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the **Apply** button.

Public Accessible Server					
No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

(Total:20) [First](#) [Prev](#) [Next](#) [Last](#)

7.3 Privilege List

Configure Privilege List, go to: **Network >> Privilege**

Setup the **Privilege IP Address List** and **Privilege MAC Address List**. The clients accessing the internet via IP addresses and/or networking devices in the list can access the network without any authentication.

Privilege List
IP Address List
MAC Address List

7.3.1 Privilege IP

Privilege IP Address List

Configure Privilege IP Address List, go to: **Network Configuration >> Privilege >> IP Address List**.

If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in the **"Granted Access by IP Address"**. The **"Remark"** field is not necessary but is useful to keep track. HSG200 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

Granted Access by IP Address		
No.	IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<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"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

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

Caution:

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

7.3.2 Privilege MAC

Privilege MAC Address List

In addition to the Privilege IP List, MAC address List allows the MAC address of the workstations that need to access the network without authentication to be set in the **“Granted Access by MAC Address”**. HSG200 allows 100 privilege MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking **Apply**.

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"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

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

Caution:

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

7.4 Disable Authentication in Public Zone

Configure Disable Authentication in Public Zone, go to: **System >> Zones Configuration**, click **Configure** in **Public Zone**.

General
WAN Configuration
WAN Traffic
Zone Configuration

Zone Settings				
Name	ESSID	Wireless Security	Default Authen Option	Details
Private		None	N/A	Configure
Public		None	Server 1	Configure

Authentication Settings					
Authentication Required For the Zone		<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Authentication Options	Auth Server	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	RADIUS	radius1	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	RADIUS	radius2	<input type="radio"/>	<input checked="" type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>

- **Authentication Required For the Zone:** When it is disabled, users will not need to authenticate before they get access to the network within Public Zone.

8 User 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) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

HTTP Protected Login function will let the client's login with https for more security. Enable to activate https (encryption) or disable to activate http (non encryption) login page.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway *
Internal Domain Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="http://www.google.com"/> *(e.g. http://www.google.com)
User Log Access IP Address	<input type="text"/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
HTTPS Protected Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time	System Time : 2010/06/17 09:34:54 Time Zone : <input type="text" value="(GMT+08:00)Taipei"/> <input type="button" value="v"/> <input checked="" type="radio"/> NTP NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil) NTP Server 2: <input type="text" value="tock.stdtime.gov.tw"/> <input type="radio"/> Manually set up

8.1.2 Internal Domain Name with Certificate

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

Internal Domain Name is the domain name of the HSG200 as seen on client machines connected under zone. It must conform to FQDN (Fully-Qualified Domain Name) standard. A user on client machine can use this domain name to access HSG200 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.

The screenshot shows the 'General Settings for the Entire System' configuration page. At the top, there are tabs for 'General', 'WAN Configuration', 'WAN Traffic', and 'Zone Configuration'. The 'General' tab is selected. Below the tabs, there is a table with two rows. The first row is labeled 'System Name' and contains a text box with the value 'Wireless Hotspot Gateway' and a red asterisk. The second row is labeled 'Internal Domain Name' and contains a text box with a red asterisk. To the right of the 'Internal Domain Name' text box is a checkbox labeled 'Use the name on the security certificate'. Below the 'Internal Domain Name' text box, there is a red note: '(FQDN of this device for internal use, e.g. controller.office-name.com)'.

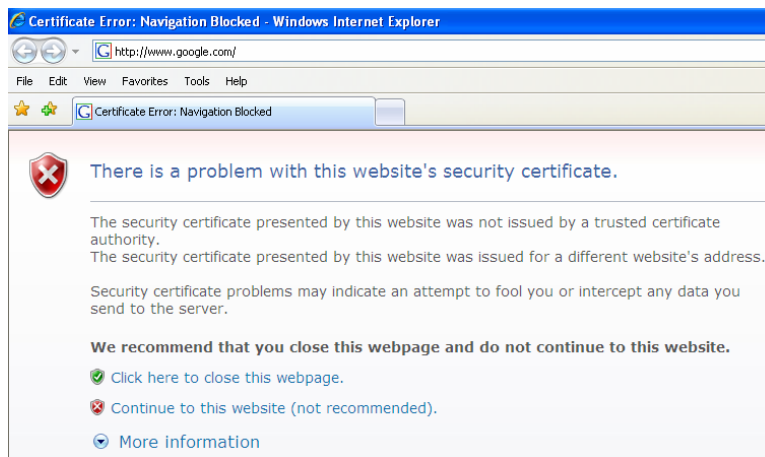
To Configure Certificate, go to: **Users >> Additional Control >> Upload File**.

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

If you already have a SSL Certificate, please Click Browse to select the file and upload it. Click **Apply** to complete the upload process. If you do not have a valid SSL Certificate, use the system default certificate.

The screenshot shows the 'Upload Certificate' configuration page. At the top, there are tabs for 'Authentication', 'Black List', 'Policy', and 'Additional Control'. The 'Additional Control' tab is selected. Below the tabs, there is a table with three rows. The first row is labeled 'Private Key' and contains a text box and a 'Browse...' button. The second row is labeled 'Customer Certificate' and contains a text box and a 'Browse...' button. The third row is labeled 'Certification Path Verification' and contains two radio buttons: 'Enable' and 'Disable'. Below the table, there is a button labeled 'Use Default Certificate'.

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.

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

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. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and click **Apply** to save the settings.

Walled Garden List			
No.	Domain Name/IP Address	No.	Domain Name/IP Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

8.1.4 Walled Garden AD List

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

This function provides advertisement links to web pages for users to access free of charge 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	Topic	Description	Display
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- Enter all items or make changes, click **Apply**, the items will be added and shown in the list.
- **URL:** Enter the URL of the advertisement website.
- **Topic:** Enter the content of the hyperlink, for instance if you enter Google in this field, on the user login page a hyperlink [Google](#) will be displayed.
- **Description:** Any additional message for administrator's reference.
- **Display:** Choose **Display** to display advertisement hyperlinks on the login pages

8.2 After User Login

8.2.1 Portal URL after successful login

Configure Portal URL after a successful user login, go to: **System >> General**.

When this function is enabled, enter the URL of a Web server as the Portal page. Once logged in successfully, users will be directed to this URL, such as *http://www.google.com*, regardless of the original homepage set in their browsers.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway *
Internal Domain Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text"/> *(e.g. http://www.google.com)
User Log Access IP Address	<input type="text"/> (e.g. 192.168.2.1)

When this function is disabled, after users logged in successfully, users will be directed to the original homepage set in their browsers.

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"/> *(1-1440)
	Multiple Login <input type="checkbox"/> (Authentication option using On-demand database will not support this function.)

8.2.3 Multiple Login

Configure Multiple Login, 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"/> *(1-1440)
	Multiple Login <input checked="" type="checkbox"/> (Authentication option using On-demand database will not support this function.)

9 Networking Features of a Gateway

9.1 IP Plug and Play

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

HSG200 supports IP PNP function. User can login and access network with any IP address setting. This function is disabled in default settings.

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

When **IP PNP** is enabled, at the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is using, authentication can still be performed through HSG200.

9.2 Dynamic Domain Name Service (DDNS)

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. HSG200 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access HSG200'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>.

9.3 Port and IP Redirect

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

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

Port and IP Redirect					
No.	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

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

10 System Management and Utilities

10.1 System Time

Configure System Time, go to: **System >> General**.

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).

Manually set up is another option to setup system time, if you choose to setup system time manually, please enter the Year, Month, Day, the current time and click Apply to activate the changes.

Time	System Time : 2010/06/17 10:41:24	
	Time Zone :	
	<input type="text" value="(GMT+08:00)Taipei"/> ▼	
	<input checked="" type="radio"/> NTP	
	NTP Server 1:	<input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil)
	NTP Server 2:	<input type="text" value="tock.stdtime.gov.tw"/>
	<input type="radio"/> Manually set up	

Note:

When system can not sync the time with NTP server, all clients will not allow to login to system. Also on-demand accounts cannot be created.

10.2 Management IP

Configure Management IP, go to: **System >> General**.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway *
Internal Domain Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text"/> *(e.g. http://www.google.com)
User Log Access IP Address	<input type="text"/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Only PCs within the Management IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, he or she can access the web management page.

Management IP Address List			
No.	IP Address/Segment	No.	IP Address/Segment
1	<input type="text" value="0.0.0.0/0.0.0.0"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

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.

10.3 User Log Access IP Address

Configure User Log Access IP History, go to: **System >> General**.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway *
Internal Domain Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="http://www.google.com"/> *(e.g. http://www.google.com)
User Log Access IP Address	<input type="text" value=""/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List

Specify an IP address of the administrator's computer or a billing system to get billing history information of HSG200 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
1	2005-02-17 18:09:03 +0800	LOGIN	aaa@w1300.tw	192.168.30.189	00:0C:F1:28:BF:D8	0	0	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
1	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	0	0
2	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	0	0
3	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			

10.4 SNMP

Configure SNMP, go to: **System >> General**. HSG200 supports SNMP v1/v2c.

If this function is enabled, the SNMP Management IP and the Community string can be assigned for SNMP access to the system.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway *
Internal Domain Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="http://www.google.com"/> *(e.g. http://www.google.com)
User Log Access IP Address	<input type="text"/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <div style="border: 2px solid red; padding: 5px; margin-top: 5px;"> Manager IP Address: <input type="text"/> * Community: <input type="text"/> * </div>

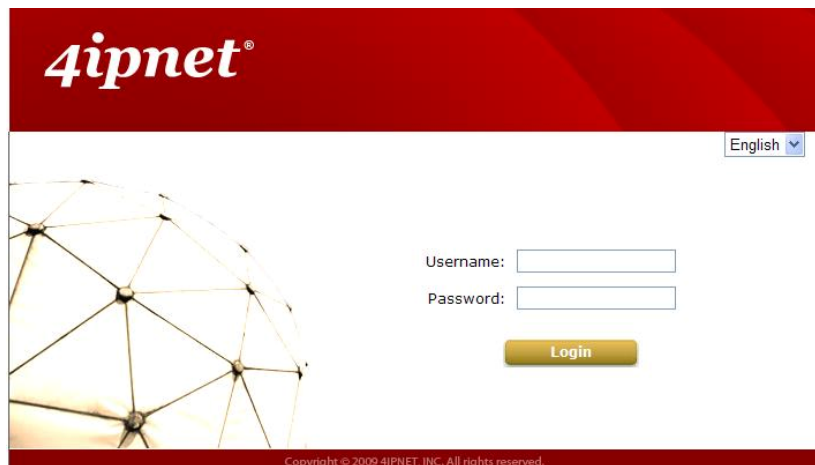
10.5 Three-Level Administration

HSG200 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

Admin: The administrator can access all configuration pages of HSG200.

Username: **admin**

Password: **admin**



After a successful login to HSG200, a web management interface with a Home manual will appear.



Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts.

User Name: **manager**

Password: **manager**

Authentication Settings					
Auth Database	Auth Server Name	Postfix	Policy	Black List	Configure
LOCAL	Server 1	local	Policy 1 ▼	None ▼	Configure
RADIUS	Server 2	radius1	Policy 2 ▼	None ▼	Configure
RADIUS	Server 3	radius2	Policy 3 ▼	None ▼	Configure
ONDEMAND	On-demand User	ondemand	Policy 4 ▼	None ▼	Configure

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**

On-demand Account Creation					
Plan	Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Cut-off	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

Note:

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

10.6 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 HSG200.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts.

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. 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"/> *

Apply

Cancel

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

Apply

Cancel

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

Apply

Cancel

Caution:

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

10.7 Backup / Restore and Reset to Factory

Configure Backup / Restore and Reset to Factory Default, go to: **Utilities >> Backup & Restore**.

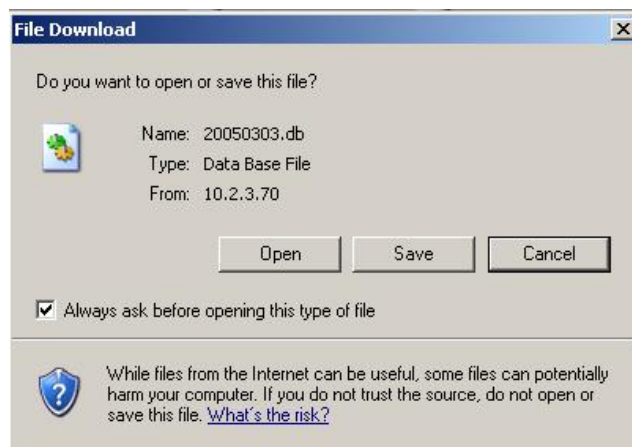
This function is used to backup/restore the HSG200 settings. Also, HSG200 can be restored to the factory default settings here.

Backup System Settings	
<div>Backup</div>	

Restore System Settings	
File Name	<input type="text"/> <div>Browse...</div>
<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 HSG200 and click **Restore** to restore to the same settings at the time when the backup file was saved.
- **Reset to Factory Default:** Click **Reset** to load the factory default settings of HSG200.

10.8 Firmware Upgrade

Configure Firmware Upgrade, go to: **Utilities** >> **System Upgrade**.

The administrator can download the latest firmware from website and upgrade the system here. Select the latest firmware with **Browse** button, then click **Apply**, the system will upload the file and restart to perform the upgrade process. It might take a few minutes before the upgrade process completes and the new firmware's WMI interface appears.

System Firmware Upgrade	
Current Version	1.00.00
Build	1.7-1.3224
File Name	<input type="text"/> <input type="button" value="Browse..."/>

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

Apply

Note:

After clicking **Apply**, the system will begin uploading the chosen firmware into the system. Once the upload process is complete system will restart to activate the new firmware. The entire process may take a few minutes until the new firmware WMI appears. When restart is complete, system will not lease IP. So, please use static IP PC to upgrade system firmware.

Caution:

1. Firmware upgrade may cause the loss of some data. You may need to manually backup user account information, please refer to the release notes for the limitation before upgrading.
2. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.

10.9 Restart

To perform system restart, go to: **Utilities >> Restart**.

This function allows the administrator to safely restart HSG200, and the process takes approximately three minutes. Click **YES** to restart HSG200; click **NO** to go back to the previous screen. Do NOT power off the power during system restart as this might damage the system. If the power needs to be turned off, it is highly recommended to restart HSG200 first and then turn off the power after completing the restart process.

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

YES

NO

Caution:

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

10.10 Network Utility

Configure Network Utility, go to: **Utilities >> Network Utilities**.

System provide some network utilities to allow administrators to use.

Wake-on-LAN is for waking up remote devices that supports Wake-on-LAN feature by entering the MAC address of the target device and then press **Wake Up** button.

Ping is to see whether a destination host is reachable and alive by entering the destination host's domain name or IP address and then press **Ping** button.

Trace Route display the actual route taken to reach the destination host by entering the destination host's domain name or IP address and then press **Start** button.

ARP Table for displaying ARP information stored on the system.

Network Utilities	
Wake-on-LAN	<input type="text"/> (MAC, e.g. XX:XX:XX:XX:XX:XX) <input type="button" value="Wake Up"/>
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"/>
ARP Table	<input type="button" value="Show"/>
Status	
Result	

10.10.1 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 LAN port. Enter the MAC Address of the desired device and click **Wake Up** button to execute this function.

10.10.2 Ping

It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.

10.10.3 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.

10.10.4 Show ARP Table

It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

10.11 Monitor IP Link

Configure Monitor IP Link, go to: **Network >> Monitor IP**.

HSG200 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 hyperlink if desired.

Monitor IP List				
No.	Protocol	IP Address	Hyperlink	Remark
1	http ▾	<input type="text"/>	Create	<input type="text"/>
2	http ▾	<input type="text"/>	Create	<input type="text"/>
3	http ▾	<input type="text"/>	Create	<input type="text"/>
4	http ▾	<input type="text"/>	Create	<input type="text"/>
5	http ▾	<input type="text"/>	Create	<input type="text"/>
6	http ▾	<input type="text"/>	Create	<input type="text"/>
7	http ▾	<input type="text"/>	Create	<input type="text"/>
8	http ▾	<input type="text"/>	Create	<input type="text"/>
9	http ▾	<input type="text"/>	Create	<input type="text"/>
10	http ▾	<input type="text"/>	Create	<input type="text"/>

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

10.12 Console Interface

Via the console port, administrators can enter the console interface for handling problems and situations occurred during operation.

1. In order to connect to the console port of HSG200, 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**.

Caution:

*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 HSG200 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, and 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.

```
Wireless Hotspot Gateway Basic Configuration
1. Utilities for network debugging
2. Change admin password
3. Reload factory default
4. Restart Wireless Hotspot Gateway
Please enter your choice:
```

- **Utilities for network debugging**

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

```
Wireless Hotspot Gateway Configuration Utility
1. Ping host(IP)
2. Trace routing path
3. Display interface settings
4. Display routing table
5. Display ARP table
6. Display system up time
7. Check service status
8. Set device into 'safe mode'
9. Synchronize clock with NTP server
10. Print the kernel ring buffer
11. Main menu
Please enter your choice:
```

- **Ping host (IP):** By sending ICMP echo request to a specified host and wait for the response to test the network status.

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

- **Change admin password**

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

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

Caution:

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 HSG200 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 HSG200**

Choosing this option will restart HSG200.

11 System Status and Reports

11.1 View the Status

This section includes **System**, **Interface**, **Routing Table**, **Online Users**, **User Log** and **E-mail & SYSLOG** to provide system status information and online user status.

11.1.1 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		1.00.00
System Name		Wireless Hotspot Gateway
Portal URL		http://www.google.com
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - On-demand User Log		N/A:N/A
Warning of Internet Disconnection		Fail
User Log	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
System Time	NTP Server	tock.stdtime.gov.tw
	Time	2010/06/17 16:17:19 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	168.95.1.1

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

<u>Item</u>		<u>Description</u>
Firmware Version		The present firmware version of HSG200
System Name		The system name. The default is HSG200
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.
Warning of Internet Disconnection		Show the status for the connection at WAN is normal or abnormal (Internet Connection Detection) and all online users are allowed/disallowed to log in the network.
User Log	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 user log information will be set.
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 login from the same local account.
DNS	Preferred DNS Server	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

11.1.2 Interface Status

View Interface Status, go to: **Status >> Interface**.

This section provides an overview of the interface for the administrator including **WAN**, **Zone Wireless General Settings**, **Zone - Private** and **Zone - Public**.

WAN		
General	MAC Address	00:1F:D4:00:51:53
	IP Address	10.26.1.151
	Subnet Mask	255.255.0.0
	Packets Out	5475
	Bytes Out	6304432
	Packets In	382007
	Bytes In	391014250
	Number of Sessions	3

Zone Wireless General Settings		
General	MAC Address	00:1F:D4:00:51:55
	Band	11ng
	Channel	1
	Transmit Power	High

Zone - Private		
General	Mode	NAT
	MAC Address	00:1F:D4:00:51:54
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
VAP 1	BSSID	00:1F:D4:00:51:55
	ESSID	W1110-Private
	Security Type	None
	Associated Clients	0

Zone - Public		
General	Mode	NAT
	MAC Address	00:1F:D4:00:51:54
	IP Address	192.168.11.254
	Subnet Mask	255.255.255.0
DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.11.1
	End IP Address	192.168.11.100
	Lease Time	1440 Min(s)
VAP 2	BSSID	06:1F:D4:00:51:55
	ESSID	W1110-2
	Security Type	None
	Associated Clients	0

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

<u><i>Item</i></u>		<u><i>Description</i></u>
WAN	MAC Address	The MAC address of the WAN port.
	IP Address	The IP address of the WAN port.
	Subnet Mask	The Subnet Mask of the WAN port.
	Packets Out/In	The total accumulated packets in/out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
	Bytes Out/In	The total accumulated bytes in/out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
	Number of Sessions	The sessions of WAN port.
Zone Wireless General Settings	MAC Address	The MAC address of the Wireless.
	Band	The current Band setting of Wireless.
	Channel	The current Channel setting of Wireless.
	Transmit Power	The current Transmit Power setting of Wireless.
Zone - General	Mode	The operation mode of the zone.
	MAC Address	The MAC address of the zone.
	IP Address	The IP address of the zone.
	Subnet Mask	The Subnet Mask of the zone.
Zone - DHCP	Status	Enable/disable stands for status of the DHCP server in this 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.
Zone - VAP	BSSID	The BSSID of this zone.
	ESSID	The ESSID of this zone.
	Security Type	The current security type of this zone.
	Associated Clients	The number of associated clients in this zone.

11.1.3 Routing Table

View System Status, go to: **Status >> Routing Table**.

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

Policy 1			
Destination	Subnet Mask	Gateway	Interface
Policy 2			
Destination	Subnet Mask	Gateway	Interface
Policy 3			
Destination	Subnet Mask	Gateway	Interface
Policy 4			
Destination	Subnet Mask	Gateway	Interface
Policy 5			
Destination	Subnet Mask	Gateway	Interface
Global Policy			
Destination	Subnet Mask	Gateway	Interface
System			
Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Private
192.168.11.0	255.255.255.0	0.0.0.0	Public
10.22.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	10.22.0.1	WAN

- **Policy 1~5:** Shows the information of the individual Policy from 1 to 5.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
 - **Destination:** The Destination IP address.
 - **Subnet Mask:** The Subnet Mask of the IP address range.
 - **Gateway:** The Gateway IP address of the interface.
 - **Interface:** Including **WAN**, **Private** and **Public**.

11.1.4 Current Users

View Current Users, go to: **Status >> Online Users**.

In this page, each online user's information including **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of **Kick Out**. Click **Refresh** to update the current users list.

Online Users List						
No.	Username		Pkts In	Bytes In	Idle (Sec.)	Kick Out
	IP Address	MAC Address	Pkts Out	Bytes Out		

Refresh

11.1.5 User Log

View User Log, go to: **Status >> User Log**.

This page is used to check the traffic history of HSG200. 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 last 2 calendar months.

User Log		
Date	Size (Byte)	
2009-04-22	65	
2009-04-23	65	
On-demand User Log		
Date	Size (Byte)	
2009-04-22	105	
2009-04-23	254	
Roaming Out User Log		
Date	Size (Byte)	
2009-04-22	106	
2009-04-23	106	
Roaming In User Log		
Date	Size (Byte)	
2009-04-22	112	
2009-04-23	112	
Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2009-04	1	Download

Caution:

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

If the **Receiver E-mail Address(es)** has been entered under the **E-mail & SYSLOG** page, the system will automatically send out these history information to that specified email address.

- **Primary User Log**

All user activities occur on the system within the nearest 72 hours excluding other user logs such as on-demand user log are recorded; in date and time order. 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.

- **On-demand User Log**

Each line is a on-demand user log record consisting of 14 fields, **Date**, **System Name**, **Type**,

Name, IP, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out, Activation Time, 1st Login Expiration Time, and Remark, of on-demand user activities.

- **Roaming Out User Log**

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 In User Log**

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.

11.1.6 Local User Monthly Network

View Local User Monthly Network Usage, go to: **Status >> User Log**.

- **Monthly Network Usage of Local User**

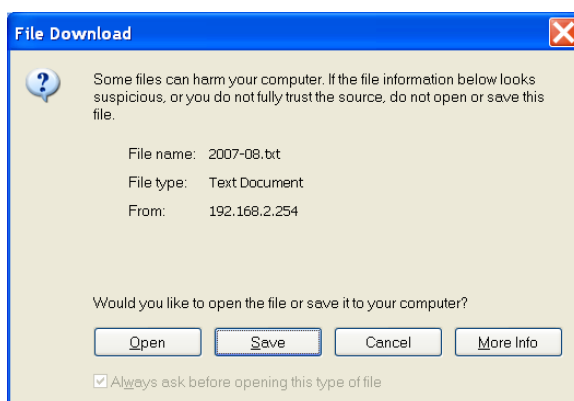
The system keeps a cumulated record of the traffic data generated by each Local user in the latest 2 calendar months. Each line in a monthly network usage of local user record consists of 6 fields, **Username**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out**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

- **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
2009-04	1	Download

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



11.2 Notification

Configure Notification, go to: **Status >> E-mail & SYSLOG**.

HSG200 can automatically send the notification of **Monitor IP Report**, **Users Log**, **On-demand User Log** and **Session Log** to up to 3 particular e-mail addresses. A trial email is provided by the system for validation.

Secondly, the system supports recording of **System Log**, **On-demand Users Log**, **Session Log** and **HTTP Web Log** via external SYSLOG servers.

Thirdly **Session Log** and **HTTP Web Log** can also be configured to be sent to an external FTP server.

In addition, **Event Log** section on WMI displays of clients associate and disassociate messages.

11.2.1 E-Mail

Configure Notification, go to: **Status >> E-mail & SYSLOG**.

- **Notification E-mail Settings:**

- **Receiver Email Address (es):** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Users Log, On-demand Users Log and Session Log, check the selection box to choose the type of notification to be sent.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Setting Test:** To test the settings immediately.
- **Sender Email 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:** 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.

Notification E-mail Settings				
Receiver E-mail Address(es)	Monitor IP Report	User Log	On-demand User Log	Session Log
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interval	1 Hour ▾	1 Hour ▾	1 Hour ▾	1 Hour ▾
SMTP Setting Test	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>	<input type="button" value="Send"/>
Sender E-mail Address	<input type="text"/>			
SMTP Server	<input type="text"/>			
SMTP Auth Method	None ▾			

11.2.2 SYSLOG

- **SYSLOG Server Settings:** There are 4 types of SYSLOG supported: **System Log**, **On-demand User Log**, **Session Log**, and **HTTP Web Log**. Enter the IP address and Port number to specify the SYSLOG server where the report should be sent to.

Except for System Log, each supported log may be assigned *Tag* info as well as SYSLOG standard attributes *Severity* and *Facility* to meet the filtering requirements on the SYSLOG Server. HTTP Web Log can further select which Service Zone Web interface information to log. For each type of log information, whenever an incident occurs and data is updated, the updated log will be immediately sent to the configured SYSLOG server.

SYSLOG Server Settings	
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"/>
System Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
On-demand User Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Tag: <input type="text"/> Severity: <input type="text" value="Emergency"/> Facility: <input type="text" value="local0"/>
Session Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Tag: <input type="text"/> Severity: <input type="text" value="Emergency"/> Facility: <input type="text" value="local0"/>
HTTP Web Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Tag: <input type="text"/> Severity: <input type="text" value="Emergency"/> Facility: <input type="text" value="local0"/> <div> <div>Logged Interface:</div> <div> <input type="checkbox"/> Private <input type="checkbox"/> Public </div> </div>

Note:

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

11.2.3 FTP

- FTP Server Settings:

FTP Server Settings	
FTP Destination	IP Address: <input type="text"/> Port : <input type="text"/> Anonymous <input checked="" type="radio"/> Yes <input type="radio"/> No FTP Setting Test <input type="button" value="Send Test Log"/>
Session Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Server Folder: <input type="text"/> ex: dir1/dir2 Interval 1 Hour*(Note: same as "Interval of Session Log" in the Notification E-mail Settings)
HTTP Web Log	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Server Folder: <input type="text"/> ex: dir1/dir2 Interval : 1 Hour <input type="button" value="v"/> Logged Interface: <input type="checkbox"/> Private <input type="checkbox"/> Public

- FTP Server Settings

FTP Destination: Configures the common settings of the FTP server that the logs will be sent to which includes the following:

- **IP Address/Port:** IP address and port number of FTP server.
- **Anonymous:** Check option "Yes" if the FTP server does not need ID credentials, otherwise check option "No" and fill in the necessary *Username* and *Password*.
- **FTP Setting Test:** To test the FTP settings correct or not.

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

- **Enable:** Decide whether or not to send Session Log file to the FTP Server configured in **FTP Destination**.
- **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.

HTTP Web Log: Records the URL of websites visited by users accessing the internet via HSG200.

- **Enable:** Decide whether or not to send HTTP Web Log file to the FTP Server configured in **FTP Destination**.
- **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.

- **Interval:** The time interval at which the Log will be sent.
- **Logged Interface:** The check box of Public or Private shall be checked to enable logging the HTTP Web Log of this interface.

11.2.4 Event Log

Event Log: The Event Log provides the system activities records. The administrator can monitor the system status by checking this log.

Event Log											
Aug 25	19:04:41	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:07	IEEE	802.11:	associated	
Aug 25	19:04:43	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:07	IEEE	802.11:	associated	
Aug 25	19:04:47	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:07	IEEE	802.11:	associated	
Aug 25	19:04:50	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:07	IEEE	802.11:	associated	
Aug 25	19:09:28	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:09	IEEE	802.11:	disassociated	
Aug 25	19:14:43	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:07	IEEE	802.11:	disassociated	
Aug 26	10:38:58	NAM	daemon.info	hostapd:	ath0ap1:	STA	00:24:2c:a7:18:d2	IEEE	802.11:	associated	
Aug 26	10:45:24	NAM	daemon.info	hostapd:	ath0ap1:	STA	00:24:2c:a7:18:d2	IEEE	802.11:	associated	
Aug 26	10:48:07	NAM	daemon.info	hostapd:	ath0ap1:	STA	00:24:2c:a7:18:d2	IEEE	802.11:	associated	
Aug 26	10:48:39	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:00	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:03	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:05	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:07	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:08	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:10	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	
Aug 26	10:49:16	NAM	daemon.info	hostapd:	ath0ap0:	STA	00:1f:d4:00:21:0d	IEEE	802.11:	associated	

In the log, normally, each line represents an event record which includes these fields:

- **Date/Time:** The time & date when the event happened
- **Hostname:** Indicate which host records this event. Note that all events in this page are local event, so the hostname in this field are all the same.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of this event.

12 Advanced Applications

12.1 Upload/Download Local Users Accounts

To Upload / Download Local Users Accounts, go to: **Users >> Authentication**, click **Configure** button of **Local**. Or click **Quick Links >> Local User Management** from system Home page.

- 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.

Local User Database Settings	
Local User List	
Account Roaming Out	<input type="radio"/> Enable <input checked="" 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.)

[Add User](#) [Upload User](#) [Download User](#)

[Search](#)

Local User List					
Username	Password	MAC Address	Applied Policy	Remark	Del All
u1	u1		None		Delete

(Total: 1/100) [First](#) [Prev](#) [Next](#) [Last](#)

Note 1: The format of each line is "Username, Password, MAC Address, Applied Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

Note 2: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.

Upload User from File	
File Name	<input type="text"/> 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 **Local** user account information and then save it on disk.

[Add User](#) [Upload User](#) [Download User](#)

[Search](#)

Local User List					
Username	Password	MAC Address	Applied Policy	Remark	Del All
u1	u1		None		Delete

(Total: 1/100) [First](#) [Prev](#) [Next](#) [Last](#)

Download User to File				
Username	Password	MAC Address	Applied Policy	Remark
user01	user01		1	

[Download](#)

12.2 RADIUS Advanced Settings

Configure RADIUS Advanced Settings, go to: **Users >> Authentication**. Click **Configure** of **RADIUS**.

➤ Complete vs. Only ID

For RADIUS authentication, there is an option to send the complete username with postfix or username only.

Username Format: When **Complete** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when **Only ID** option is checked, only the username will be transferred to the external RADIUS server for authentication.

➤ NAS Identifier

System will send this value to the external RADIUS server, if the external RADIUS server needs this.

➤ NAS Port Type

System will send this value to the external RADIUS server, if the external RADIUS server needs this.

➤ Class-Policy Mapping

This function is to assign a *Policy* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Policy.

RADIUS Policy Mapping - Server 2			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
No.	Class Attribute Value	policyName	Remark
1	<input type="text"/>	Policy 1 ▾	<input type="text"/>
2	<input type="text"/>	Policy 1 ▾	<input type="text"/>
3	<input type="text"/>	Policy 1 ▾	<input type="text"/>
4	<input type="text"/>	Policy 1 ▾	<input type="text"/>
5	<input type="text"/>	Policy 1 ▾	<input type="text"/>

12.3 Roaming Out

Configure local user Roaming Out, go to: **Users >> Authentication**, click **configure of Local**.

Under certain configurations, HSG200 can act as a RADIUS server for Roaming Out local user logged 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 *Roaming Out & 802.1X Client Device Settings* will be available to define the client device authorized to roam by entering the 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.)
Roaming Out & 802.1X Client Device Settings	

Roaming Out & 802.1x Client Device Settings				
No.	Type	IP Address	Subnet Mask	Secret Key
1	Roaming Out ▼	10.0.0.0	255.0.0.0 (/8) ▼	••••••••
2	Disable ▼		255.255.255.255 (/32) ▼	
3	Disable ▼		255.255.255.255 (/32) ▼	
4	Disable ▼		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 HSG200, setup it's RADIUS server to this HSG200 with same postfix, then the local user in this HSG200 can login success from another HSG200 by RADIUS authentication.

12.4 Customizable Pages

Configure Custom Pages, go to: **System >> Zone Configuration**, click **Configure** in **Public** zone.

There are several user login and logout pages that can be customized by the administrator.

You can select **Template Page** or **External Page**.

Custom Pages	Type : <input checked="" type="radio"/> Template Page <input type="radio"/> External Page	
	Color for Title Background :	<input type="text" value="728B99"/> Select (RGB values in hex mode)
	Color for Title Text :	<input type="text" value="F3F3F3"/> 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)
	Copyright :	<input type="text" value="Copyright ©"/>
	Logo Image File :	<input type="button" value="Preview and Edit the Image File"/>
	Login Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Logout Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Redeem Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Login Success Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Login Failed Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Logout Success Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Logout Failed Page	<input type="button" value="Configure"/> <input type="button" value="Preview"/>
	Disclaimer Page	Status: <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="button" value="Configure"/> <input type="button" value="Preview"/>

- **Template Page:**

To utilize the template user pages stored locally in the system, choose **Template Page** and configure the necessary settings as follows. Click **Select** hyperlink to pick up a color for each item and then fill in your copyright message. You can also upload a Logo image file for your template with the **Preview and Edit the Image File** button. Click the button of **Configure**, the setup page will appear for the corresponding page where you can change the text displayed as you wish. After finishing the setting, click **Preview** to see the result. If you are happy with the customized pages, click **Apply** to activate the changes made.

- **Disclaimer Page:**

- The **Disclaimer Page** is for the hotspot owner or MIS staff who want to display 'terms of use' or announcement information before the user login page. Click the button of **Configure**, the setup page will appear. An unauthorized client will receive a disclaimer page once opening the web browser. If a client select "I agree" and clicks "Next," then he or she will proceed to the User Login

Page for client to login with username and password.

- **External Page:**

Choose the **External Page** option if you wish to use user pages located on a designated website.

Click the button of **Configure** for each custom pages and enter the URL of its' corresponding external login page and then click **Apply**.

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

Appendix A. Network Configuration on PC & User Login

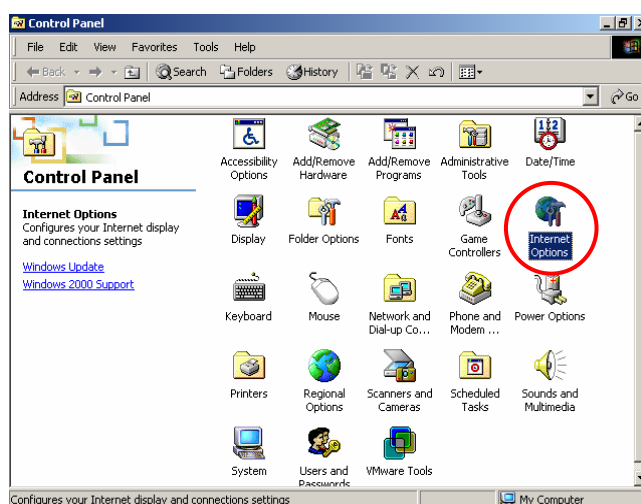
■ Network Configuration on PC

After HSG200 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

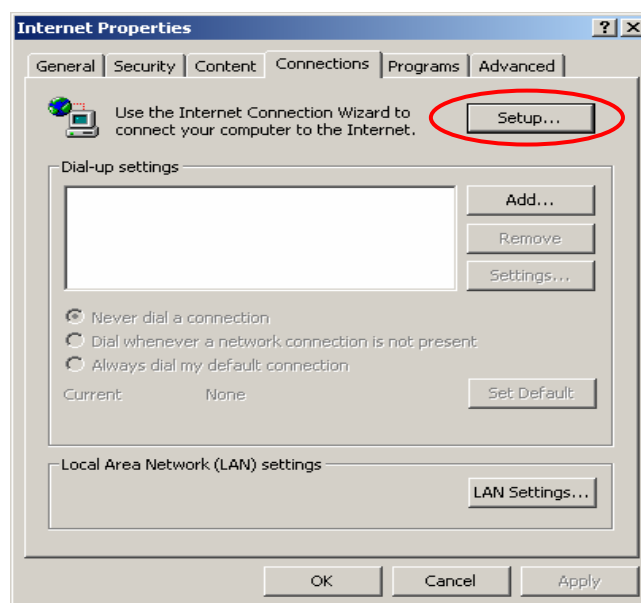
• Internet Connection Setup

■ Windows 9x/2000

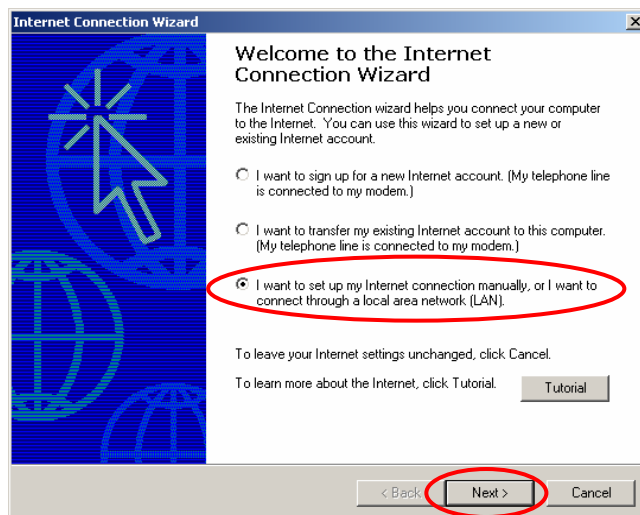
- 1) Choose **Start >> Control Panel >> Internet Options**.



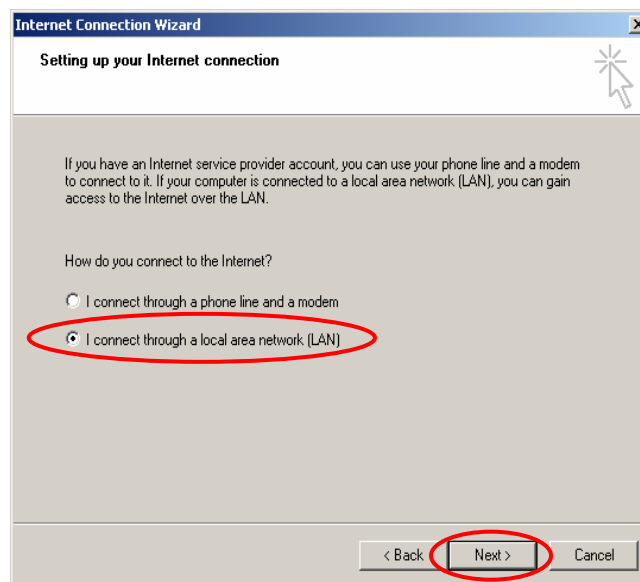
- 2) Choose the **Connections** tab, and then click **Setup**.



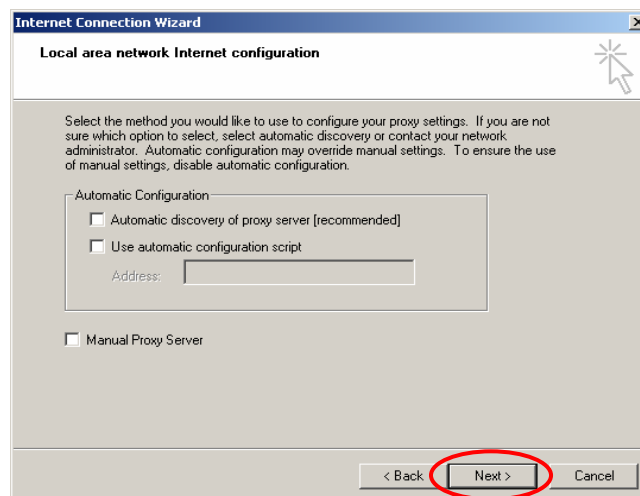
- 3) Choose “**I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)**”, and then click **Next**.



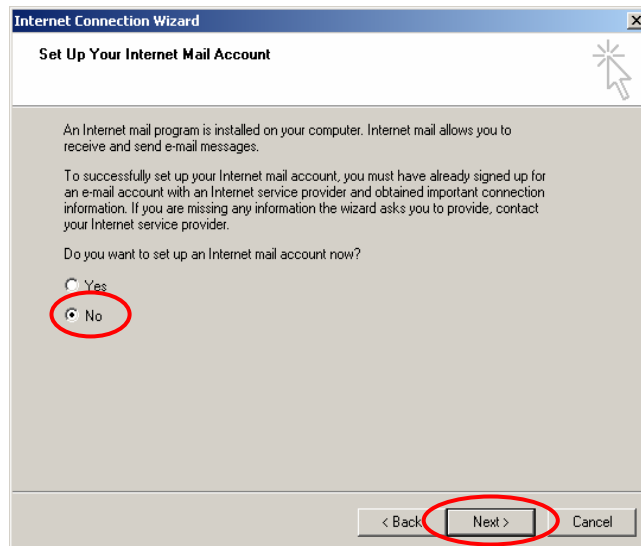
- 4) Choose “**I connect through a local area network (LAN)**” and then click **Next**.



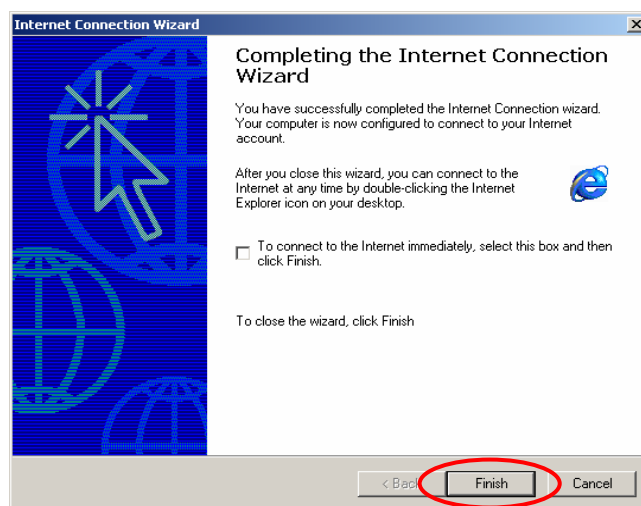
- 5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click **Next**.



6) Choose **"No"** and then click **Next**.

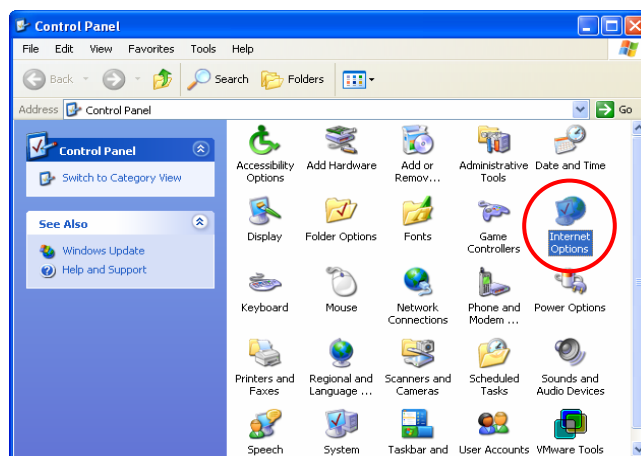


7) Finally, click **Finish** to exit the **Internet Connection Wizard**. Now, the set up is completed.

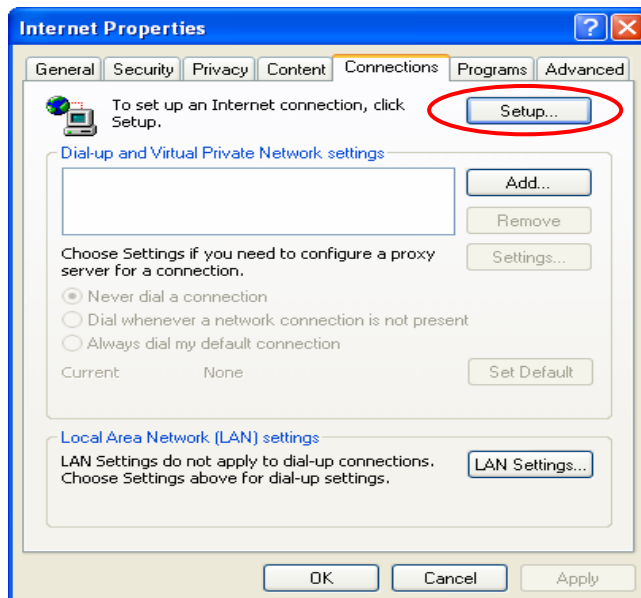


Windows XP

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



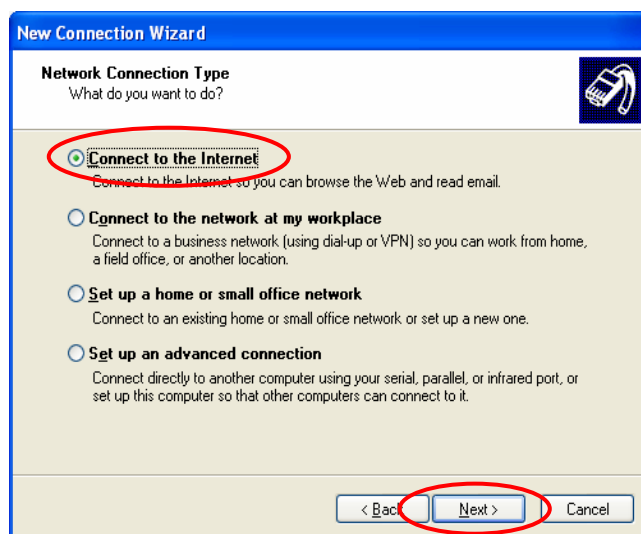
- 2) Choose the **Connections** tab, and then click **Setup**.



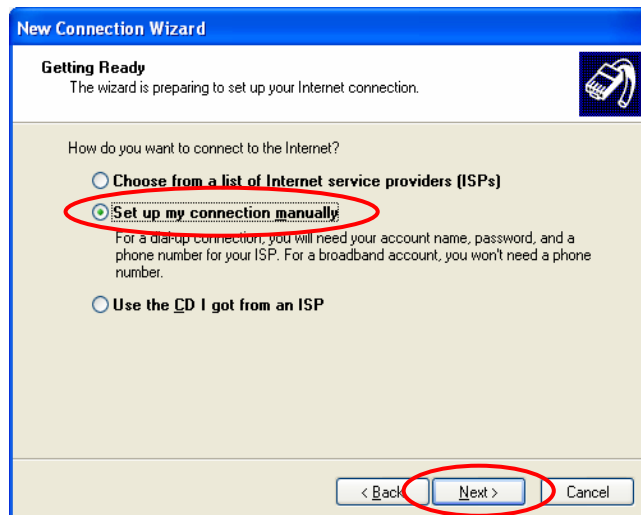
- 3) When the **Welcome to the New Connection Wizard** window appears, click **Next**.



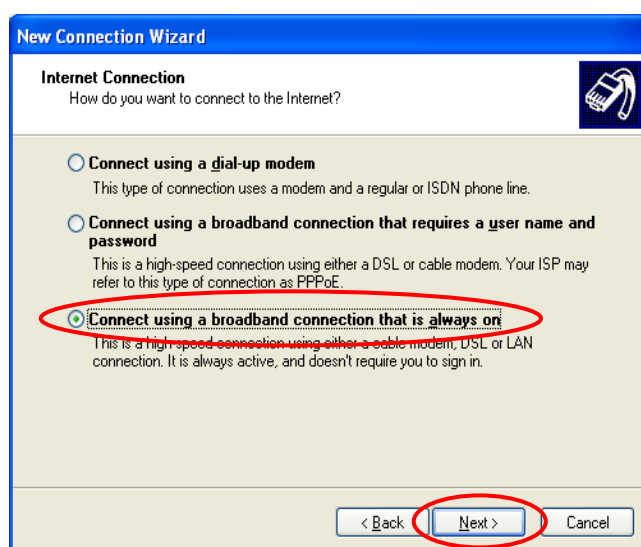
- 4) Choose **"Connect to the Internet"** and then click **Next**.



- 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.



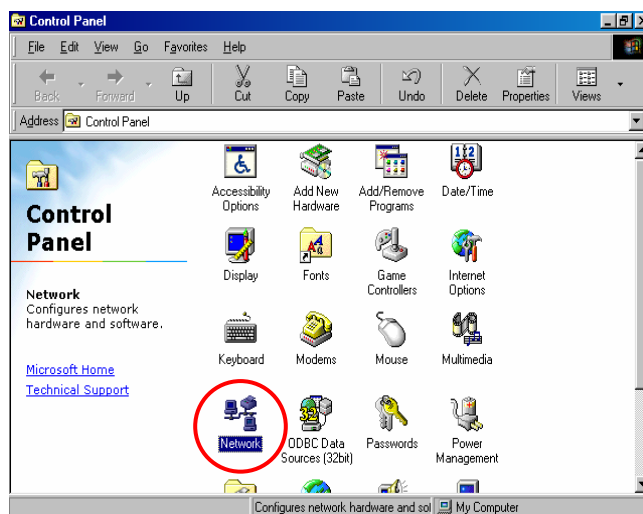
• TCP/IP Network Setup

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, HSG200 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”**.

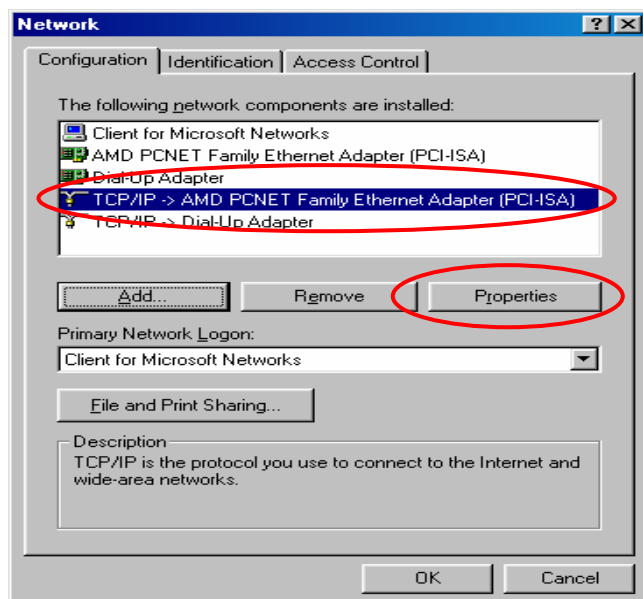
If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

▪ Check the TCP/IP Setup of Window 9x/ME

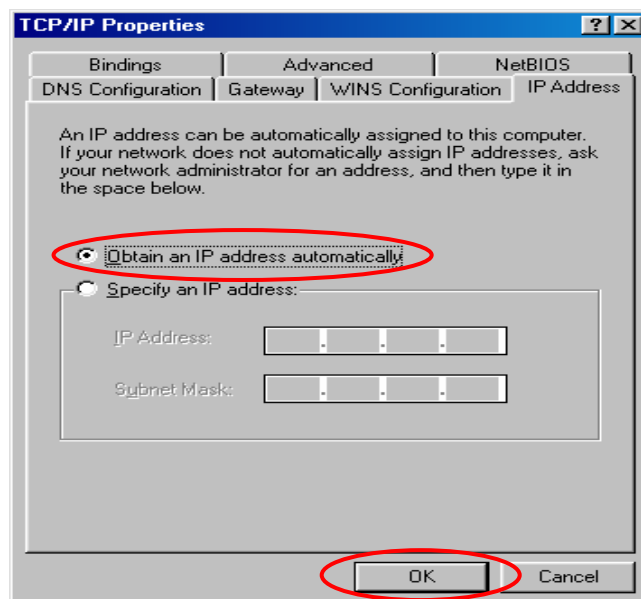
- 1) Choose **Start >> Control Panel >> Network**.



- 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 HSG200.

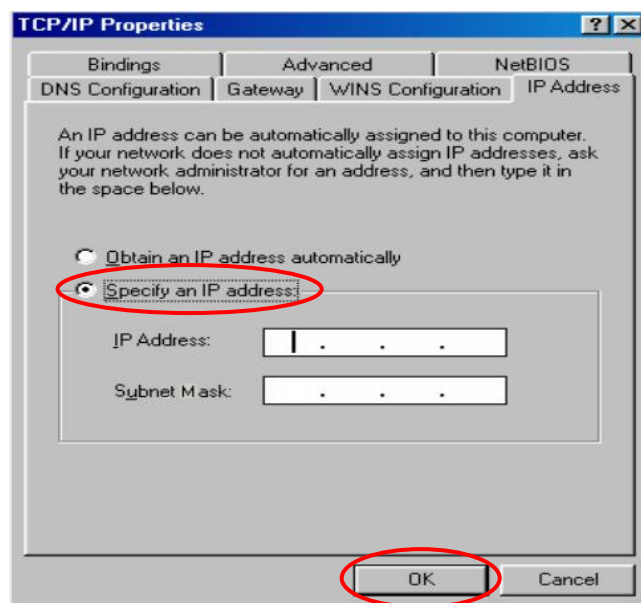


- 4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of HSG200.

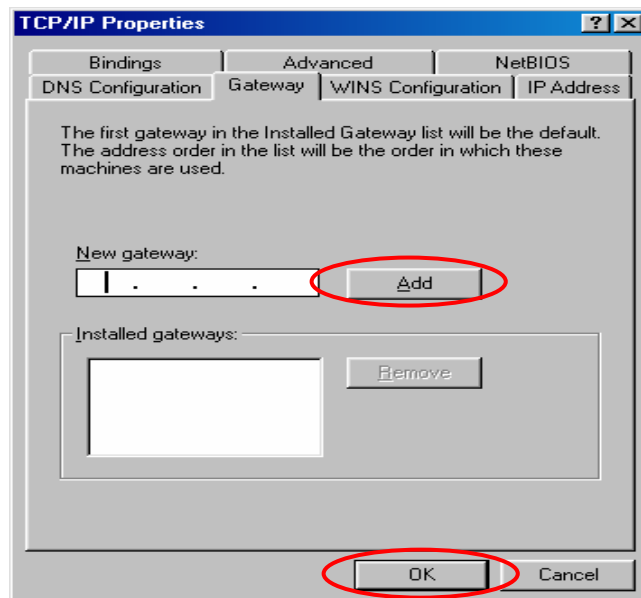
Caution:

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

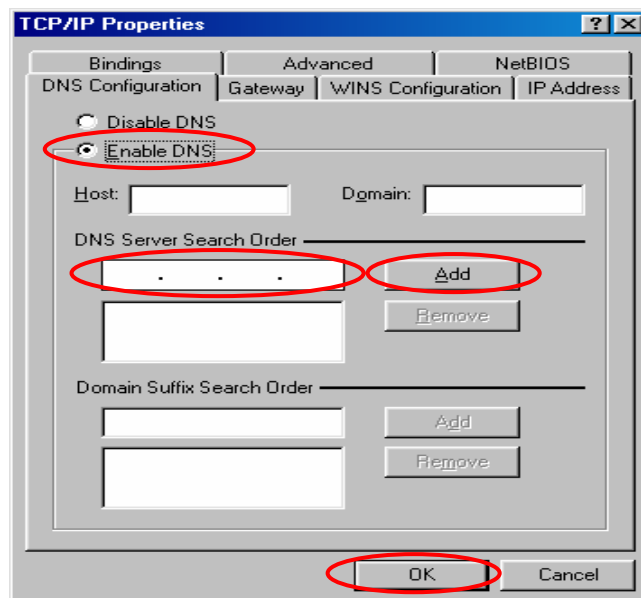
- 4.1) Click on the **IP Address** tab and choose **"Specify an IP address"**. Enter the *IP Address*, *Subnet Mask* and then click **OK**.



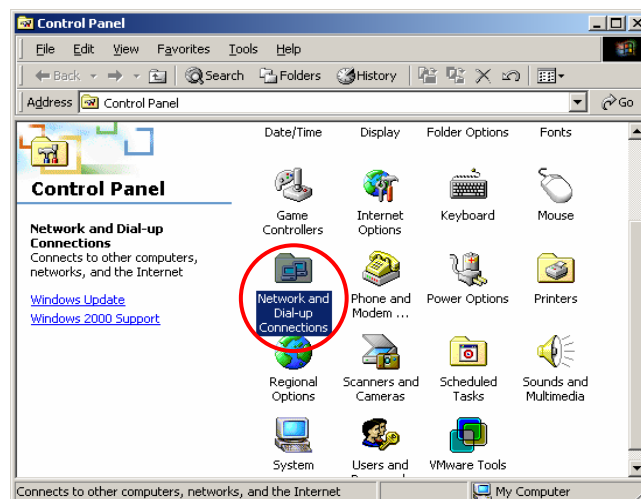
- 4.2) Click on the **Gateway** tab. Enter the gateway address of HSG200 in the **"New gateway"** field and click **Add**. Then, click **OK**.



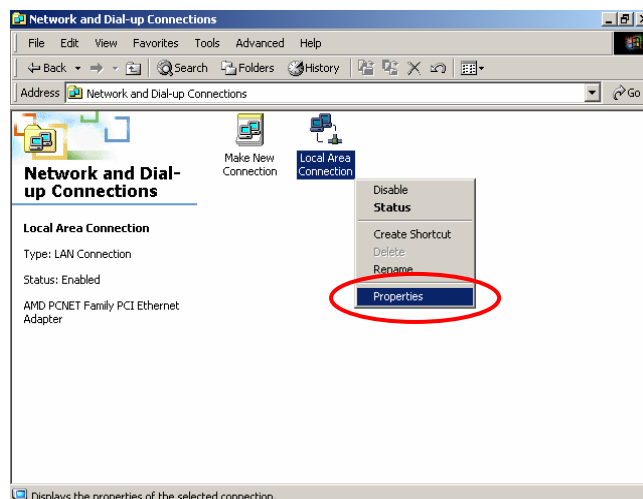
- 4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **"Enable DNS"** and enter *DNS Server address*. Click **Add**, and then click **OK** to complete the configuration.



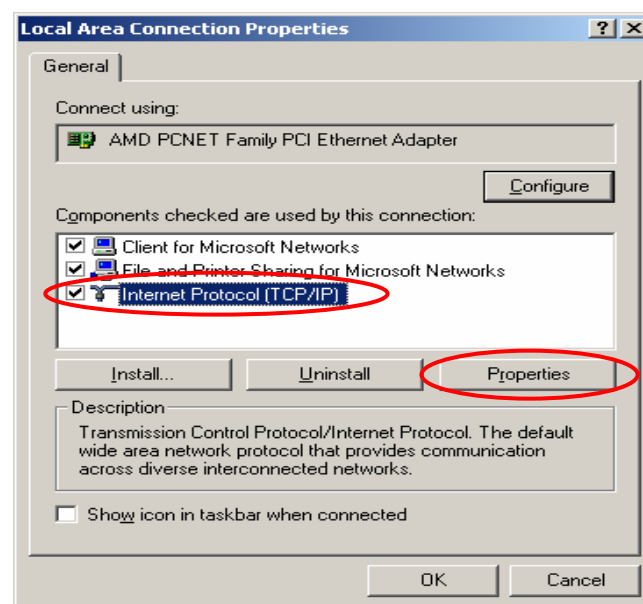
- Check the TCP/IP Setup of Window 2000
- 1) Select **Start >> Control Panel >> Network and Dial-up Connections**.



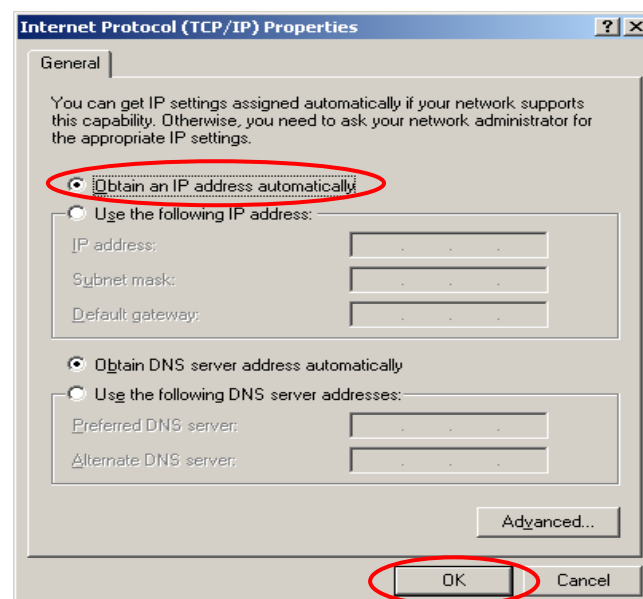
- 2) Right click on the **Local Area Connection** icon and select **"Properties"**.



- 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 HSG200.

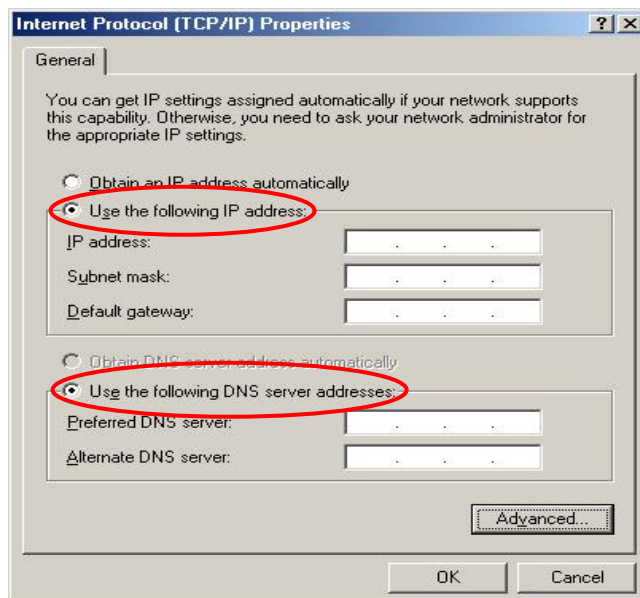


- 5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of HSG200.

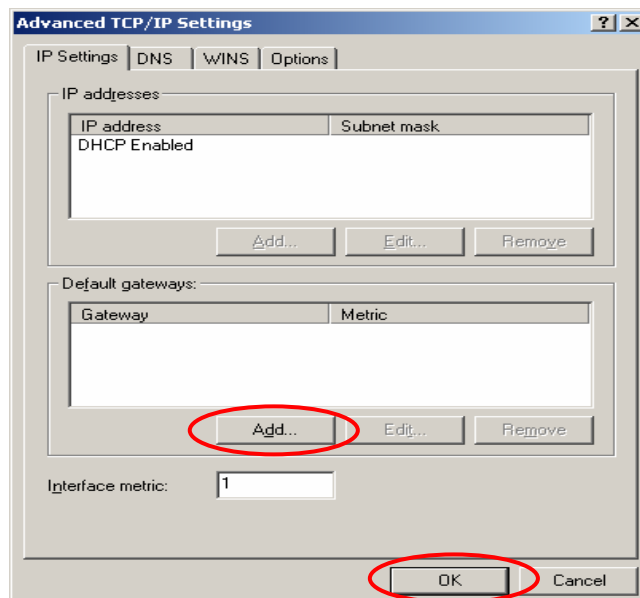
Caution:

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

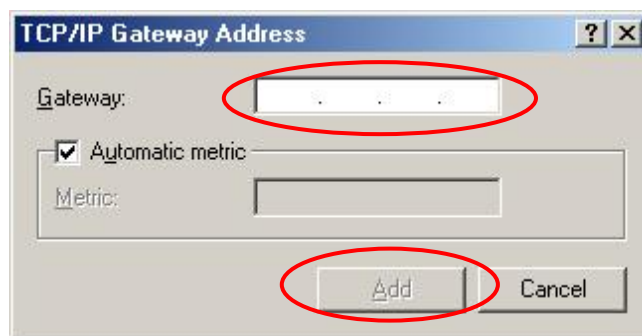
- 5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click **OK**.
- 5.2) Click **Advanced** to enter the **Advanced TCP/IP Settings**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

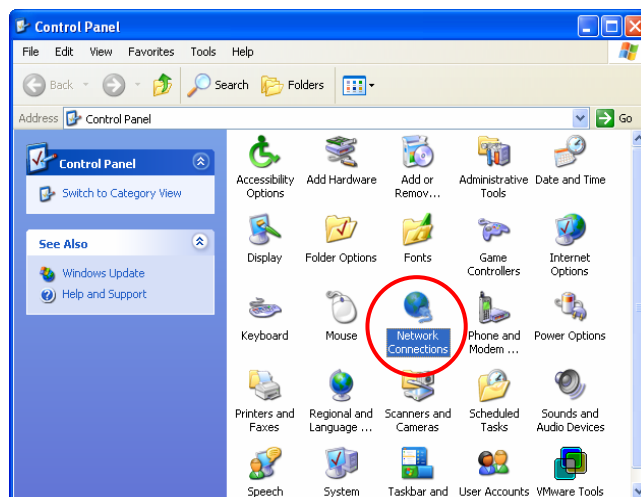


- 5.4) Enter the gateway address of HSG200 in the **"Gateway"** field, and then click **Add**. After back to the **IP Settings** tab, click **OK** to complete the configuration.

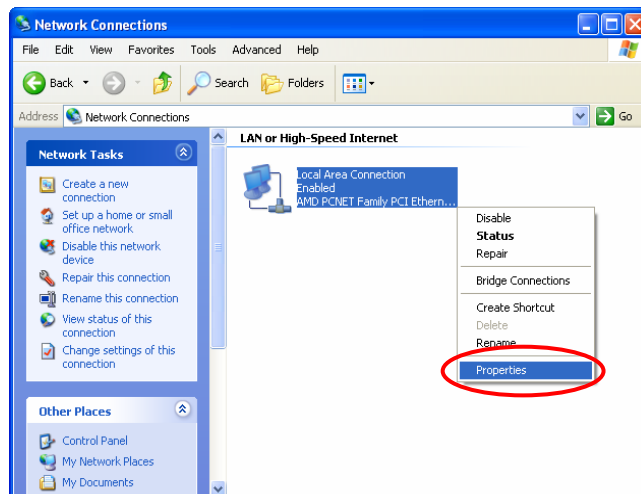


▪ Check the TCP/IP Setup of Window XP

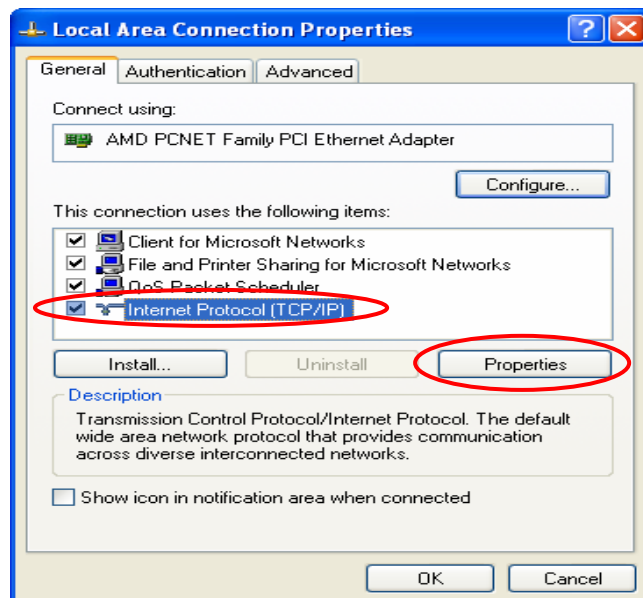
- 1) Select **Start >> Control Panel >> Network Connection**.



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

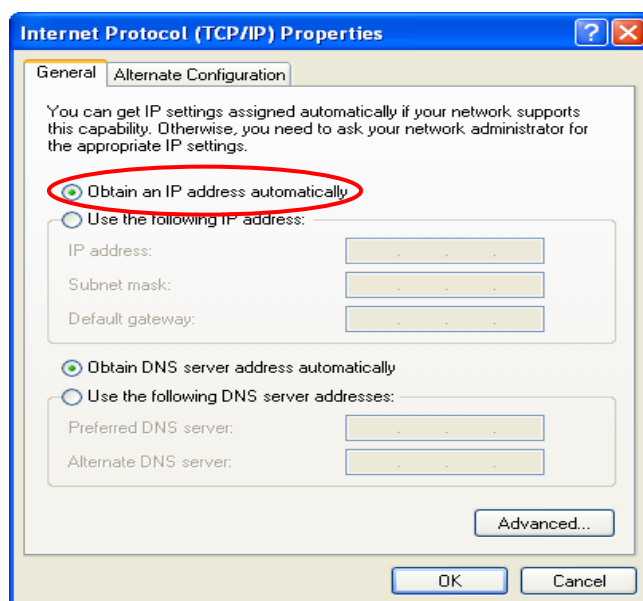


- 3) Click on the **General** tab and choose "**Internet Protocol (TCP/IP)**", and then click **Properties**. Now, you can choose to use DHCP or a specific IP address.



- 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 HSG200.

- 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 HSG200.

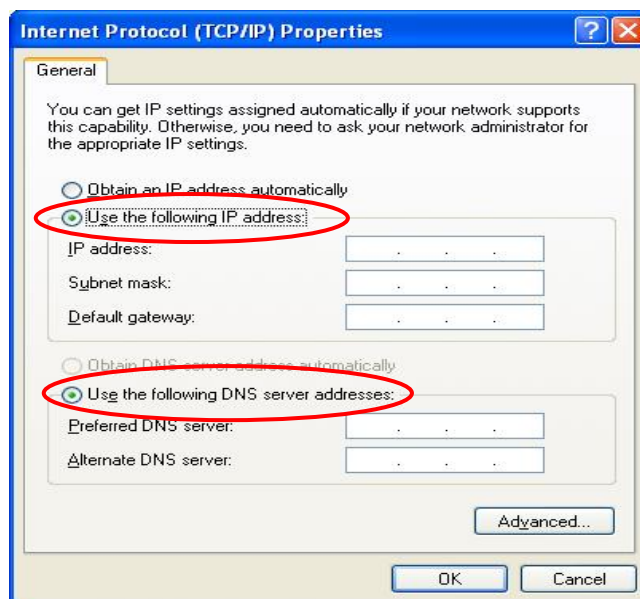


Caution:

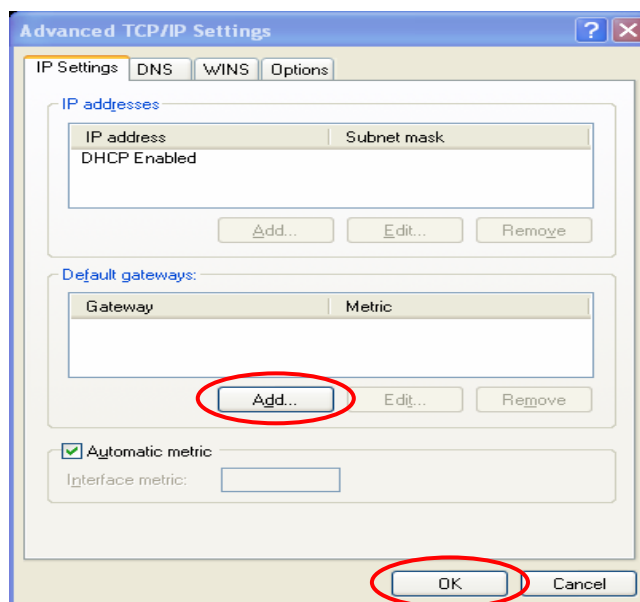
If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

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**.

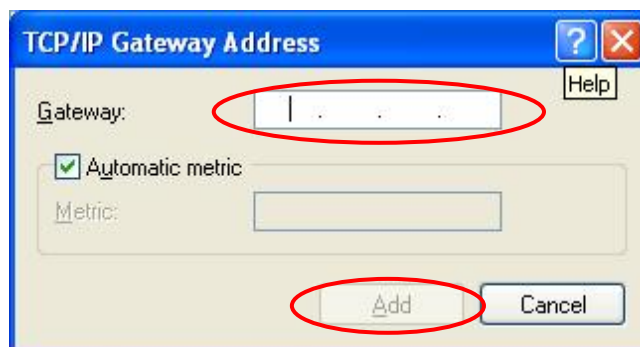
5.2) Click **Advanced** to enter the **Advanced TCP/IP Settings** window.



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 HSG200 in the **"Gateway"** field, and then click **Add**. After back to the **IP Settings** tab, click **OK** to finish the configuration.



Appendix B. Policy Priority

▪ Global Policy, Authentication Policy and User Policy

HSG200 supports multiple Policies, including one **Global Policy** and 5 individual **Policy** can be assign to different **Authentication Server**. **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 Authentication Server. For some authentication, such as Local and RADIUS, user can be assigned to different Policy individually. So one user may be applied different policy at the same time. Which policy is actually applied to this user?

The Policy Priority are enforced as follows:

User Policy >> Authentication Policy >> Global Policy

Now, let us discuss different user policy type:

- For Local and RADIUS, the users can be assigned to different Policy individually. For example, a Local user, user01, is assigned to Policy1 and the Local Authentication is assigned to Policy2. Then user01 login to Public Zone will get Policy1. This is a common case for users that can assign Policy individually.
- For Local and RADIUS, if these users are not assigned any User Policy individually, they will be the same as other users within the same authentication server. For example, a Local user, user01, the Local Authentication is assigned to Policy3. Then user01 login to Public Zone will get Policy3. This is another common case for users that is assigned Policy by the authentication server.
- If User is not assigned a Policy individually and the authentication server is also not assigned a Policy, then the users will be applied the Global Policy. For example, a Local user, user01, is assigned to *None* Policy and the Local Authentication is also assigned to *None Policy* in User list. Then user01 logging to Public Zone will be applied with the Global Policy.

As a conclusion, the Global Policy has the lowest policy priority; on the other hand, the User Policy has the highest one.

Appendix C. WDS Management

The Public Zone of HSG200 supports up to 2 WDS links. WDS (Wireless Distribution System) is a function used to connect APs (Access Points) wirelessly to extend wireless coverage. The WDS management function of the system can help administrators to setup two WDS links.

Configure WDS, go to: **System >> Zone Configuration**, click **Configure** in **Public** zone.

Zone Settings				
Name	ESSID	Wireless Security	Default Authen Option	Details
Private	HSG200-1	None	N/A	Configure
Public	HSG200-2	None	On-demand User	Configure

WDS (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 two WDS links.

WDS1 Settings : Public	
Basic	WDS Status : <input type="radio"/> Enable <input checked="" type="radio"/> Disable MAC Address of Remote AP : <input type="text"/>
Security	Security Type : <input type="text" value="None"/>

WDS2 Settings : Public	
Basic	WDS Status : <input type="radio"/> Enable <input checked="" type="radio"/> Disable MAC Address of Remote AP : <input type="text"/>
Security	Security Type : <input type="text" value="None"/>

- **WDS Status:** Select **Enable** to active this WDS link.
- **MAC Address of Remote AP:** Enter the MAC of the remote AP that create WDS link with HSG200.
- **Security Type:**
 - **WEP:** **WEP Key Length** may be *64 bits*, *128 bits* or *152 bits*; and **WEP Key Format** can be *ASCII* or *HEX*. Lastly, enter the **WEP Key**.
 - **WPA-PSK:** Select the preferred ciphering method, *TKIP* or *AES* and enter the **PSK / Pass-phrase**.

Appendix D. RADIUS Accounting

This section will briefly introduce the basic configuration of RADIUS server to work with VSA for the purpose to control the maximum client volume usage (upload; download or upload + download traffic).

This **VSA** will be sent from RADIUS server to gateway along with an **Access-Accept** packet. In other words, when the external RADIUS server accepts the request, it will reply not only an **Access-Accept** but also a maximum value in bytes each user is allowed to transfer. This value can be the maximum upload traffic, the maximum download traffic, or the sum of the download and upload traffics in bytes per user. Gateway will check this value every minute; if the user traffics reach this value, gateway will stop the session of this user and send a "Stop" to RADIUS server.

1. Description

VSA is designed to allow vendors to support their own extended Attributes not covered in common attributes. It MUST not affect the operation of the RADIUS protocol.

The **Attribute Type** of VSA is "26" and the "**Vendor ID**" should be determined before proceeding to RADIUS configuration; in this example; the **Vendor ID** is "21920". "**Attribute Number**" and "**Attribute Value**" can then be designed to provide additional control over RADIUS.

Attribute Name	Attribute Number	Attribute Value
HSG200-Byte-Amount	10	To be defined by administrator for different user group
HSG200-MaxByteIn	11	To be defined by administrator for different user group
HSG200-MaxByteOut	12	To be defined by administrator for different user group
HSG200-Byte-Amount-4GB	20	To be defined by administrator for different user group
HSG200-MaxByteIn-4GB	21	To be defined by administrator for different user group
HSG200-MaxByteOut-4GB	22	To be defined by administrator for different user group

If the amount of traffics is larger than 4 GB, the attributes of "XXXX-4GB" will be used. For example, if the amount is 5 GB, the following settings should be set: "HSG200-Byte-Amount = 1048576" and "HSG200-Byte-Amount-4GB = 1".

On the other hand, when the administrator fills in all attributes, the user will be kicked out from system if any condition is reached. For example, if the administrator sets "HSG200-Byte-Amount = 1048576"; "HSG200 - MaxByteIn = 1048576" and "HSG200- MaxByteOut = 1048576", the user will be kicked out from system when the downlink, uplink, or total traffic exceeds the limit.

2. VSA configuration in RADIUS server (IAS Server)

This section will guide you through a VSA configuration in your external RADIUS server. Before getting started, please access your external RADIUS server's desktop directly or remotely from other PC.

Step 1

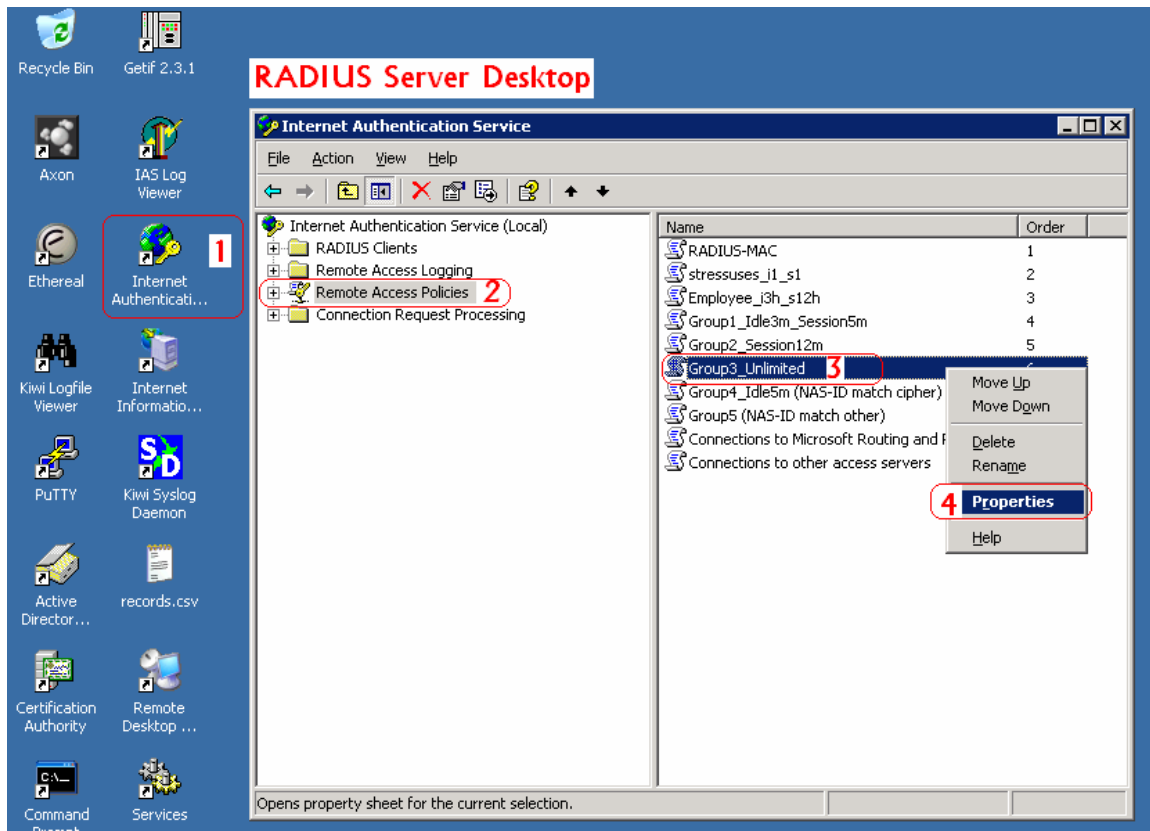
Confirm the following key elements in RADIUS server: users, groups, and policies.

- ◆ Verify whether there are already **users** in RADIUS Server.
- ◆ Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in RADIUS Server.
- ◆ Verify whether there are already **Policies** and assigned **Groups** belonging to these **Policies** in RADIUS Server.

Step 2

Run "Internet Authentication Server" and open "Remote Access Policies"

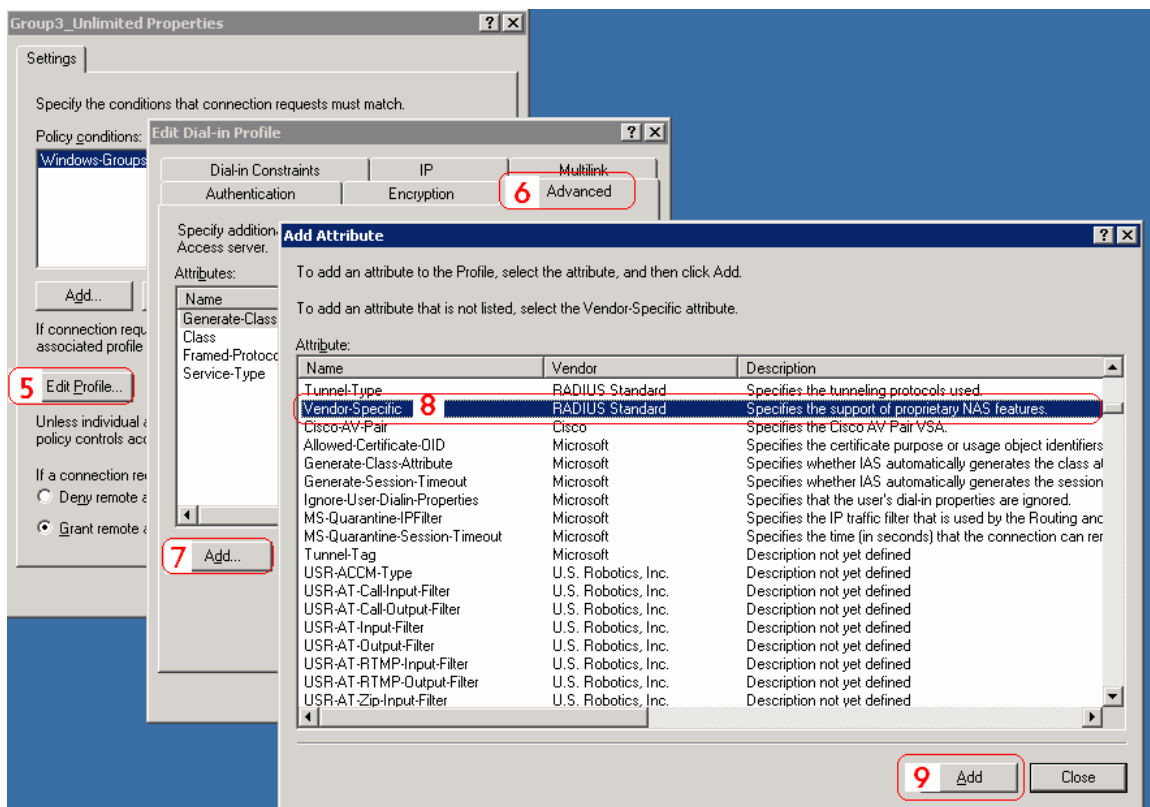
Select a **Policy** with right click and scroll down to its **Properties** page



Step 3

Click **Edit Profile** and select the **Advanced** Tag.

Click **Add** to add a new **Vendor-specific** attribute.



Step 4

Add a new attribute under **Vendor-specific**

Set "**Vendor Code** = 21920".

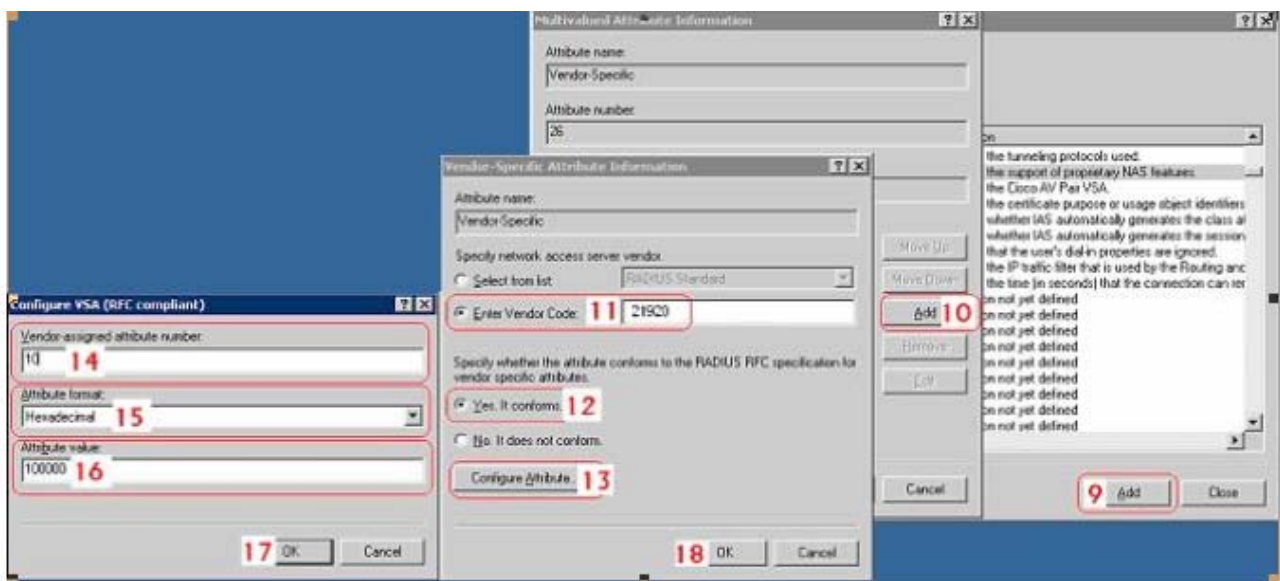
Check **Yes** to conform to the RADIUS RFC.

Click **Configure Attribute** to proceed.

Set "**Vendor-assigned attribute number** = 10"

Select "**Attribute format** = Hexadecimal"

Set "**Attribute Value** = 1000000"



Step 5

Confirm whether the **Vendor-specific Attribute** has been added successfully

Multivalued Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value
Vendor code: 21920	100000

Max download + upload traffic is 1 M Bytes

Move Up
Move Down
Add
Remove
Edit

19 OK Cancel

Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Generate-Class-Attribute	Microsoft	False
Class	RADIUS Standard	Class03
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed
Vendor-Specific	RADIUS Standard	100000

Add... Edit... Remove

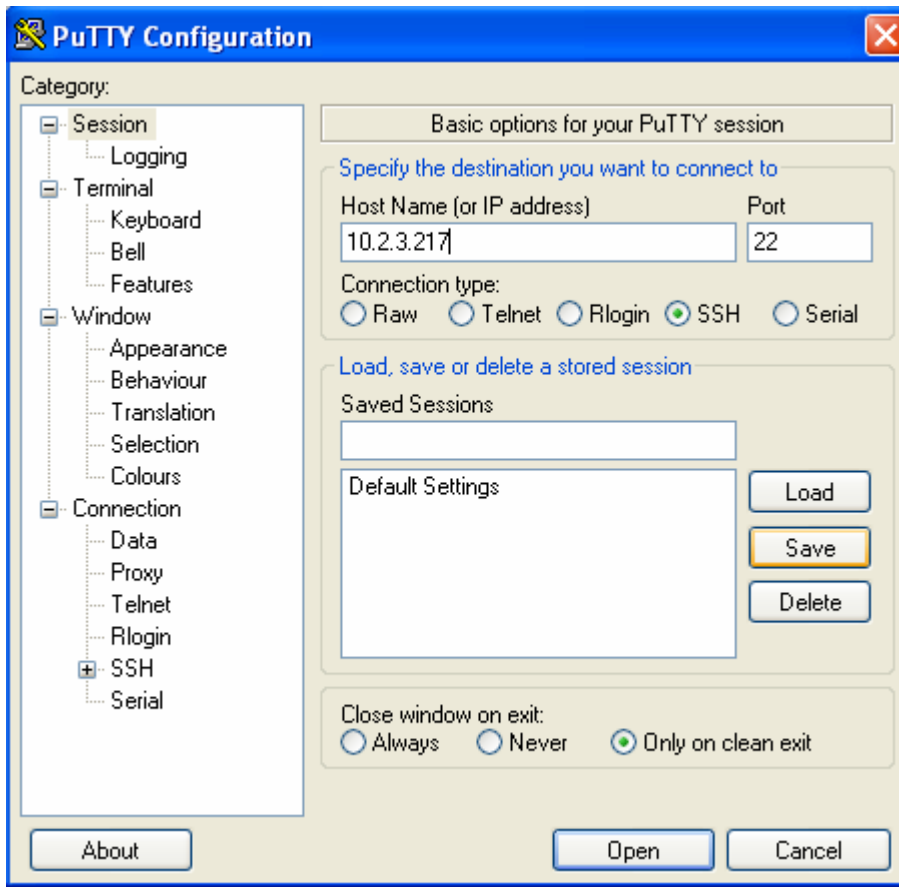
21 OK Cancel 20 Apply

Step 6

Follow the same steps to create other **Vendor-specific Attribute** if needed.

3. VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through **VSA** configuration with FreeRADIUS v1.0.5 running on "Fedora". Before getting started, open the shell of RADIUS server; for example, use *PuTTY* to access the Linux host:



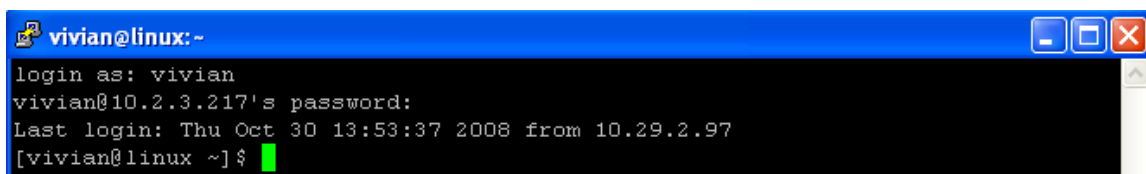
Step 1

Confirm the following key elements in RADIUS server: users, groups

- ◆ Verify whether there are already **users** in RADIUS Server.
- ◆ Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in RADIUS Server.

Step 2

Log in the Linux host of the RADIUS server.



Step 3

Create a file "dictionary.HSG200" under the "freeradius" folder.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary.
```

Step 4

Edit and save the contents of the file "dictionary.HSG200" as follows:

```
VENDOR                                21920
#
#      Standard attribute
#
ATTRIBUTE      -Byte-Amount          10      interger
```

Administrator can also add other attributes as the table stated in Section 2 with the same format.

```
VENDOR                                21920
#
#      Standard attribute
#
ATTRIBUTE      -Byte-Amount          10      interger
ATTRIBUTE      -MaxByteIn            11      interger
ATTRIBUTE      -MaxByteIn            12      interger
ATTRIBUTE      -Byte-Amount-4GB      20      interger
ATTRIBUTE      -MaxByteIn-4GB        21      interger
ATTRIBUTE      -MaxByteIn-4GB        22      interger
```

Step 5

Edit the file "dictionary" under the folder "freeradius".

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary
```

Step 6

To include "dictionary.HSG200" in the dictionary of RADIUS server, insert it in an incremental position as follows.

```
$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.
$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.ern
```

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 response. In this example, the maximum download and upload traffics in bytes for **group03 users** is 1MBytes.

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
VALUES ('group03', cipherium-Byte-Amount, '=', '1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

Step 9

Restart RADIUS daemon 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. On-demand Account types & Billing Plan

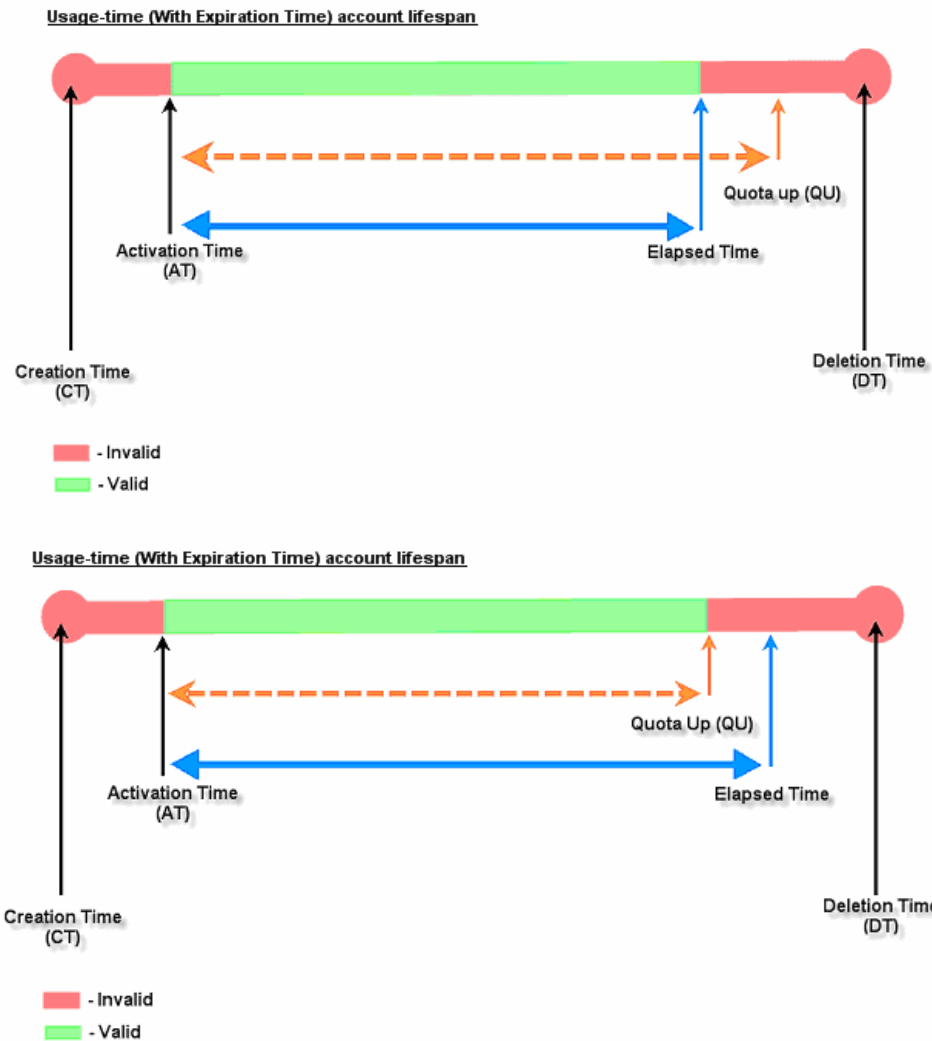
This section explains the parameters as well as the different account types provided when editing billing plans in On-demand authentication.

- **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	2
Account Type	Usage-time ▼
Expiration Time	<input checked="" type="radio"/> With Expiration Time <input type="radio"/> No Expiration Time
Quota	1 day(s) 2 hr(s) 3 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 4 day(s) 5 hour(s) <small>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</small>
Valid Period	After activation, account will be expired in 6 day(s) <small>*(Must be larger than 0)</small>
Price	7 (\$) <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	

TIP:

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



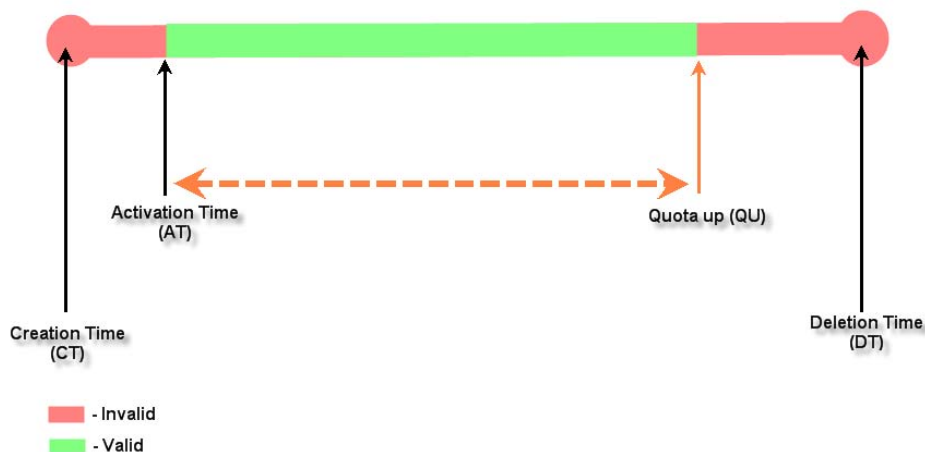
- **Usage-time with No Expiration Time:** Can access internet as long as account has remaining quota (usable time). Need to activate the purchased account within a given time period by logging in for the first time. Ideal for short term usage. For example in coffee shops, airport terminals etc. Only 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	<div>2 day(s) 3 hr(s) 4 min(s)</div> <div>*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)</div>
Account Activation	<div>First time login must be done within 5 day(s) 6 hour(s)</div> <div>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</div>
Price	<div>7 (\$)</div> <div>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</div>
Group	Group 1 ▾
Reference	

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

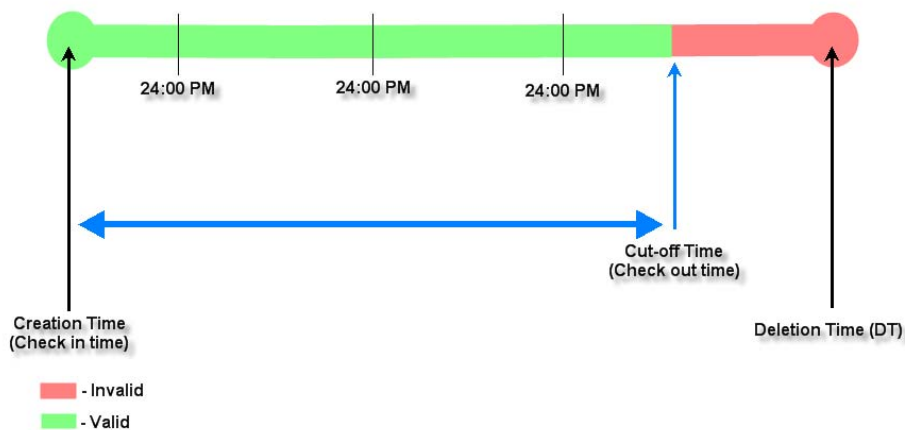
Editing Billing Plan	
Plan	5
Account Type	Hotel Cut-off-time ▼
Hotel Cut-off Time	13 : 00 *(HH:MM; range : 00:00 ~ 23:59)
Grace Period	Account remains usable for 0 ▼ hour(s) after cut-off.
Unit Price	60 per day (\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1 ▼
Reference	

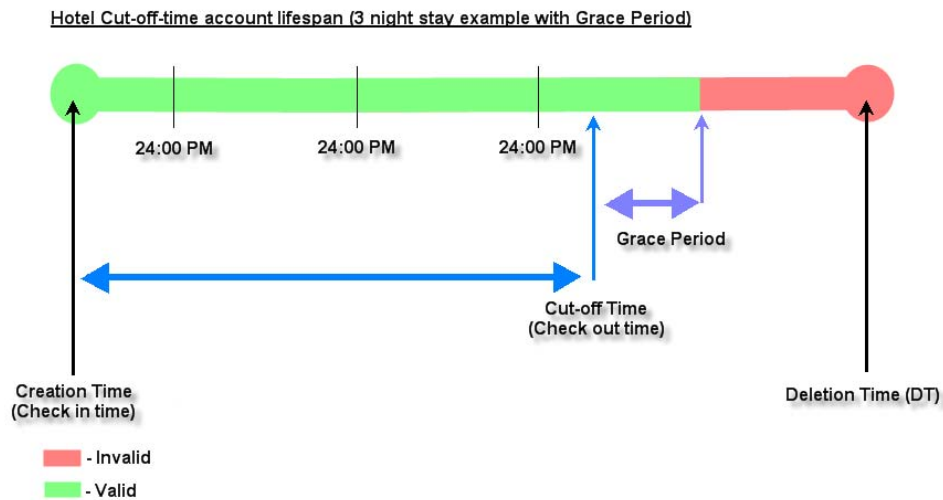
TIP:

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)





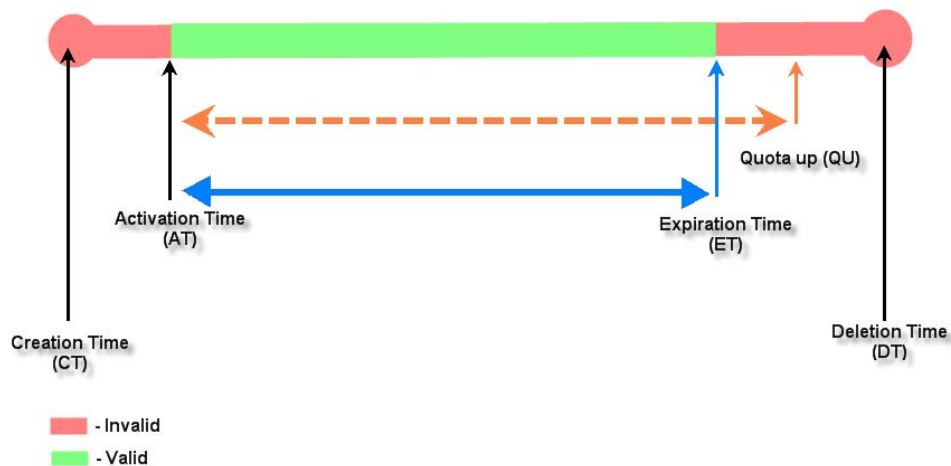
- **Volume:** Can access internet as long as account valid with remaining quota (traffic volume). Account expires when *Valid Period* has been used up or quota depleted. Ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous regardless of logging in or out.
 - **Quota** is the total Mbytes (1 ~ 2000), 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	4
Account Type	Volume
Quota	500 Mbyte(s) <small>*(Range : 1 ~ 2000)</small>
Account Activation	First time login must be done within 4 day(s) 5 hour(s) <small>*(Range of hour(s) : 0 ~ 23; they cannot both be zero)</small>
Valid Period	After activation, account will be expired in 6 day(s) <small>*(Must be larger than 0)</small>
Price	7 (\$) <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1
Reference	

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.

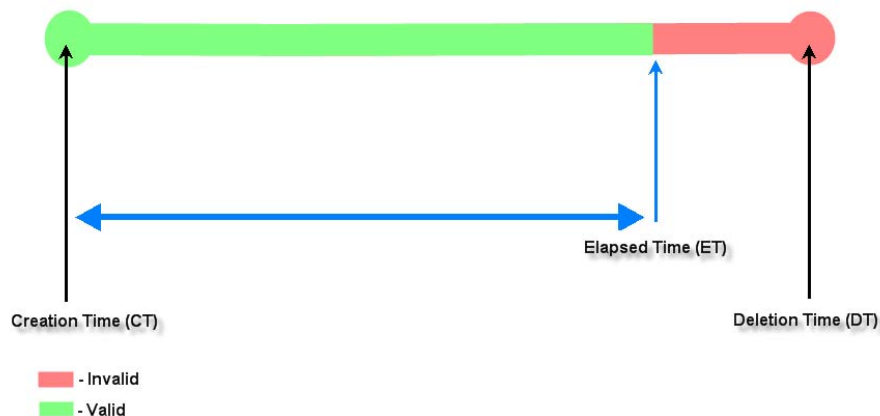
Editing Billing Plan	
Plan	7
Account Type	Duration-time ▼
Counting Method	<input checked="" type="radio"/> Elapsed Time <input type="radio"/> Begin-and-end Time <input type="radio"/> Cut-off Time
Begin Time	Upon Account Creation
Elapsed Time	8 day(s) 9 hr(s) 0 min(s) <small>*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)</small>
Price	47 (\$) <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	

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 Date Time" specifies that the account is valid between the two time points.

Apply Cancel

Duration-time (Elapsed Time) account lifespan



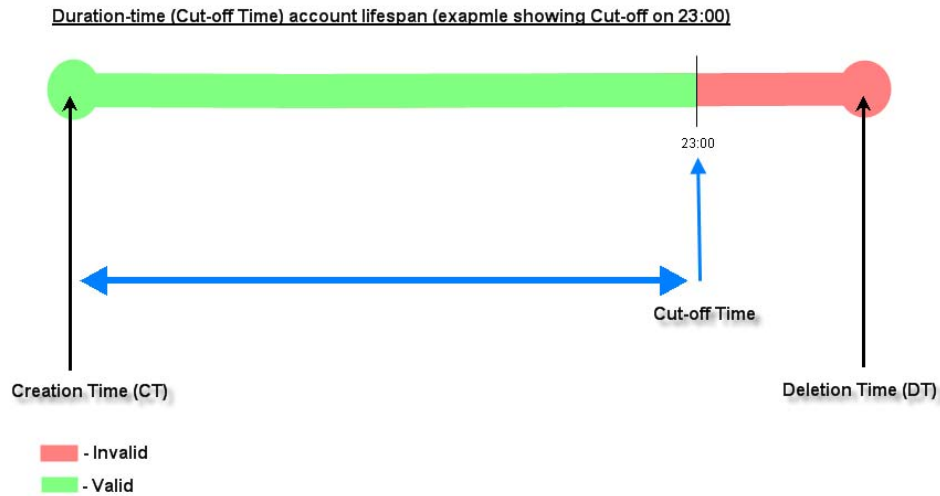
- **Duration-time with Cut-off Time:** **Cut-off Time** is the clock time at which the on-demand account is cut off (made expired) by the system on that day. For example a shopping mall closing hour is 23:00, operators selling on-demand tickets can create use this plan to create ticket set to be Cut-off 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	1
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	10 : 00 <small>*(HH:MM; range : 00:00 ~ 23:59)</small>
Price	4 (\$) <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	5

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 Date Time" specifies that the account is valid between the two time points.

Apply Cancel



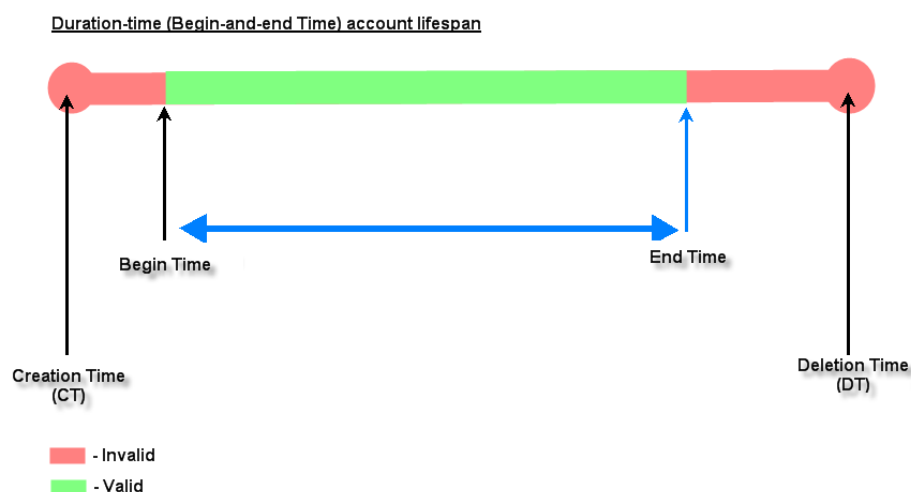
- **Duration-time with Begin-and End Time:** Define explicitly the *Begin Time* and *End Time* of the account. Count down begins immediately after account activation and expires when the *End Time* has been reached. Ideal for providing internet service throughout a specific period of time. For example 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	6
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	00 : 01 , Jan 01 2010
End Time	03 : 03 , Jun 10 2014
Price	7000 (\$) <small>*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)</small>
Group	Group 1 ▼
Reference	

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 Date Time" specifies that the account is valid between the two time points.

Apply Cancel



Appendix F. External Payment Gateways

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via Authorize.net, PayPal, SecurePay or WorlPay, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access with credit cards.

1. Payments via Authorize.Net

Configure Payments via Authorize.Net, go to:

Users >> 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 style="border: 1px solid black; padding: 5px;"> 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>			

Choose Billing Plan for Authorize.Net Payment Page				
Plan	Enable/Disable		Quota	Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	5 hr(s) 5 min(s)	0
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
3	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	10 hr(s) 6 min(s)	9000
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Until 18:30	88
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
7	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	20.73 Mbyte(s)	0.59
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	600 Mbyte(s)	6.99

Client's Purchasing Record	
Starting Invoice Number	<input type="text" value="Hotspot"/> - <input type="text" value="0000000"/> * <input type="checkbox"/> Change the Number
Description (Item Name)	<input type="text" value="Internet Access"/> *
E-mail Header	<input type="text" value="Enjoy Online!"/> *

Service Disclaimer Content

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

Choose Billing Plan for Authorize.Net Payment Page

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

Client's Purchasing Record

- **Starting Invoice Number:** An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.
- **Description (Item Name):** This is the item information to describe the product (for example, Internet Access).
- **Email Header:** Enter the information that should appear in the header of the invoice.

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

Authorize.Net Payment Page Fields Configuration		
Item	Displayed Text	Required
<input checked="" type="checkbox"/> Credit Card Number	Credit Card Number *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Credit Card Expiration Date	Credit Card Expiration Date *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> 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	
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	

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:** 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 (at the end of the credit card number found either on the front of the card 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 name.
- **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.

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 / Choose Billing Plan for PayPal Payment Page**

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

Choose Billing Plan for PayPal Payment Page			
Plan	Enable/Disable		Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	5 hr(s) 5 min(s)
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
3	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	10 hr(s) 6 min(s)
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Until 18:30
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
7	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	20.73 Mbyte(s)
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
10	<input checked="" type="radio"/> Enable	<input checked="" type="radio"/> Disable	600 Mbyte(s)
			6.99

- **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 00000001 * <input type="checkbox"/> Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

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

Client's Purchasing Record:

- **Starting 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.

3. Payments via SecurePay

Configure Payments via SecurePay, go to: **Users >> Authentication >> On-demand User>> 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 <input type="button" value="Trusted CA Management"/>
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		
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		

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>

➤ **SecurePay Page Configuration**

Merchant ID: The ID that is associated with the Merchant Account.

Merchant 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.

➤ **Choose Billing Plan for SecurePay Payment Page**

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.

4. Payments via World Pay

Configure Payments via WorldPay, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> WorldPay.

WorldPayPaymentConfiguration	
WorldPayInstallationID	<input type="text"/> *
Payment Gateway URL	<input type="text" value="https://select.wp3.rbsworldpay.com/wcc/purchase"/> *
Currency	GBP (Pound Sterling) ▼ *

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>

WorldPayBillingConfiguration				
Plan	Enable/Disable		Quota	Price
1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	15 min(s) connection time quota with expiration	10.91
2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	11 min(s) connection time quota	1
3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Valid until 12:00 the following day	5
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1
5	<input type="radio"/> Enable	<input type="radio"/> Disable		
6	<input type="radio"/> Enable	<input type="radio"/> Disable		
7	<input type="radio"/> Enable	<input type="radio"/> Disable		
8	<input type="radio"/> Enable	<input type="radio"/> Disable		
9	<input type="radio"/> Enable	<input type="radio"/> Disable		
10	<input type="radio"/> Enable	<input type="radio"/> Disable		

WorldPayNoteContent
<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>

➤ WorldPay Payment Configuration

WorldPayInstallation 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 Billing Configuration

These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

➤ WorldPay Note 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.

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	
<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	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.