PheeNet

802.11bng Wireless Hotspot Gateway

User's Manual   *Ver 0.0.5*   *WAS-105R*

Copyright

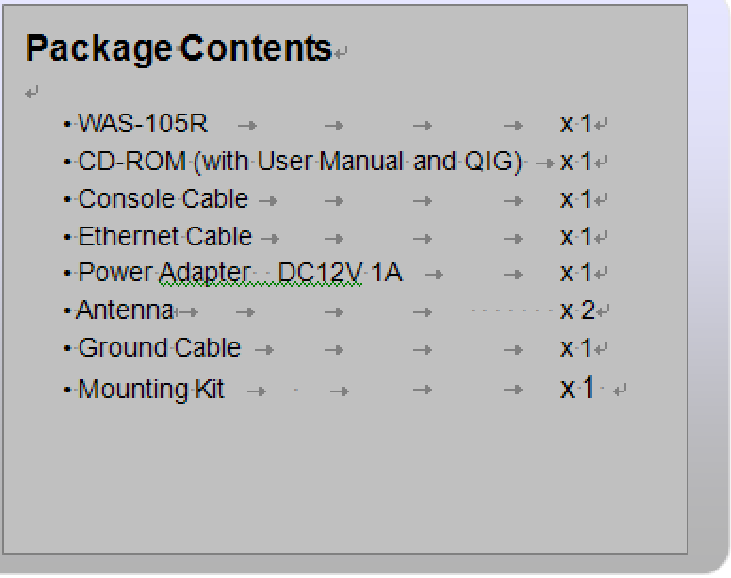
Table of Contents

Chapter 1. Before You Start

1.1 Preface

The **WAS-105R** is the most economical yet feature-rich **Wireless Hotspot Gateway**, targeting mini-size stores who want to provide small, single-point wireless Internet access service. WAS-105R is a perfect choice for beginners to run hotspot businesses. It does not cost a fortune to buy a pile of equipment, nor does it take the skills of an expert to glue multiple applications out of multiple freeware. Feature-packed for hotspot operation, WAS-105R comes with **built-in 802.11n/b/g 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, PayPal credit card gateway, traffic logs, IP sharing** and etc.

1.2 Package Contents



Package Contents

• WAS-105R	x 1
• CD-ROM (with User Manual and QIG)	x 1
• Console Cable	x 1
• Ethernet Cable	x 1
• Power Adapter DC12V 1A	x 1
• Antenna	x 2
• Ground Cable	x 1
• Mounting Kit	x 1

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

Chapter 2. System Overview

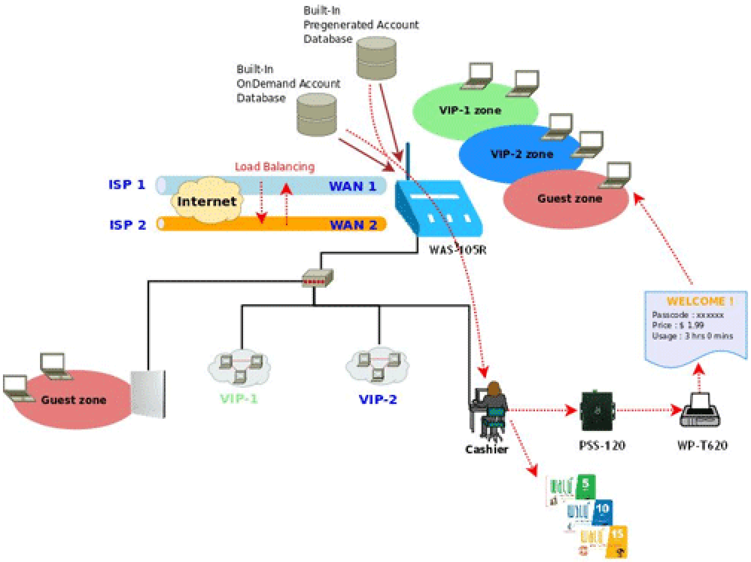
2.1 Introduction of WAS-105R

The WAS-105R – Wireless Hotspot Controller, built-in Wifi-N technology with data rate up to 300 Mbps, applies to public access network such as WiFi-Hotspot, network management guest access, hospitality deployments – which requires reliability, efficiency, and security. It combines an IP Router /Firewall, Multi-WAN/ QoS enforcement and Access Controller for use in wireless hotspot environments. One single WAS-105R can serve Suggest 100 simultaneous users, takes control over authentication, authorization, accounting and routing to the Internet as well as to the operating central. Built-in AAA system allows hotspot owners set up public access services without extra RADIUS server.

2.2 System Concept

WAS-105R Wireless Hotspot Controller provides authentication, authorization and accounting for a wired/or wireless networks. Hotspot technology allows Internet providers to offer Internet access to customers, while applying certain Internet use rules and limitation. It is convenient for Internet cafes, hotels, airports, schools and universities. The Internet provider gets complete tracking records of per customer time spent on the network, data amount sent/ received, real-time accounting and more.

To begin browsing, a client must go through a registration process with the provider, then enter a Passcode / Username of access ticket in a browser Login window that appears on the attempt to open a webpage. Hotspot technology proposes providers to establish and administrate a user database, which can be useful for enterprise such as airports, hotels or universities that offer wireless or Ethernet Internet connectivity to employees, students, guests or other groups of users.



2.3 Specification

➢ Network

- ➔ Support NAT or Router Mode
- ➔ Support static IP , Dynamic IP(DHCP Client), PPPoE and PPTP on WAN connection
- ➔ DHCP Server Per VLAN; Multiple DHCP Networks
- ➔ 802.3 Bridging
- ➔ Proxy DNS/Dynamic DNS
- ➔ Support NAT
  - ✓ IP/Port destination redirection
  - ✓ DMZ server mapping
  - ✓ Virtual server mapping
- ➔ Built-in with DHCP server
- ➔ NTP Client
- ➔ Vitual DMZ
- ➔ Virtual Server (IP /Port Forwarding)
- ➔ Binding VLAN with Ethernet and Wireless interface
- ➔ H.323, SIP Pass-through
- ➔ Support MAC Filter
- ➔ Support IP Filter
- ➔ Support Walled garden (free surfing zone)
- ➔ Support MAC-address and IP-address pass through
- ➔ IP Plug and Play (IP PnP)

➢ User Management

- ➔ Suggest 100 simultaneous authentication users
- ➔ Max 3069 Accounts
- ➔ Support Pregenerated Users On-Demand Users and Local Radius Accounts.
- ➔ Users Session Management
- ➔ Configurable user Black list (with Time-based control)
- ➔ Allows MAC address and user identity binding for local user authentication
- ➔ SSL protected login portal page
- ➔ Session idle timer
- ➔ Login Session idle time out setting
- ➔ Session and account expiration control
- ➔ User Log and traffic statistic notification via automatically email service
- ➔ Login time frame control
- ➔ Session limit
- ➔ Real-Time Online Users Traffic Statistic Reporting

- ➔ Support local account roaming
- ➔ Seamless Mobility : User-centric networking manages wired and wireless users as they roam between ports or wireless APs

➢ Multiple Service Domain

- ➔ The network is divided into maximum 8 group, each defined by a pair of VLAN tag and ESSID
- ➔ Each Domain has its own **(1) login portal page (2) authentication options (3) LAN interface IP address range (4) Session number limit control (5) Traffic shaping (6) IP Plug and Play (IP PnP) (7) Multiple Authentication**
- ➔ Enable DHCP or not, and DHCP address range
- ➔ Enable authentication or not
- ➔ Enable Guest service or not
- ➔ Types of authentication options (Local RADIUS, Remote RADIUS, LDAP, On-Demand and Pregenerated)
- ➔ Bandwidth (Distribution or Individual)
- ➔ Scheduling authentication service control on different Service Domain

➢ Authentication

- ➔ Authentication: single sign-on (SSO) client with authentication integrated into the local authentication environment through local/domain, LDAP, RADIUS, MAC authentication, and 802.1x
  - ✓ Customizable Login and Logout Portal Pages
  - ✓ Customizable Advertisement Links on Login Portal Page
- ➔ User authentication with UAM (Universal Access Method), 802.1x /EAPoLAN ,MAC address
- ➔ Allow MAC address and users identity binding for local user authentication
- ➔ Support Multiple Login service on one Accounts
- ➔ Each group (role) may get different network policies in different Service Domain
- ➔ Max simultaneous user session (TCP/UDP) limit
- ➔ Configurable user black list
- ➔ Export/Import local users list to/from a text file
- ➔ Web-based Captive Portal for SSL browser-based authentication
- ➔ Authentication Type
  - ✓ IEEE802.1X(EAP, EAP/TLS, EAP/TTLS, EAP/GTC, EAP/MD5, EAP/MSCHAP-V2)
  - ✓ RFC2865 RADIUS Authentication
  - ✓ RFC3579 RADIUS Support for EAP
  - ✓ RFC3748 Extensible Authentication Protocol
  - ✓ MAC Address authentication
  - ✓ Web-based captive portal authentication

安

➢ Accounting :

- ➔ Provides billing plans for pregenerated accounts
- ➔ Provides billing plans for on-demand accounts
- ➔ Enables session expiration control for both Pregenerated tickets and On-Demand accounts by Time(Hours) and Data Volume(MB)
- ➔ Detailed per-user traffic history based on time and data volume for both Pregenerated tickets and On-Demand accounts
- ➔ Support Local RADIUS, Pregenerated, On-Demand and external RADIUS server
- ➔ Contain 10 configurable billing plans for On-Demand accounts
- ➔ Support credit card billing system by Papal
- ➔ Support automatic email network traffic history

➢ Security

- ➔ Layer 2 User Isolation
- ➔ Blocks client to client discovery within a specified VLAN
- ➔ Setting for TKIP/CCMP/AES key's refreshing periodically
- ➔ Hidden ESSID support
- ➔ Setting for " Deny Any " connection request
- ➔ MAC Address Filtering (MAC ACL)
- ➔ Support Data Encryption : WEP(64/128-bit), WAP, WAP2
- ➔ Support various authentication methods : WPA-PSK, WPA-RADIUS, IEEE802.1X
- ➔ Support VPN pass-through
- ➔ Encryption Type
  - ✓ WEP: 64, 128 and 152 bit
  - ✓ WAP-TKIP , WPA-PSK –TKIP, WPA-AES, WPS-PSK-AES
  - ✓ WAP2/802.11i :WPA2-AES, WAP2-PSK-AES, WAP2-TKIP, WPA-PSK-TKIP
  - ✓ Secure Socket Layer (SSL) and TLS : RC4 128-bit and RSA1024-bit and 2048-bit

➢ Dual WAN

- ➔ Load Balancing
  - ✓ Outbound Fault Tolerance
  - ✓ Outbound load balance
  - ✓ Multiple Domain Support
  - ✓ By Traffic
- ➔ Bandwidth Management by individual and users group
- ➔ WAN Connection Detection

➢ QoS Enforcement

- ➔ Packet classification via DSCP (Differentiated Services code Point)
- ➔ Traffic Analysis and Statistics
- ➔ Diff/TOS
- ➔ IEEE 802.1Q Tag VLAN priority control
- ➔ IEEE 802.11e WMM
- ➔ Automatic mapping of WMM priorities to 802.1p and IP DSCP
- ➔ Upload and Download Traffic Management

➢ Wireless

- ➔ Transmission power control : 7 Levels
- ➔ Channel selection : Manual or Auto
- ➔ No. of associated clients per AP : 32
- ➔ Setting for max no associated clients : Yes
- ➔ No. of BBSID (Virtual AP) : 8
- ➔ No. of Max. WDS setting : 4
- ➔ Preamble setting : Short / Long
- ➔ Setting for 802.11b/g/n mix, 802.11b only or 802.11 b/g only or 802.11n only
- ➔ Setting for transmission speed
- ➔ IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- ➔ IEEE802.11i Preauth (PMSKA Cache)
- ➔ IEEE802.11d Multi country roaming
- ➔ Automatic channel assignment
- ➔ Coordinated Access ensures optimal performance of nearby APs on the same channel
- ➔ Secure wireless bridge connects access points without wire
- ➔ Monitoring and reporting

➢ System Administration

- ➔ Intuitive Web Management Interface
- ➔ Three administrator accounts
- ➔ Provide customizable login and logout portal page
- ➔ CLI access (Remote Management) via Telnet and SSH
- ➔ Remote firmware upgrade (via Web)
- ➔ Utilities to backup and restore the system configuration
- ➔ Remote Link Test – Display connect statistics
- ➔ Full Statistics and Status Reporting
- ➔ Real time traffic monitor

- Ping Watchdog
- Traffic history report via email to administrator
- Users' session log can be sent by external Syslog Server or E-mail
- Even Syslog
- SNMP v1, v2c,v3
- SNMP Traps to a list of IP Address
- Support MIB-II
- Spanning Tree Protocol
- NTP Time Synchronization
- Customizable Time Display Format for System
- Administrative Access : HTTP / HTTPS

WAS-105R Hardware Specifications	
Base Platform	AR7240+AR9283
CPU Clock Speed	400 MHz
Wireless Radio	802.11bgn
Serial Port	1 (DB-9)
USB Port (Optional)	1 (Optional 3G interface radio with major brands – ODM only)
Reset Switch Built-in	Push-button momentary contact switch
RF Channel Scan Hardware Button	Hardware Push-button to scan for a better channel to use
Standards Conformance	IEEE 802.3 / IEEE 802.3u
Ethernet Configuration	10/100BASE-TX auto-negotiation Ethernet port x 3 (RJ-45 connector) WAN * 2 LAN * 1 Auto MDI/MDI-X enabled , IEEE802.3af Power Over Ethernet Compatible , Auto Fail over
SDRAM	On board : 64 Mbytes
Flash	On board : 16 Mbytes
Built-In LED Indicators	1x Power, 2 x WAN ,1x LAN , 1x Status, 1x System, 1x Printer

Wireless Specifications	
Network Standards Conformance	IEEE802.11 b /g /n compliant
Data Transfer Rate	IEEE802.11b：1 / 2 / 5.5 / 11Mbps (auto sensing) IEEE802.11g：6 / 9 / 12 / 18 / 24 / 36 / 48 / 54(auto sensing) IEEE802.11n : 300 (auto sensing)
Frequency Range	IEEE802.11b/g： 2.412 ~ 2.462GHz (USA) 2.412 ~ 2.484GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI) 2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)
Media Access Protocol	CSMA / CA with ACK
Modulation Method	IEEE802.11b：DSSS (DBPK,DQPSK,CCK) IEEE802.11g/n：OFDM(64-QAM,16-QAM,QPSK,BPSK)
Operating Channels	802.11b/g/n : 11 for FCC,14 for Japan,13 for Europe, 2 for Spain, 4 for France
RF Output Power	100mW
Transmit Power Variation	802.11g/n : Up to 16 dBm 802.11b : up to 18 dBm
Frequency Response flatness	±1dB over operating range
Receiver Sensitivity	802.11b/g /n -90dBm@1Mbps, -86dBm@6Mbps,-84dBm@11Mbps,-69dBm@54Mbps
Environmental & Mechanical Characteristics	
Operating Temperature	-20 °C ~ 50 °C
Storage Temperature	-20 °C ~ 60 °C
Operating Humidity	10% to 80% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Antenna Connector	SMA-Type Connector
Power Supply	110 – 220V AC Power ; 12 VDC, 1.5A input. Support 802.3af Compliant , Power Over Ethernet (48V/0.3 A)
Unit Dimensions	205 x 125 x 35 (mm) (Width x Depth x Height)
Unit Weight	600g
Form Factor	Wall Mountable , Metal case compliant with IP50 standard
Certifications	FCC,CE, IP50,ROHS compliant

Chapter 3. Base Installations

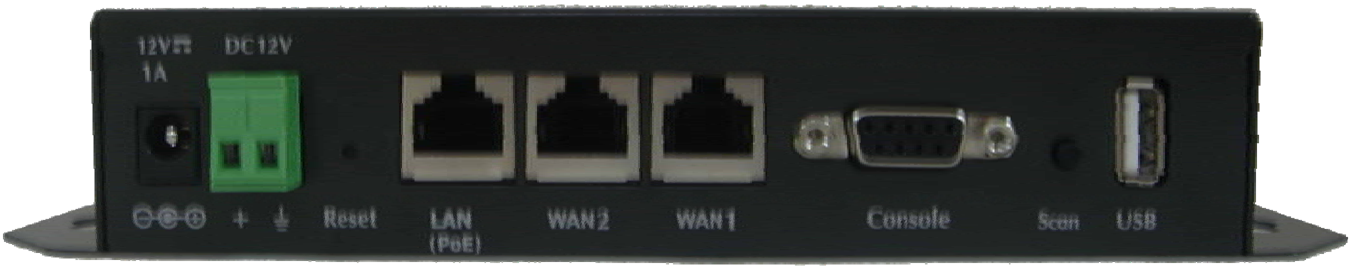
3.1 Installations

3.1.1 System Requirements

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

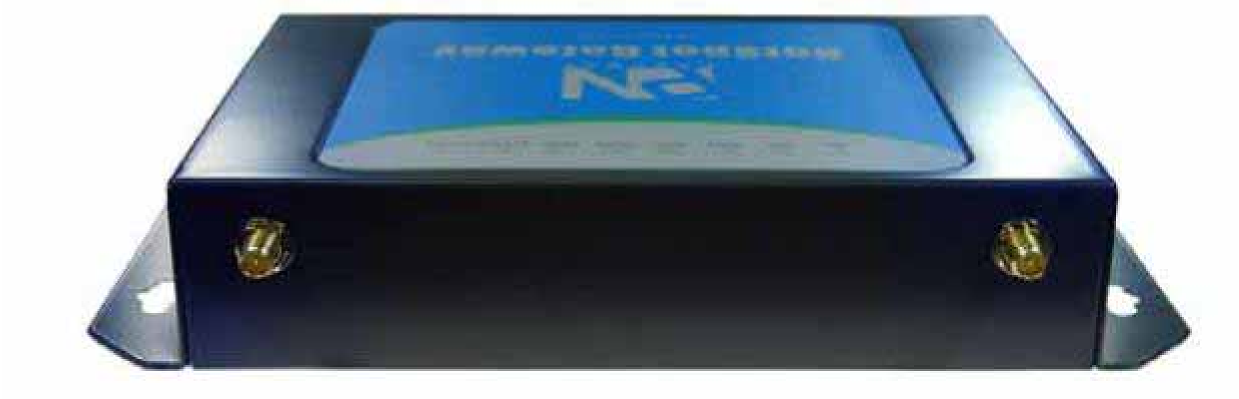
3.1.2 Panel Function Descriptions

Front Panel



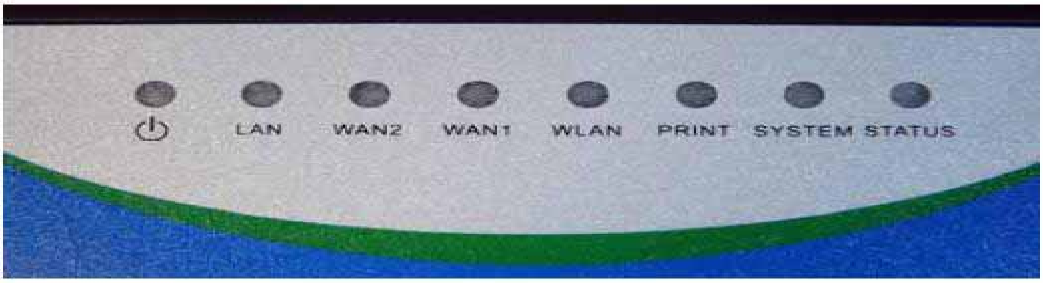
1. **Power SOCKET (12V DC) :** Attach the power socket here.
2. **Reset :** Press the Reset button once to restart the system, The LED except Power indicator will be off before restarting.
3. **LAN(POE) :** Clients devices connect to WAS-105R via LAN ports
4. **WAN1/WAN2 :** Two WAN ports are available on the system.
5. **Console :** The serial RS-232 DB9 cable attaches here.
6. **Scan Button :**
   - ➔ Press and hold the Scan button for **3** seconds until **STATUS LED FLASH** and release to Scan New AP's Channel.
   - ➔ Press and hold the Scan button for more than **10** seconds until **SYSTEM LED FLASH** to reset the system to default configurations.
7. **USB :** (option)

Rear Panel



1. WAS-105R supports 1 RF interface with 2 SMA connectors for Antenna connection.

LED Panel



1. **Power :** LED ON indicates power on, OFF indicates power off.
2. **WAN1/WAN2/LAN :** LED ON indicates connection, OFF indicates disconnection, FLASH indicates packets transmitting.
3. **WLAN :** LED ON indicates Wireless ready.
4. **PRINT :** LED ON indicates PSS-120 ready.
5. **SYSTEM :** LED ON/FLASH indicates Flash busy, OFF indicates Flash Idle
6. **STATUS :** LED ON indicates System up, OFF indicates down, FLASH indicates Scan button activated.

3.1.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of WAS-105R

1. Place the WAS-105R at a best location.

   The best location for WAS-105R is usually at the center of your wireless network.

2. Connect WAS-105R to your outbound network device.

   Connect one end of the Ethernet cable to the WAN1/WAN2 port of WAS-105R on the front panel. On your environment, connect the other end of the cable to the external Internet . The WAN1/WAN2 LED indicator should be ON to indicate a proper connection.

3. Connect WAS-105R to your network device.

   Connect one end of the Ethernet cable to LAN port of WAS-105R on the front panel. Connect the other end of cable to a PC for configuring the system. The LAN LED indicator should be ON to indicate a proper connection.

4. There are two ways to supply power over to WAS-105R

   ➔ Connect the DC power adapter to the WAS-105R power socket on the front panel.

Please only use the power adapter supplied with the WAS-105R package. Using a different power adapter may damage this system

   ➔ WAS-105R is capable of transmitting DC current via its LAN(PoE) port. Connect an IEEE 802.3af-compliant PSE device, e.g. A PoE Switch, to the LAN(PoE) port of WAS-105R with the Ethernet cable.

Now, the hardware installation is completed.

To double verify the wired connection between WAS-105R and your switch/router/hub, please check the LED status indication of these network devices.

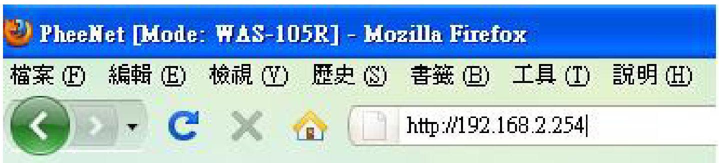
3.2 Software Configuration

3.2.1 Getting Start

Step :

1. Once the hardware installation is done, set DHCP in TCP/IP of the administrator's PC to get an IP address automatically. Connect the PC to the LAN(PoE) port of WAS-105R. An IP address will be assigned to the PC automatically via the WAS-105R.

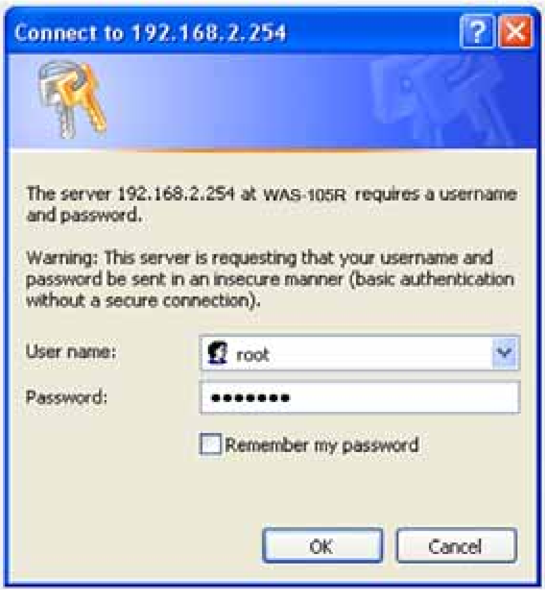
2. Launch a web browser to access the web GUI of WAS-105R by entering "**http://192.168.2.254**" in the address field.



PheeNet [Mode: WAS-105R] - Mozilla Firefox

http://192.168.2.254

3. The following Administrator Login Page will appear. Enter "**root**" in the Username field, and "**default**" in the Password field. Click **OK** button to login.



Connect to 192.168.2.254

The server 192.168.2.254 at WAS-105R requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: root

Password: ••••••••

□ Remember my password

If you can't get the login screen, you may have incorrectly set your PC to obtain an IP address automatically from LAN port or the IP address used does not have the same subnet as the URL. Please use default IP address such as 192.168.2.xx in your network and then try it again.

You can login as **root**, **admin** or **operator**. The default username and password as follows.

- Root : The administrator can access all area of the WAS-105R

  Username : **root**

  Password : **default**

- admin : The admin can access the area under *Service Domain*, *Wireless* and *Advanced* setting (**Please see Appendix B**.)

  Username : **admin**

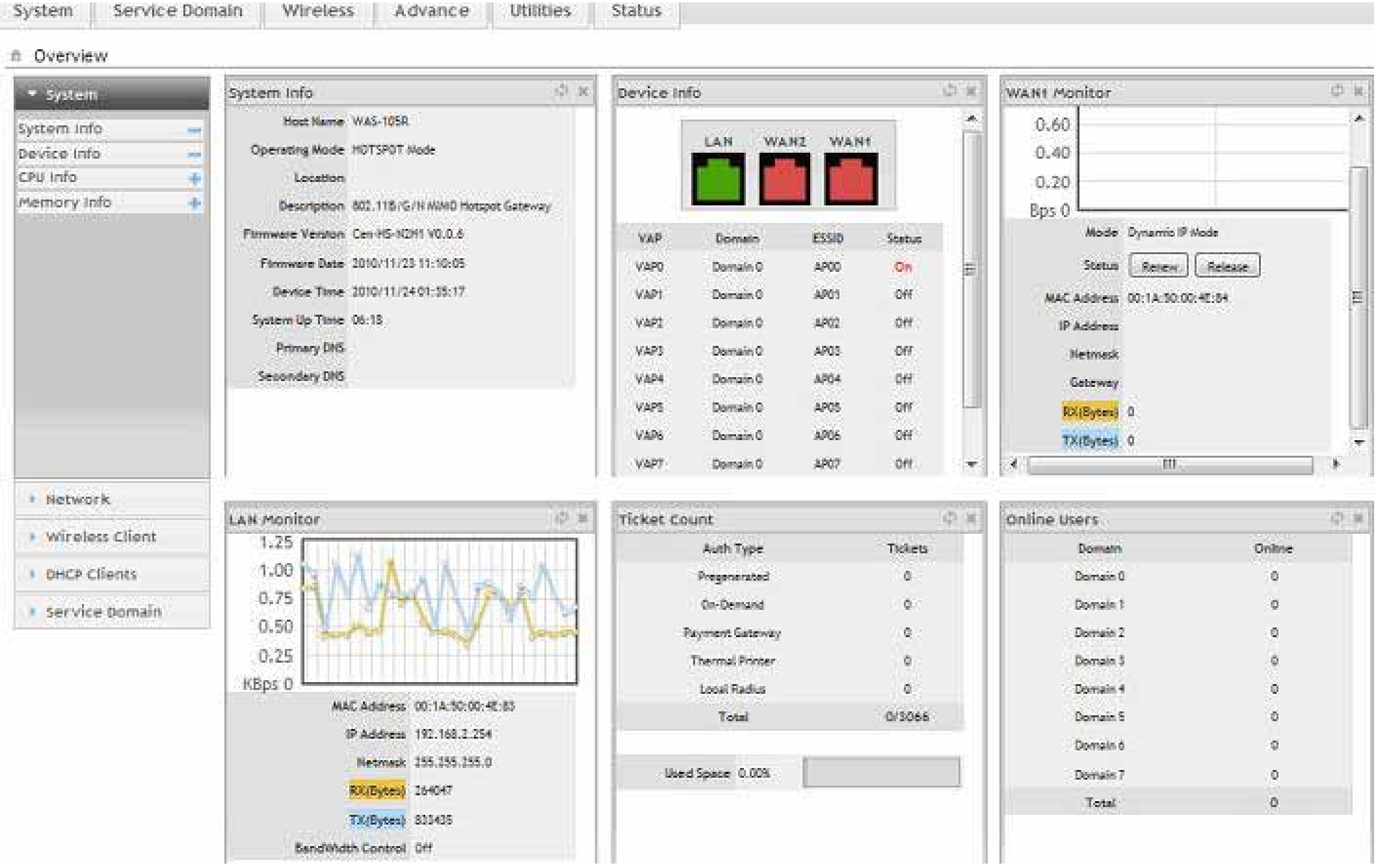
  Password : **admin**

- operator : The operator only can access the area of *On-Demand authentication* to create, edit and print out the new on-demand user accounts. (**Please see Appendix B**.)

  Username : **operator**

  Password : **1234**

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



System Info

Host Name	WAS-105R
Operating Mode	HOTSPOT Mode
Location	
Description	802.11B/G/N MIMO Hotspot Gateway
Firmware Version	Cen-HS-N2H1 V0.0.6
Firmware Date	2010/11/23 11:10:05
Device Time	2010/11/24 01:35:17
System Up Time	06:18
Primary DNS	
Secondary DNS	

Device Info

VAP	Domain	ESSID	Status
VAP0	Domain 0	AP00	On
VAP1	Domain 0	AP01	Off
VAP2	Domain 0	AP02	Off
VAP3	Domain 0	AP03	Off
VAP4	Domain 0	AP04	Off
VAP5	Domain 0	AP05	Off
VAP6	Domain 0	AP06	Off
VAP7	Domain 0	AP07	Off

WAN1 Monitor

Mode	Dynamic IP Mode
Status	Renew Release
MAC Address	00:1A:50:00:4E:84
IP Address	
Netmask	
Gateway	
RX(Bytes)	0
TX(Bytes)	0

LAN Monitor

MAC Address	00:1A:50:00:4E:83
IP Address	192.168.2.254
Netmask	255.255.255.0
RX(Bytes)	264047
TX(Bytes)	833435
BandWidth Control	Off

Ticket Count

Auth Type	Tickets
Pregenerated	0
On-Demand	0
Payment Gateway	0
Thermal Printer	0
Local Radius	0
Total	0/3066

Used Space 0.00%

Online Users

Domain	Online
Domain 0	0
Domain 1	0
Domain 2	0
Domain 3	0
Domain 4	0
Domain 5	0
Domain 6	0
Domain 7	0
Total	0

3.2.2 Quick Configuration

WAS-105R provides wireless and wired network service with authentication required for clients in Service Domain. Clients in the each Service Domain are isolated with each other. WAS-105R supports 8 Service Domains, Domain-0 to Domain-7. Administrator can select authentication type on each Service Domain. If *Authentication Required* is enabled, the clients are required to get authenticated successfully before access the Internet.

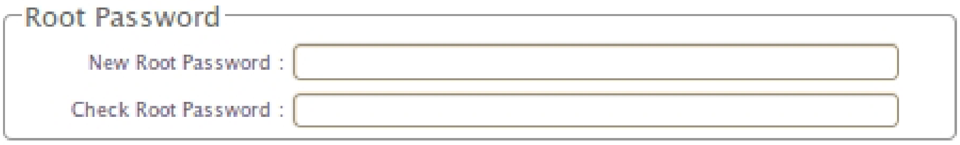
Configuration Steps :

Step 1 : Change Root's Password

➔ Click **System -> Management**, the Management Setup page will appear.

➔ Enter a ***New Root Password*** for the Root account ad retype in the ***Check Root Password*** field. (**4-30** alphanumeric and specific characters; **not** support **Space**)

➔ Click Save button.



Root Password

New Root Password :

Check Root Password :

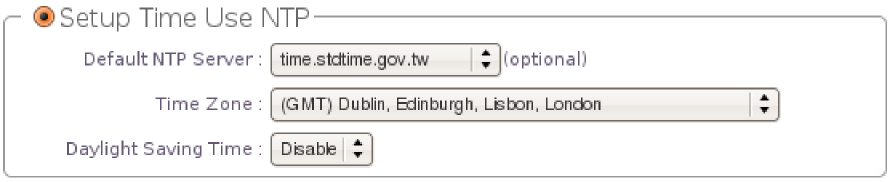
For security concern, it is strongly recommended to change the Root password.

Step 2 : Choose System's Time Zone

➔ Click **System -> Time Server**, the Time Server Setup page will appear.

➔ Select the appropriate NTP Server, Time Zone from drop-down list.

➔ Click ***Save*** button.



● Setup Time Use NTP

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight Saving Time : Disable

Before Hotspot service active, make sure the Local Time is correctly.

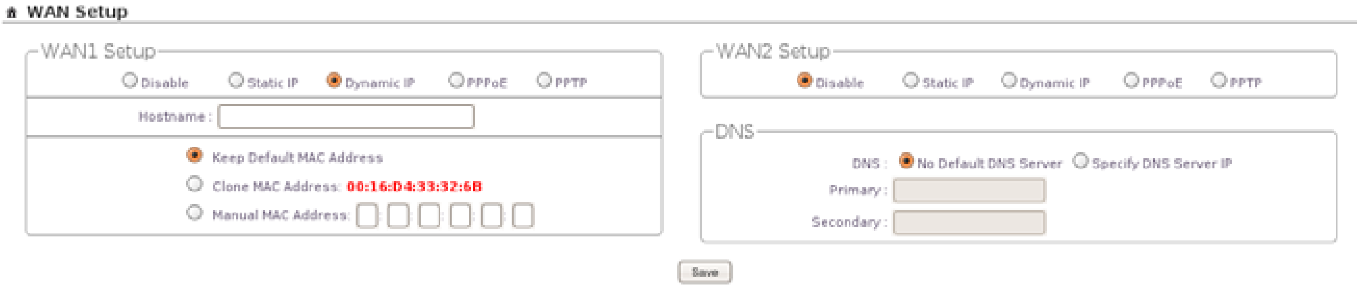
Step 3 : Select Connection Type for WAN1 Port and Set DNS Server

➔ Click **System -> WAN**, the WAN Setup page will appear.

➔ Select the appropriate Connection Type for WAN1 port, there are four types of WAN1 connections to be selected from: **Static IP**, **Dynamic IP**, **PPPoE Client** and **PPTP Client**.

➔ Enter the IP Address of a DNS Server provided by your ISP(Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

➔ Click ***Save*** button.


WAN Setup

WAN1 Setup
○ Disable ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP
Hostname :
● Keep Default MAC Address
○ Clone MAC Address: 00:16:D4:33:32:6B
○ Manual MAC Address:

WAN2 Setup
● Disable ○ Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

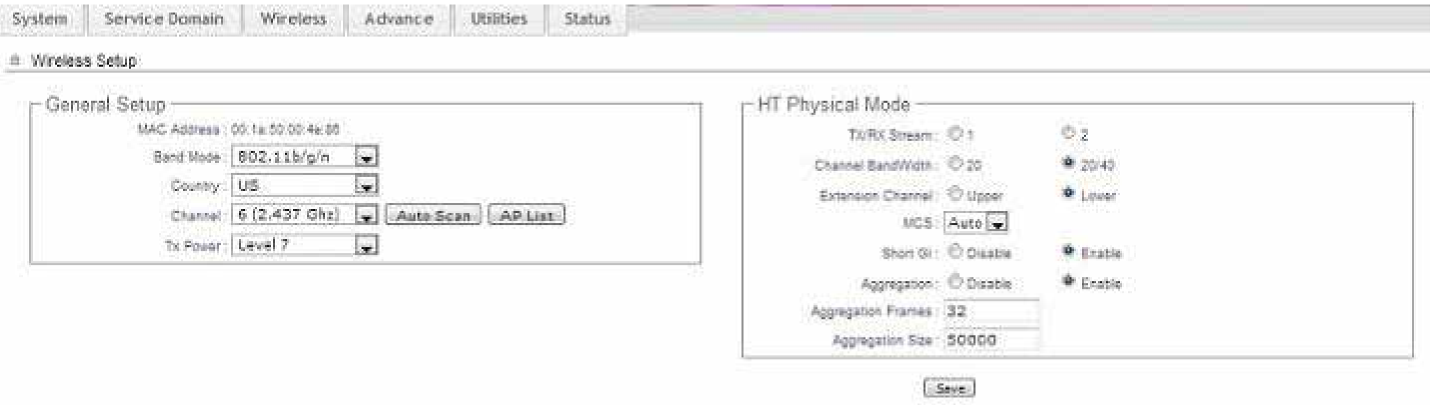
DNS
DNS : ● No Default DNS Server ○ Specify DNS Server IP
Primary :
Secondary :

Step 4 : Configure Wireless General Settings

➔ Click **Wireless -> General Setup**, the Wireless General Setup page will appear.

➔ Select desired wireless **Band**, **Channel**.

➔ Click ***Save*** button



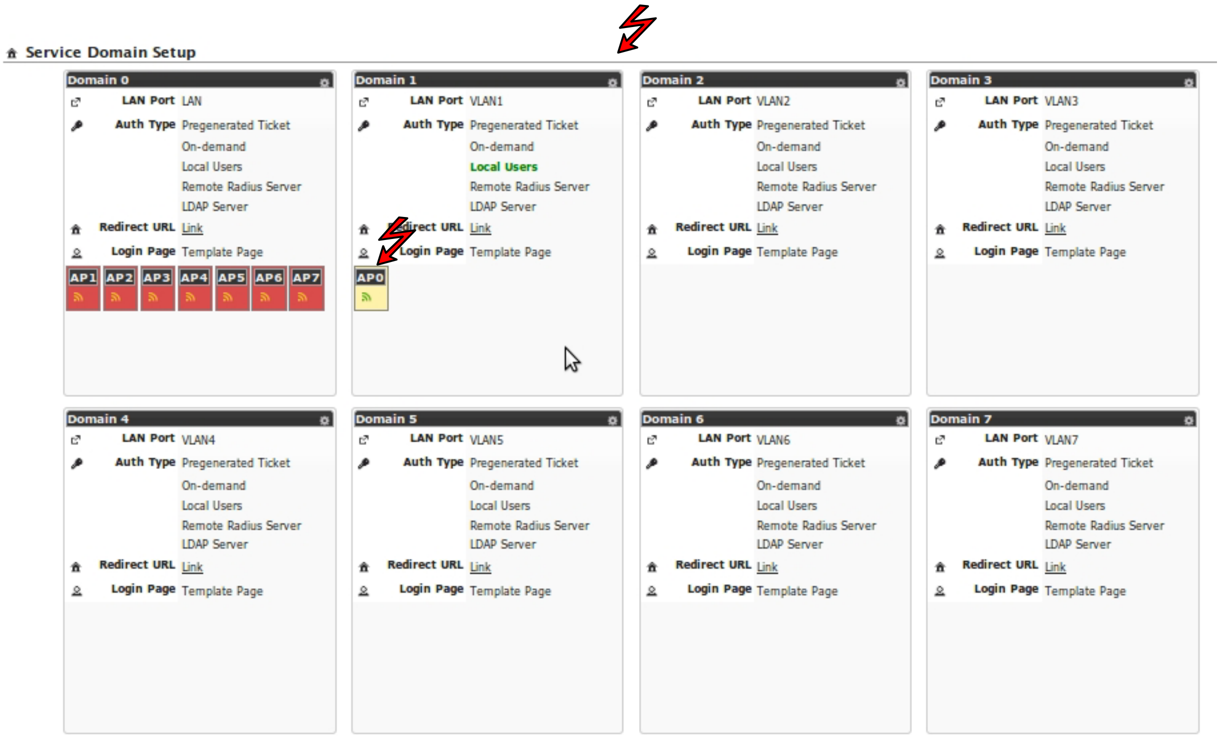
Wireless Setup

General Setup
MAC Address : 00:1a:50:00:4e:88
Band Mode : 802.11b/g/n
Country : US
Channel : 6 (2.437 Ghz)
Tx Power : Level 7

HT Physical Mode
TX/RX Stream : ○ 1 ○ 2
Channel BandWidth : ○ 20 ● 20/40
Extension Channel : ○ Upper ● Lower
MCS : Auto
Short GI : ○ Disable ● Enable
Aggregation : ○ Disable ● Enable
Aggregation Frames : 32
Aggregation Size : 50000

Step 5 : Set Virtual AP and Select Authentication Type for Service Domain

➔ Click **Service Domain**, the Service Domain Setup page will appear.



Service Domain Setup

Domain 0
LAN Port LAN
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page
AP1 AP2 AP3 AP4 AP5 AP6 AP7

Domain 1
LAN Port VLAN1
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page
AP0

Domain 2
LAN Port VLAN2
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 3
LAN Port VLAN3
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

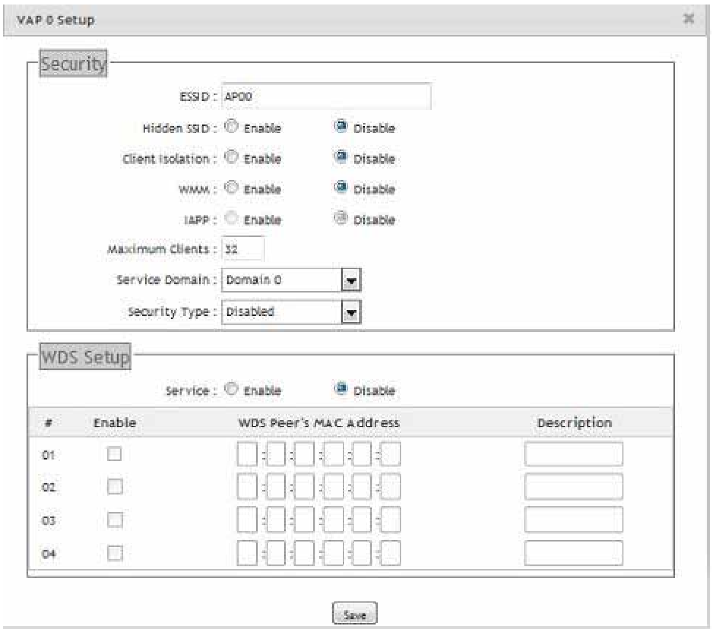
Domain 4
LAN Port VLAN4
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 5
LAN Port VLAN5
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 6
LAN Port VLAN6
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 7
LAN Port VLAN7
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

➔ Move **AP0 Icon** to Domain 1 window and click, the VAP0 Setup page will appear.



VAP 0 Setup

Security

ESSID : AP00
Hidden SSID : ○ Enable ● Disable
Client Isolation : ○ Enable ● Disable
WMM : ○ Enable ● Disable
IAPP : ○ Enable ● Disable
Maximum Clients : 32
Service Domain : Domain 0
Security Type : Disabled

WDS Setup

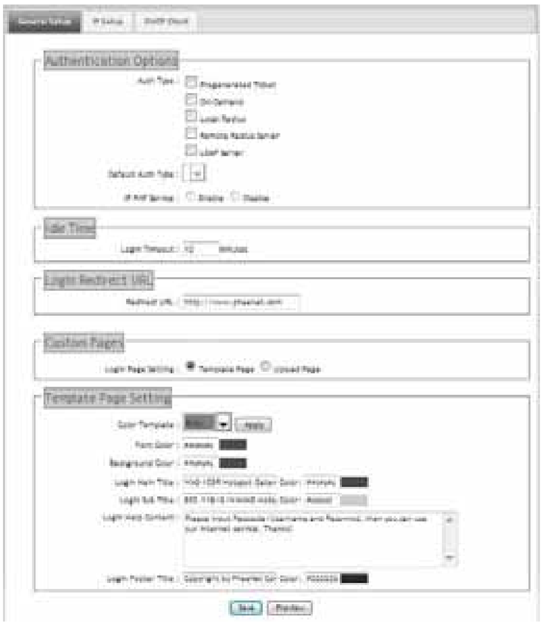
Service : ○ Enable ● Disable

#	Enable	WDS Peer's MAC Address	Description
01	□	__:__:__:__:__:__	
02	□	__:__:__:__:__:__	
03	□	__:__:__:__:__:__	
04	□	__:__:__:__:__:__	

Save

➔ Select desired wireless **ESSID** and related settings.

➔ Click **Tool Icon** on ***Domain 1*** window, the Service Domain1 Setup page will appear. For each Service Domain(by default, authentication is **None**), authentication type can be selected in ***None***, ***Pregenerated Ticket***, ***On-Demand***, ***Local Radius***, ***Remote Radius Server*** and ***LDAP Server***. and select one authentication type for Default Auth Type. Below depicts an example for **Local Radius**.



Authentication Options

Auth Type : □ Pregenerated Ticket □ On-Demand □ Local Radius □ Remote Radius Server □ LDAP Server

Default Auth Type :

IP PnP Service : ○ Enable ○ Disable

Idle Time

Login Timeout : 10 minutes

Login Redirect URL

Redirect URL : http://www.planet.com

Custom Pages

Login Page Setting : ● Template Page ○ Upload Page

Template Page Setting

Color Template : Apply

Font Color :

Background Color :

Login Main Title :

Login Sub Title :

Login Help Content : Please input Passcode / Username and Password, then you can use our Internet service. Thanks!

Login Footer Title :

Save Preview

➔ Select ***Local Radius*** for Domain0's Authentication Type.

➔ Enter the ***Redirect URL*** that users should be initially directed to when successfully authenticated to the network.

➔ Configure related settings for the selected Auth Type.

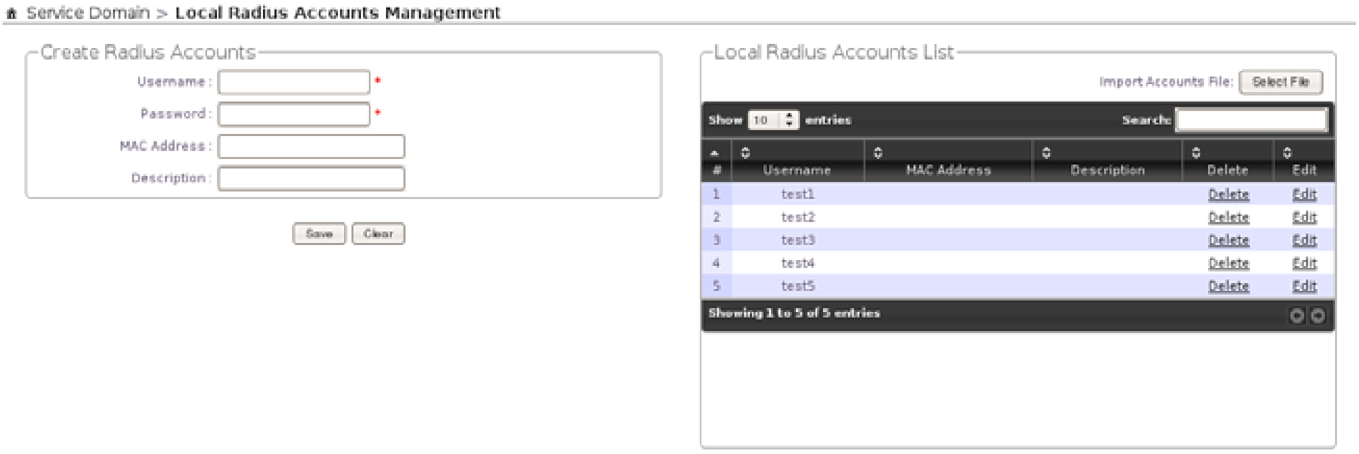
➔ Click ***Save*** button.

Step 6 : Add Local Radius Accounts

➔ Click **Service Domain -> Authentication -> Local Radius Accounts**, the Local Radius Accounts Management page will appear.

➔ A new account can be added into the Local Radius Database. To add a account here, enter the Username(e.g. **test1**), Password(e.g. **11111**), MAC Address(optional, to specify the valid MAC address of this account) and Description.

➔ More accounts can be added by clicking the Save button.



Service Domain > Local Radius Accounts Management

Create Radius Accounts

Username : *

Password : *

MAC Address :

Description :

Save Clear

Local Radius Accounts List

Import Accounts File: Select File

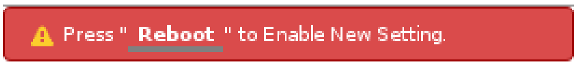
Show 10 entries Search:

#	Username	MAC Address	Description	Delete	Edit
1	test1			Delete	Edit
2	test2			Delete	Edit
3	test3			Delete	Edit
4	test4			Delete	Edit
5	test5			Delete	Edit

Showing 1 to 5 of 5 entries

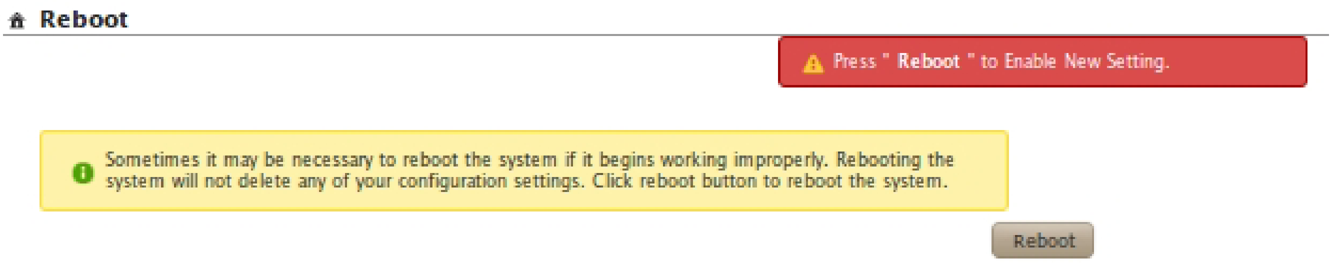
Step 7 : Restart WAS-105R

➔ Click **Reboot**, the Reboot page will appear



Press " Reboot " to Enable New Setting.

➔ Click ***Reboot*** button to start the restarting process.



Reboot

Press " Reboot " to Enable New Setting.

Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Please don't interrupt the system during the restarting process.

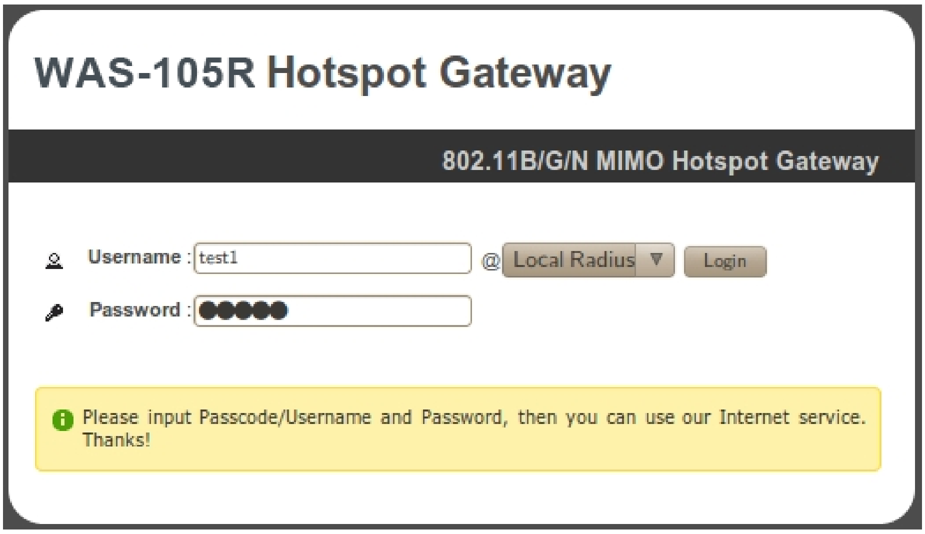
➔ When the “Home Page” appears, it means the restart process is now completed.

3.2.3 Access Internet

To verify whether the configuration of the new Local Radius accounts created via the **Quick Configuration** has been completed successfully :

Step :

1. Connect a client device (e.g. Notebook) with wireless interface to scan the configured ESSID of WAS-105R (e.g. **AP00**) and get associated with this ESSID.
2. The client device will obtain an IP address automatically via DHCP from WAS-105R. Open a web browser on a client device, access any URL, and then the Domain1 **User Login Page** will appear.



WAS-105R Hotspot Gateway

802.11B/G/N MIMO Hotspot Gateway

Username : test1 @ Local Radius ▼ Login

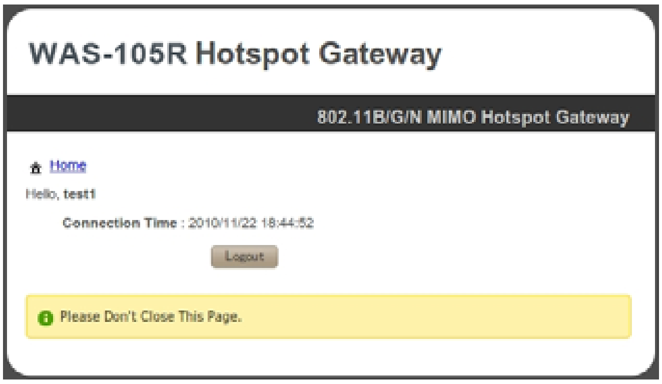
Password : ●●●●●

Please input Passcode/Username and Password, then you can use our Internet service. Thanks!

3. Enter the ***Username*** and ***Password*** of a Local Radius account previously generated via **Quick Configuration** (e.g. "**test1**" as the *Username* and "**11111**" as the *Password*); then Click **Login** button.

Congratulation !

The Timer page will appear after a client has successfully logged into WAS-105R and has been authenticated by the system. Now, you are connected the network and Internet!



WAS-105R Hotspot Gateway

802.11B/G/N MIMO Hotspot Gateway

Home

Hello, test1

Connection Time : 2010/11/22 18:44:52

Logout

Please Don't Close This Page.

Chapter 4. Web Interface Configuration

When Hotspot mode is activated, the system can be configured as a Wireless Hotspot Gateway. This section provides information in configuring the Hotspot mode with graphical illustrations. WAS-105R provides functions as stated below where they can be configured via a user-friendly web based interface.

OPTION	**System**	**Service Domain**	**Wireless**	**Advanced**	**Utilities**	**Status**
Function	WAN	Service Domain	General Setup	DMZ	Profile Setting	Overview
	WAN Traffic	Authentication	Advanced Setup	IP Filter	Firmware Upgrade	Extra Info
	LAN	Walled Garden	Virtual AP Setup	MAC Filter	Network Utility	Event Log
	DDNS	Notification	Associated Clients	Virtual Server	Format Database	
	Management	Online Users	WDS Status	Time Policy	Reboot	
	Time Server					
	SNMP					

After finishing the configuration of the settings, please click Save button and pay attention to see if a Reboot message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All online users will be disconnected during restart.

4.1 Connect WAS-105R to the external Network

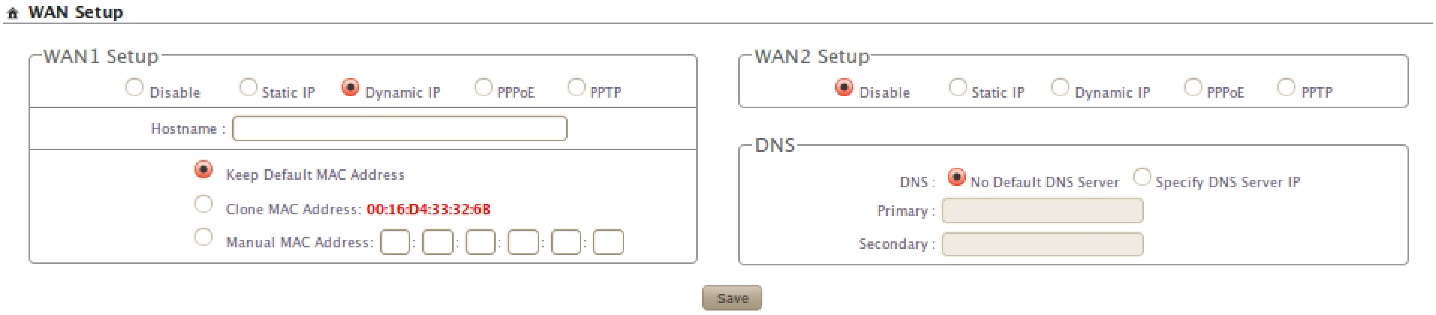
4.1.1 Network Requirement

Basically, in general network environment, the main role of WAS-105R is a Gateway. It manages all the network from internal network to Internet.

Then, the first step is to prepare an Internet connection from your ISP and connect it to the WAN or WAN2 port of WAS-105R.

4.1.2 Configure WAN Port

Here is instruction for how to setup the WAN. There are **two** WAN port can selected and configured. The connection types for each WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**, Please click on **System -> WAN** and follow the below setting.



WAN Setup

WAN1 Setup

○ Disable ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP

Hostname :

● Keep Default MAC Address

○ Clone MAC Address: 00:16:D4:33:32:6B

○ Manual MAC Address: □:□:□:□:□:□

WAN2 Setup

● Disable ○ Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

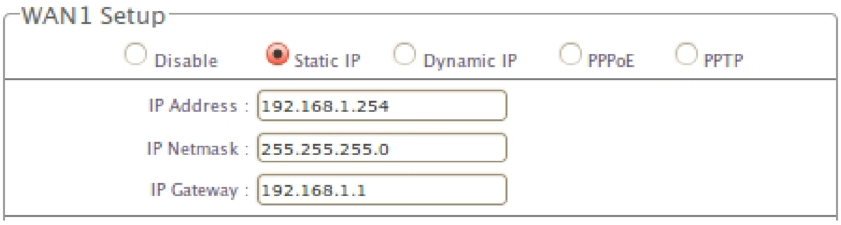
DNS

DNS : ● No Default DNS Server ○ Specify DNS Server IP

Primary :

Secondary :

- **Static IP :** The administrator can manually setup the WAN IP address when static IP is available/ preferred.



WAN1 Setup

○ Disable ● Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

IP Address : 192.168.1.254

IP Netmask : 255.255.255.0

IP Gateway : 192.168.1.1

➔ **IP Address :** The IP address of the WAN port.

➔ **IP Netmask :** The Subnet mask of the WAN port.

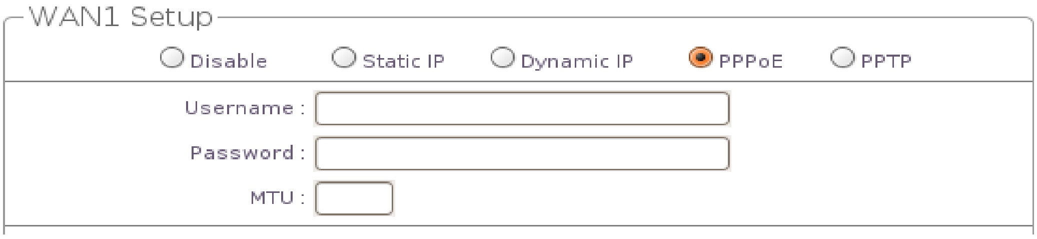
➔ **IP Gateway :** The IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. WAS-105R will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the WAS-105R's external network interface.

- **Dynamic IP :** This configuration type is applicable when the WAS-103R is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically. If the IP Address do not assigned from DHCP server, the system need manual connect to DHCP server.

  ➔ **Hostname :** The Hostname of the WAN port

- **PPPoE :** This configuration type is applicable when the WAS-105R is connected to a network with the presence of a PPPoE server.



WAN1 Setup

○ Disable ○ Static IP ○ Dynamic IP ● PPPoE ○ PPTP

Username :

Password :

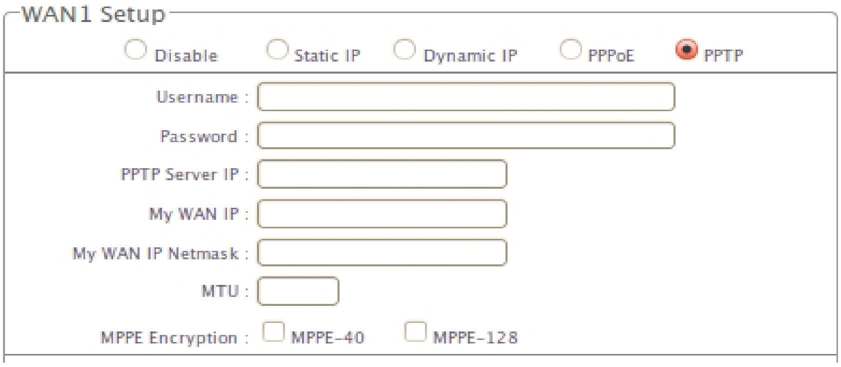
MTU :

➔ **User Name :** Enter User Name for PPPoE connection

➔ **Password :** Enter Password for PPPoE connection

➔ **MTU :** MTU stands for Maximum Transmission Unit. For PPPoE connections, you may need to set the MTU setting in order to work correctly with your ISP. Default is **1492** bytes.

- **PPTP :** The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



WAN1 Setup

○ Disable ○ Static IP ○ Dynamic IP ○ PPPoE ● PPTP

Username :

Password :

PPTP Server IP :

My WAN IP :

My WAN IP Netmask :

MTU :

MPPE Encryption : □ MPPE-40 □ MPPE-128

➔ **Username :** Enter User Name for PPTP connection

➔ **Password :** Enter Password for PPTP connection

➔ **PPTP Server IP Address :** The IP address of the PPTP server

➔ **My WAN IP :** The IP address of the WAN port

➔ **My WAN IP Netmask :** The Subnet mask of the WAN port

➔ **MTU :** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.

➔ **MPPE Encryption :** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.

■ **DNS :** Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.

➔ **Primary :** The IP address of the primary DNS server.

➔ **Secondary :** The IP address of the secondary DNS server.

■ **MAC Clone :** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.

➔ **Keep Default MAC Address :** Keep the default MAC address of WAN port on the system.

➔ **Clone MAC Address :** If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.

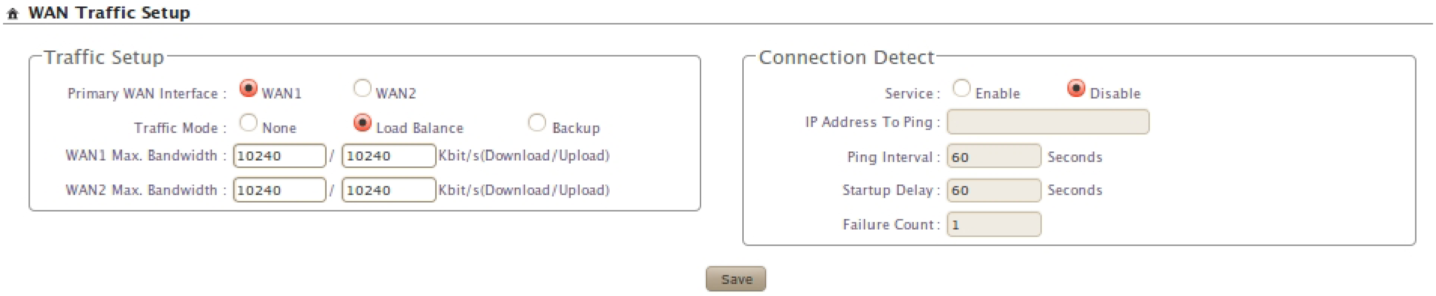
> The Clone MAC Address field will display MAC address of the PC connected to system. Click ***Save*** button can make clone MAC effective.

➔ **Manual MAC Address :** Enter the MAC address registered with your ISP.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.1.3 Configure WAN Traffic

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



WAN Traffic Setup

Traffic Setup

Primary WAN Interface : ● WAN1 ○ WAN2

Traffic Mode : ○ None ● Load Balance ○ Backup

WAN1 Max. Bandwidth : 10240 / 10240 Kbit/s(Download/Upload)

WAN2 Max. Bandwidth : 10240 / 10240 Kbit/s(Download/Upload)

Connection Detect

Service : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 60 Seconds

Startup Delay : 60 Seconds

Failure Count : 1

- **Traffic Setup :**
  - ➔ **Primary WAN Interface :** Select desired primary WAN interface for system.
  - ➔ **Traffic Mode :** There are **three** types : **None**, **Load Balance** and **Backup**.
    - ✓ **Load Balance :** Outbound load balancing is supported by the system. When enabled, the system will allocate traffic between WAN1 and WAN2 dynamically according to designed algorithms based on the Bandwidth.
      - **WAN1 Max. Bandwidth :** Specify the maximum download and upload bandwidth that can be shared by clients of the WAN1 port.
      - **WAN2 Max. Bandwidth :** Specify the maximum download and upload bandwidth that can be shared by clients of the WAN2 port.

On the Load Balance traffic mode, the primary WAN port is WAN1. When the WAN1 connection is down, the WAN2 will backup automatically.

- ✓ **Backup :** When primary WAN interface is WAN1 and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. When WAN1 connection is up, the route traffic will be connected back to WAN1 automatically.

- **Connection Detect :** The connect detect sets the WAS-105R Device to continuously ping a user defined IP address (it can be the Internet gateway for example). If it is unable to ping under the user defined constraints, the WAS-105R device will change **Primary WAN** interface to secondary WAN interface automatically . This option only for "**Load Balance**" or "**Backup**" traffic mode.

➔ **Service :** By default, it's “Disable”. To “Enable” to activate this function.

➔ **IP Address To Ping :** specify an IP address of the target host which will be monitored

➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent. Default is **60** seconds.

➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **60** seconds.

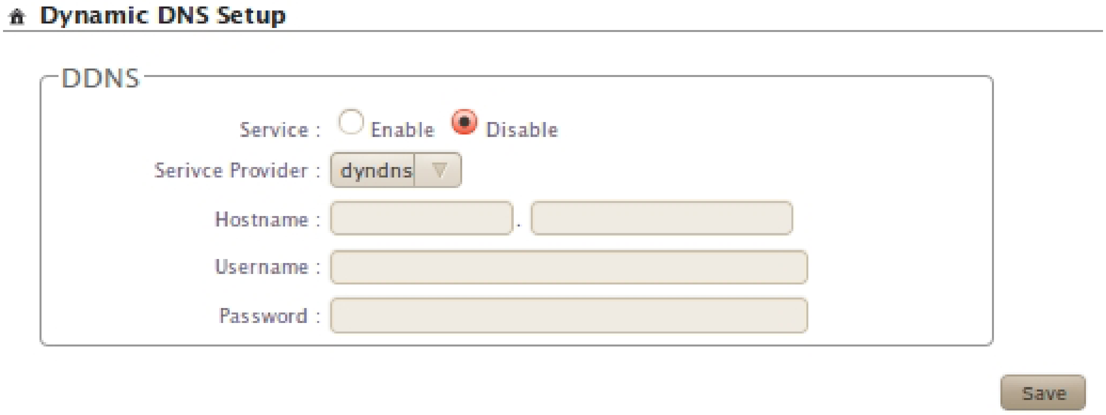
➔ **Failure Count :** specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the primary WAN traffic will be routed secondary WAN.

If Connection Detect is disabled on “**Load Balance**” or “**Backup**”, the system will use default value.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.1.4 Configure Dynamic DNS

Dynamic DNS allows you to make an assumed name as a dynamic IP address to a static hostname. Please click on **System -> DDNS** and follow the below setting.



Dynamic DNS Setup

DDNS

Service : ○ Enable ● Disable

Serivce Provider : dyndns

Hostname : .

Username :

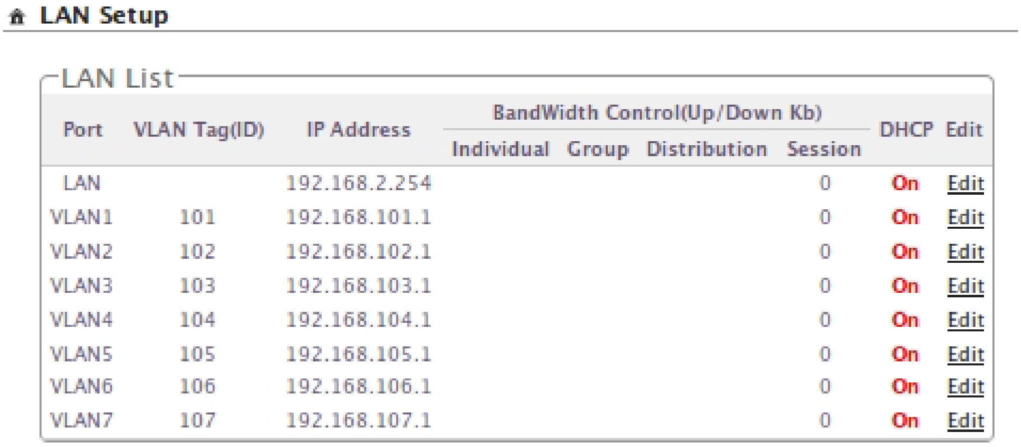
Password :

- **Enabled:** Select Enable for DDNS function, each time your IP address for WAN is changed, the information will be updated to DDNS service provider automatically.
- **Service Provider:** Select the correct Service Provider from the drop-down list, here included are *dyndns*, *dhs*, *ods* and *tzo* embedded in the WAS-105R.
- **Hostname:** This field represents the Host Name you register to Dynamic-DNS service and expect to export to the world.
- **User Name & Password:** User Name and Password is used as an identity to login DDNS service.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.1.5 Configure Local(LAN/VLAN) Network

Here is the instruction for how to setup the local LAN/VLAN IP Address and Netmask. Please click on **System -> LAN** , the LAN List should be appear. This page shows information of LAN's/VLAN's settings.



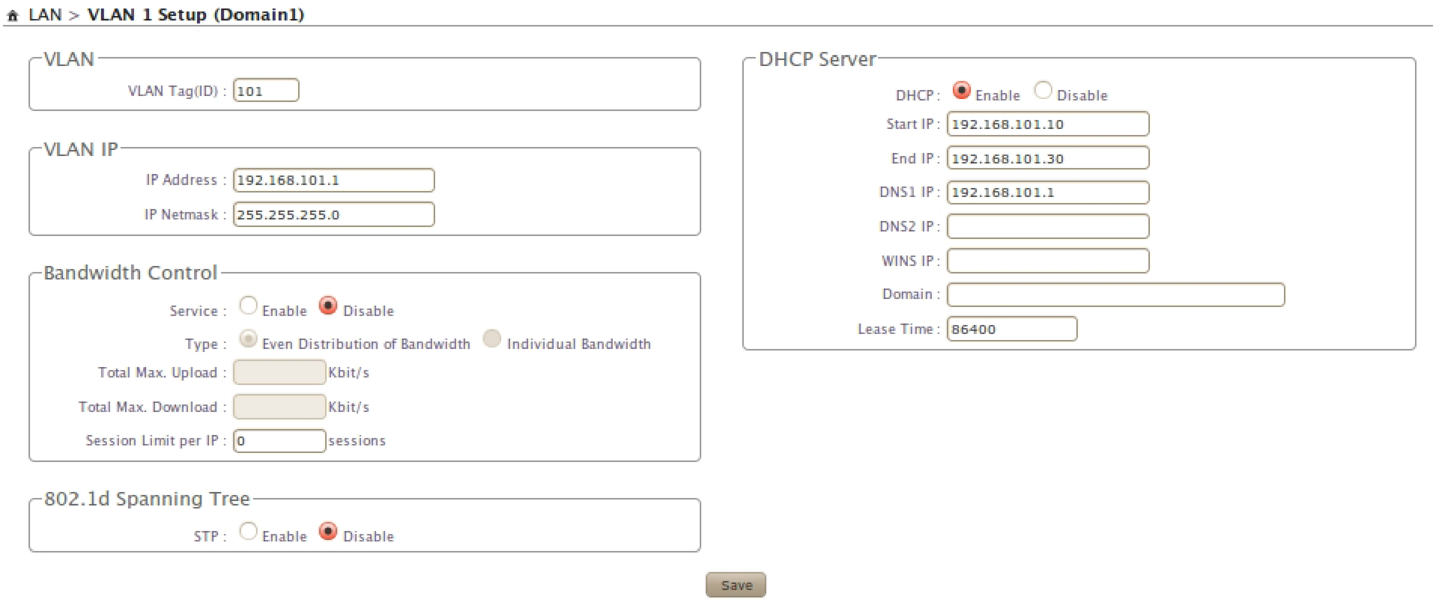
LAN Setup

LAN List

Port	VLAN Tag(ID)	IP Address	BandWidth Control(Up/Down Kb)				DHCP	Edit
			Individual	Group	Distribution	Session		
LAN		192.168.2.254				0	On	Edit
VLAN1	101	192.168.101.1				0	On	Edit
VLAN2	102	192.168.102.1				0	On	Edit
VLAN3	103	192.168.103.1				0	On	Edit
VLAN4	104	192.168.104.1				0	On	Edit
VLAN5	105	192.168.105.1				0	On	Edit
VLAN6	106	192.168.106.1				0	On	Edit
VLAN7	107	192.168.107.1				0	On	Edit

- **Port :** Indicate the system's LAN/VLAN port.
- **VLAN Tag(ID) :** Indicate the VLAN tag of the respective VLAN port. Only for VLAN1 ~ VLAN7
- **IP Address : ** Indicate the IP address of the respective LAN/VLAN port.
- **Individual :** Indicate the Individual Max. Upload/Download of the respective LAN/VLAN port.
- **Group :** Indicate the Group Upload/Download of the respective LAN/VLAN port.
- **Distribution :** Indicate the Distribution Upload/Download of the respective LAN/VLAN port.
- **Session :** Indicate the Session of the respective LAN/VLAN port.
- **DHCP :** Indicate the DHCP server status of the respective LAN/VLAN.
- **Edit :** Click **Edit** button to configure LAN/VLAN's settings.

Click “**Edit**” button on this page, the setup page should be appear. Below depicts an example for **VLAN1**.



LAN > **VLAN 1 Setup (Domain1)**

VLAN

VLAN Tag(ID) : 101

VLAN IP

IP Address : 192.168.101.1

IP Netmask : 255.255.255.0

Bandwidth Control

Service : ○ Enable ● Disable

Type : ● Even Distribution of Bandwidth ○ Individual Bandwidth

Total Max. Upload : Kbit/s

Total Max. Download : Kbit/s

Session Limit per IP : 0 sessions

802.1d Spanning Tree

STP : ○ Enable ● Disable

DHCP Server

DHCP : ● Enable ○ Disable

Start IP : 192.168.101.10

End IP : 192.168.101.30

DNS1 IP : 192.168.101.1

DNS2 IP :

WINS IP :

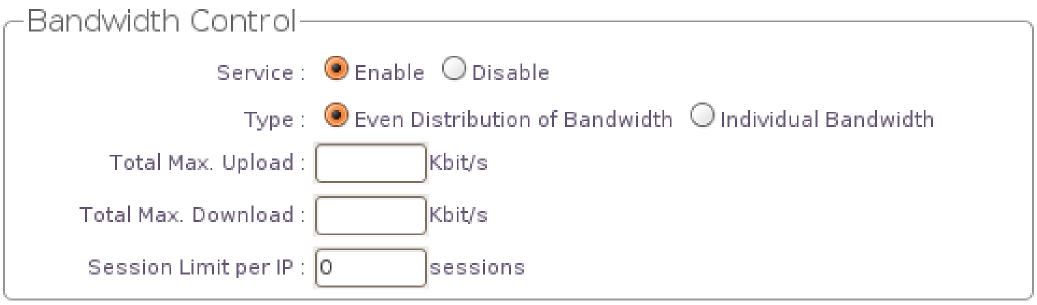
Domain :

Lease Time : 86400

- **VLAN Tag(ID) :** Virtual LAN, the system supports **7** tagged VLAN port. The valid values are from **0** to **4094**.

Some system and VLAN switch do not support VLAN tag 0 and 1

- **IP Address :** The IP address of the VLAN port; The default VLAN1's ~ VLAN7's IP address as **192.168.101.1** ~ **192.168.107.1**.
- **IP Netmask :** The Subnet mask of the VLAN port; default Netmask is 255.255.255.0
- **Bandwidth Control :** By default, it's "**Disable**". To "**Enable**" to use bandwidth control.



Bandwidth Control

Service : ● Enable ○ Disable

Type : ● Even Distribution of Bandwidth ○ Individual Bandwidth

Total Max. Upload : Kbit/s

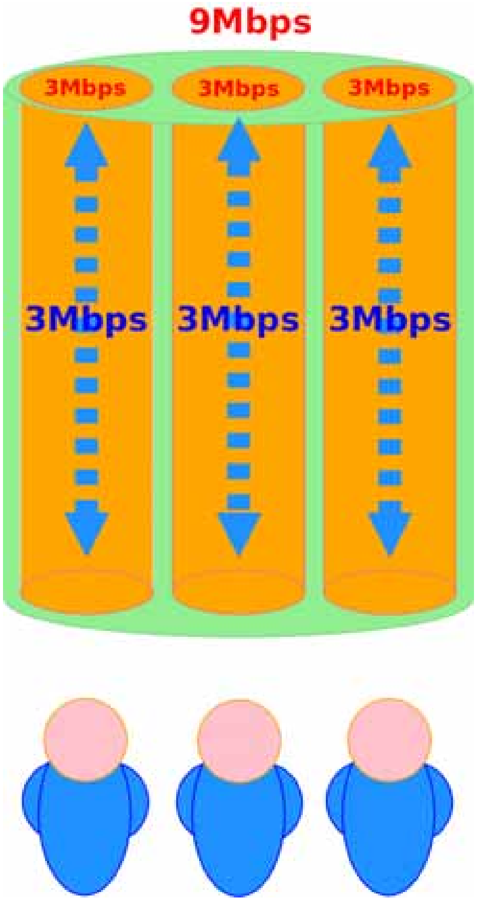
Total Max. Download : Kbit/s

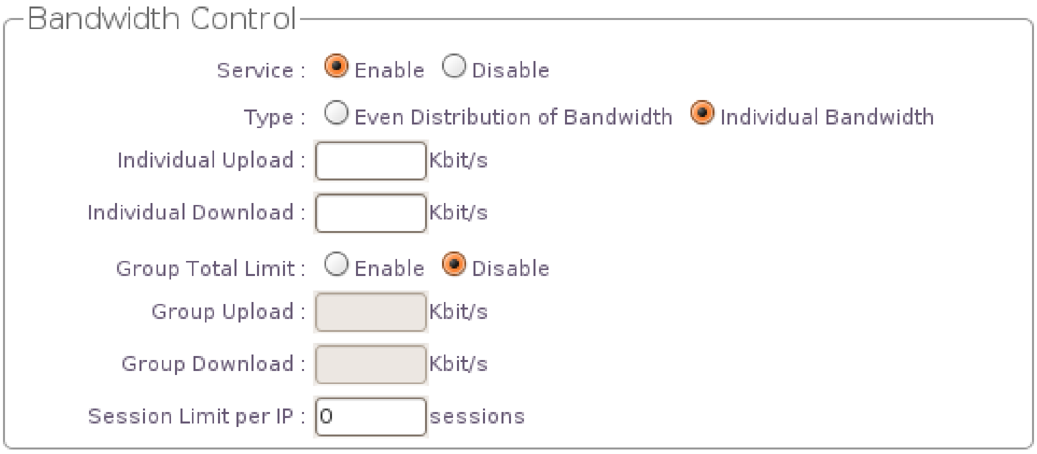
Session Limit per IP : 0 sessions

➔ **Type :** Enable the desire option among "**Even Distribution of Bandwidth**" or "**Individual Bandwidth**"

➔ **Even Distribution of Bandwidth :** Set users distribute Total Max. Upload/Download. Below depicts an example for **Even Distribution of Bandwidth**, set Total Max. Upload or Download to 9 Mbps, if one user access Internet, the maximum upload or download is 9 Mbps; if three users access Internet at the same time, the maximum upload or download is 3 Mbps by each user.

- ✓ **Total Max. Upload :** The Total Max. Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s
- ✓ **Total Max. Download :** The Total Max. Download is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s





Bandwidth Control

Service : ● Enable ○ Disable

Type : ○ Even Distribution of Bandwidth ● Individual Bandwidth

Individual Upload : Kbit/s

Individual Download : Kbit/s

Group Total Limit : ○ Enable ● Disable

Group Upload : Kbit/s

Group Download : Kbit/s

Session Limit per IP : 0 sessions

➔ **Individual Bandwidth :** Set each users Individual Upload/Download. Below depicts an example for **Individual Bandwidth**, set Group Upload or Download to 6 Mbps and Individual Upload or Download to 3 Mbps, if one user access Internet, the maximum upload or download is 3 Mbps; if three users access Internet at the same time, the maximum upload or download is 3 Mbps by each user.

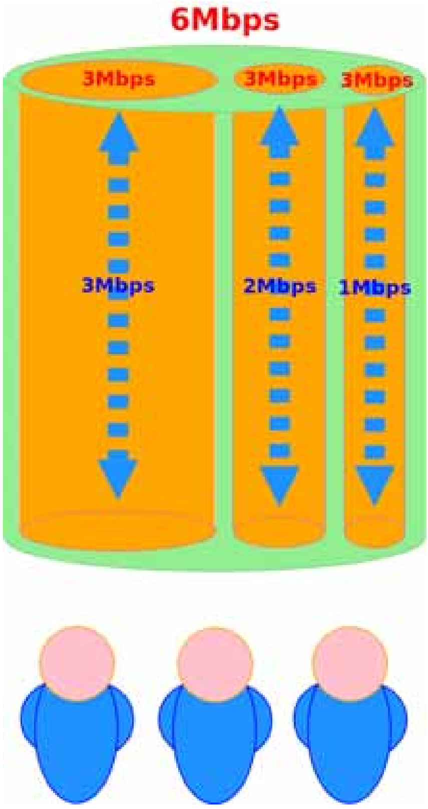
✓ **Individual Upload :** The Individual Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

✓ **Individual Download :** The Individual Download is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

✓ **Group Total Limit :** By default, it's "**Disable**". To "**Enable**" to activate Group Total Limit.

- **Group Upload :** The Group Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

寓 **Group Download :** The Group Download is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s



- ➔ **Guest Service :** By default, it's “**Disable**”. To ***Enable*** to activate bandwidth control service for guest users.
  - ✓ **Guest Upload :** The Guest Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s
  - ✓ **Guest Download :** The Guest Download is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s
- ➔ **Session Limit per IP :** The number of sessions is in the range of **10~500**, 0 indicates unlimited, default is **0**.

- ■ **STP :** By default, it's “**Disable**”. To “**Enable**” to activate STP.

The spanning tree network protocol provides a loop free topology for any bridged LAN/VLAN. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **DHCP :** Check “**Enable**” to activate DHCP Server on VLAN/LAN port.

  ➔ **Start IP / End IP :** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.

  ➔ **DNS1 / DNS2 IP :** The Domain Name System (DNS) is an Internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the WAS-105R.

DNS1 server IP is mandatory. It is used by the *DNS Proxy* and for the device management purpose.

DNS2 server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

  ➔ **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.

  ➔ **Domain :** Enter the domain name for this network.

  ➔ **Lease Time:** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server.

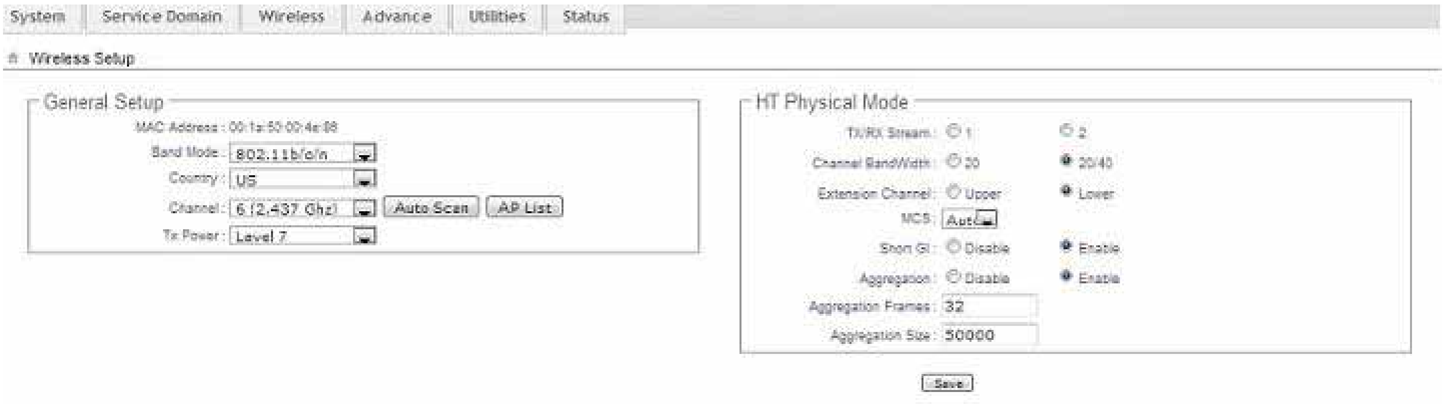
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.2 Create Your Wireless Network

The system manager can configure related wireless settings, **General Settings, Advanced Settings, Virtual AP Setting, Security Settings** and **Access Control Settings**.

4.2.1 Configure Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



General Setup

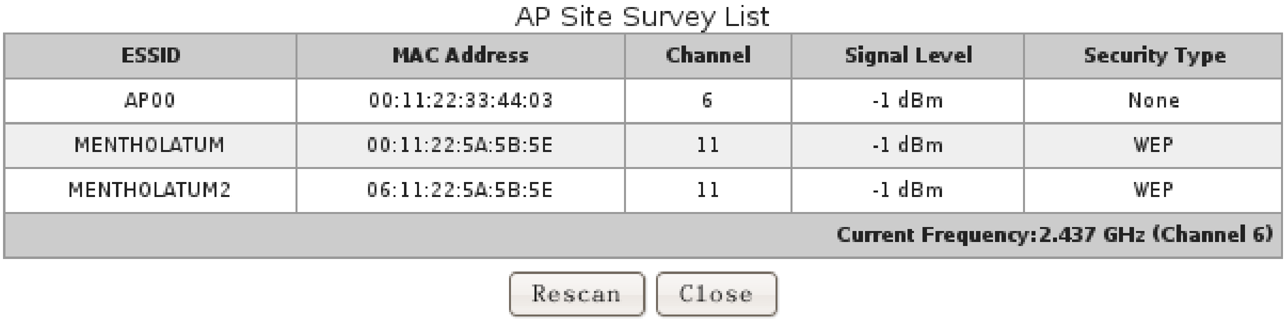
MAC Address : 00:1a:50:00:4e:08
Band Mode : 802.11b/g/n
Country : US
Channel : 6 (2.437 Ghz)
Tx Power : Level 7

HT Physical Mode

TX/RX Stream : ○ 1 ○ 2
Channel BandWidth : ○ 20 ● 20/40
Extension Channel : ○ Upper ● Lower
MCS : Auto
Short GI : ○ Disable ● Enable
Aggregation : ○ Disable ● Enable
Aggregation Frames : 32
Aggregation Size : 50000

- **MAC address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11b/g, 802.11b/g/n and 802.11n.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1Mbps to 54Mbps for 802.11b/g modes, or 1Mbps to 11Mbps for 802.11b mode.
- **Country :** Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from **1** to **11** for **US** country code, or **1** to **13** for **ETSI** country code, or **1** to **14** for Japan(Channel **14** only for **802.11b** Rate).

Click "**Auto Scan**", the channel will change to next channel. Click "**AP List**" button, the system will show current all AP list.



AP Site Survey List

ESSID	MAC Address	Channel	Signal Level	Security Type
AP00	00:11:22:33:44:03	6	-1 dBm	None
MENTHOLATUM	00:11:22:5A:5B:5E	11	-1 dBm	WEP
MENTHOLATUM2	06:11:22:5A:5B:5E	11	-1 dBm	WEP
				Current Frequency:2.437 GHz (Channel 6)

- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select LEVEL 1 to LEVEL 7 needed for your environment. If you are not sure of which setting to choose, then keep the default setting, **LEVEL 7**.

When **Band Mode** select in **802.11b/g/n or 802.11n**, the **HT Physical Mode** settings should be show immediately.

- **Tx/Rx Stream :** By default, it's **2**.
- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel :** Only for Channel Bandwidth "**40**" MHz. Select the desired channel bonding for control.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation :** By default, it's "Enable". To "Disable" to deactivated Aggregation.

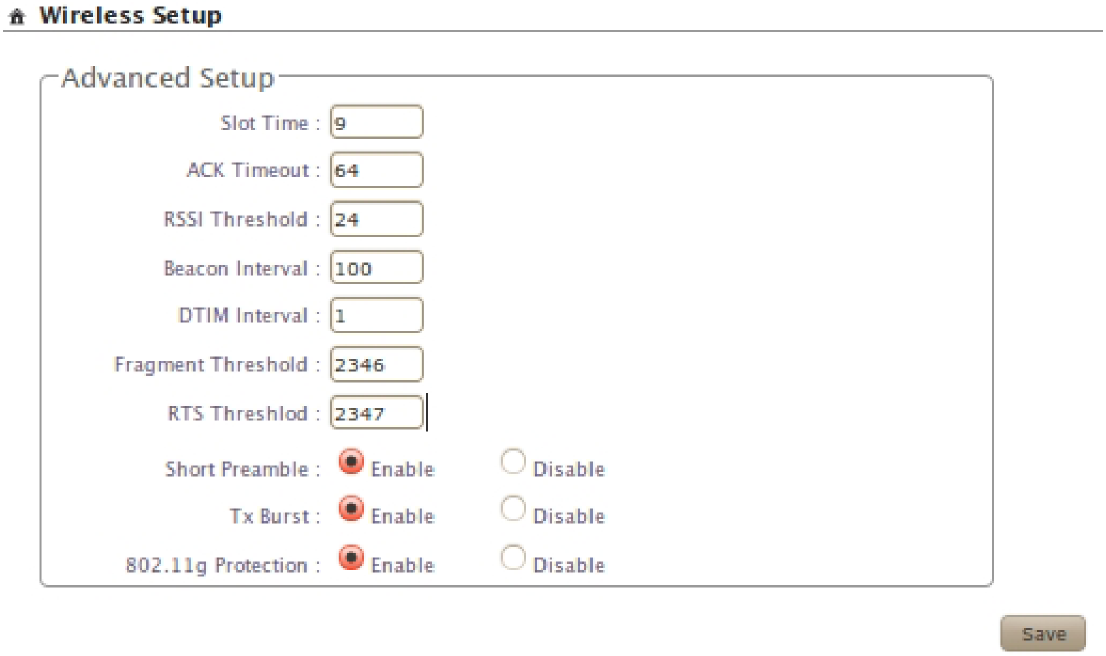
A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

- **Aggregation Frames :** The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- **Aggregation Size :** The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

4.2.2 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



Wireless Setup

Advanced Setup

Slot Time : 9

ACK Timeout : 64

RSSI Threshold : 24

Beacon Interval : 100

DTIM Interval : 1

Fragment Threshold : 2346

RTS Threshlod : 2347

Short Preamble : ● Enable ○ Disable

Tx Burst : ● Enable ○ Disable

802.11g Protection : ● Enable ○ Disable

- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.

  All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

> Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI(Received Signal Strength Indication) Threshold is in the range of **-127 ~ 128**. The default value is **24**. RSSI Threshold can be used to control the level of noise received by the device.
- **Beacon Interval :** Beacon Interval is in the range of **40**~**3500** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.
- **DTIM Interval :** The DTIM interval is in the range of **1**~**255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **802.11g Protection :** Click ***Enable*** button to activate 802.11g Protection Mode, and Disable to inactivate 802.11g Protection Mode.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

4.2.3 Create Virtual AP

The WAS-105R support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into 8 logical access points, each of which can have a different set of security, VLAN Tag(ID) and network settings. If wireless client connect to wired area network with VLAN Tag(ID), the administrator can use dump switch or VLAN switch on wired area network, a **Figure 4-1** shows multiple SSIDs with different VLAN settings use dump switch connect to wired area. a **Figure 4-2** shows multiple SSIDs with different VLAN settings use VLAN switch connect to wired area.

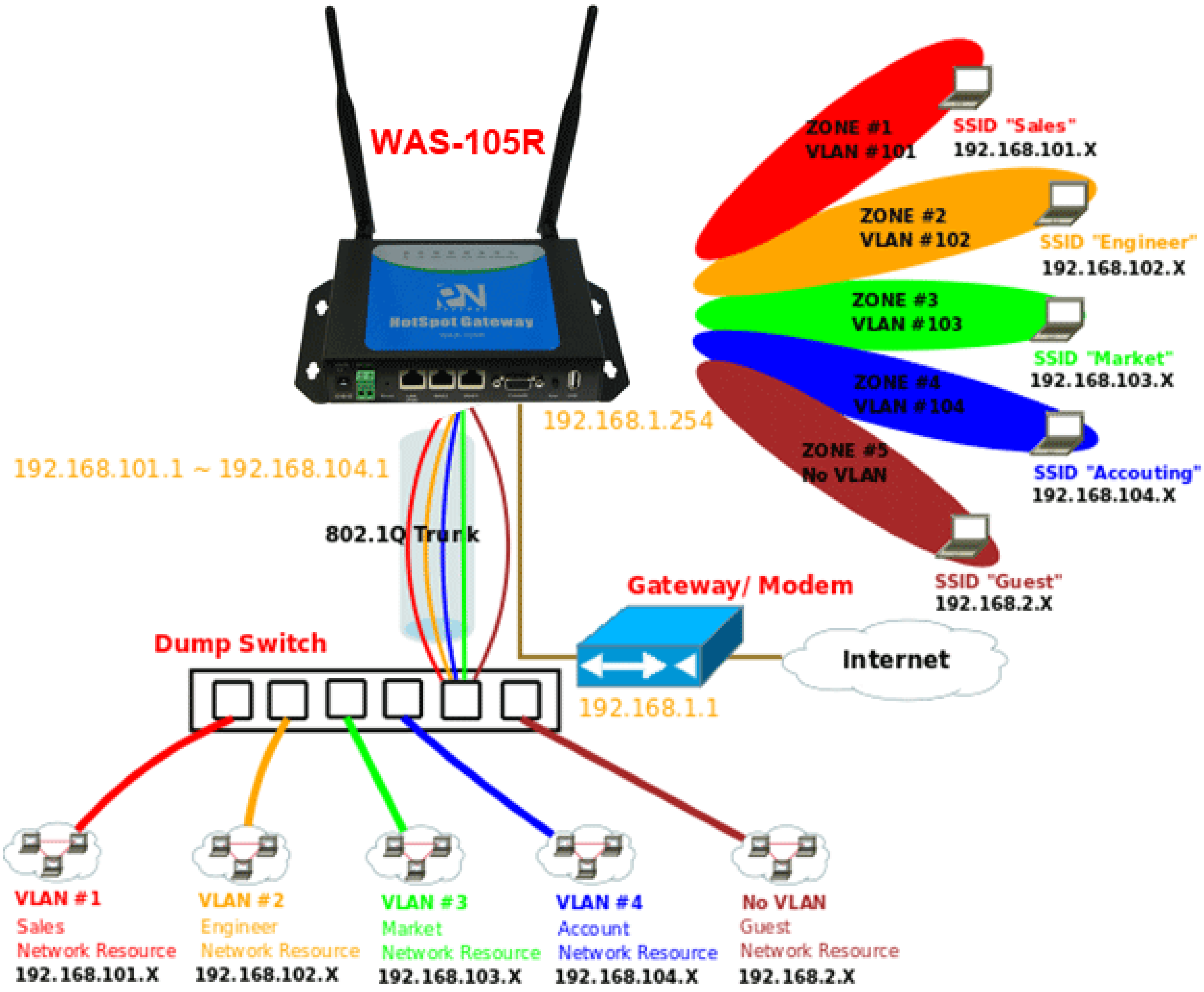


Figure 4-1 Multiple SSIDs with different VLAN settings use dump switch connect to wired area.

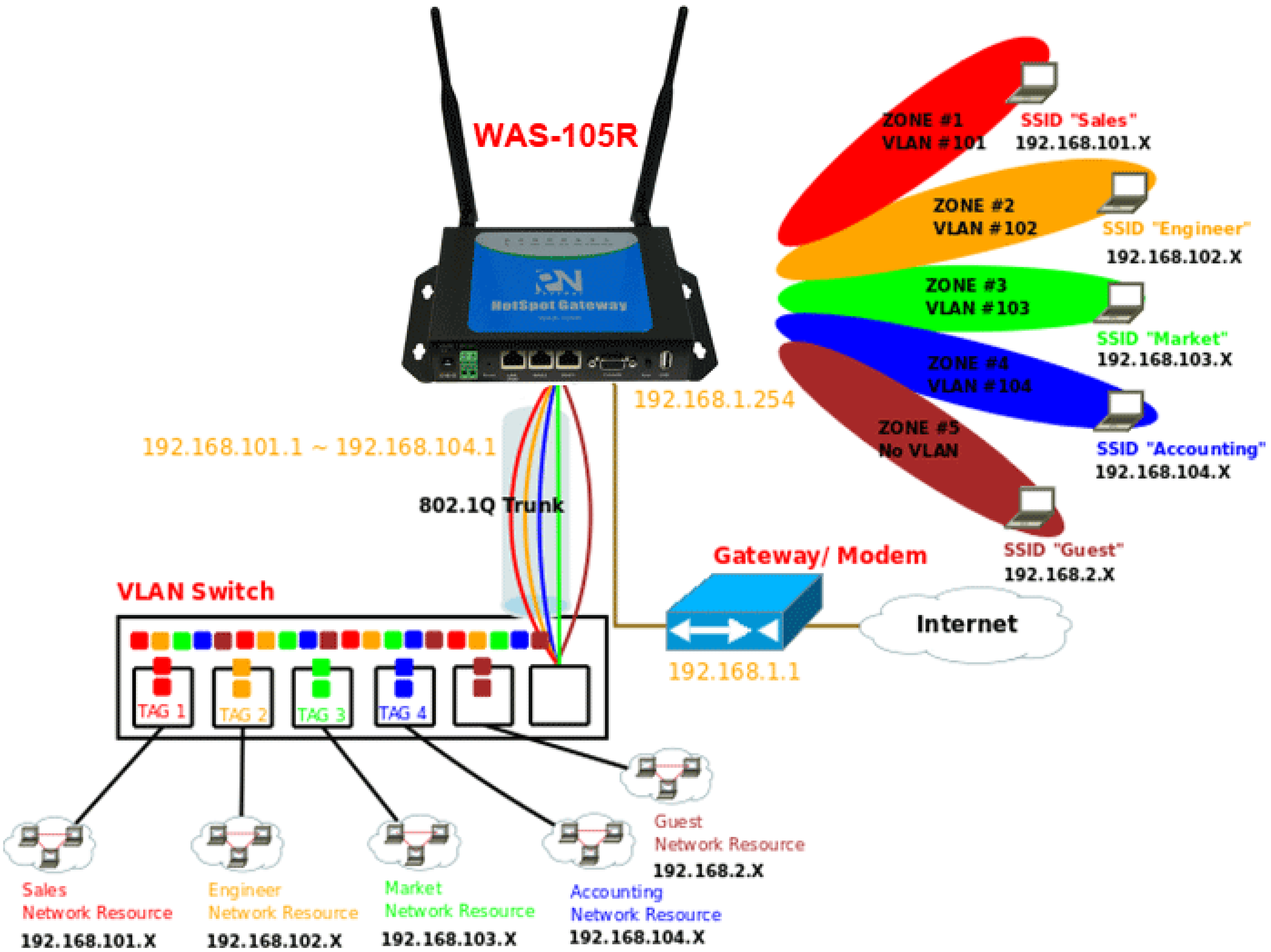
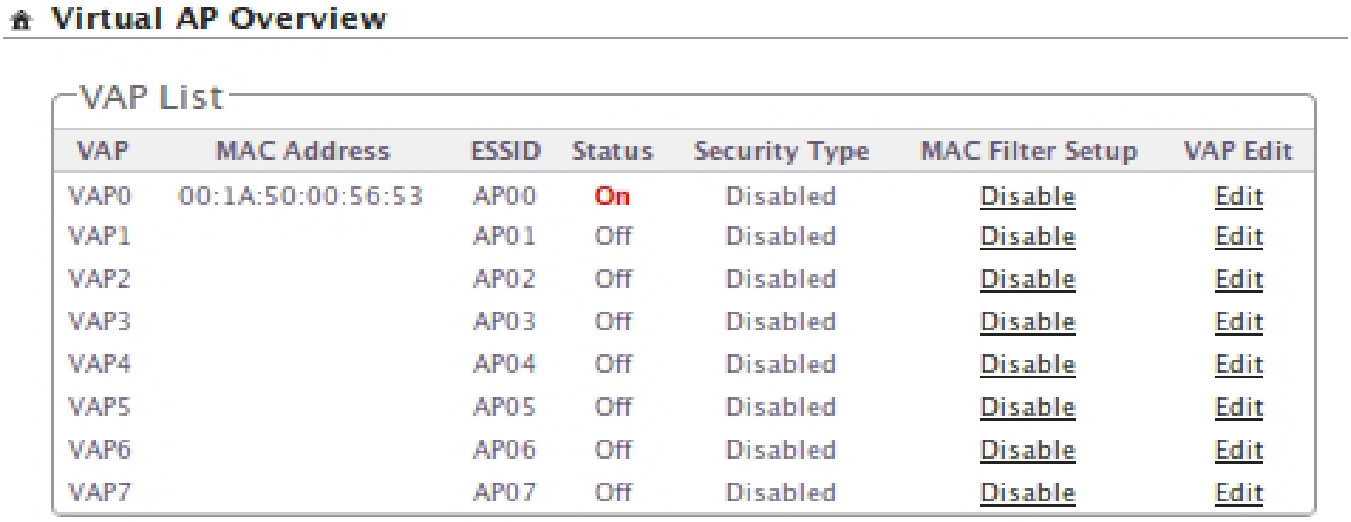


Figure 4-2 Multiple SSIDs with different VLAN settings use VLAN switch connect to wired area.

The administrator can create Virtual AP via this page. Please click on **Wireless -> Virtual AP Setup** and follow the below setting.



Virtual AP Overview

VAP List

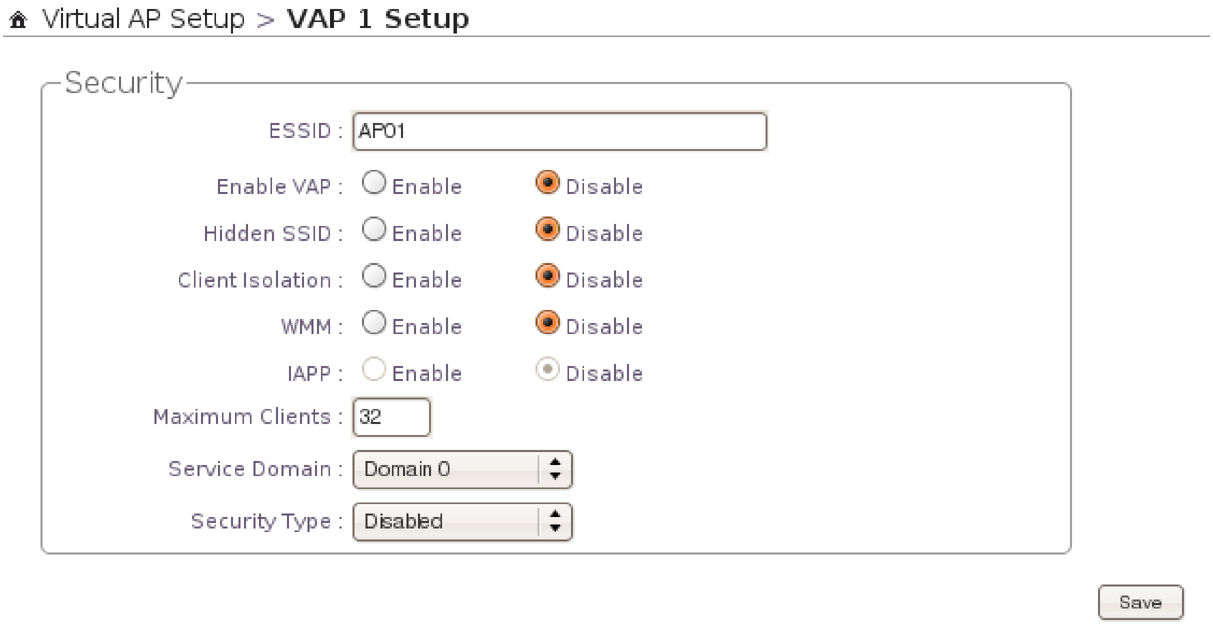
VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Setup	VAP Edit
VAP0	00:1A:50:00:56:53	AP00	On	Disabled	Disable	Edit
VAP1		AP01	Off	Disabled	Disable	Edit
VAP2		AP02	Off	Disabled	Disable	Edit
VAP3		AP03	Off	Disabled	Disable	Edit
VAP4		AP04	Off	Disabled	Disable	Edit
VAP5		AP05	Off	Disabled	Disable	Edit
VAP6		AP06	Off	Disabled	Disable	Edit
VAP7		AP07	Off	Disabled	Disable	Edit

- **VAP :** Indicate the system's Virtual AP.
- **MAC Address :** The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here.
- **ESSID :** Indicate the ESSID of the respective Virtual AP
- **Status :** Indicate the current Status of the respective Virtual AP. The **VAP0** always on.
- **Security Type :** Indicate an used security type of the respective Virtual AP.
- **MAC Filter :** Indicate an used MAC filter of the respective Virtual AP. Click button to configure MAC Filter of the respective Virtual AP.
- **Edit :** Click **Edit** button to configure Virtual AP's settings.

4.2.3.1 Configure Virtual AP

For each Virtual AP, administrators can configure general settings and security type.

Click **Wireless -> Virtual AP**, click "**Edit**" of Virtual AP List and then Virtual AP Configuration page appears.



Virtual AP Setup > VAP 1 Setup

Security

ESSID :	AP01	
Enable VAP :	○ Enable	● Disable
Hidden SSID :	○ Enable	● Disable
Client Isolation :	○ Enable	● Disable
WMM :	○ Enable	● Disable
IAPP :	○ Enable	● Disable
Maximum Clients :	32	
Service Domain :	Domain 0	
Security Type :	Disabled	

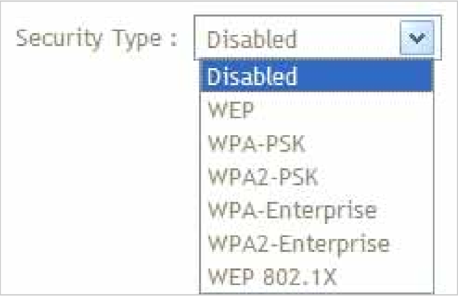
- **ESSID :** Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.
- **Enable AP :** By default, it's "***Disable***" for VAP1 ~ VAP7. **The VAP0 always enabled**.

Select "***Enable***" to activate VAP or click "***Disable***" to deactivate this function

- **Hidden SSID :** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.
- **Client Isolation :** Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients.
- **WMM :** Select Enable, the packets with QoS WMM will has higher priority.
- **IAPP Support :** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.

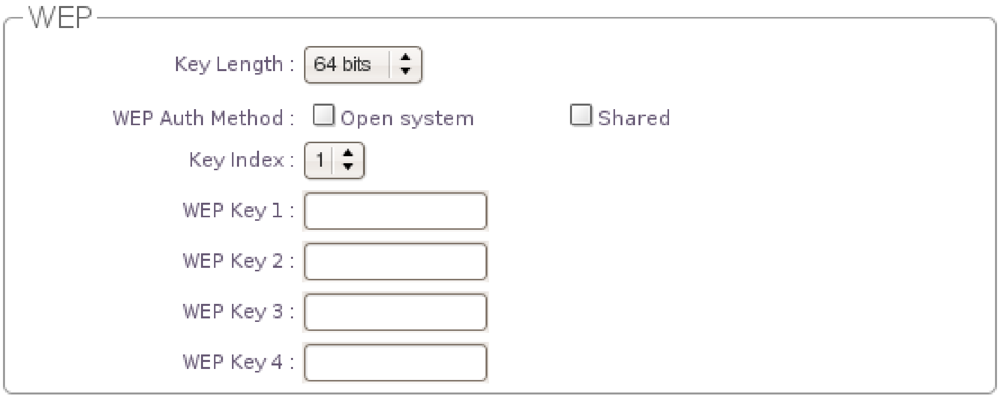
IAPP only used on WPA-PSK and WPA2-PSK security type. Only one of VAPs can be enabled

- **Maximum Clients :** Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.
- **Service Domain :** Select the desired Service Domain from the drop-down list.
- **Security Type :** Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and WEP 802.1X.


Security Type : Disabled

➔ **Disable :** Data are unencrypted during transmission when this option is selected.

➔ **WEP :** WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select ***WEP*** as the security type from the drop down list as desired.



WEP

Key Length : 64 bits

WEP Auth Method : □ Open system □ Shared

Key Index : 1

WEP Key 1 :

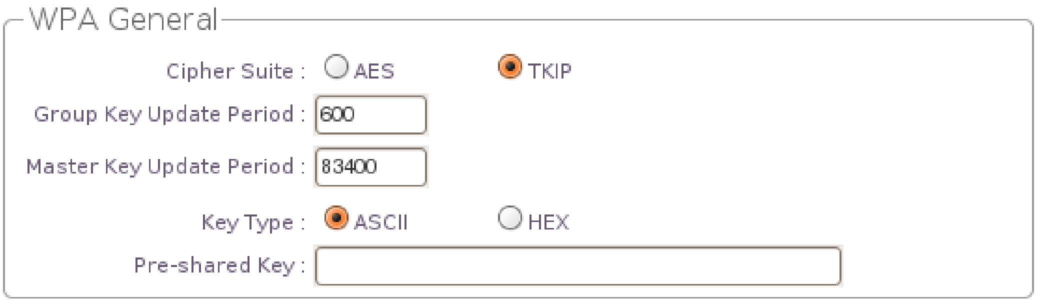
WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- ✓ **Key Length :** Select the desire option are ***64 bits***, ***128 bits*** or ***152 bits*** from drop-down list.
- ✓ **WEP auth Method :** Enable the desire option among ***Open system*** or ***Shared***.
- ✓ **Key Index :** Select key index used to designate the WEP key during data transmission. 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3, or 4.
- ✓ **WEP Key :** Enter HEX format WEP key value; the system support up to 4 sets of WEP keys.

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK (WPA2-PSK) protected access.



WPA General

Cipher Suite : ○ AES ● TKIP

Group Key Update Period : 600

Master Key Update Period : 83400

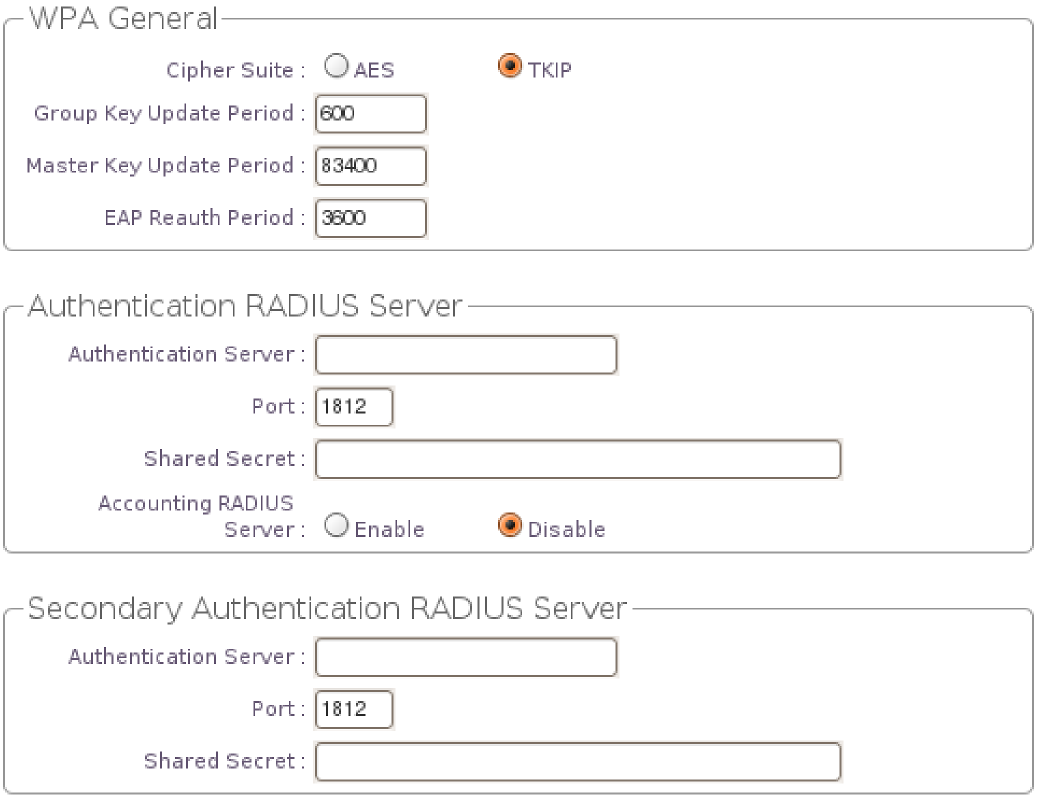
Key Type : ● ASCII ○ HEX

Pre-shared Key :

- ✓ **Cipher Suite :** Check on the respected button to enable either **AES** or **TKIP** cipher suites; default is **TKIP**.
- ✓ **Group Key Update Period :** This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is **600** seconds.
- ✓ **Master Key Update Period :** This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is **83400** seconds.
- ✓ **Key Type :** Check on the respected button to enable either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the information for pre-shared key; the format of the information shall according to the key type selected.

Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

➔ **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this selected. The WAS-105R support two 802.1x Authentication/ Accounting Radius Server



WPA General

Cipher Suite : ○ AES ● TKIP

Group Key Update Period : 600

Master Key Update Period : 83400

EAP Reauth Period : 3600

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Accounting RADIUS Server : ○ Enable ● Disable

Secondary Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

✓ **WPA General Settings :**

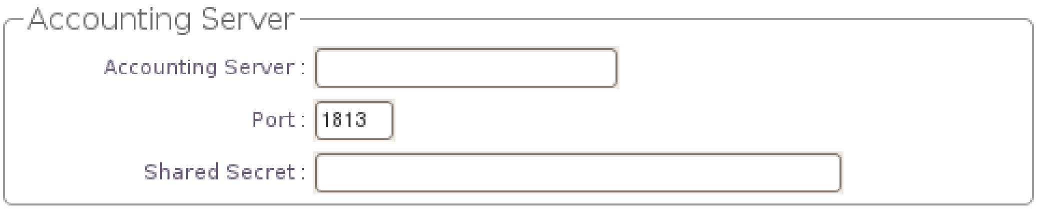
- **Cipher Suite :** Check on the respected button to enable either **AES** or **TKIP** cipher suites.
- **Group Key Update Period :** This time interval for re-keying GTK (broadcast/ multicast encryption keys) in seconds. Enter the time-length required; the default time is **600** seconds.
- **Master Key Update Period :** This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is **83400** seconds.
- **EAP Reauth Period :** EAP re-authentication period in seconds; default is **3600**; **0** indicates **disable** re-authentication.

✓ **Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

- **Shared secret :** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- **Accounting RADIUS Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

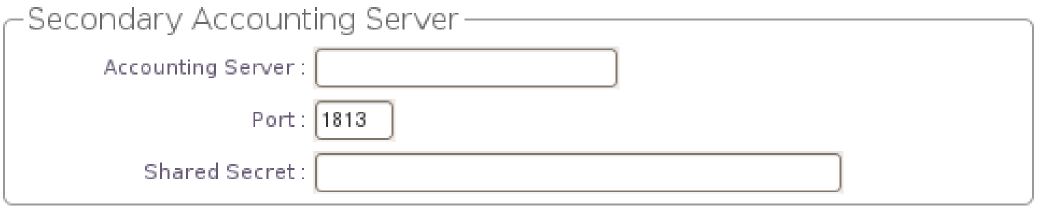


Accounting Server

Accounting Server :

Port : 1813

Shared Secret :



Secondary Accounting Server

Accounting Server :

Port : 1813

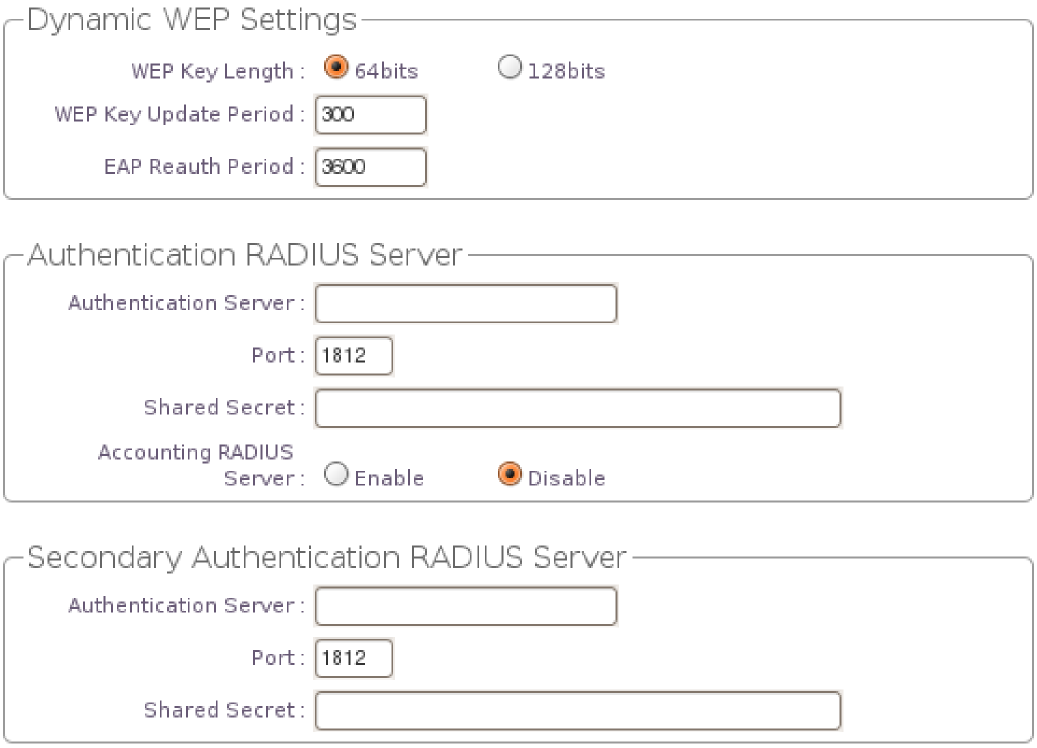
Shared Secret :

- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port :** The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

✓ **Dynamic WEP Settings :**

- **WEP Key length :** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- **WEP Key Update Period :** The time interval WEP will then be updated; the unit is in seconds; default is **300** seconds; **0** indicates no re-key.
- **EAP Reauth Period :** EAP re-authentication period in seconds; default is **3600**; **0** indicates **disable** re-authentication.



Dynamic WEP Settings

WEP Key Length : ● 64bits ○ 128bits

WEP Key Update Period : 300

EAP Reauth Period : 3600

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Accounting RADIUS Server : ○ Enable ● Disable

Secondary Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

✓ **Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.
- **Accounting RADIUS Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

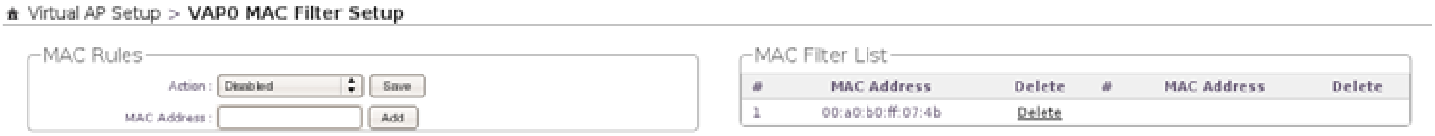
✓ **Accounting Server Settings :**

- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port :** The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2.3.2 Block Wireless Clients

In this function, the administrator can be allow or reject clients to access Virtual AP. Please click on **Wireless -> Virtual AP Setup**, then click button on column of MAC Filter Setup. The MAC Filter Configuration page appears. Follow the below setting.



Virtual AP Setup > **VAP0 MAC Filter Setup**

MAC Rules

Action : Disabled [Save]

MAC Address : [Add]

MAC Filter List

#	MAC Address	Delete	#	MAC Address	Delete
1	00:a0:b0:ff:07:4b	Delete			

- **Action :** Select the desired access control type from the drop-down list; the options are "**Disabled**", "**Only Deny List MAC**" or "**Only Allow List MAC**".

  define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients – **Action** is set to **Only Deny List MAC**.

  define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – **Action** is set to **Only Allow List MAC**.

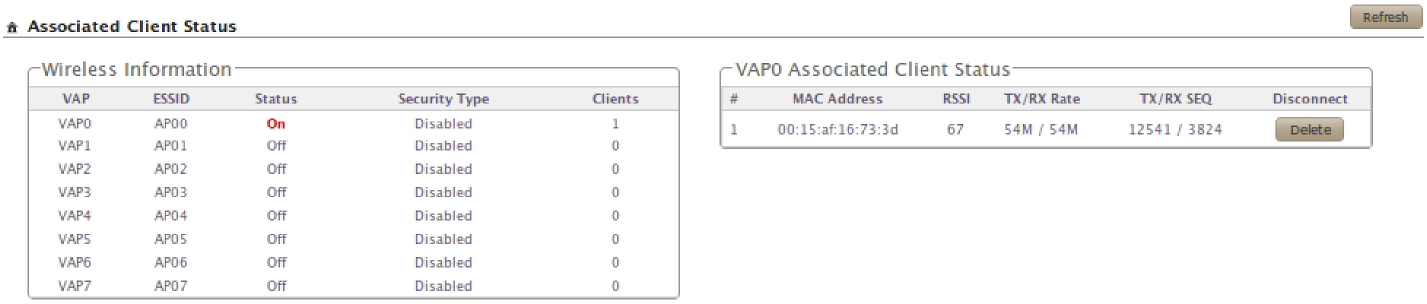
- **MAC Address :** Enter MAC address in this field. There are maximum **20** clients users allowed in this MAC address list.

The MAC Address of the wireless clients can be added and removed to the MAC Filter List using the "**Add**" and "**Delete**" buttons. Click ***Reboot*** button to activate your changes

MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

4.2.3.3 Monitor Associated Wireless Clients

The administrator can obtain detailed wireless information and all associated clients status via this page. Please click on **Wireless -> Associated Clients**. The the **Associated Clients Status** appears.



Associated Client Status

Wireless Information

VAP	ESSID	Status	Security Type	Clients
VAP0	AP00	On	Disabled	1
VAP1	AP01	Off	Disabled	0
VAP2	AP02	Off	Disabled	0
VAP3	AP03	Off	Disabled	0
VAP4	AP04	Off	Disabled	0
VAP5	AP05	Off	Disabled	0
VAP6	AP06	Off	Disabled	0
VAP7	AP07	Off	Disabled	0

VAP0 Associated Client Status

#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	Disconnect
1	00:15:af:16:73:3d	67	54M / 54M	12541 / 3824	Delete

- **Wireless Information :** Display the Virtual AP configuration information of the system.
  - ➔ **VAP :** Display number of system's Virtual AP.
  - ➔ **ESSID :** Extended Service Set ID of the Virtual AP.
  - ➔ **Status :** Display Virtual AP status currently.
  - ➔ **Security Type :** Security type activated by the Virtual AP.
  - ➔ **Clients :** Number of clients currently associated to the Virtual AP.

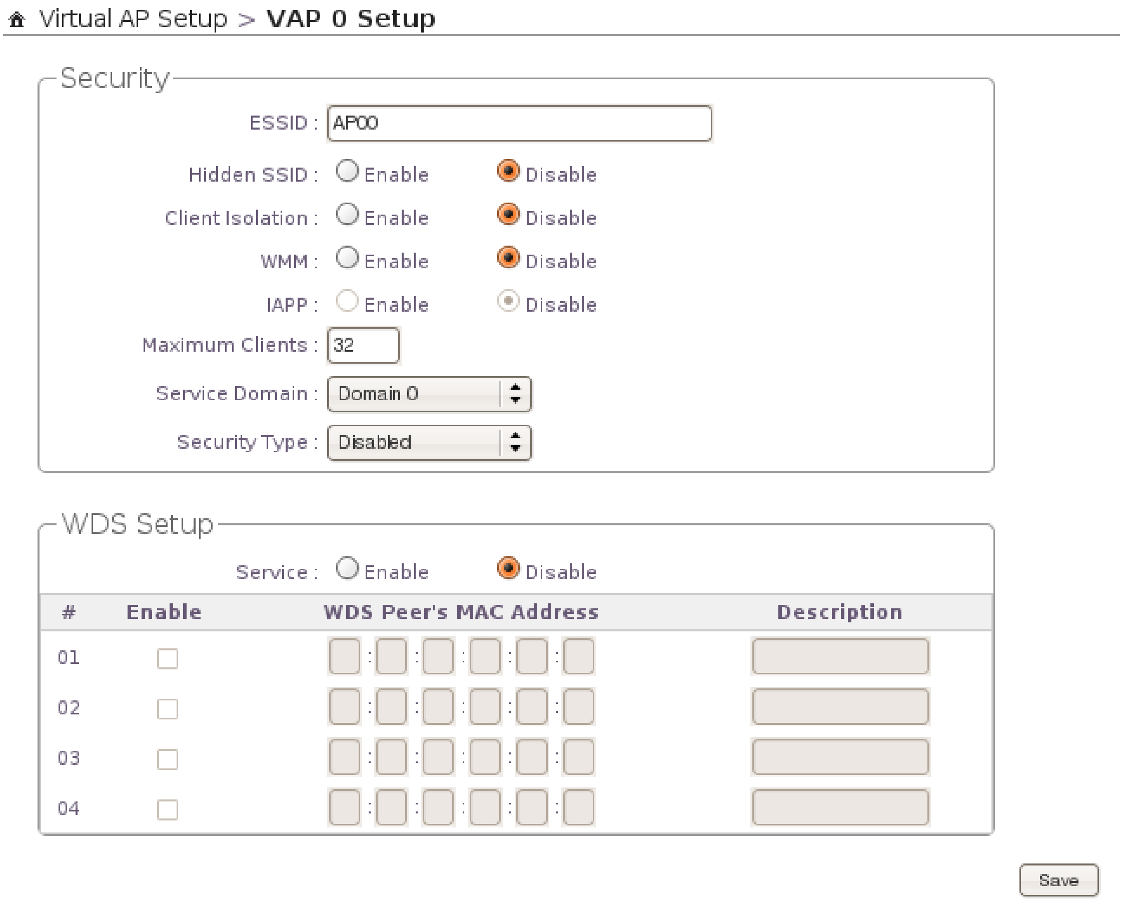
- **Associated Client Status :** Display the Virtual AP configuration information of the system.
  - ➔ **AP :** Virtual AP which the device is associated with.
  - ➔ **RSSI :** Indicate the RSSI of the respective client's association.
  - ➔ **TX/RX Rate :** Indicate the TX/RX Rate of the respective client's association.
  - ➔ **TX/RX SEQ :** Indicate the TX/RX sequence of the respective client's association.
  - ➔ **Disconnect :** Administrator can kick out a specific client, click "**Delete**" button to kick out specific client

4.3 Expand Your Wireless Network

4.3.1 Create WDS Link

The administrator can create WDS Links for expanding wireless network via this page.

Please click on **Wireless -> Virtual AP Setup -> VAP0 Setup** and follow the below setting.



Virtual AP Setup > **VAP 0 Setup**

Security

ESSID : AP00

Hidden SSID : ○ Enable ● Disable

Client Isolation : ○ Enable ● Disable

WMM : ○ Enable ● Disable

IAPP : ○ Enable ● Disable

Maximum Clients : 32

Service Domain : Domain 0

Security Type : Disabled

WDS Setup

Service : ○ Enable ● Disable

#	Enable	WDS Peer's MAC Address	Description
01	□	: : : : :	
02	□	: : : : :	
03	□	: : : : :	
04	□	: : : : :	

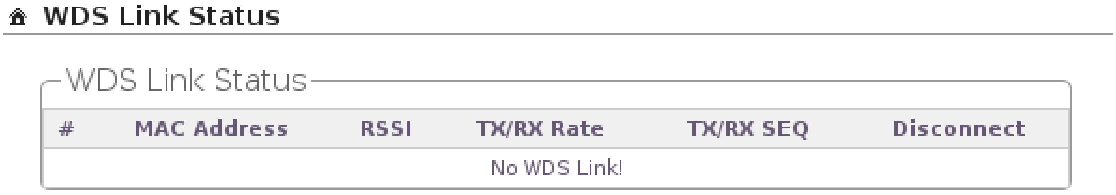
- **Service :** By default, it's "Disable". To "Enable" to activate WDS.
- **Enable :** Click ***Enable*** checkbox to create WDS link.
- **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.
- **Description :** Description of WDS link.

If WDS activate, the Security Type only support "WEP" on VAP0

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.3.2 View WDS Link Status

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



WDS Link Status

WDS Link Status

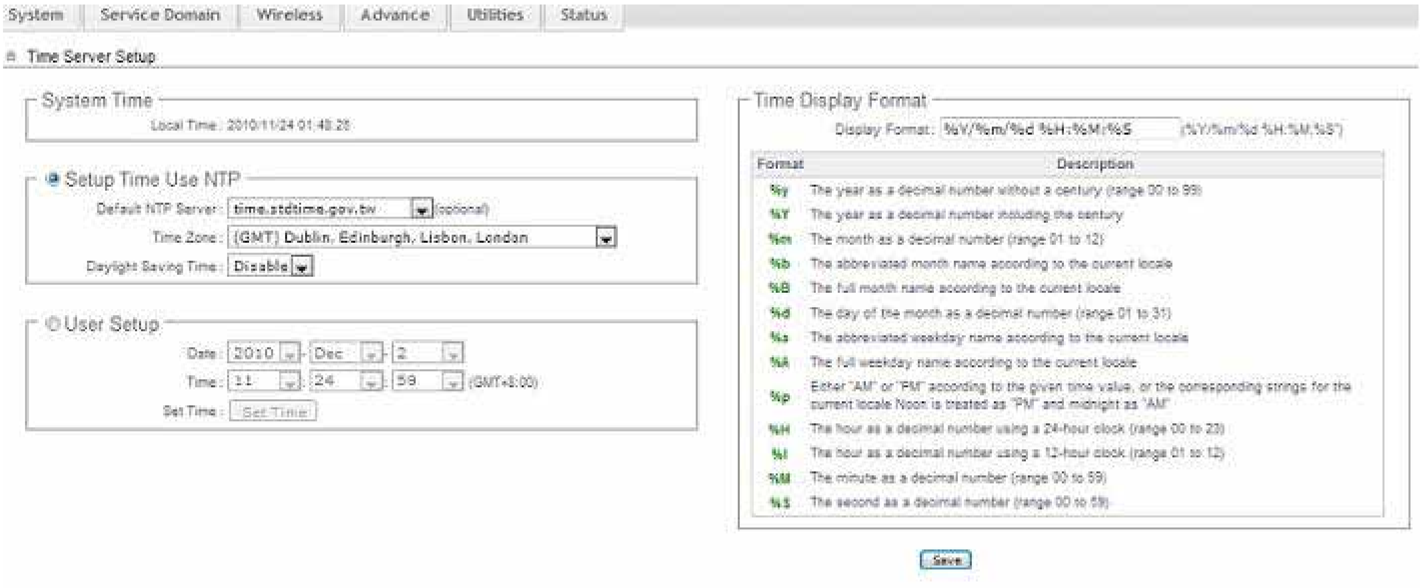
#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	Disconnect
No WDS Link!					

- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of the respective WDS's link.
- **TX/RX Rate :** Indicate the TX/RX Rate of the respective WDS's link.
- **TX/RX SEQ :** Indicate the TX/RX sequence of the respective WDS's link.
- **Disconnect :** Administrator can kick out a specific client, click “**Delete**” button to kick out specific WDS's link

4.4 Manage the System

4.4.1 Configure System Time

System time can be configured via this page where manual setting and NTP server configuration are both supported. Please click on **System -> Time Server** and follow the below setting.



System Time

Local Time : 2010/11/24 01:48:28

● Setup Time Use NTP

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight Saving Time : Disable

○ User Setup

Date : 2010 - Dec - 2

Time : 11 : 24 : 59 (GMT+8:00)

Set Time : Set Time

Time Display Format

Display Format : %Y/%m/%d %H:%M:%S ("%Y/%m/%d %H:%M:%S")

Format	Description
%y	The year as a decimal number without a century (range 00 to 99)
%Y	The year as a decimal number including the century
%m	The month as a decimal number (range 01 to 12)
%b	The abbreviated month name according to the current locale
%B	The full month name according to the current locale
%d	The day of the month as a decimal number (range 01 to 31)
%a	The abbreviated weekday name according to the current locale
%A	The full weekday name according to the current locale
%p	Either "AM" or "PM" according to the given time value, or the corresponding strings for the current locale Noon is treated as "PM" and midnight as "AM"
%H	The hour as a decimal number using a 24-hour clock (range 00 to 23)
%I	The hour as a decimal number using a 12-hour clock (range 01 to 12)
%M	The minute as a decimal number (range 00 to 59)
%S	The second as a decimal number (range 00 to 59)

Save

- **System Time :** Display the current time of the system.
- **Setup Time Use NTP :** Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
  - ➔ **Daylight saving time :** Enable Daylight saving time from where the accurate time needed.

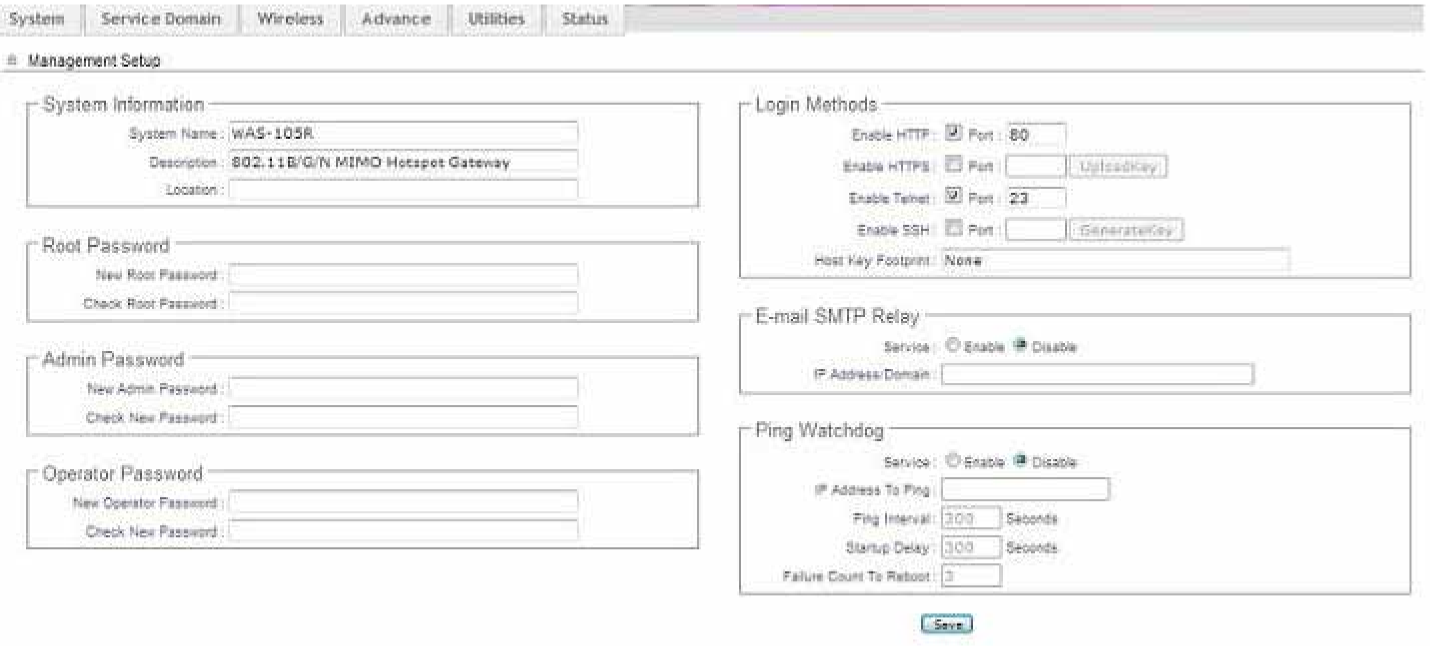
> If Time server setting selected in “Setup Time User NTP”, please verify system's Default Gateway and DNS setting first.

- **User Setup :** Administrator can set Time manually. Click “**Set Time**” button and “**Save**” button to change Local Time.
- **Time Display Format :** Administrator can set system's time format. Enter a desired time format or use the default provided.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.4.2 Configure Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.



System Information
System Name : WAS-105R
Description : 802.11B/G/N MIMO Hotspot Gateway
Location :

Root Password
New Root Password :
Check Root Password :

Admin Password
New Admin Password :
Check New Password :

Operator Password
New Operator Password :
Check New Password :

Login Methods
Enable HTTP : ☑ Port : 80
Enable HTTPS : ☐ Port :
Enable Telnet : ☑ Port : 23
Enable SSH : ☐ Port :
Host Key Footprint : None

E-mail SMTP Relay
Service : ○ Enable ● Disable
IP Address/Domain :

Ping Watchdog
Service : ○ Enable ● Disable
IP Address To Ping :
Ping Interval : 300 Seconds
Startup Delay : 300 Seconds
Failure Count To Reboot : 3

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default provided.
  - ➔ **Description :** Denote further information of the system.
  - ➔ **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.
- **Root Password :** Log in as a root user and is allowed to change its own. Root user also can change **admin** user's and **operator** user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.
- **Admin Password :** Log in as a admin user and is allowed to change its own. Admin user also can change operator user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.

- **operator Password :** Log in as a operator user and is **not** allowed to change its own. Click ***Save*** button to activate the new password.

  ➔ **New Password :** Please input the new password of administrator.

  ➔ **Check New Password :** Please input again the new password of administrator.

- **Admin Login Methods :** The admin manager can enable or disable system login methods, it also can change services port. Click ***Save*** button to activate the admin login methods.

  ➔ **Enable HTTP :** Select Enable HTTP to activate HTTP Service

  ➔ **HTTP Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **80**

  ➔ **Enable HTTPS :** Select Enable HTTPS to activate HTTPS Service

  ➔ **HTTPS Port :** Please input 1 ~ 65535 value to set HTTPS Port; default value is **443**

If you already have an SSL Certificate, please click “UploadKey” button to select the file and upload it.

  ➔ **Enable Telnet :** Select Enable Telnet to activate Telnet Service

  ➔ **Telnet Port :** Please input 1 ~ 65535 value to set Telnet Port; default value is **23**

  ➔ **Enable SSH :** Select Enable SSH to activate SSH Service

  ➔ **SSH Port :** Please input 1 ~ 65535 value to set SSH Port; default value is **22**

Click “GenerateKey” button to generate RSA private key. The “Display the host key footprint” gray blank will be show content of RSA key.

- **E-main SMTP Relay :** Select Enable Service to activate Email SMTP Relay function. Enter SMTP relay server in IP Address/ Domain field.

- **Ping Watchdog :** The ping watchdog sets the WAS-105R Device to continuously ping a user defined IP address (it can be the Internet gateway for example). If it is unable to ping under the user defined constraints, the WAS-105R device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

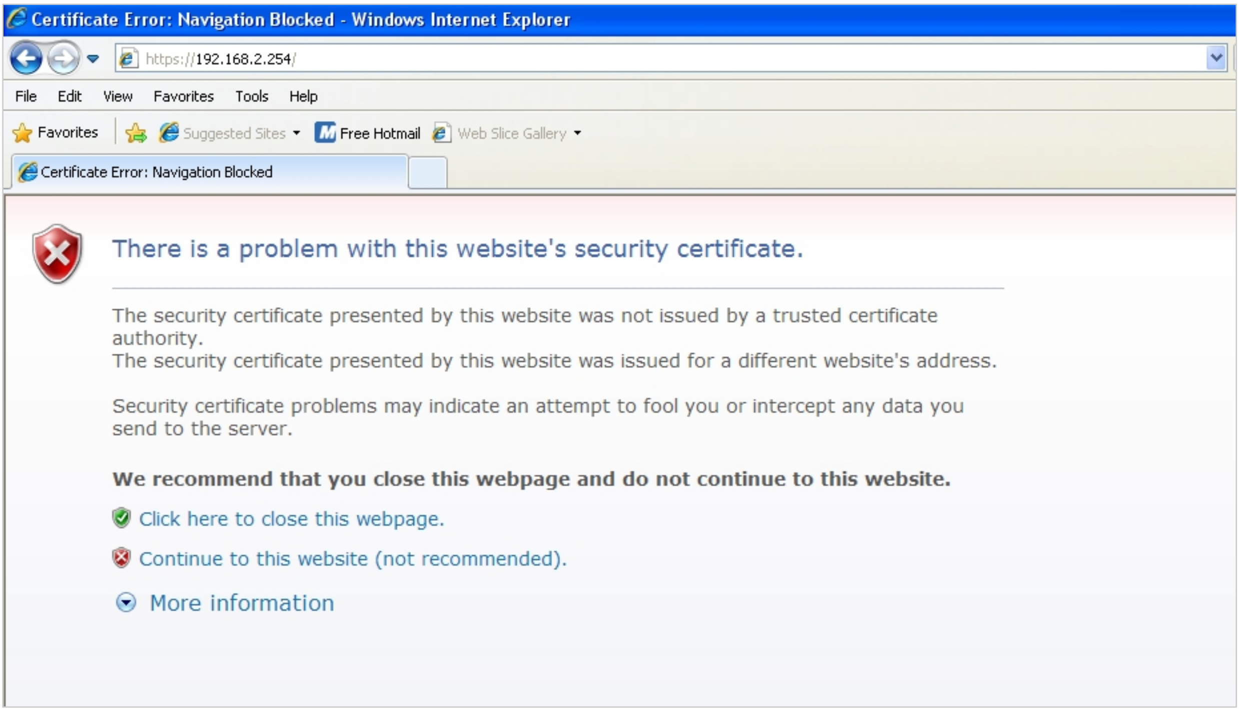
  ➔ **Enable Ping Watchdog :** control will enable Ping Watchdog Tool.

  ➔ **IP Address To Ping :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

- ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.
- ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- ➔ **Failure Count To Reboot :** specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE8 when they try to access WAS-105R's GUI (https://192.168.2.254). There will be a “Certificate Error”, because the browser treats WAS-105R as an illegal website.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

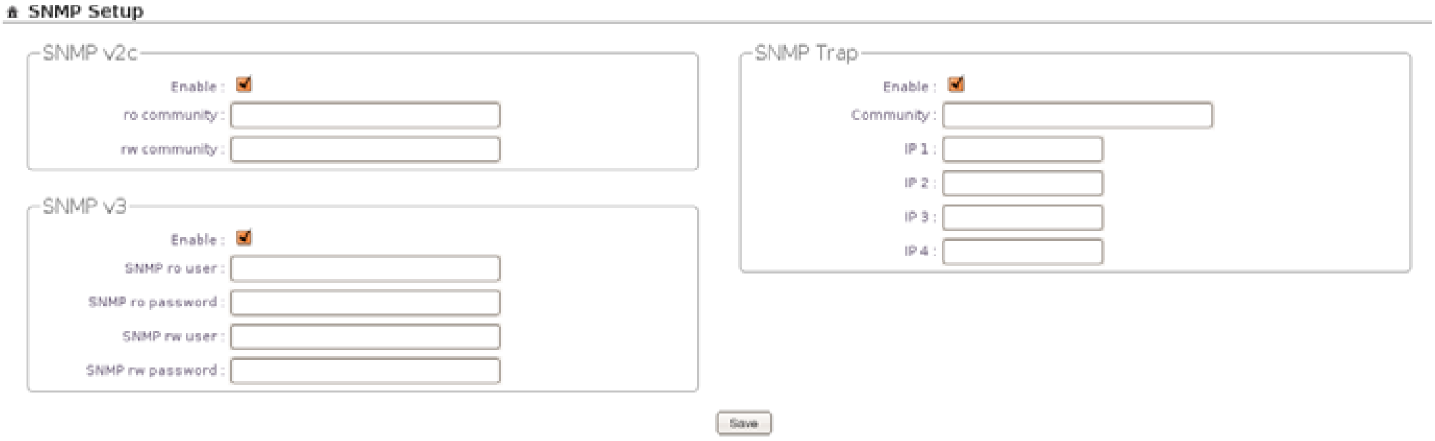
Continue to this website (not recommended).

More information

Click “***Continue to this website***” to access the WAS-105R's GUI. The WAS-105R's Home page will be appear.

4.4.3 Configure SNMP

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and follow the below setting.



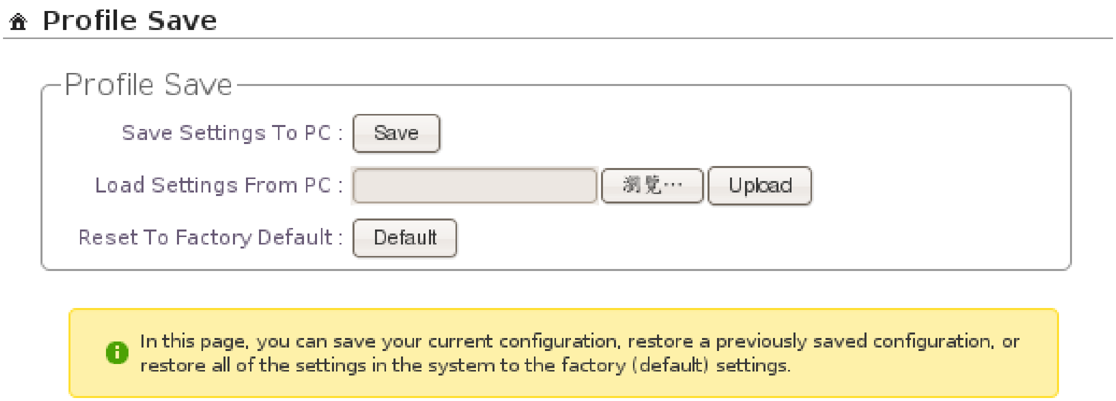
- **SNMP v2c Enable :** Check to enable SNMP v2c.
  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.
- **SNMP v3 Enable :** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.
  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.
- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.
  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.4.4 Backup / Restore and Reset to Factory

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.



Profile Save

Profile Save

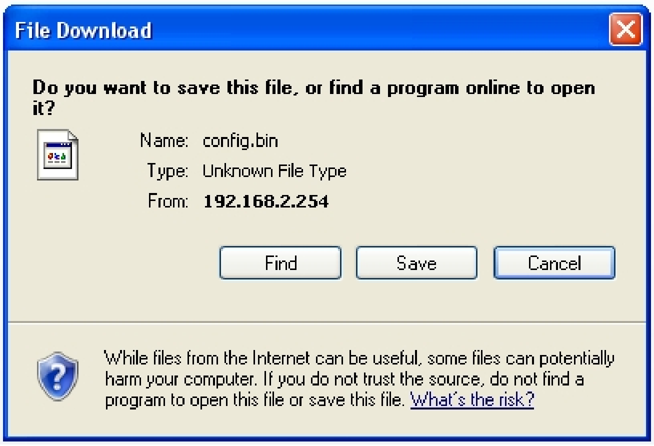
Save Settings To PC :

Load Settings From PC :

Reset To Factory Default :

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

- **Save Settings To PC :** Click ***Save*** button to save the current configuration and **database** to a local disk.



File Download

Do you want to save this file, or find a program online to open it?

Name: config.bin

Type: Unknown File Type

From: 192.168.2.254

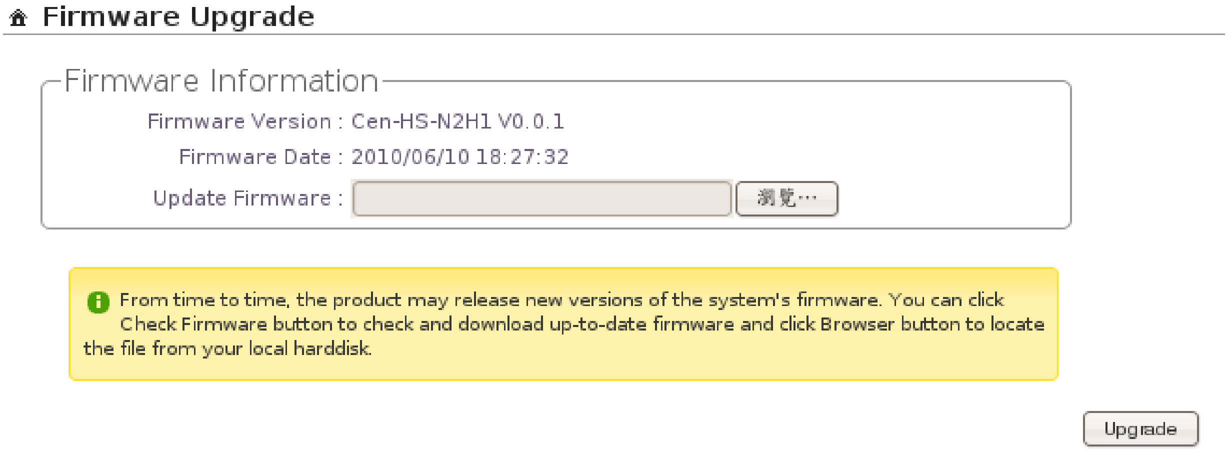
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file and database to restore, and then click ***Upload*** button to upload. The system will **restart** after uploading configuration and database.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings. The system will **restart** after uploading configuration and database.

4.4.5 Firmware Upgrade

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



Firmware Upgrade

Firmware Information

Firmware Version : Cen-HS-N2H1 V0.0.1

Firmware Date : 2010/06/10 18:27:32

Update Firmware :

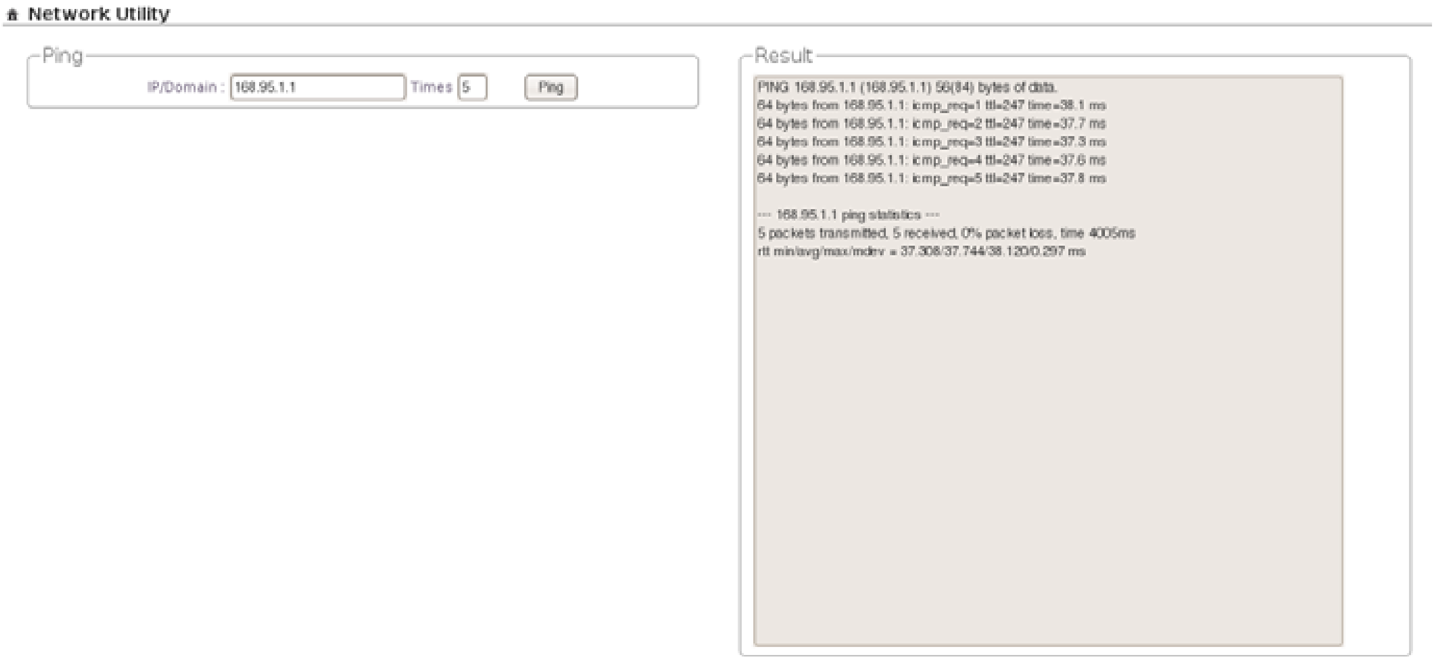
From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

1. To prevent data loss during firmware upgrade, please backup current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

4.4.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.



IP/Domain : 168.95.1.1 Times 5

```
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_req=1 ttl=247 time=38.1 ms
64 bytes from 168.95.1.1: icmp_req=2 ttl=247 time=37.7 ms
64 bytes from 168.95.1.1: icmp_req=3 ttl=247 time=37.3 ms
64 bytes from 168.95.1.1: icmp_req=4 ttl=247 time=37.6 ms
64 bytes from 168.95.1.1: icmp_req=5 ttl=247 time=37.8 ms

--- 168.95.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 37.308/37.744/38.120/0.297 ms
```

- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.

  ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.

  ➔ **Times:** By default, it's 5 and the range is from 1 to 60. It indicates number of connectivity test.

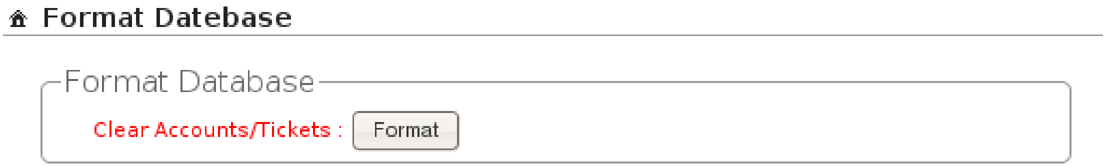
- **Traceroute :** Allows tracing the hops from the AC-920X device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test

  ➔ **Destination Host :** Specifies the Destination Host for the finding the route taken by ICMP packets across the network.

  ➔ **MAX Hop :** Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

4.4.7 Format Database

This function allows administrator to format system's database. Click ***Format*** button to proceed and take around three minutes to complete.



Format Datebase

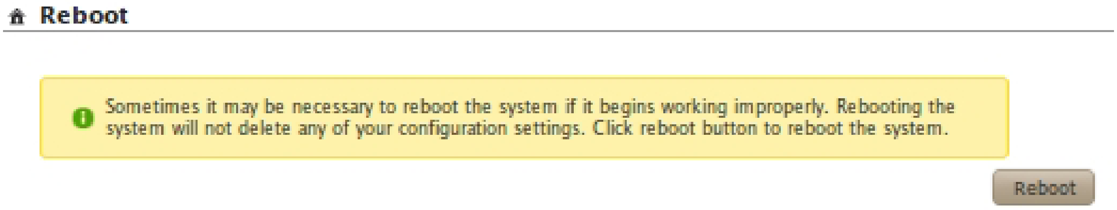
Format Database

Clear Accounts/Tickets : Format

Do not interrupt during format database including power on/off as this may damage system.

4.4.8 Reboot

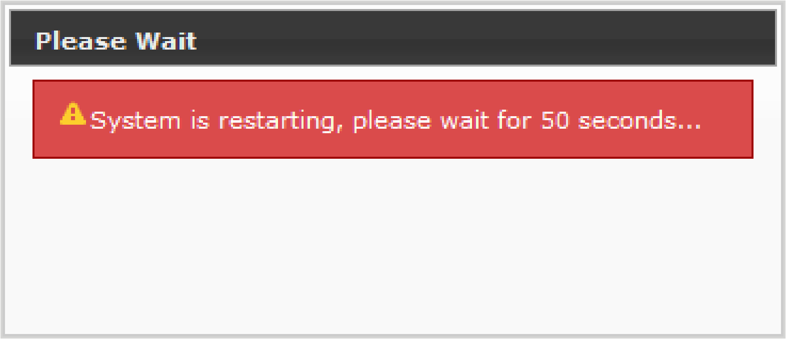
This function allows administrator to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



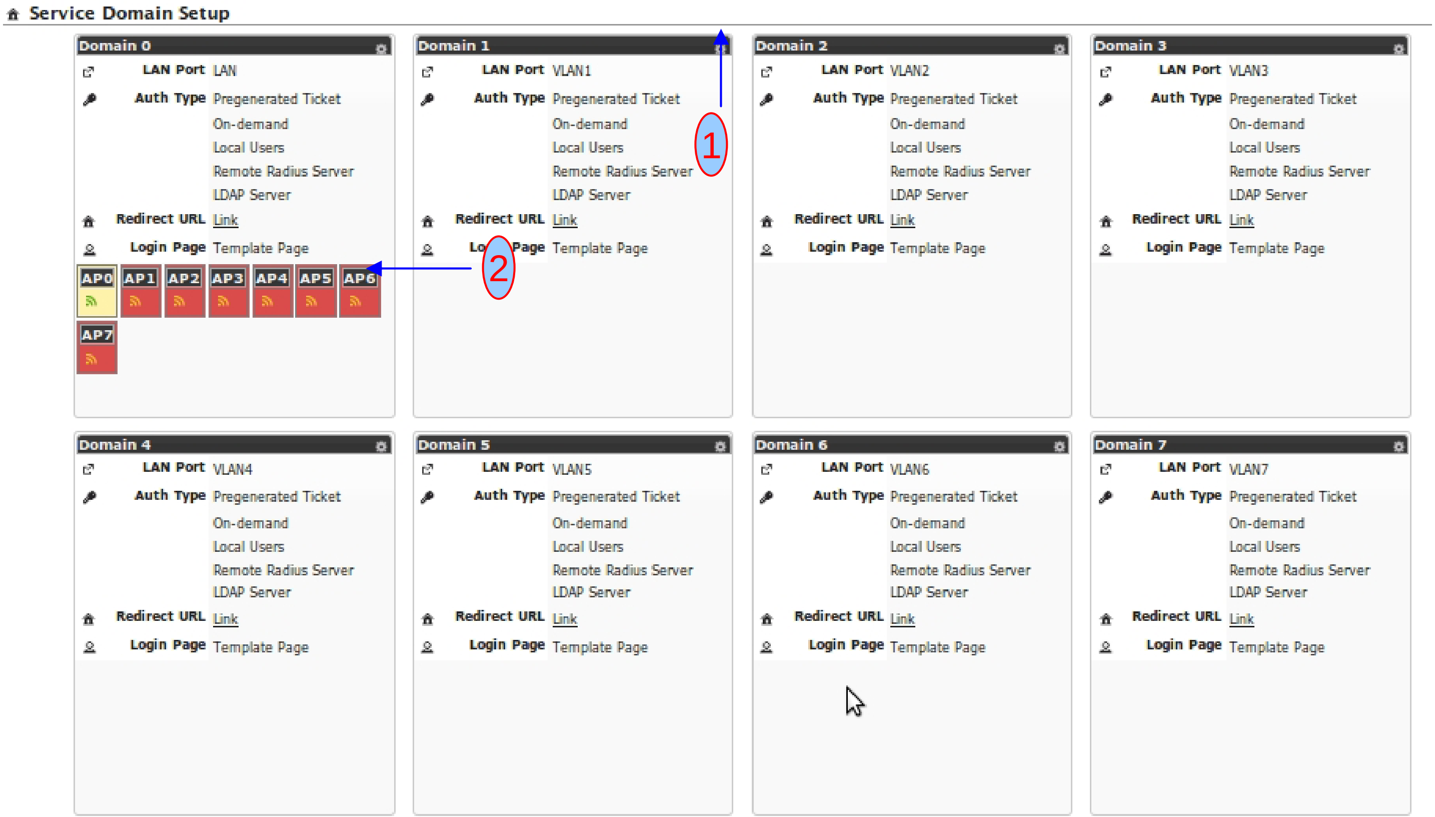
Please Wait

⚠System is restarting, please wait for 50 seconds...

The **Home** page appears upon the completion of reboot.

4.5 Access to External Network With Service Domain

WAS-105R support **9** Service Domain, administrator can quick setup hotspot via this page. Each VAP can move to different Domain.



Service Domain Setup

Domain 0
LAN Port LAN
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 1
LAN Port VLAN1
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 2
LAN Port VLAN2
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 3
LAN Port VLAN3
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 4
LAN Port VLAN4
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 5
LAN Port VLAN5
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

Domain 6
LAN Port VLAN6
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

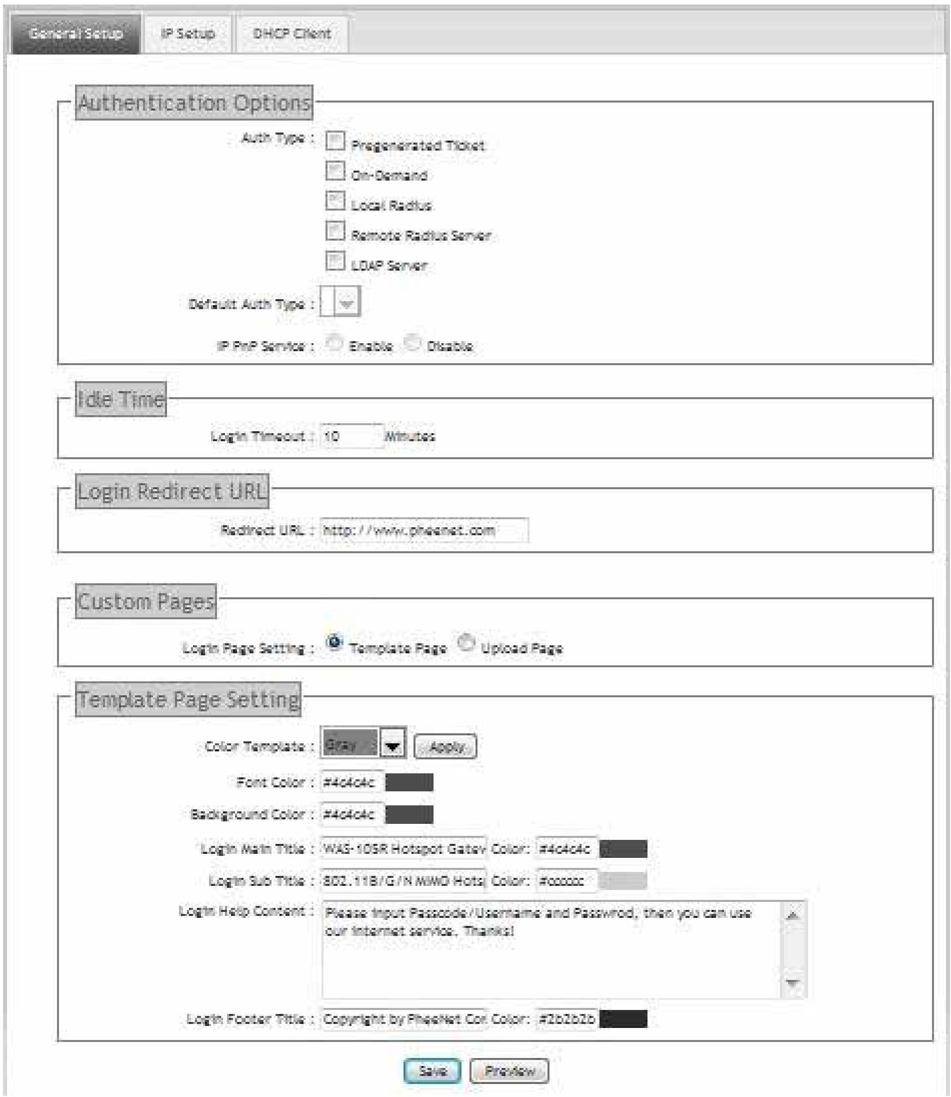
Domain 7
LAN Port VLAN7
Auth Type Pregenerated Ticket
On-demand
Local Users
Remote Radius Server
LDAP Server
Redirect URL Link
Login Page Template Page

- **LAN Port :** The bonding interface for this Service Domain
- **Auth Type :** The authentication type for this Service Domain. There are **six** types : None, Pregenereated Ticket. On-demand, Local Users, Remote Radius Server and LDAP.
- **Redirect URL :** The redirect URL for this Login page of Service Domain. Click Hyperlinks to enter redirect URL.
- **Login Page :** The custom page for this Service Domain. There are two types : Template page or Upload page
- ⚙ **:** Click tools icon(number 1) on the top-right corner of each Domain settings window, the Service Domain page will pop-up.
- 📶 **:** Click signal icon(number 2) on each VAP field, the VAP Setup will pop-up.

4.5.1 Configure Service Domain

Administrator can configure Service Domain with different authentication service type, IP PnP service, guest free service, idle time , redirect URL, scheduling authentication service and customization login page.

Click on **Service Domain** -> **tools icon** or **Service Domain** -> **Service Domain#** to enter **Service Domain Setup** page.



Authentication Options

Auth Type : □ Pregenerated Ticket
□ On-Demand
□ Local Radius
□ Remote Radius Server
□ LDAP Server

Default Auth Type :

IP PnP Service : ○ Enable ○ Disable

Idle Time

Login Timeout : 10 Minutes

Login Redirect URL

Redirect URL : http://www.pheenet.com

Custom Pages

Login Page Setting : ● Template Page ○ Upload Page

Template Page Setting

Color Template : Gray

Font Color : #4c4c4c

Background Color : #4c4c4c

Login Main Title : WAS-105R Hotspot Gatev Color: #4c4c4c

Login Sub Title : 802.11B/G/N MIMO Hots Color: #cccccc

Login Help Content : Please input Passcode/Username and Passwrod, then you can use our Internet service. Thanks!

Login Footer Title : Copyright by PheeNet Cor Color: #2b2b2b

- **Authentication Options :** Select authentication type for this Service Domain. The system supports multiple authentication in one Service Domain.

  Auth Type : Select desired authentication type for this Service Domain, each Domain support multiple authentications .

  Default Auth Type : Select default authentication type for this Service Domain.

- **Pregenerated Ticket :** Select desired tickets database for Pregenerated authentication after creating the database of Pregenerated Tickets.

- **Login Options :** When authentication type selected in Auth Type, the Login Options setting field will appear.

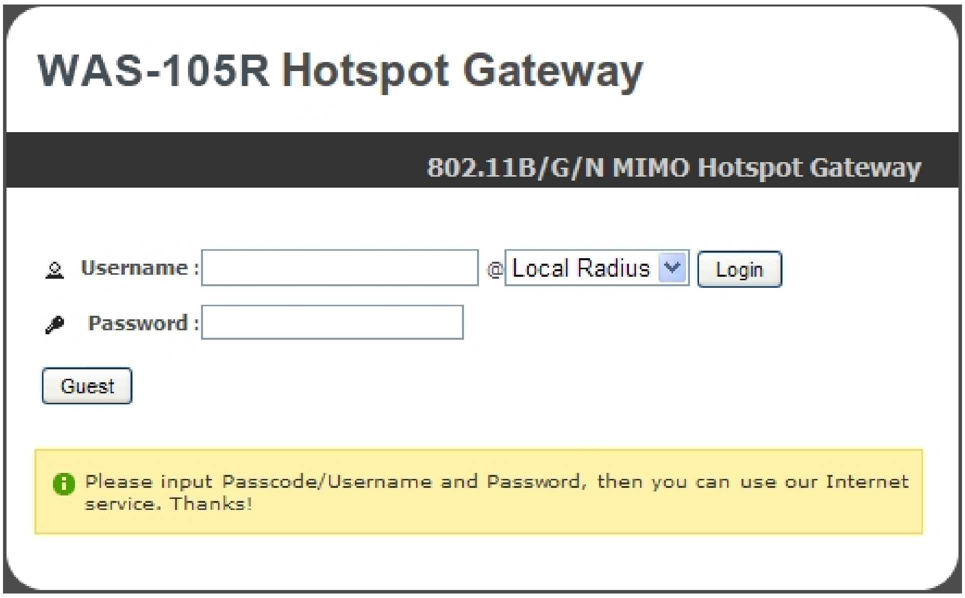
  ➔ **Idle Time :** Enter Idle timeout for this Service Domain. If users has idled with no network activities, the system will automatically logout the users. The Login Timeout can be set between **1** to **60** minutes, and the default timeout is **10** minutes.

  ➔ **Login Redirect URL:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set, such as http://www.yahoo.com.tw. Regardless of the original webpage set in the users' computers, they will be redirect to this page after login.

  ➔ **Time Policy :** Select desired scheduling of the respective Service Domain for authentication service. Scheduling setting is on **Time Policy** page.

  ➔ **IP PnP :** IP Plug and Play, the AC-920X supports IP PnP for the respective Server Domain. At the user end, a static IP address can be used to connect the system. Regardless of what the IP address at the user end is, authentication can still be performed through AC-920X.

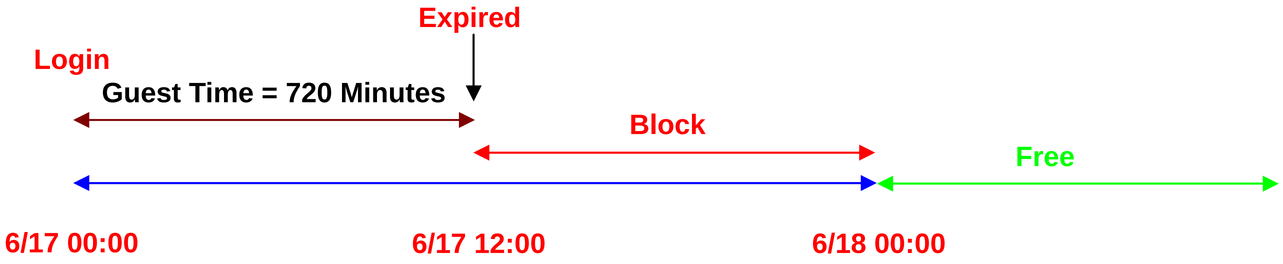
- **Guest Service :** By default; it's "**Disable**". To ***Enable*** to activated guest service limitation, the **Guest** button will appear on the login portal window. Below depicts an example Guest Service.



Please input Passcode/Username and Password, then you can use our Internet service. Thanks!

- ✓ **Guest Count Limit :** Enter maximum number of guest to a desired number in the range of **1~100**. The default value is **5**. For example, while the number of the guest is set to 5, only 5 guest are allowed to connect to Internet via controller at the same time.
- ✓ **Guest Time :** Enter maximum free service time for guest user within **24** hours. The default is **10** *Minutes*, the range is between **1** to **720** *Minutes*.

恩



- ■ **Customize Page**: Configure Custom pages for this Service Domain. Administrator can select **Template Page** or **Upload Customize Page**.
  - ✓ **Template Page :** Choose **Template Page** to make a customized login page. Click select to pick up a color and then fill in all of the banks. You also can use **Color Template** for your template. If you use Color Template, please click "**Apply**" button to change all color. You can change the text as your wish. After finishing the setting, Click "**Save**" button and "**Preview**" button to see the result.
  - ✓ **Upload Page :** Choose the **Upload Page** selection and click "**Upload**" button to upload the designated page and photo. The upload files will be listed on the **File List** field. Below depicts an example for upload File List. The file name of upload page must be "**login.html**"

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Example for Upload Page :

Here the codes are supplied. Please note that the **red** part is for the login feature(**can't not modified**), the **green** part can be modified freely by administrators.

```
<html>
<head>
<title><?hHotspot_main_title></title>
<?JAVASCRIPT>
</head>
<body>
<h1><?hHotspot_main_title></h1>
<p><?hHotspot_sub_title><p>
<div id="CW_MSG"></div><!--Main Login Form Content-->
<div id="CW_INFO"><span id="CW_HELP"></span></div><!--Main Help Content-->
<div id="WALLED"></div><!-- Walled Garden-->
<?hHotspot_footer_title>
</body>
</html>
```

If login page need insert images or css file, please include path "**/upload/vlan0/**" ~ "**/upload/vlan7/**", the "**vlan0**" ~"**vlan7**" indicate "**Service Domain0**" ~ "**Server Domain7**", below depicts an example for insert image001.gif image file to login page of Service Domain0.

```
<img src="/upload/vlan0/image001.gif">
```

Below depicts an example for **<div id="WALLED"></div>** content

```
<div class="ad"><a href="http://www.google.com" title="" target="_blank">Google</a></div>
```

You only can modify <div class="ad">, here is define CSS content for **<div class="ad">**

```
.ad{
   float: left;
   display: inline=block;
   text-align: center;
   width: 100px;
   margin: 5px;
```

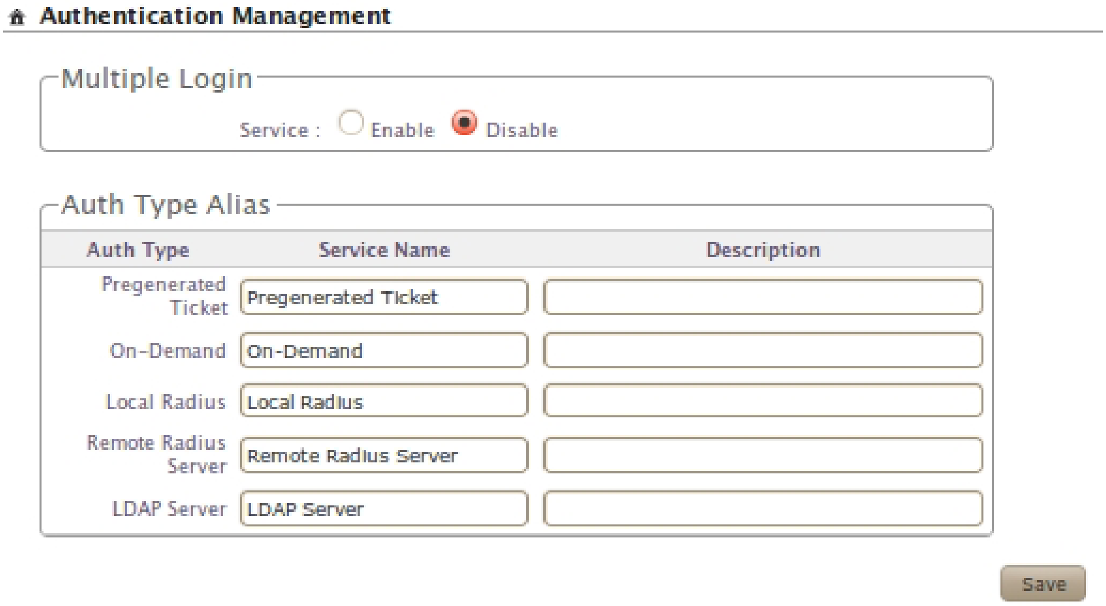
```
    padding: 5px;
    background: #fff;
    font-size: 14px;
    font-weight: bold;
}


.ad a{
    text-decoration: none;
    color: red;
}

.ad:hover, .ad a:hover, ad a:active{
    background: #333333;
    color: blue;
}
```

4.5.2 Configure Authentication

WAS-105R support **5** types of authentication : *None*, *Pregenerated Tickets*, *On-Demand Users*, *Local Radius Accounts*, *Remote Radius Server* and *Remote LDAP Server*. This section depicts to configure the settings for pregenerated tickets, on-demand users and authentication server. If authentication selected in ***None***, the clients can access Internet without authentication.

4.5.2.1 Authentication Management

The WAS-105R supports multiple login for one accounts and administrator can configure alias name of the respective authentication type on login page. Please click on **Service Domain -> Authentication -> Authentication Management**, and follow the below setting.



Authentication Management

Multiple Login

Service : ○ Enable ● Disable

Auth Type Alias

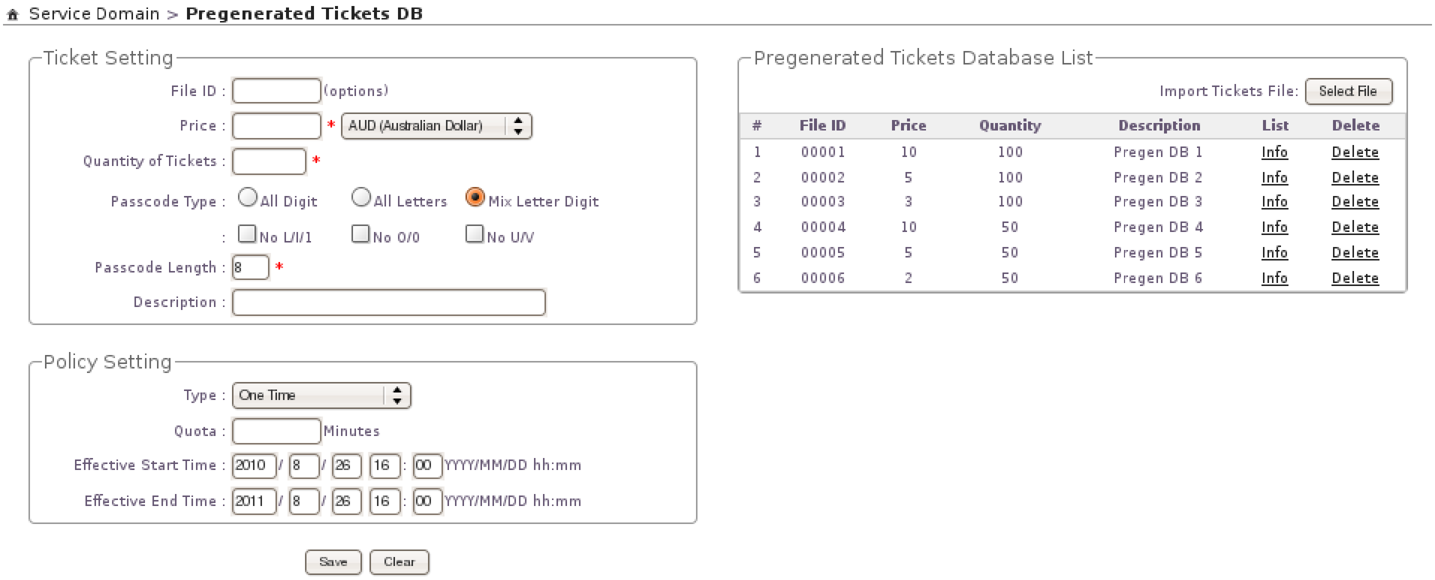
Auth Type	Service Name	Description
Pregenerated Ticket	Pregenerated Ticket	
On-Demand	On-Demand	
Local Radius	Local Radius	
Remote Radius Server	Remote Radius Server	
LDAP Server	LDAP Server	

- **Multiple Login :** Click ***Enable*** button to activate multiple login service, and Disable to inactivate multiple login service.
- **Auth Type :** Denote authentication type of the system.
- **Service Name :** Enter desired alias name of the respective authentication type.
- **Description :** Enter desired description name of the respective authentication type.

Change these settings as described here and click Save button to save your changes. Click Reboot button to activate your changes

4.5.2.2 Configure Pregenerated Tickets

This section is for administrators to pregenerated authentication tickets for entire external Network. There are three types of time policy ticket can be generated (**One Time**, **Multiple Times**, **Volume** and **Unlimited Until End Time**). Please click on **Service Domain -> Authentication -> Pregenerated Tickets**, and follow the below setting.



Service Domain > **Pregenerated Tickets DB**

Ticket Setting

File ID : (options)

Price : * AUD (Australian Dollar)

Quantity of Tickets : *

Passcode Type : ○ All Digit ○ All Letters ● Mix Letter Digit

: □ No L/I/1 □ No 0/0 □ No U/V

Passcode Length : 8 *

Description :

Policy Setting

Type : One Time

Quota : Minutes

Effective Start Time : 2010 / 8 / 26 16 : 00 YYYY/MM/DD hh:mm

Effective End Time : 2011 / 8 / 26 16 : 00 YYYY/MM/DD hh:mm

Save Clear

Pregenerated Tickets Database List

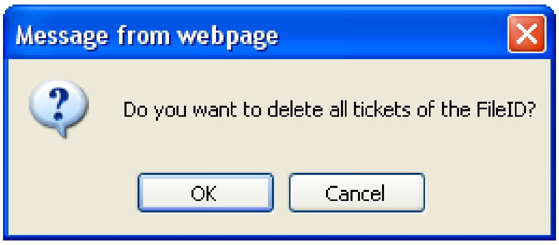
Import Tickets File: Select File

#	File ID	Price	Quantity	Description	List	Delete
1	00001	10	100	Pregen DB 1	Info	Delete
2	00002	5	100	Pregen DB 2	Info	Delete
3	00003	3	100	Pregen DB 3	Info	Delete
4	00004	10	50	Pregen DB 4	Info	Delete
5	00005	5	50	Pregen DB 5	Info	Delete
6	00006	2	50	Pregen DB 6	Info	Delete

- **File ID :** Enter the **8 hex digit** number for identifying tickets databases
- **Price :** The price charged for this tickets databases
- **Currency :** Select currency from drop-down list for this tickets databases
- **Quantity of Tickets :** Specify desired quantity of tickets for this databases
- **Passcode Type :** There are different passcode type for this tickets databases: **All Digit**, **All Letters**, **Mix Letter Digit**. Select All Letters or Mix Letter Digit, the sub-item should be shown-up. Select desired excluding letters for passcode of ticket databases.
- **Passcode Length :** Specify desired passcode length between **8** to **32** for this tickets databases
- **Description :** Enter the tickets databases description
- **Policy Type :** There are different policy for this tickets databases: **One Time**, **Multiple Times**, **Volume** and **Unlimited Until End Time**. Select *One Time* or *Multiple Times* or *Volume*, the **Quota** sub-item should be shown-up.
- **Quota :** Enter the time quota for One Time and Multiple Times policy (the maximum volume allowed is **527040** minutes, default is **60** minutes); or enter the volume quota for Volume policy (the maximum volume allowed is **102400** MB, default is **10** MB)
- **Effective Starting Time :** Specify desired effective starting time for this tickets databases
- **Effective Ending Time :** Specify desired effective ending time for this tickets databases

Click ***Save*** button for generate ticket databases on Pergenerated Tickets Database List.

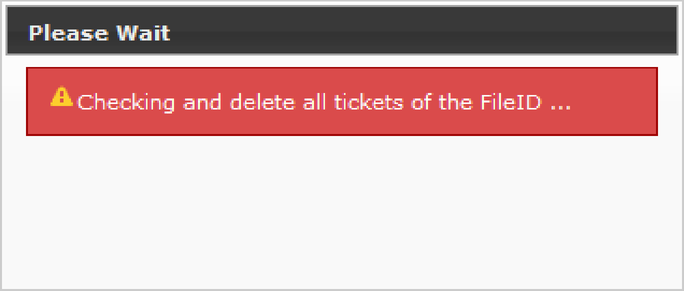
- **Delete :** Click ***Delete*** button to delete selected tickets databases. After clicking delete button, the alert message appears as below .



Message from webpage

Do you want to delete all tickets of the FileID?

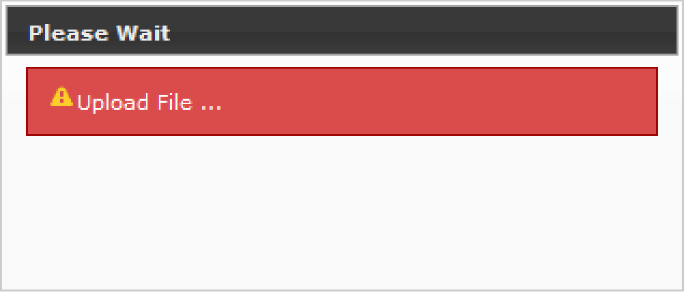
Click ***OK*** button, the system will check and delete selected pregenerated tickets database. The Success message will appear after deleting database.



Please Wait

⚠Checking and delete all tickets of the FileID ...

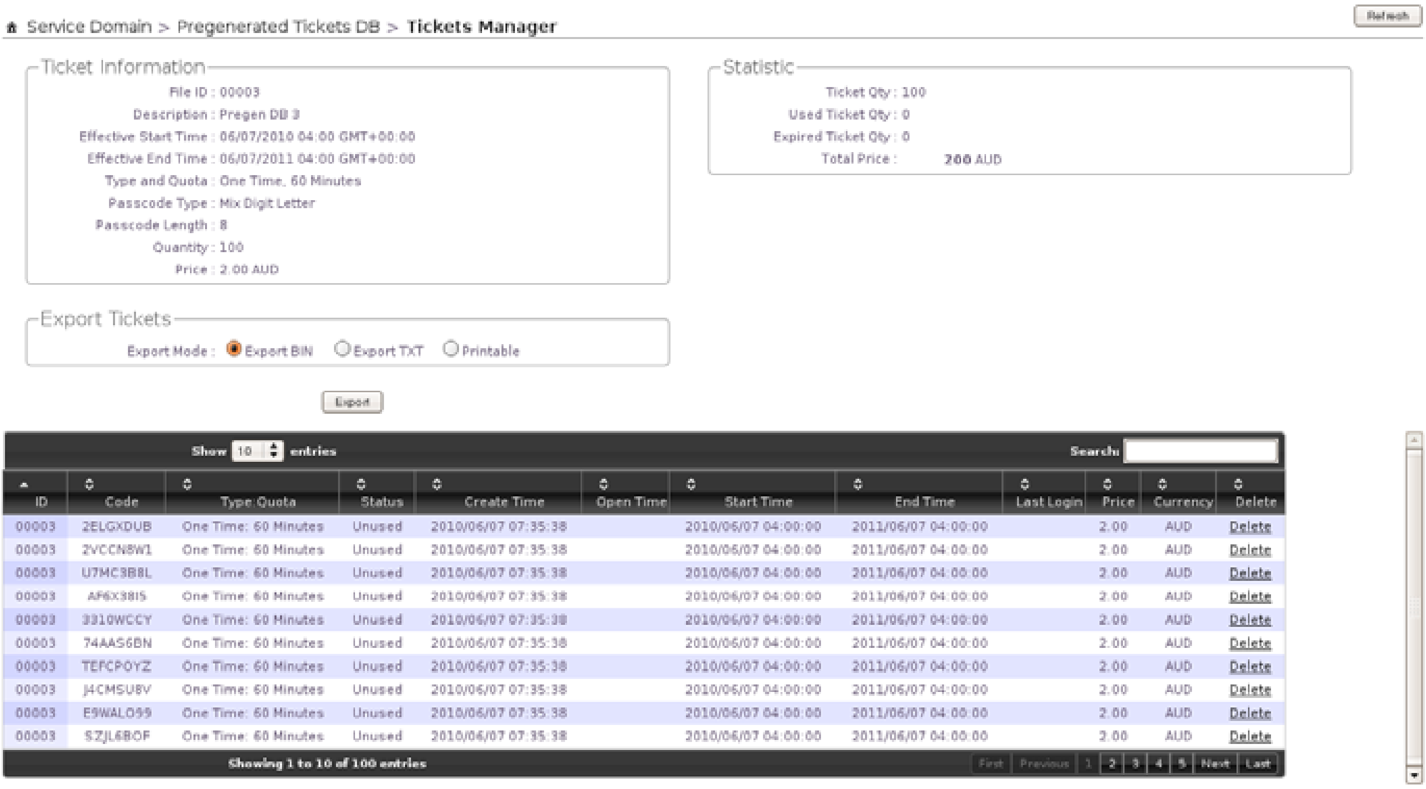
- **Import Tickets File :** Click this to enter the import tickets. Click ***Select File*** button to select the binary file for the tickets upload. The the "**Upload File ...**" message will appear.



Please Wait

⚠Upload File ...

- **List :** Click “**Info**” button to view information of each tickets databases. Below depicts an example for information of Pregenetated tickets databases.



Service Domain > Pregenerated Tickets DB > **Tickets Manager**

Ticket Information

File ID : 00003
Description : Pregen DB 3
Effective Start Time : 06/07/2010 04:00 GMT+00:00
Effective End Time : 06/07/2011 04:00 GMT+00:00
Type and Quota : One Time, 60 Minutes
Passcode Type : Mix Digit Letter
Passcode Length : 8
Quantity : 100
Price : 2.00 AUD

Statistic

Ticket Qty : 100
Used Ticket Qty : 0
Expired Ticket Qty : 0
Total Price : 200 AUD

Export Tickets

Export Mode : ● Export BIN ○ Export TXT ○ Printable

Show 10 entries — Search:

ID	Code	Type:Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
00003	2ELGXDUB	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	2VCCN8W1	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	U7MC3B8L	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	AF6X38I5	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	3310WCCY	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	74AAS6BN	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	TEFCPOYZ	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	J4CMSU8V	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	E9WALO99	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete
00003	SZJL6BOF	One Time: 60 Minutes	Unused	2010/06/07 07:35:38		2010/06/07 04:00:00	2011/06/07 04:00:00		2.00	AUD	Delete

Showing 1 to 10 of 100 entries

First Previous 1 2 3 4 5 Next Last

➔ **Ticket Information :** Show information for selected tickets database

✓ **File ID:** Identifying tickets databases

✓ **Description :** Denote information of the tickets databases

✓ **Effective Starting Time :** Denote effective starting time of the tickets databases

✓ **Effective Ending Time :** Denote effective ending time of the tickets databases

✓ **Type and Quota :** Denote tickets database time/volume policy and service quota.

✓ **Passcode Type :** Denote passcode type of the tickets databases

✓ **Passcode Length :** Denote ticket's passcode length

✓ **Quantity :** Denote ticket's quantity in this tickets databases

✓ **Price :** The price charged for this tickets database.

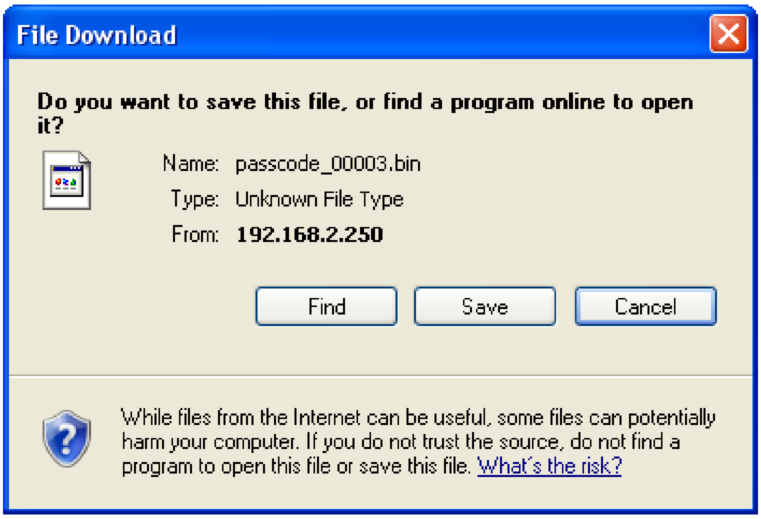
➔ **Statistic :** Show tickets database statistic information.

✓ **Ticket Qty :** Denote ticket's quantity in this tickets databases

- ✓ **Used Ticket Qty :** Denote used ticket's quantity in this tickets databases
- ✓ **Expired Ticket Qty :** Denote expired ticket's quantity in this tickets databases
- ✓ **Total Price :** Denote total ticket's price and currency in this tickets database

➔ **Export Tickets :** There are **three** methods to backup your information of ticket databases

- ✓ **Export BIN :** The administrator can backup ticket database or copy to other WAS-105R. Click ***Export*** button, the ticket databases (***FileID_passcode.bin***) will be download from system. Below depicts an example for exporting tickets database.



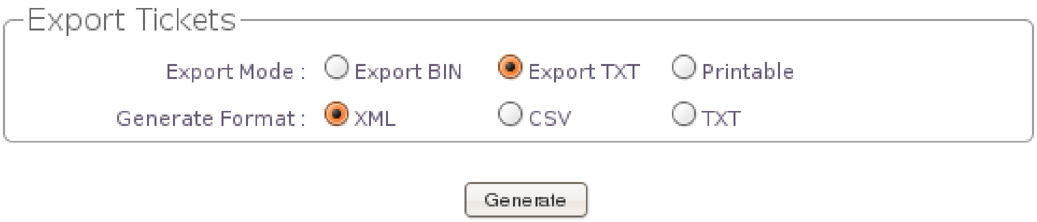
File Download

Do you want to save this file, or find a program online to open it?

Name: passcode_00003.bin
Type: Unknown File Type
From: **192.168.2.250**

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

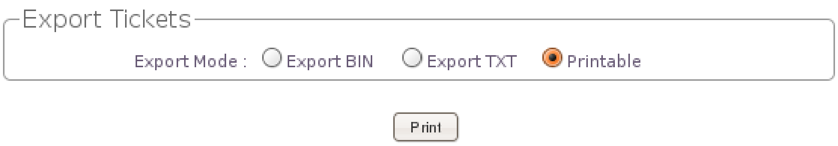
- ✓ **Export TXT :** There are **three** type of file list: XML, CSV and TXT(only Passcode). Click ***Generate*** button, the passcode list of ticket databases will be download from system.



Export Tickets

Export Mode : ○ Export BIN ● Export TXT ○ Printable
Generate Format : ● XML ○ CSV ○ TXT

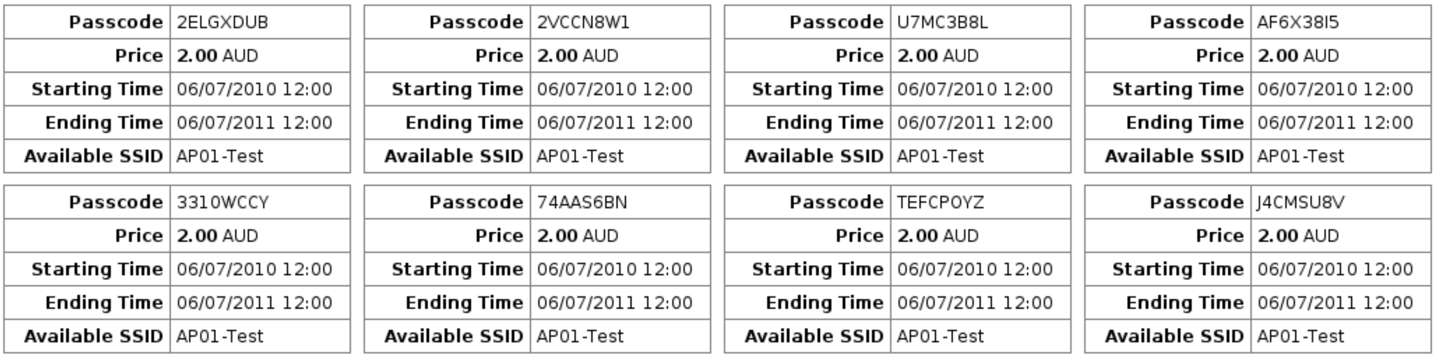
- ✓ **Printable :** The selected ticket databases can be previewed on the screen. Click ***Print*** button, the tickets will be shown including the information of **Passcode**, **Price**, **Start Time**, **End Time**, and **Available SSID** on the screen. Administrator can print tickets on the screen for customer.



Export Tickets

Export Mode : ○ Export BIN ○ Export TXT ● Printable

Below depicts an example for printable tickets



Passcode	2ELGXDUB	**Passcode**	2VCCN8W1	**Passcode**	U7MC3B8L	**Passcode**	AF6X38I5
Price	**2.00** AUD	**Price**	**2.00** AUD	**Price**	**2.00** AUD	**Price**	**2.00** AUD
Starting Time	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00
Ending Time	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00
Available SSID	AP01-Test	**Available SSID**	AP01-Test	**Available SSID**	AP01-Test	**Available SSID**	AP01-Test
Passcode	3310WCCY	**Passcode**	74AAS6BN	**Passcode**	TEFCPOYZ	**Passcode**	J4CMSU8V
Price	**2.00** AUD	**Price**	**2.00** AUD	**Price**	**2.00** AUD	**Price**	**2.00** AUD
Starting Time	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00	**Starting Time**	06/07/2010 12:00
Ending Time	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00	**Ending Time**	06/07/2011 12:00
Available SSID	AP01-Test	**Available SSID**	AP01-Test	**Available SSID**	AP01-Test	**Available SSID**	AP01-Test

➔ **Tickets List :** Show tickets information

- ✓ **Code :** User can used ticket's *Passcode* for access Internet.
- ✓ **Type/Quota :** Denote ticket's time/volume policy and service quota.
- ✓ **Status :** Show ticket's status. There three types of status : **Unused**, **Used** and **Expired**.
- ✓ **Create Time :** Denote the ticket create time
- ✓ **Open Time :** The ticket used for the first time
- ✓ **Start Time :** Denote effective starting time of the ticket
- ✓ **End Time :** Denote effective ending time of the ticket
- ✓ **Last Login :** Denote the ticket last login time
- ✓ **Price/Currency :** The price charged for this ticket.
- ✓ **Delete :** This will delete the ticket individually.

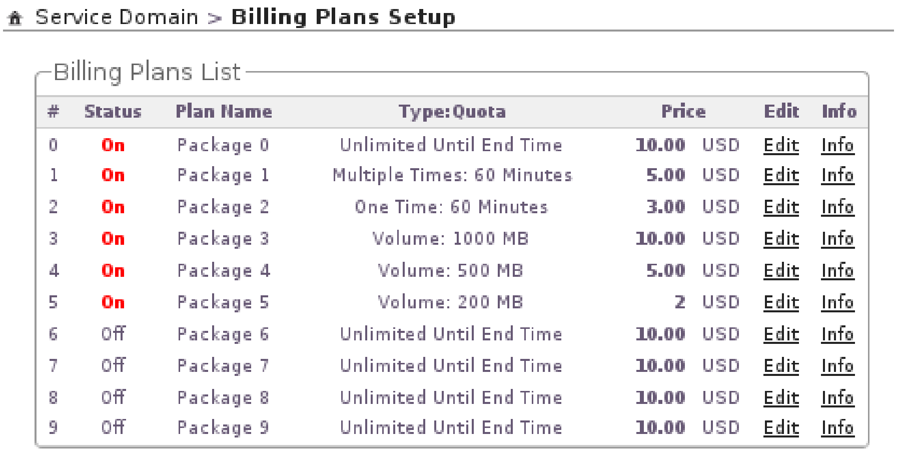
Click "**Refresh**" button to renew this page.

After you login system via Pregenerated authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)
If Timer Page doesn't appear in the browser, please enter "http(s)://hs.logout" to open Timer Page.

4.5.2.3 Configure On-Demand

Administrators can enable and configure this authentication method to provide clients access in a Hotspot environment. Major functions include billing plans creation, accounts creation, accounts monitoring list, thermal printer support, billing report statistics, and external payment gateway support. There are three method to generate on-demand accounts : **Generate by Manual**, **Print from Thermal Printer**, **Generate after Online Payments**.

Click on **Service Domain -> Authentication -> On-Demand**, then the Billing Plans List page will appears.



Service Domain > **Billing Plans Setup**

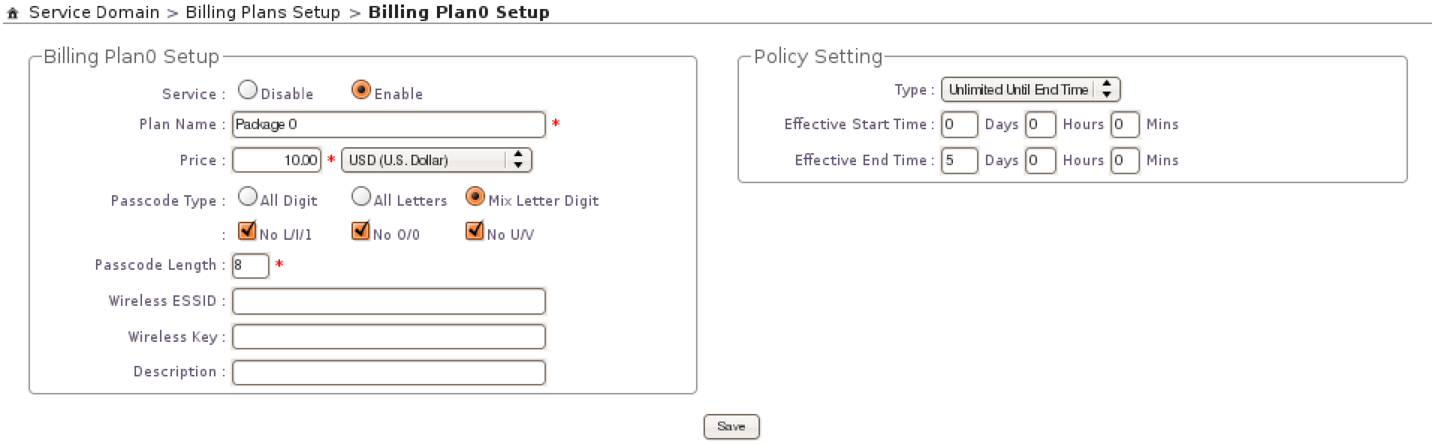
Billing Plans List

#	Status	Plan Name	Type:Quota	Price		Edit	Info
0	On	Package 0	Unlimited Until End Time	10.00	USD	Edit	Info
1	On	Package 1	Multiple Times: 60 Minutes	5.00	USD	Edit	Info
2	On	Package 2	One Time: 60 Minutes	3.00	USD	Edit	Info
3	On	Package 3	Volume: 1000 MB	10.00	USD	Edit	Info
4	On	Package 4	Volume: 500 MB	5.00	USD	Edit	Info
5	On	Package 5	Volume: 200 MB	2	USD	Edit	Info
6	Off	Package 6	Unlimited Until End Time	10.00	USD	Edit	Info
7	Off	Package 7	Unlimited Until End Time	10.00	USD	Edit	Info
8	Off	Package 8	Unlimited Until End Time	10.00	USD	Edit	Info
9	Off	Package 9	Unlimited Until End Time	10.00	USD	Edit	Info

- **Status :** Display billing plan status currently.
- **Plan Name :** Display name of respective billing plan
- **Type/Quota :** Denote respective billing plan time/volume policy and service quota
- **Price :** The price charged for respective billing rule.
- **Edit :** This will edit billing plan individually. There are **10** billing plan can be edited.
- **Info :** This will show accounts list and create accounts individually.

4.5.2.3.1 Create Billing Plans

Click Edit button on Billing Plans List page to enter the Billing Plan Setup page. In the Billing Plan Setup page, Administrator may configure plans.



Service Domain > Billing Plans Setup > **Billing Plan0 Setup**

Billing Plan0 Setup

Service : ○ Disable ● Enable
Plan Name : Package 0 *
Price : 10.00 * USD (U.S. Dollar)
Passcode Type : ○ All Digit ○ All Letters ● Mix Letter Digit
: ☑ No L/I/1 ☑ No O/0 ☑ No U/V
Passcode Length : 8 *
Wireless ESSID :
Wireless Key :
Description :

Policy Setting

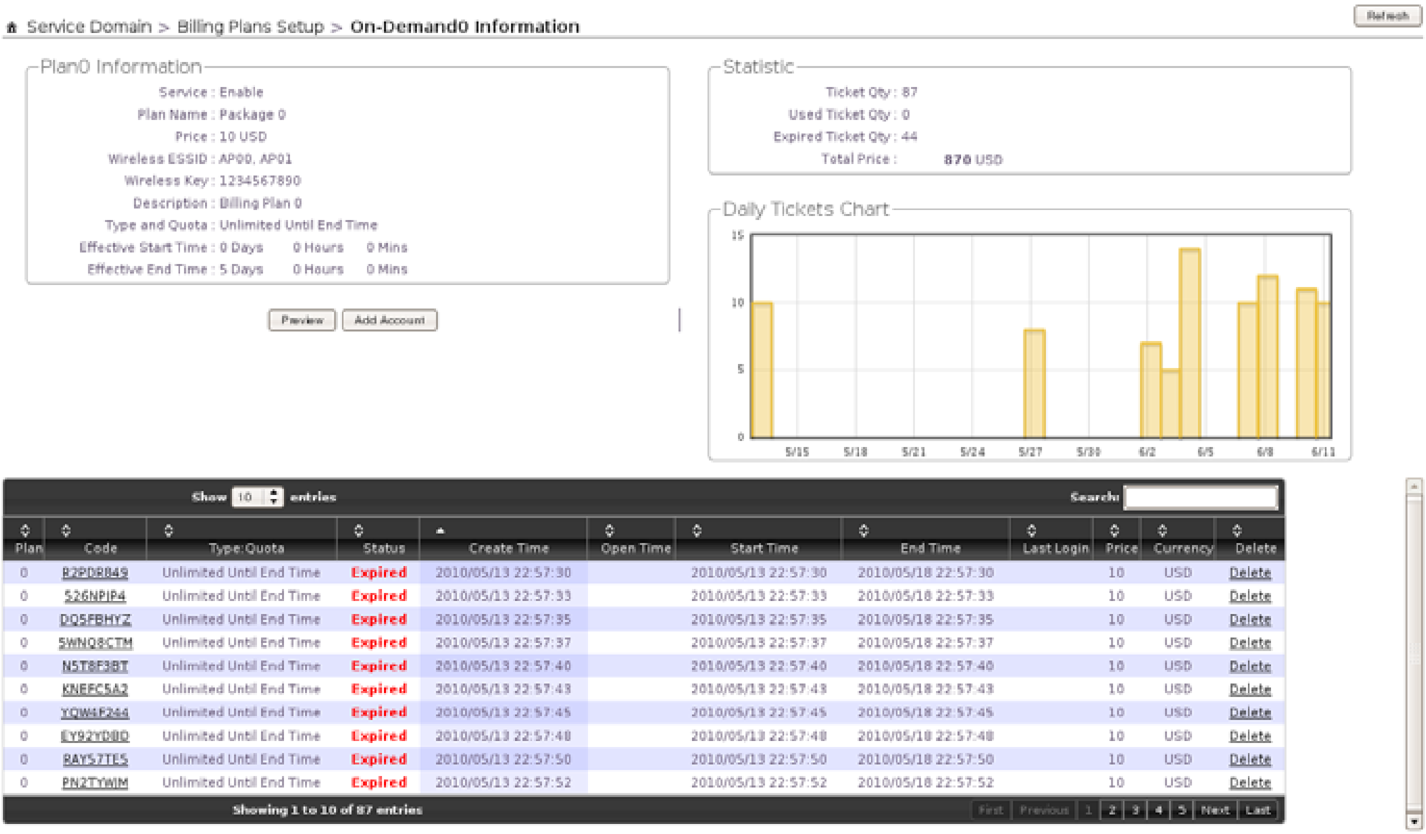
Type : Unlimited Until End Time
Effective Start Time : 0 Days 0 Hours 0 Mins
Effective End Time : 5 Days 0 Hours 0 Mins

- **Status :** By default, it's "***Disable***". To "***Enable***" to activate this billing plan.
- **Plan Name :** Enter plan name for this billing plan.
- **Price :** The price charged for this billing plan.
- **Passcode Type :** There are different passcode type for this billing plan: **All Digit**, **All Letters**, **Mix Letter Digit**. Select All Letters or Mix Letter Digit, the sub-item should be shown-up. Select desired excluding letters for passcode of ticket databases.
- **Passcode Length :** Specify desired passcode length between **8** to **32** for this billing plan.
- **Wireless ESSID :** Enter the ESSID of AP.
- **Wireless Key :** Enter the Wireless key of the AP such as WEP or WPA
- **Description :** Enter any additional information that will appear at the bottom of the receipt.
- **Policy Type:** There are different policy for this billing plan: **One Time**, **Multiple Times**, **Volume** and **Unlimited Until End Time**. Select *One Time* or *Multiple Times* or *Volume*, the **Quota** sub-item should be shown-up.
- **Quota :** Enter the time quota for One Time and Multiple Times policy (the maximum volume allowed is **527040** minutes, default is **60** minutes); or enter the volume quota for Volume policy (the maximum volume allowed is **102400** MB, default is **10** MB)
- **Effective Starting Time :** Specify desired effective starting time for this billing plan.
- **Effective Ending Time :** Specify desired effective ending time for this billing plan.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.5.2.3.2 Create On-Demand Users

After configuring billing plans, administrator can create and delete on-demand users on this section. Click ***Info*** button on **Billing Plans List page** to enter the **On-Demand Information** page. In the On-Demand Information page. Administrator may create and delete on-demand users.



Plan0 Information

Service : Enable
Plan Name : Package 0
Price : 10 USD
Wireless ESSID : AP00, AP01
Wireless Key : 1234567890
Description : Billing Plan 0
Type and Quota : Unlimited Until End Time
Effective Start Time : 0 Days 0 Hours 0 Mins
Effective End Time : 5 Days 0 Hours 0 Mins

Statistic

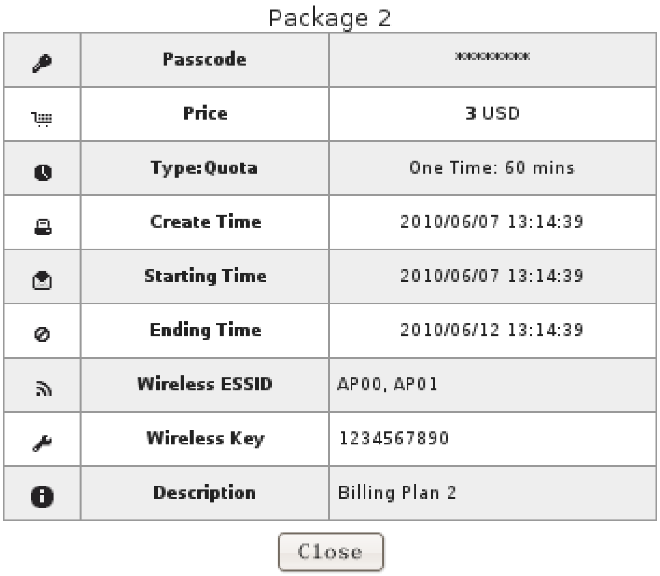
Ticket Qty : 87
Used Ticket Qty : 0
Expired Ticket Qty : 44
Total Price : 870 USD

Plan	Code	Type:Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
0	R2PDR849	Unlimited Until End Time	Expired	2010/05/13 22:57:30		2010/05/13 22:57:30	2010/05/18 22:57:30		10	USD	Delete
0	S26NPIP4	Unlimited Until End Time	Expired	2010/05/13 22:57:33		2010/05/13 22:57:33	2010/05/18 22:57:33		10	USD	Delete
0	DQ5FBHYZ	Unlimited Until End Time	Expired	2010/05/13 22:57:35		2010/05/13 22:57:35	2010/05/18 22:57:35		10	USD	Delete
0	SWNQ8CTM	Unlimited Until End Time	Expired	2010/05/13 22:57:37		2010/05/13 22:57:37	2010/05/18 22:57:37		10	USD	Delete
0	N5T8F3BT	Unlimited Until End Time	Expired	2010/05/13 22:57:40		2010/05/13 22:57:40	2010/05/18 22:57:40		10	USD	Delete
0	KNEFC5A2	Unlimited Until End Time	Expired	2010/05/13 22:57:43		2010/05/13 22:57:43	2010/05/18 22:57:43		10	USD	Delete
0	YQW4F244	Unlimited Until End Time	Expired	2010/05/13 22:57:45		2010/05/13 22:57:45	2010/05/18 22:57:45		10	USD	Delete
0	EY92YD8D	Unlimited Until End Time	Expired	2010/05/13 22:57:48		2010/05/13 22:57:48	2010/05/18 22:57:48		10	USD	Delete
0	RAY57TE5	Unlimited Until End Time	Expired	2010/05/13 22:57:50		2010/05/13 22:57:50	2010/05/18 22:57:50		10	USD	Delete
0	PN2TYWIM	Unlimited Until End Time	Expired	2010/05/13 22:57:52		2010/05/13 22:57:52	2010/05/18 22:57:52		10	USD	Delete

Showing 1 to 10 of 87 entries

- **Plan Information :** Show plan information in this billing plan
  - ➔ **Status :** Display billing plan status currently.
  - ➔ **Plan Name :** Display plan name in this billing plan.
  - ➔ **Price :** The price charged in this billing plan.
  - ➔ **Wireless ESSID :** The ESSID of AP in this billing plan.
  - ➔ **Wireless Key :** The Wireless key of the AP in this billing plan.
  - ➔ **Description :** Additional information in this billing plan.
  - ➔ **Type and Quota :** Denote time/volume policy and service quota in this billing plan
  - ➔ **Effective Starting Time :** Denote effective starting time in this billing plan
  - ➔ **Effective Ending Time :** Denote effective ending time in this billing plan

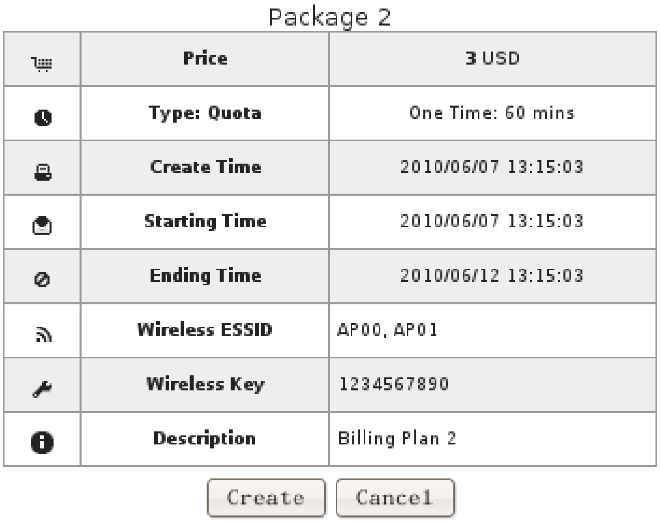
Click ***Preview*** button to preview ticket in the billing plan. Below depicts an example for previewing ticket. Click ***Close*** button to close window.



Package 2

	Passcode	********
	Price	3 USD
	Type:Quota	One Time: 60 mins
	Create Time	2010/06/07 13:14:39
	Starting Time	2010/06/07 13:14:39
	Ending Time	2010/06/12 13:14:39
	Wireless ESSID	AP00, AP01
	Wireless Key	1234567890
	Description	Billing Plan 2

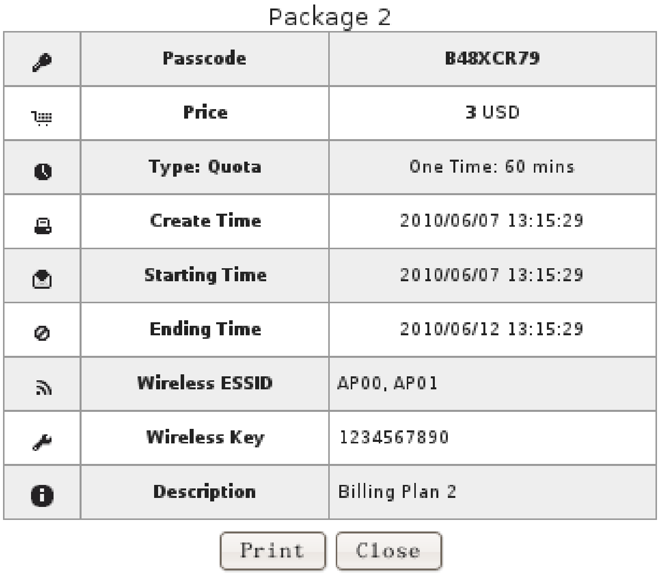
Click ***Add Accounts*** button, the create page will appear as below. Click ***Cancel*** button to close window.



Package 2

	Price	3 USD
	Type: Quota	One Time: 60 mins
	Create Time	2010/06/07 13:15:03
	Starting Time	2010/06/07 13:15:03
	Ending Time	2010/06/12 13:15:03
	Wireless ESSID	AP00, AP01
	Wireless Key	1234567890
	Description	Billing Plan 2

Click ***Create*** button to add new account for this billing plan. Below depicts an example for creating ticket.

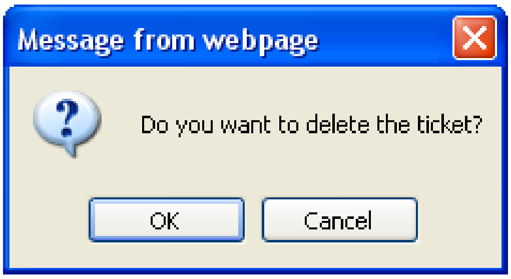


Package 2

Passcode	**B48XCR79**
Price	3 USD
Type: Quota	One Time: 60 mins
Create Time	2010/06/07 13:15:29
Starting Time	2010/06/07 13:15:29
Ending Time	2010/06/12 13:15:29
Wireless ESSID	AP00, AP01
Wireless Key	1234567890
Description	Billing Plan 2

- **Statistic :** Show on-demand users statistic information for this billing plan
  - ➔ **Ticket Qty :** Denote ticket's quantity in this billing plan
  - ➔ **Used Ticket Qty :** Denote used ticket's quantity in this billing plan
  - ➔ **Expired Ticket Qty :** Denote expired ticket's quantity in this billing plan
  - ➔ **Total Price :** Denote total ticket's price and currency in this billing plan
- **Daily Tickets Chart :** Show ticket's quantity of chart for this billing plan
- **Tickets List :** Show tickets information
  - ➔ **Plan :** Denote billing plan for this ticket.
  - ➔ **Code :** User can used ticket's *Passcode* for access Internet.
  - ➔ **Type/Quota :** Denote ticket's time/volume policy and service quota.
  - ➔ **Status :** Show ticket's status. There three types of status : **Unused**, **Used** and **Expired**.
  - ➔ **Create Time :** Denote the ticket create time
  - ➔ **Open Time :** The ticket used for the first time
  - ➔ **Start Time :** Denote effective starting time of the ticket
  - ➔ **End Time :** Denote effective ending time of the ticket
  - ➔ **Last Login :** Denote the ticket last login time
  - ➔ **Price/Currency :** The price charged for this ticket.

➔ **Delete :** This will delete the ticket individually. When administrator click **Delete** button, the alert message will appear as below.



Message from webpage

Do you want to delete the ticket?

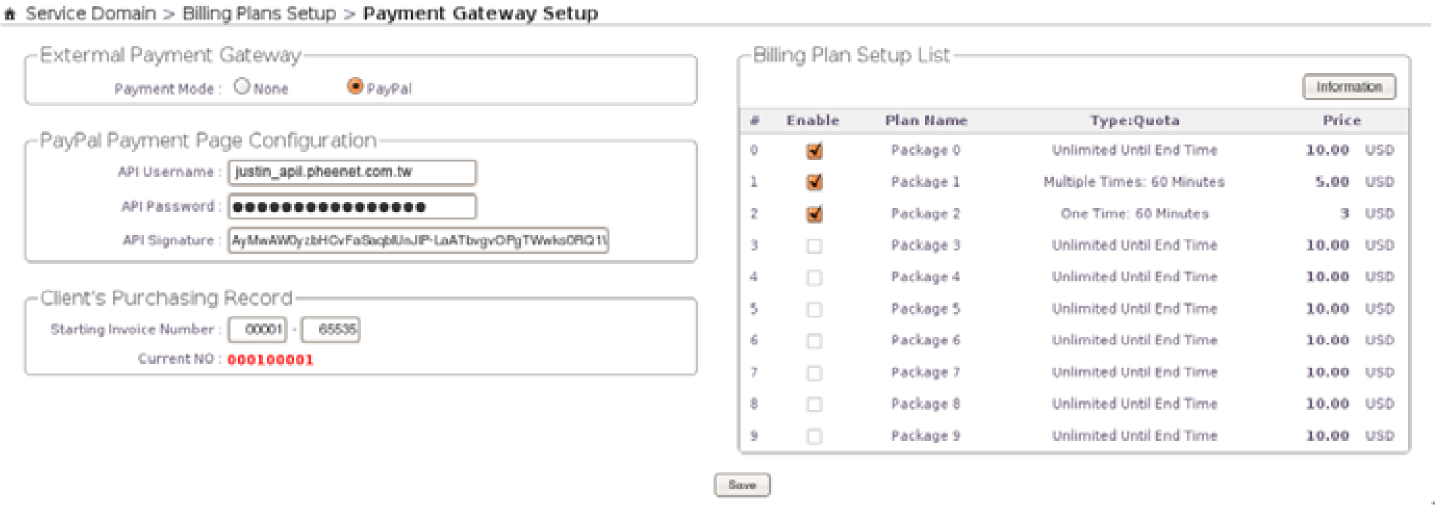
On this List, it only shows all of generated tickets through clicking **Add Accounts** button.

After you login system via **On-Demand** authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)

If Timer Page doesn't appear in the browser, please enter “http(s)://hs.logout” to open Timer Page.

4.5.2.3.3 Configure External Payment Gateway

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



Service Domain > Billing Plans Setup > **Payment Gateway Setup**

External Payment Gateway

Payment Mode : ○ None ● PayPal

PayPal Payment Page Configuration

API Username : justin_apil.pheenet.com.tw

API Password : ●●●●●●●●●●●●●●●●

API Signature : AyMwAW0yzbHCvFaSaqbUnJIP-LaATbvgvOPgTWwks0RQ1\

Client's Purchasing Record

Starting Invoice Number : 00001 - 65535

Current NO : 000100001

Billing Plan Setup List

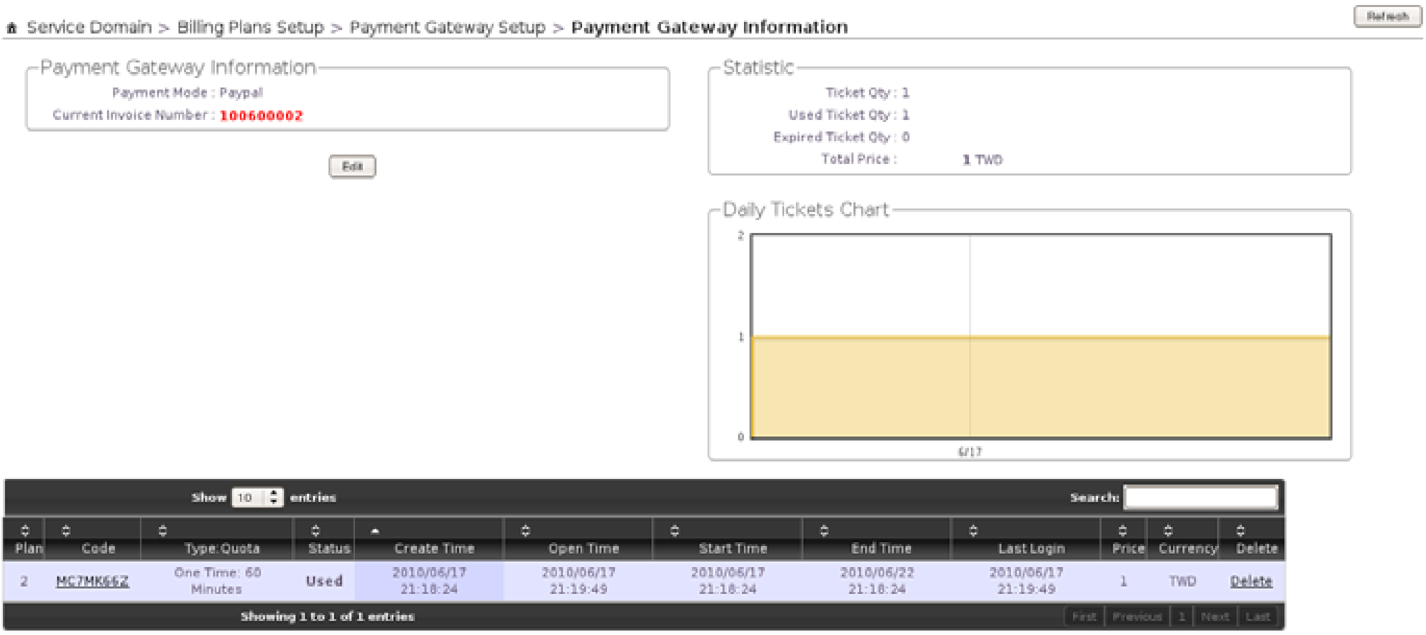
#	Enable	Plan Name	Type:Quota	Price	
0	☑	Package 0	Unlimited Until End Time	10.00	USD
1	☑	Package 1	Multiple Times: 60 Minutes	5.00	USD
2	☑	Package 2	One Time: 60 Minutes	3	USD
3	□	Package 3	Unlimited Until End Time	10.00	USD
4	□	Package 4	Unlimited Until End Time	10.00	USD
5	□	Package 5	Unlimited Until End Time	10.00	USD
6	□	Package 6	Unlimited Until End Time	10.00	USD
7	□	Package 7	Unlimited Until End Time	10.00	USD
8	□	Package 8	Unlimited Until End Time	10.00	USD
9	□	Package 9	Unlimited Until End Time	10.00	USD

Select Paypal to enable External Payment Gateway. Before setting up "**PayPal**", it is required that the merchant owners have a valid PayPal "**API Username**", "**API Password**".

Please see **Appendix C – Accepting Payments via PayPal**, **Appendix D – Examples of Making Payments for End Users** for more information about setting up a PayPal Business Account, relevant maintenance functions, and example for end users.

After opening a PayPal Business Account, the merchant should find the "**API Signature**" of this PayPal account to continue "External Payment Gateway Setup".

- **API Username :** This is the "Login ID"(E-mail address) that is associated with the PayPal Business Account.
- **API Password :** This is the "Login Password" that is associated with the PayPal Business Account.
- **API Signature :** This the key used by Paypal to validate all the transactions.
- **Invoice Number :** An invoice number may be provided as additional information against a transaction.
- **Current No. :** Show current invoice number.
- **Information :** Click this button to view accounts information for PayPal.



Service Domain > Billing Plans Setup > Payment Gateway Setup > **Payment Gateway Information**

Payment Gateway Information

Payment Mode : Paypal
Current Invoice Number : 100600002

Statistic

Ticket Qty : 1
Used Ticket Qty : 1
Expired Ticket Qty : 0
Total Price : 1 TWD

Daily Tickets Chart

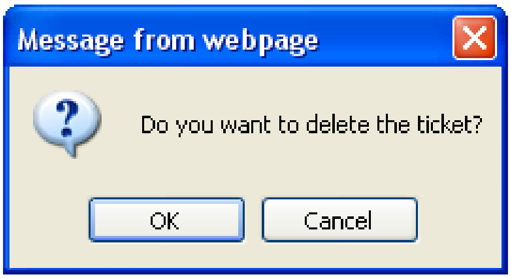
Show 10 entries Search:

Plan	Code	Type:Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
2	MC7MK66Z	One Time: 60 Minutes	Used	2010/06/17 21:18:24	2010/06/17 21:19:49	2010/06/17 21:18:24	2010/06/22 21:18:24	2010/06/17 21:19:49	1	TWD	Delete

Showing 1 to 1 of 1 entries

- **Payment Gateway Information :** Show current ticket's invoice number.
- **Statistic :** Show on-demand users statistic information for this billing plan
  - ➔ **Ticket Qty :** Denote ticket's quantity in this billing plan
  - ➔ **Used Ticket Qty :** Denote used ticket's quantity in this billing plan
  - ➔ **Expired Ticket Qty :** Denote expired ticket's quantity in this billing plan
  - ➔ **Total Price :** Denote total ticket's price and currency in this billing plan
- **Daily Tickets Chart :** Show ticket's quantity of chart for this billing plan
- **Tickets List :** Show tickets information
  - ➔ **Plan :** Denote billing plan for this ticket.
  - ➔ **Code :** User can used ticket's *Passcode* for access Internet.
  - ➔ **Type/Quota :** Denote ticket's time/volume policy and service quota.
  - ➔ **Status :** Show ticket's status. There are three types of status : **Unused**, **Used** and **Expired**.
  - ➔ **Create Time :** Denote the ticket create time
  - ➔ **Open Time :** The ticket used for the first time
  - ➔ **Start Time :** Denote effective starting time of the ticket
  - ➔ **End Time :** Denote effective ending time of the ticket
  - ➔ **Last Login :** Denote the ticket last login time
  - ➔ **Price/Currency :** The price charged for this ticket.

➔ **Delete :** This will delete the ticket individually. When administrator click **Delete** button, the alert message will appear as below.



Do you want to delete the ticket?

On this List, it only shows all of generated tickets through **External Payment Gateway**.

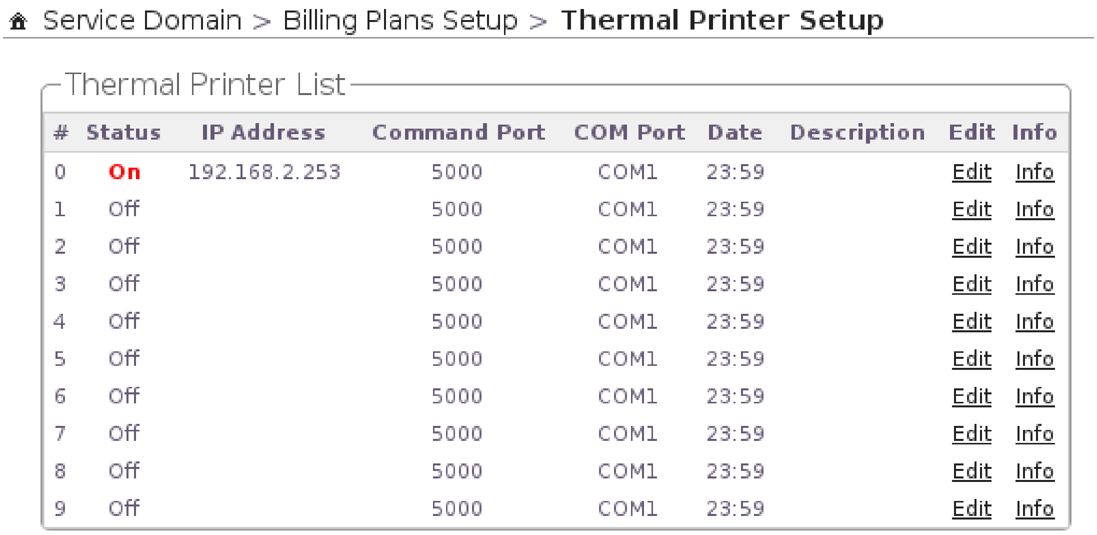
After you login system via **On-Demand** authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)

If Timer Page doesn't appear in the browser, please enter “http(s)://hs.logout” to open Timer Page.

If administrator wants to refund transaction, please see **Appendix E. Issue Refund for PayPal**

4.5.2.3.4 Configure Thermal Printer

WAS-105R can generate ticket of on-demand users manually or automatically from Thermal Printer. Please click on **Service Domain -> Authentication -> On-Demand -> Thermal Printer Setup** to enter the **Thermal Printer List** page. In the Thermal Printer List page. Administrator may configure Thermal Printer setting and generate tickets manually and delete tickets.



Service Domain > Billing Plans Setup > **Thermal Printer Setup**

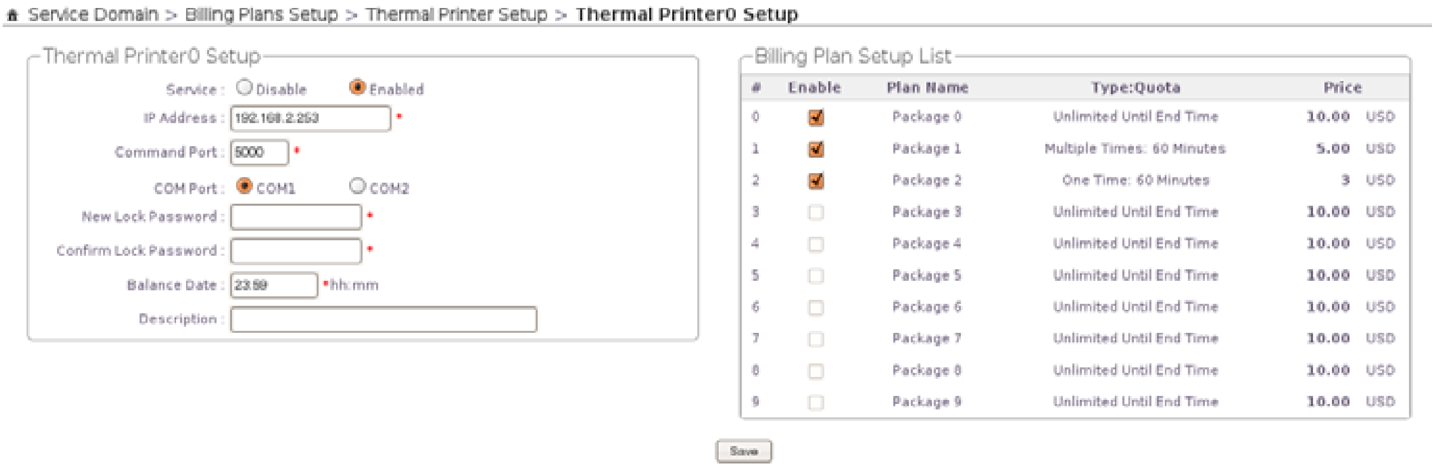
Thermal Printer List

#	Status	IP Address	Command Port	COM Port	Date	Description	Edit	Info
0	On	192.168.2.253	5000	COM1	23:59		Edit	Info
1	Off		5000	COM1	23:59		Edit	Info
2	Off		5000	COM1	23:59		Edit	Info
3	Off		5000	COM1	23:59		Edit	Info
4	Off		5000	COM1	23:59		Edit	Info
5	Off		5000	COM1	23:59		Edit	Info
6	Off		5000	COM1	23:59		Edit	Info
7	Off		5000	COM1	23:59		Edit	Info
8	Off		5000	COM1	23:59		Edit	Info
9	Off		5000	COM1	23:59		Edit	Info

If administrator wants to generate tickets from Thermal Printer, system must use **PSS-120** to control Thermal Printer.

- **Status :** Display Thermal Printer status currently.
- **IP Address :** Denote IP address of respective PSS-120
- **Command Port :** Denote command port of respective Thermal Printer
- **COM Port :** Denote COM port of respective PSS-120
- **Date :** Denote balance date of respective Thermal Printer
- **Description :** Denote information of respective Thermal Printer
- **Edit :** This will edit billing plan individually. There are **10** billing plan can be edited.
- **Info :** This will show accounts list and create accounts individually.

Click ***Edit*** button to enter **Thermal Printer Setup** page. In the Thermal Printer Setup page, administrator may configure related settings.



🏠 Service Domain > Billing Plans Setup > Thermal Printer Setup > **Thermal Printer0 Setup**

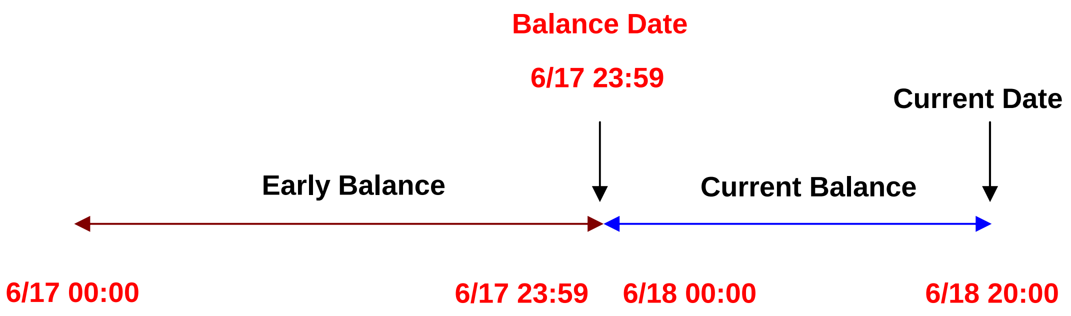
Thermal Printer0 Setup

Service :	○ Disable ● Enabled
IP Address :	192.168.2.253 *
Command Port :	5000 *
COM Port :	● COM1 ○ COM2
New Lock Password :	*
Confirm Lock Password :	*
Balance Date :	23:59 *hh:mm
Description :	

Billing Plan Setup List

#	Enable	Plan Name	Type:Quota	Price	
0	☑	Package 0	Unlimited Until End Time	10.00	USD
1	☑	Package 1	Multiple Times: 60 Minutes	5.00	USD
2	☑	Package 2	One Time: 60 Minutes	3	USD
3	□	Package 3	Unlimited Until End Time	10.00	USD
4	□	Package 4	Unlimited Until End Time	10.00	USD
5	□	Package 5	Unlimited Until End Time	10.00	USD
6	□	Package 6	Unlimited Until End Time	10.00	USD
7	□	Package 7	Unlimited Until End Time	10.00	USD
8	□	Package 8	Unlimited Until End Time	10.00	USD
9	□	Package 9	Unlimited Until End Time	10.00	USD

- **Service :** By default, it's “**Disable**”. To “**Enable**” to activate this function.
- **IP Address :** Enter IP address of PSS-120
- **Command Port :** Enter command port of the Thermal Printer
- **COM Port :** Select COM port for PSS-120
- **Balance Date :** Enter balance date for statement printing from Thermal Printer. Thermal Printer can print “**Current Balance**” or “**Early Balance**” statement. Below depicts an example for Balance Date.

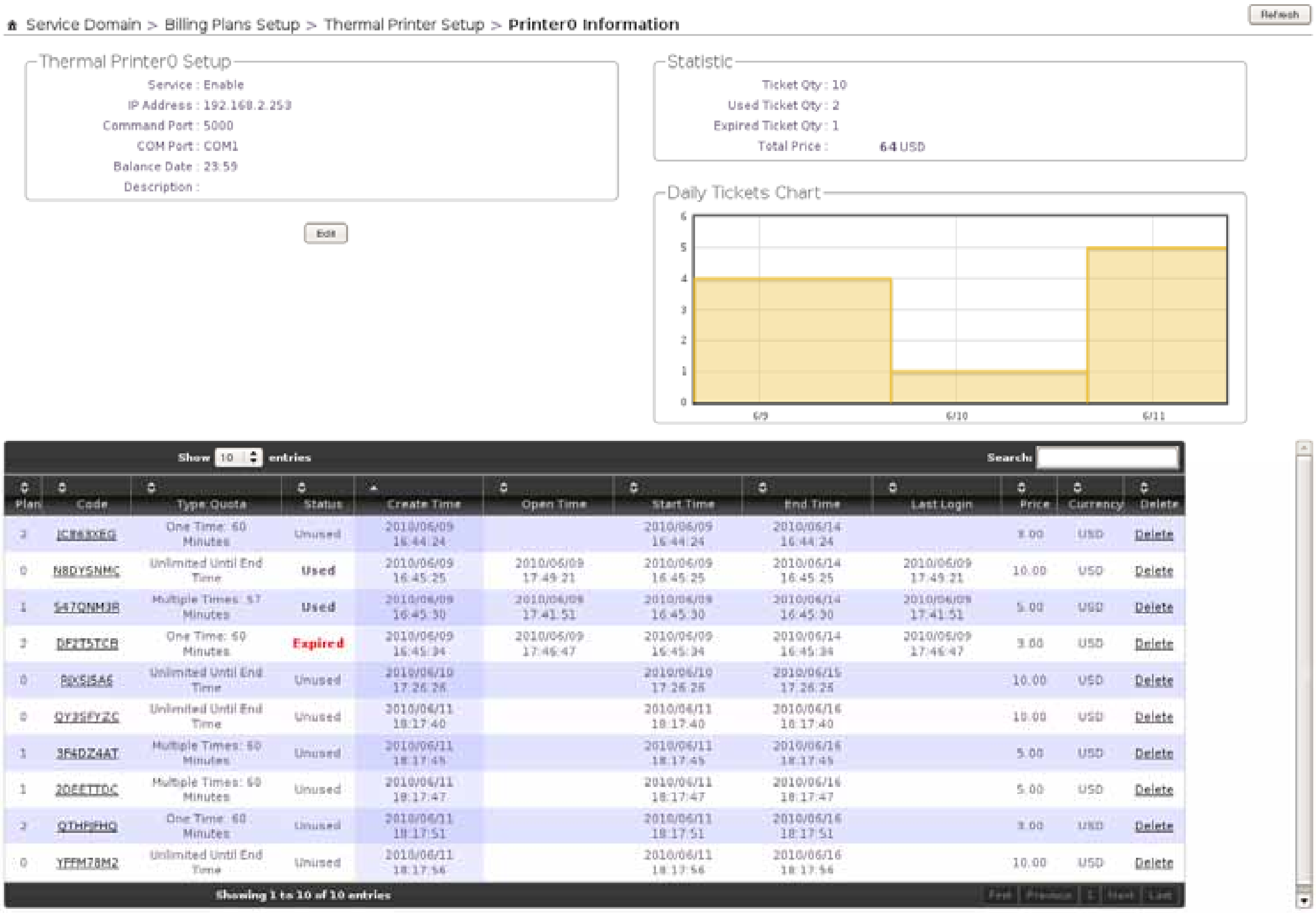


- **Description :** Enter additional information for this Thermal Printer

After configuring Thermal Printer general setting, administrator must select billing plan for this Thermal Printer.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Click ***Info*** button to enter **Thermal Printer Information** page. In the Thermal Printer Information page, administrator may generated and delete ticket manually.



Service Domain > Billing Plans Setup > Thermal Printer Setup > **Printer0 Information**

Thermal Printer0 Setup

Service : Enable
IP Address : 192.168.2.253
Command Port : 5000
COM Port : COM1
Balance Date : 23:59
Description :

Statistic

Ticket Qty : 10
Used Ticket Qty : 2
Expired Ticket Qty : 1
Total Price : 64 USD

Show 10 entries Search:

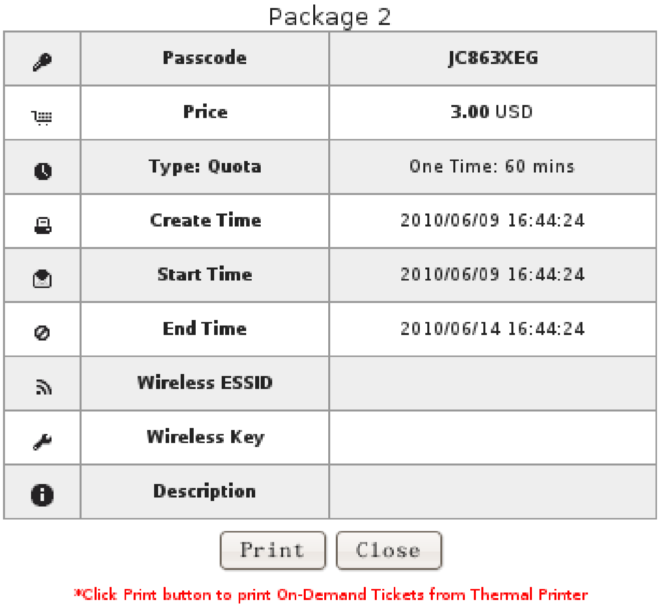
Plan	Code	Type Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
2	JC8K8XEG	One Time: 60 Minutes	Unused	2010/06/09 16:44:24		2010/06/09 16:44:24	2010/06/14 16:44:24		3.00	USD	Delete
0	N8DYSNMC	Unlimited Until End Time	**Used**	2010/06/09 16:45:25	2010/06/09 17:49:21	2010/06/09 16:45:25	2010/06/14 16:45:25	2010/06/09 17:49:21	10.00	USD	Delete
1	S47QNM3R	Multiple Times: 57 Minutes	**Used**	2010/06/09 16:45:30	2010/06/09 17:41:51	2010/06/09 16:45:30	2010/06/14 16:45:30	2010/06/09 17:41:51	5.00	USD	Delete
2	DF2T5TCB	One Time: 60 Minutes	**Expired**	2010/06/09 16:45:34	2010/06/09 17:46:47	2010/06/09 16:45:34	2010/06/14 16:45:34	2010/06/09 17:46:47	3.00	USD	Delete
0	RJXSJSA6	Unlimited Until End Time	Unused	2010/06/10 17:26:26		2010/06/10 17:26:26	2010/06/15 17:26:26		10.00	USD	Delete
0	QY3SFYZC	Unlimited Until End Time	Unused	2010/06/11 18:17:40		2010/06/11 18:17:40	2010/06/16 18:17:40		10.00	USD	Delete
1	3F4DZ4AT	Multiple Times: 60 Minutes	Unused	2010/06/11 18:17:45		2010/06/11 18:17:45	2010/06/16 18:17:45		5.00	USD	Delete
1	2DEETTDC	Multiple Times: 60 Minutes	Unused	2010/06/11 18:17:47		2010/06/11 18:17:47	2010/06/16 18:17:47		5.00	USD	Delete
2	QTHRJFHQ	One Time: 60 Minutes	Unused	2010/06/11 18:17:51		2010/06/11 18:17:51	2010/06/16 18:17:51		3.00	USD	Delete
0	YFFM78M2	Unlimited Until End Time	Unused	2010/06/11 18:17:56		2010/06/11 18:17:56	2010/06/16 18:17:56		10.00	USD	Delete

Showing 1 to 10 of 10 entries

- **Thermal Printer Information :** Show setting information in this Thermal Printer.
  - ➔ **Status :** Display Thermal Printer status currently.
  - ➔ **IP Address :** Denote IP address for this PSS-120
  - ➔ **Command Port :** Denote command port for this Thermal Printer
  - ➔ **COM Port :** Denote COM port for this PSS-120
  - ➔ **Date :** Denote balance date for this Thermal Printer
  - ➔ **Description :** Denote additional information for this Thermal Printer

Click ***Edit*** button to enter Thermal Printer Setup page.

- **Statistic :** Show on-demand users statistic information for this billing plan
  - ➔ **Ticket Qty :** Denote ticket's quantity in this Thermal Printer.
  - ➔ **Used Ticket Qty :** Denote used ticket's quantity in this Thermal Printer.
  - ➔ **Expired Ticket Qty :** Denote expired ticket's quantity in this Thermal Printer.
  - ➔ **Total Price :** Denote total ticket's price and currency in this Thermal Printer.
- **Daily Tickets Chart :** Show ticket's quantity of chart for this billing plan
- **Tickets List :** Show tickets information
  - ➔ **Plan :** Denote billing plan for this ticket.
  - ➔ **Code :** User can used ticket's *Passcode* for access Internet. Clicking **hyperlinks** to view this ticket information as below. Click ***Print*** button, the ticket will print from Thermal Printer again.



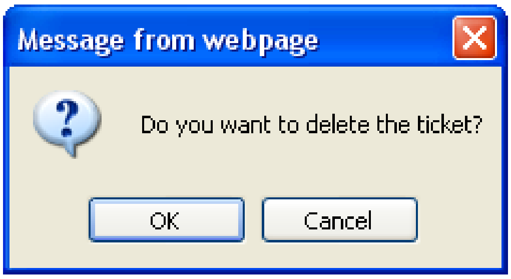
Package 2

Passcode	**JC863XEG**
Price	**3.00** USD
Type: Quota	One Time: 60 mins
Create Time	2010/06/09 16:44:24
Start Time	2010/06/09 16:44:24
End Time	2010/06/14 16:44:24
Wireless ESSID	
Wireless Key	
Description	

*Click Print button to print On-Demand Tickets from Thermal Printer

  - ➔ **Type/Quota :** Denote ticket's time/volume policy and service quota.
  - ➔ **Status :** Show ticket's status. There three types of status : **Unused**, **Used** and **Expired**.
  - ➔ **Create Time :** Denote the ticket create time
  - ➔ **Open Time :** The ticket used for the first time
  - ➔ **Start Time :** Denote effective starting time of the ticket
  - ➔ **End Time :** Denote effective ending time of the ticket
  - ➔ **Last Login :** Denote the ticket last login time
  - ➔ **Price/Currency :** The price charged for this ticket.

➔ **Delete :** This will delete the ticket individually. When administrator click **Delete** button, the alert message will appear as below.


Message from webpage

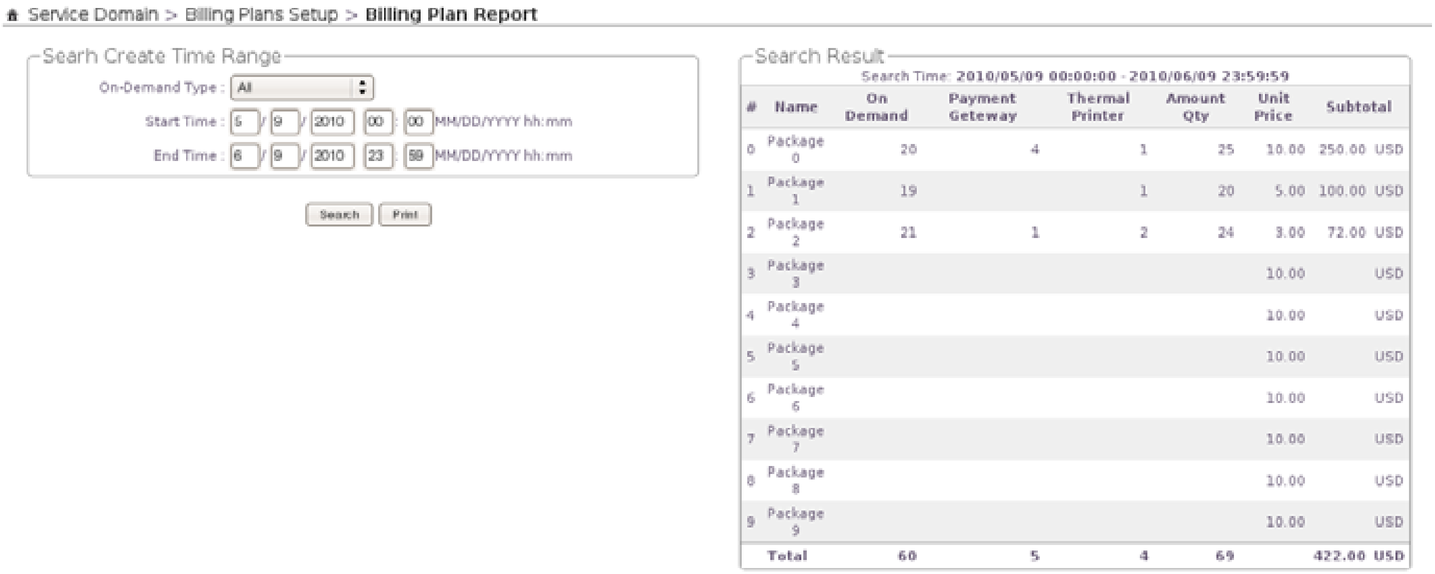
Do you want to delete the ticket?

On this List, it only shows all of generated tickets from Thermal Printer.

After you login system via **On-Demand** authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)
If Timer Page doesn't appear in the browser, please enter "http(s)://hs.logout" to open Timer Page.

4.5.2.3.5 Billing Plan Report

Click on **Service Domain -> Authentication -> On-Demand** to enter the **Billing Plans Report** page. Administrator can get a complete report or a report of a particular period.



Service Domain > Billing Plans Setup > **Billing Plan Report**

Searh Create Time Range

On-Demand Type : All

Start Time : 5 / 9 / 2010 00 : 00 MM/DD/YYYY hh:mm

End Time : 6 / 9 / 2010 23 : 59 MM/DD/YYYY hh:mm

Search Result

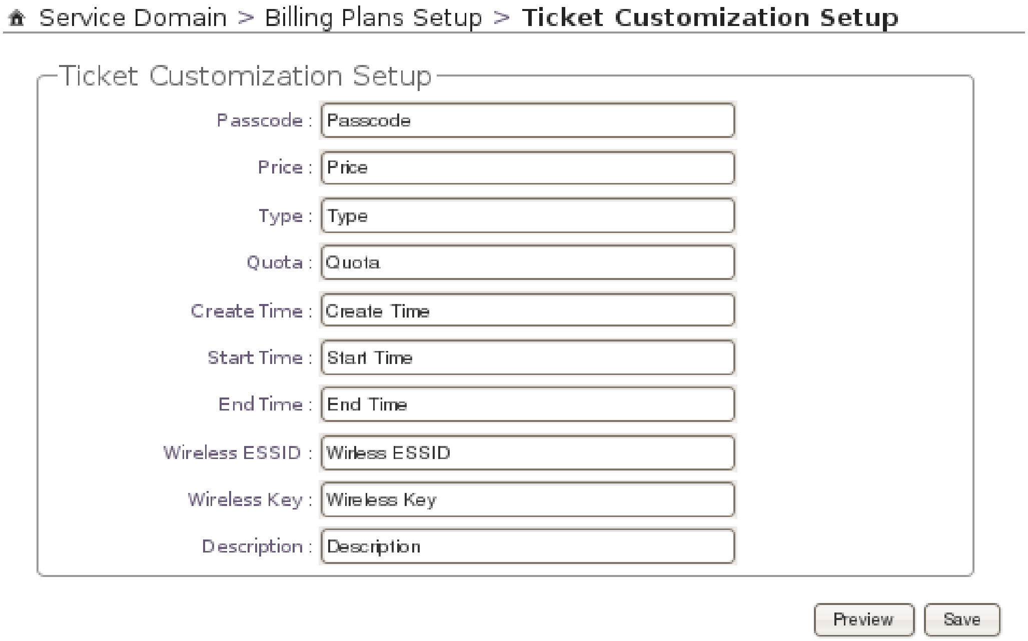
Search Time: 2010/05/09 00:00:00 - 2010/06/09 23:59:59

#	Name	On Demand	Payment Geteway	Thermal Printer	Amount Qty	Unit Price	Subtotal
0	Package 0	20	4	1	25	10.00	250.00 USD
1	Package 1	19		1	20	5.00	100.00 USD
2	Package 2	21	1	2	24	3.00	72.00 USD
3	Package 3					10.00	USD
4	Package 4					10.00	USD
5	Package 5					10.00	USD
6	Package 6					10.00	USD
7	Package 7					10.00	USD
8	Package 8					10.00	USD
9	Package 9					10.00	USD
	Total	60	5	4	69		422.00 USD

- **On-Demand Type :**There are **four** type can be selected : **ALL**, **On-Demand**, **Payment Gateway** and **Thermal Printer**.
- **Search :** Select a time period to get a period report. The report tells the total income and individual accounting of each plan for all plans available for that period of time.
- **Print :** Administrator can print report on the screen.

4.5.2.3.6 Ticket Customization

Click on **Service Domain -> Authentication -> On-Demand** to enter the **Ticket Customization** page. Administrator can edit text on printed ticket on this page. **4-32 characters** supported on these text setting field.

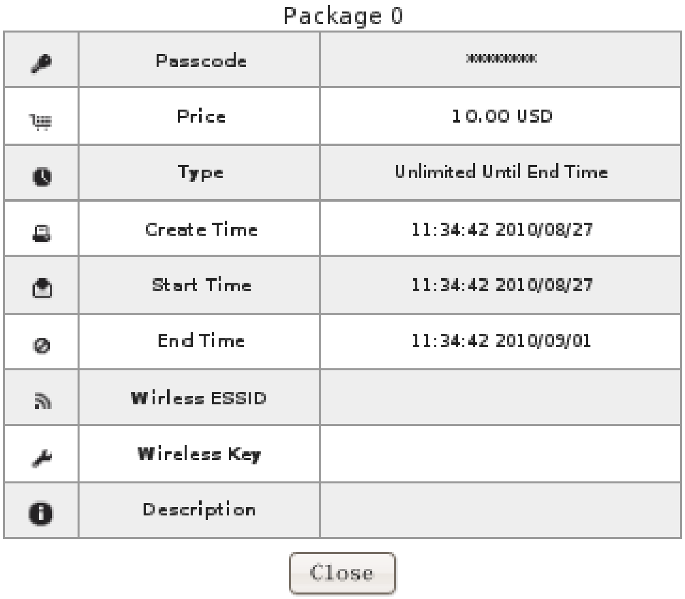


Service Domain > Billing Plans Setup > **Ticket Customization Setup**

Ticket Customization Setup

Passcode :	Passcode
Price :	Price
Type :	Type
Quota :	Quota
Create Time :	Create Time
Start Time :	Start Time
End Time :	End Time
Wireless ESSID :	Wirless ESSID
Wireless Key :	Wireless Key
Description :	Description

Change these settings as described here and click ***Save*** button to save your changes. Click ***Preview*** button to preview ticket in the **Billing Plan 0**. Below depicts an example for previewing ticket. Click ***Close*** button to close window.



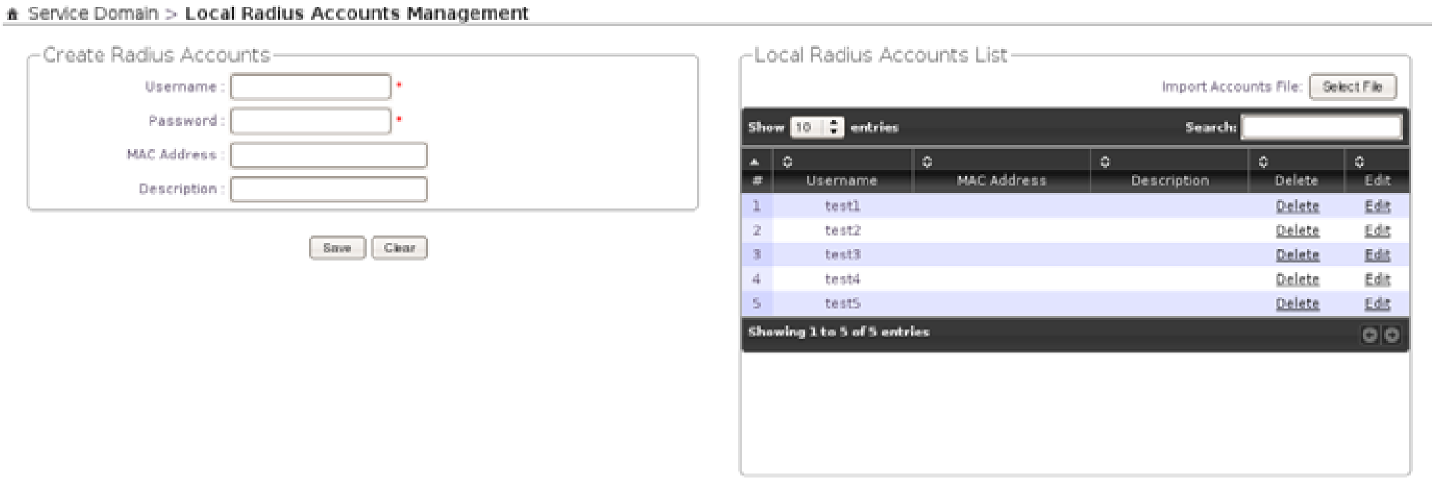
Package 0

Passcode	********
Price	10.00 USD
Type	Unlimited Until End Time
Create Time	11:34:42 2010/08/27
Start Time	11:34:42 2010/08/27
End Time	11:34:42 2010/09/01
Wirless ESSID	
Wireless Key	
Description	

Click ***Reboot*** button to activate your changes

4.5.2.4 Configure Local Radius Accounts

WAS-105R provide Local Radius server authentication. Please click on **Service Domain** -> **Authentication** -> **Remote Radius Server**, the page of **Remote Radius Server Setup** will appear. Administrator can add accounts by manual or import accounts file.



Service Domain > Local Radius Accounts Management

Create Radius Accounts

Username : *
Password : *
MAC Address :
Description :

Save Clear

Local Radius Accounts List

Import Accounts File: Select File

Show 10 entries Search:

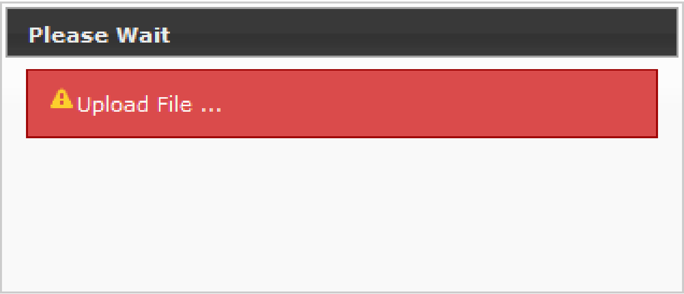
#	Username	MAC Address	Description	Delete	Edit
1	test1			Delete	Edit
2	test2			Delete	Edit
3	test3			Delete	Edit
4	test4			Delete	Edit
5	test5			Delete	Edit

Showing 1 to 5 of 5 entries

- **Username :** Enter the Username for local radius authentication. **4-16** alphanumeric and specify characters supported.
- **Password :** Enter the Password for local radius authentication. **4-16** alphanumeric and specify characters supported.
- **MAC Address :** Enter the MAC address for local radius authentication.(**optional**)
- **Description :** Enter appropriate text to denote this account.

Click ***Save*** button to add new account, all of accounts can be **edited**(**Username can not edit**) and **deleted**.

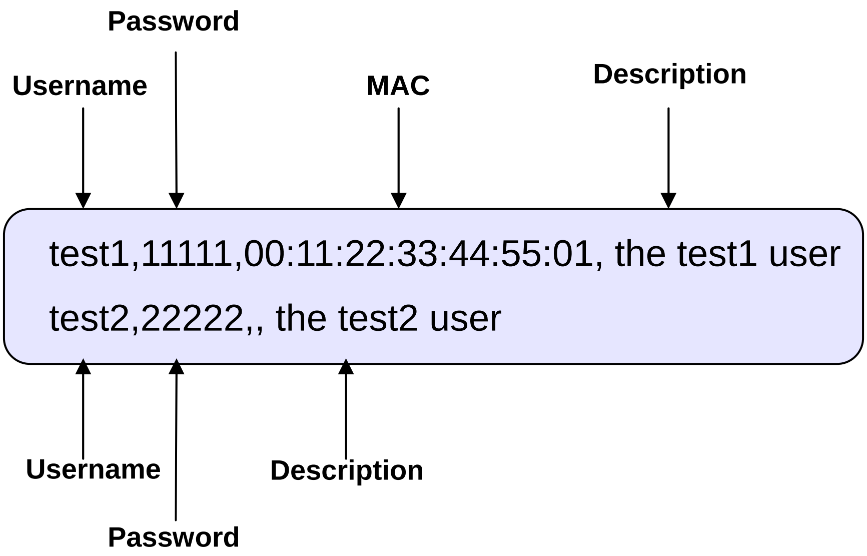
- **Import Accounts File :** Click this to enter the import accounts. Click Select File button to select the text file for the accounts upload. The the "**Upload File ...**" message will appear.



Please Wait

⚠Upload File ...

The upload file should be a text file and the format of each line is “**Username, Password, MAC, Description**” without the **quotes**. There must be no **spaces** between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding accounts by uploading a file, the existing accounts in the embedded database, uploading precess will fail. Below depicts an example for text file.



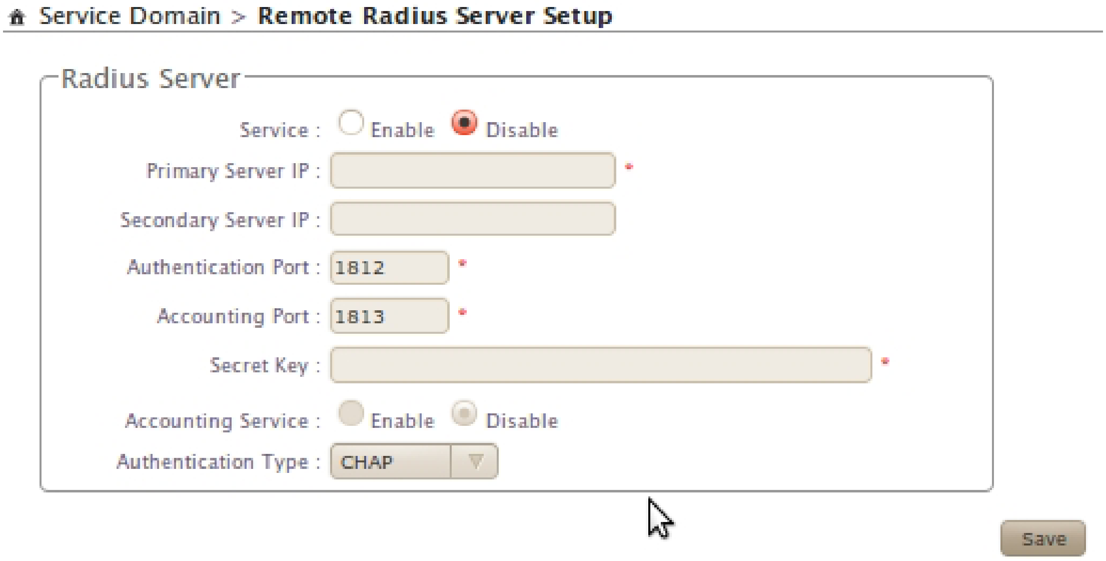
```
test1,11111,00:11:22:33:44:55:01, the test1 user
test2,22222,, the test2 user
```

- **Search :** Enter a keyword to be searched in the text field and all matching the keyword will be listed.

These settings will become effective immediately after clicking the **Save** button.

4.5.2.5 Configure Remote Radius Server

WAS-105R provide remote Radius server authentication. Please click on **Service Domain** -> **Authentication** -> **Remote Radius Server**, the page of **Remote Radius Server Setup** will appear



Service : ○ Enable ● Disable

Primary Server IP : *

Secondary Server IP :

Authentication Port : 1812 *

Accounting Port : 1813 *

Secret Key : *

Accounting Service : ○ Enable ○ Disable

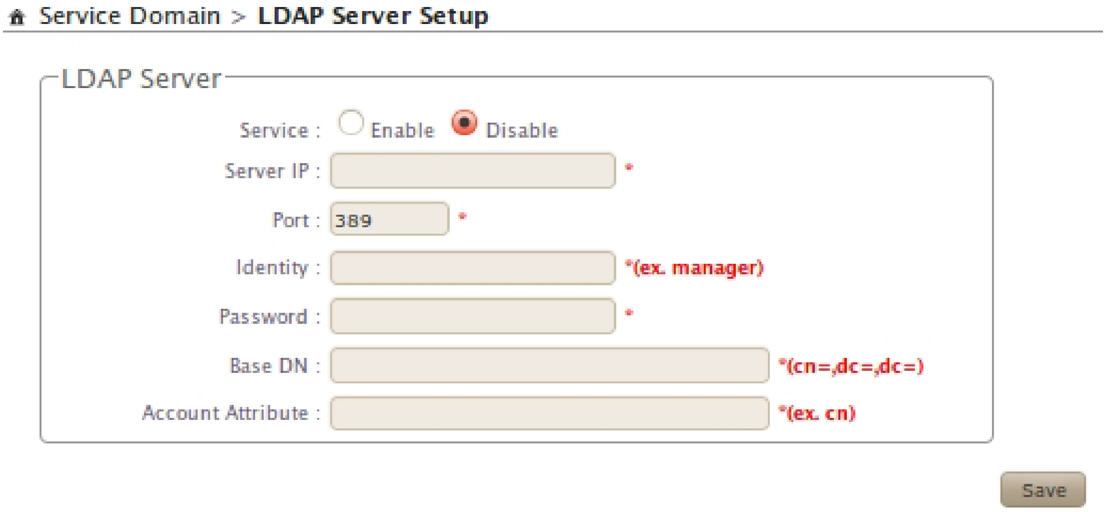
Authentication Type : CHAP

- **Service :** By default, it's “**Disable**”. To “**Enable**” to activate this function.
- **Primary/Secondary Server IP :** Enter the IP address of the Authentication RADIUS server.
- **Authentication Port :** The port number used by Authentication RADIUS server. Use the default **1812** or enter port number specified.
- **Accounting Port :** The port number used by Accounting RADIUS server. Use the default **1813** or enter port number specified.
- **Secret Key:** The secret key for system to communicate with RADIUS server. Support 1 to 64 characters.
- **Accounting Service :** Select this to enable or disable the “Accounting Service” for accounting capabilities.
- **Authentication Type :** Select the desired authentication type from the drop-down list; the options are **CHAP** and **PAP**.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.5.2.6 Configure LDAP Server

WAS-105R provide remote LDAP server authentication. Please click on **Service Domain** -> **Authentication** -> **LDAP,**, the page of **LDAP Server Setup** will appear



Service Domain > **LDAP Server Setup**

LDAP Server

Service : ○ Enable ● Disable

Server IP : *

Port : 389 *

Identity : *(ex. manager)

Password : *

Base DN : *(cn=,dc=,dc=)

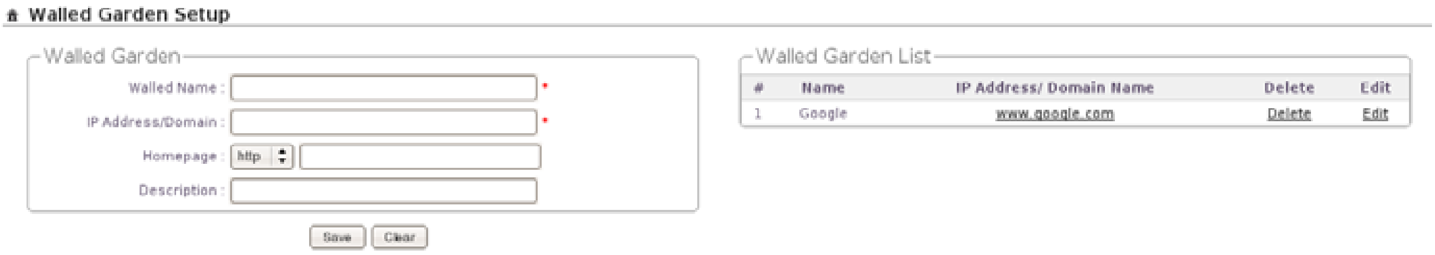
Account Attribute : *(ex. cn)

- **Service :** By default, it's “**Disable**”. To “**Enable**” to activate this function.
- **Server IP :** Enter the IP address of the LDAP server.
- **Port :** Enter the Port of the LDAP server, default port is **389**.
- **Identity :** Enter the Administrator's Identity for access to the directory service.
- **Password :** Enter the Administrator's Password for access to the directory service.
- **Base DN :** Enter the **Base Distinguished Name** (DN) in the **Base DN** field. The base DN indicates the starting point for searches in this LDAP server.
- **Account Attribute :** Enter the account attribute of the LDAP server.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.5.3 Configure Walled Garden

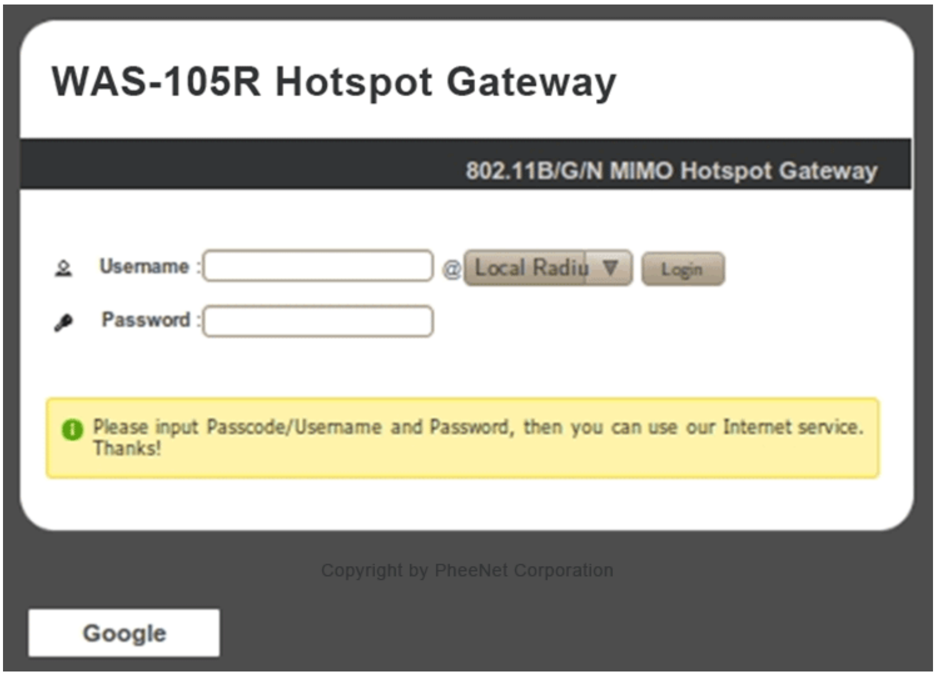
This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. Up to **20** address or domain names of the websites can be defined in this list. User without the network access right can still have a chance to experience the actual network service free of charge. Please click on **Service Domain** -> **Walled Garden**, the page of **Walled Garden Setup** will appear. Enter the Walled Name, IP Address/Domain, Homepage and Description, then click “**Save**” button to add website on the list.



#	Name	IP Address/ Domain Name	Delete	Edit
1	Google	www.google.com	Delete	Edit

Click ***Reboot*** button to activate your changes.

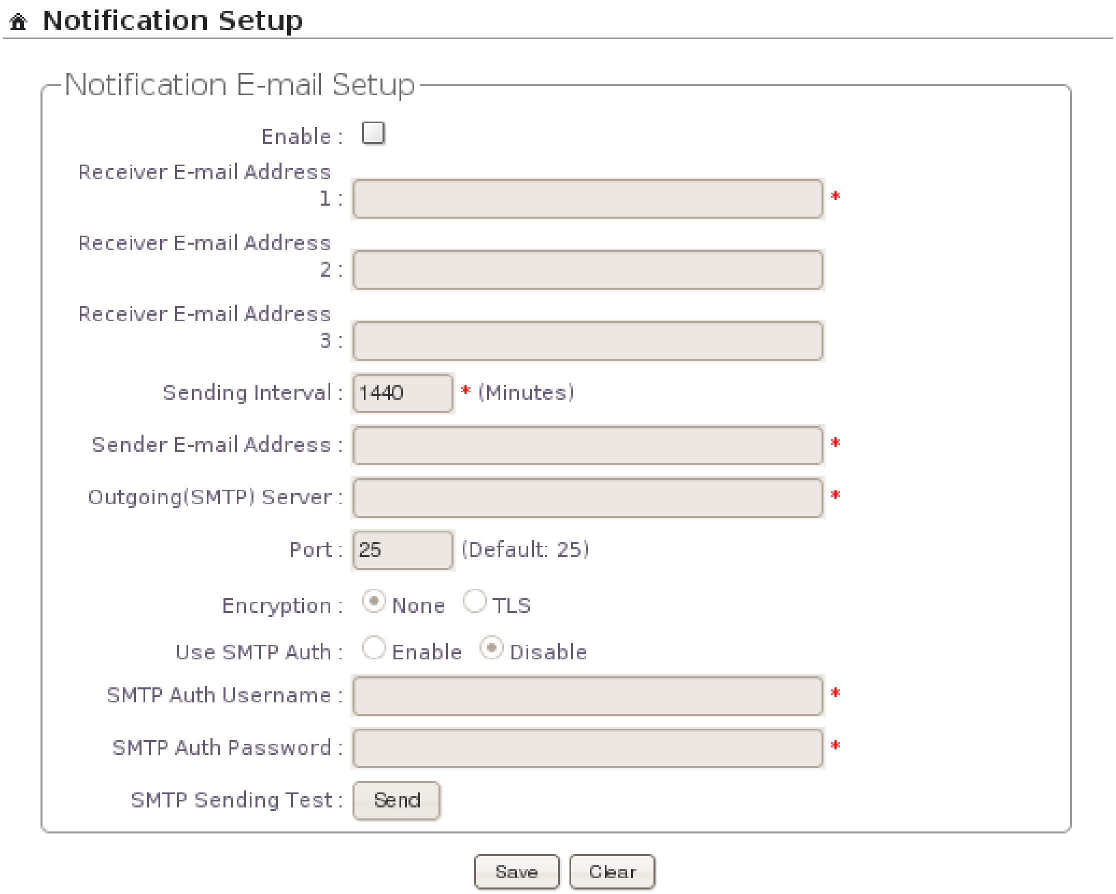
After add website on the list, the Walled Name will appear on Login page. Below depicts an example for Walled Garden.



Please input Passcode/Username and Password, then you can use our Internet service. Thanks!

4.5.4 Configure Notification

WAS-105R can automatically send the notification of Users Log to 3 particular E-mail addresses. A trial email is provided by the system for validation. Please click on **Service Domain** -> **Notification**, the page of **Notification E-mail Setup** will appear



Notification Setup

Notification E-mail Setup

Enable : □

Receiver E-mail Address 1 : *

Receiver E-mail Address 2 :

Receiver E-mail Address 3 :

Sending Interval : 1440 * (Minutes)

Sender E-mail Address : *

Outgoing(SMTP) Server : *

Port : 25 (Default: 25)

Encryption : ● None ○ TLS

Use SMTP Auth : ○ Enable ● Disable

SMTP Auth Username : *

SMTP Auth Password : *

SMTP Sending Test : Send

Save Clear

- **SMTP Server Setup :**
  - ➔ **Enabled :** Click Enabled to activated SMTP Server
  - ➔ **Sender From :** The E-mail address of the administrator in charge of monitoring. This will show up as the sender's E-mail.
  - ➔ **SMTP Server :** The IP address / Domain of the sender's SMTP server.
  - ➔ **Port :** The port of the sender's SMTP server. (Default is 25)
  - ➔ **Encryption :** Some SMTP server need encryption linking for sending E-mail. The system provides encryption for sender's SMTP server
  - ➔ **SMTP Auth :** Some SMTP server need authentication username and password for sending E-mail. The system provides authentication for sender's SMTP server
  - ➔ **Username :** The sender's authentication username for STMP server

➔ **Password:** The sender's authentication password for STMP server

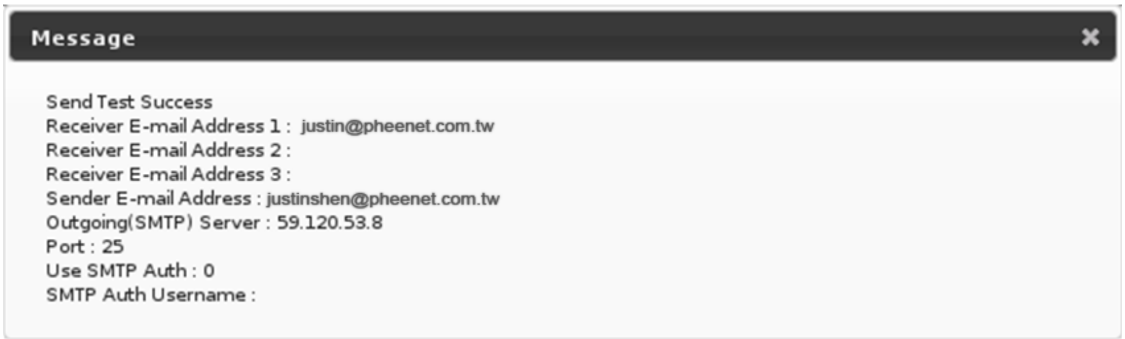
- **Notification E-mail Setup :**

➔ **Receiver E-mail Address (es) :** Up to 3 E-mail address can be set up to receive the notification. These are the receiver's E-mail address.

➔ **Sending Interval :** The time interval (in minute) to send the E-mail report. (Default is **1440** minutes; the range is between **10** to **4200** minutes)

➔ **SMTP Sending Test :** Click ***Send*** button to verify Notification E-mail settings. Below depicts an example for success sending test.

- **Syslog Setup :** There are 2 types of Syslog supported : **Syslog Log** and **Session Log**. Enter the specify IP address and Port number to sent report.



Send Test Success
Receiver E-mail Address 1 : justin@pheenet.com.tw
Receiver E-mail Address 2 :
Receiver E-mail Address 3 :
Sender E-mail Address : justinshen@pheenet.com.tw
Outgoing(SMTP) Server : 59.120.53.8
Port : 25
Use SMTP Auth : 0
SMTP Auth Username :

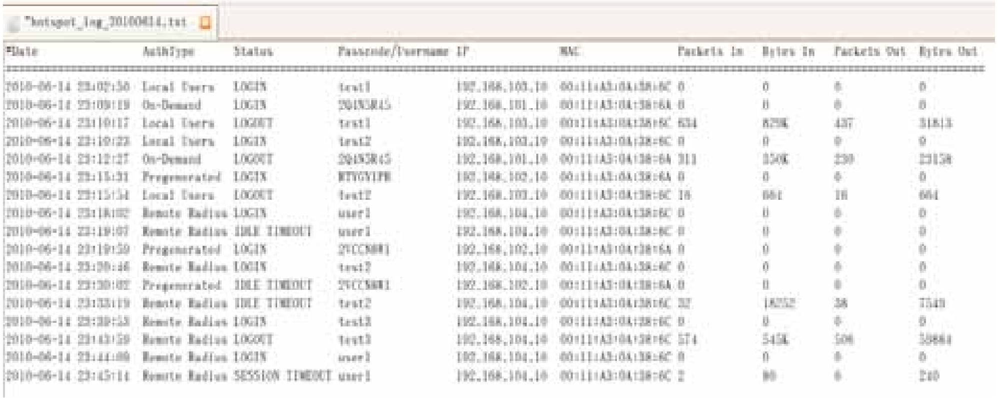
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

The history is saved in the DRAM, if you restart system, the history traffic will empty.

If the history E-mail has been entered above Notification settings, after **Sending Interval**, the system will send **History** E-mail to receiver's E-mail address automatically.

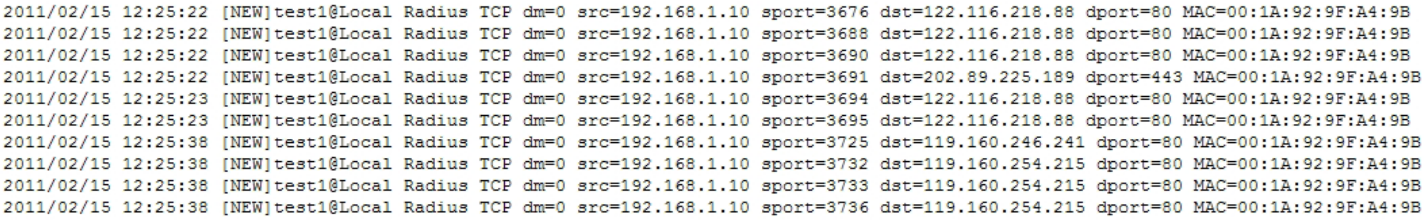
- **Traffic Log :**

As shown in the following figure, each line is traffic history record consisting of 10 fields : **Date**, **Auth Type**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out**.



```
#Date               AuthType      Status          Passcode/Username IP              MAC               Packets In  Bytes In  Packets Out  Bytes Out
=====================================================================================================================================================
2010-06-14 23:02:36 Local Users   LOGIN           test1            192.168.103.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:09:19 On-Demand     LOGIN           2Q4N3R45         192.168.101.10  00:11:A3:0A:38:6A 0           0         0            0
2010-06-14 23:10:17 Local Users   LOGOUT          test1            192.168.103.10  00:11:A3:0A:38:6C 634         829K      437          31813
2010-06-14 23:10:23 Local Users   LOGIN           test2            192.168.103.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:12:27 On-Demand     LOGOUT          2Q4N3R45         192.168.101.10  00:11:A3:0A:38:6A 311         350K      239          23158
2010-06-14 23:15:31 Pregenerated  LOGIN           RTYGYIPB         192.168.102.10  00:11:A3:0A:38:6A 0           0         0            0
2010-06-14 23:15:34 Local Users   LOGOUT          test2            192.168.103.10  00:11:A3:0A:38:6C 16          661       16           664
2010-06-14 23:18:02 Remote Radius LOGIN           user1            192.168.104.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:19:07 Remote Radius IDLE TIMEOUT    user1            192.168.104.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:19:59 Pregenerated  LOGIN           2YCCN8W1         192.168.102.10  00:11:A3:0A:38:6A 0           0         0            0
2010-06-14 23:20:46 Remote Radius LOGIN           test2            192.168.104.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:30:02 Pregenerated  IDLE TIMEOUT    2YCCN8W1         192.168.102.10  00:11:A3:0A:38:6A 0           0         0            0
2010-06-14 23:33:19 Remote Radius IDLE TIMEOUT    test2            192.168.104.10  00:11:A3:0A:38:6C 32          18252     38           7349
2010-06-14 23:39:53 Remote Radius LOGIN           test3            192.168.104.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:43:59 Remote Radius LOGOUT          test3            192.168.104.10  00:11:A3:0A:38:6C 574         545K      506          38884
2010-06-14 23:44:09 Remote Radius LOGIN           user1            192.168.104.10  00:11:A3:0A:38:6C 0           0         0            0
2010-06-14 23:45:14 Remote Radius SESSION TIMEOUT user1            192.168.104.10  00:11:A3:0A:38:6C 2           88        6            240
```

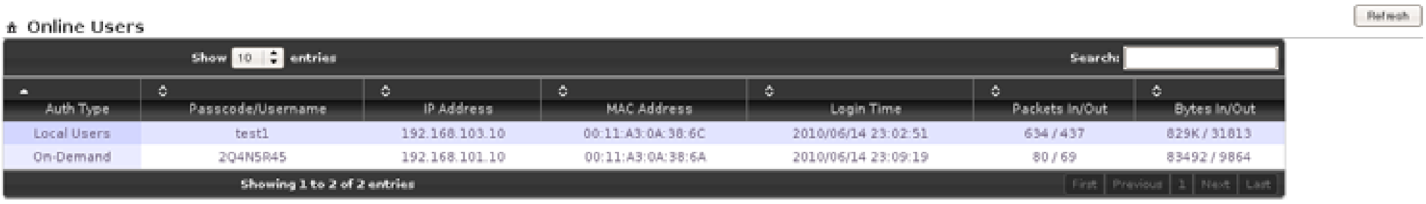
- **Date :** Display the date of user log.
- **Auth Type :** There will shows **5** types of authentication : **Pregenerated**, **On-Demand**, **Local Users**(Local Radius Users), **Remote Radius**, **LDAP** and **Guest**.
- **Status :** There will show **10** types of status as below :
  - ✓ **LOGIN :** Indicate that the user login system.
  - ✓ **LOGOUT :** Indicate that the user logout system.
  - ✓ **IDLE TIMEOUT :** Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
  - ✓ **USE UP :** Indicate that the user's service time is done.
  - ✓ **SESSION TIMEOUT :** Indicate that the user session timeout for **Remote Radius**.
  - ✓ **VOLUME USE UP :** Indicate that the user's bandwidth is done.
  - ✓ **KICK :** Indicate that the system kick out the user.
  - 疝 **TIME OUT OF RANGE :** Indicate that the service time of Service Domain is not on schedule.
- **Passcode/Username :** Indicate the user's passcode or username.
- **IP :** Indicate the user's IP address
- **MAC :** Indicate the user's MAC address
- **Packets In :** Indicate the current user's packets in.
- **Bytes In :** Indicate the current user's bytes in.
- **Packet Out :** Indicate the current user's packets out.
- **Bytes Out :** Indicate the current user's bytes out.
- **Session Log :** The system can recored connection details of each user accessing the Internet and sent out to a specified Syslog Server or E-Mail based on defined interval time. As shown in the following figure, each line is traffic history record consisting of 10 fields, **Date**, **Time**, **Session Type**, **Username**, **Service Domain**, **Source IP**, **Source Port**, **Destination IP**, **Destination Port**, **MAC.**



```
2011/02/15 12:25:22 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3676 dst=122.116.218.88 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:22 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3688 dst=122.116.218.88 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:22 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3690 dst=122.116.218.88 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:22 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3691 dst=202.89.225.189 dport=443 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:23 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3694 dst=122.116.218.88 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:23 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3695 dst=122.116.218.88 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:38 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3725 dst=119.160.246.241 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:38 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3732 dst=119.160.254.215 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:38 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3733 dst=119.160.254.215 dport=80 MAC=00:1A:92:9F:A4:9B
2011/02/15 12:25:38 [NEW]test1@Local Radius TCP dm=0 src=192.168.1.10 sport=3736 dst=119.160.254.215 dport=80 MAC=00:1A:92:9F:A4:9B
```

4.5.5 Monitor Online Users

The administrator can view status of all online users on each Service Domain. Please click on **Service Domain** -> **Online Users**, the page of **Online Users** will appear. Below depicts an example for Online User Information. There provided information of **Passocde**, **IP Address**, **MAC Address**, **Login Time**, **Packets In**/**Out** and **Bytes In**/**Out**.



Auth Type	Passcode/Username	IP Address	MAC Address	Login Time	Packets In/Out	Bytes In/Out
Local Users	test1	192.168.103.10	00:11:A3:0A:38:6C	2010/06/14 23:02:51	634 / 437	829K / 31813
On-Demand	2Q4N5R45	192.168.101.10	00:11:A3:0A:38:6A	2010/06/14 23:09:19	80 / 69	83492 / 9864

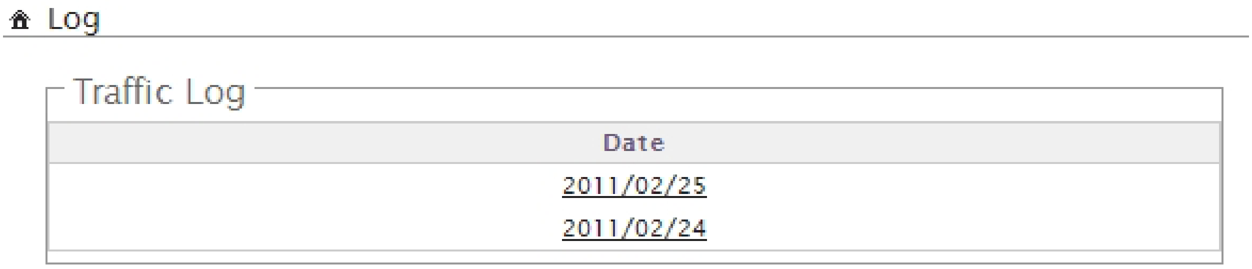
Showing 1 to 2 of 2 entries

- **Auth Type :** Indicate the current user's authentication type.
- **Passcode/Username :** Indicate the current user's passcode or username.
- **IP Address :** Indicate the current user's IP address.
- **MAC Address :** Indicate the current user's MAC address.
- **Login Time :** Indicate the login time for this user.
- **Packets In/Out :** Indicate the current user's packets in and out.
- **Bytes In/Out :** Indicate the current user's bytes in and out.
- **Logout :** Click Logout to logout online users.

Click “**Refresh**” button to renew this page.

4.5.6 Log Information

The WAS-105R can record authentication traffic history and the system will automatically send out the history information via notification service(See **Notification** page). The history of each day will be saved separately in the DRAM for 3 days and sorted by time, the traffic provides all login and logout activity of specific date. Other informations include Passocde/Username, IP Address, MAC Address, Packets In/Out and Bytes In/Out. Please click on **Service Domain** -> **Log Info**, the page of **Log Info** will appear.



Log

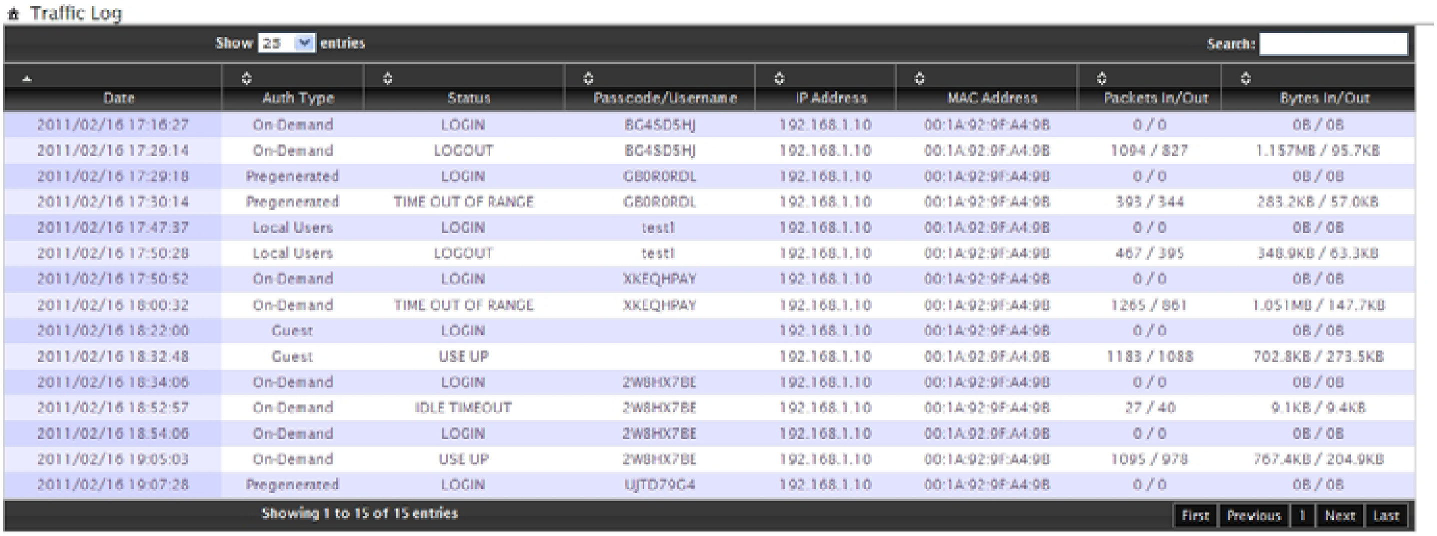
Traffic Log

Date
2011/02/25
2011/02/24

The all history log are saved in the DRAM, if you need restart system and also keep the history, please manually copy and save the informations before restarting.

- **Traffic Log :**

As shown in the following figure, each line is traffic history record consisting of 10 fields : **Date**, **Auth Type**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out**.



Traffic Log

Show 25 entries Search:

Date	Auth Type	Status	Passcode/Username	IP Address	MAC Address	Packets In/Out	Bytes In/Out
2011/02/16 17:16:27	On-Demand	LOGIN	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:29:14	On-Demand	LOGOUT	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	1094 / 827	1.157MB / 95.7KB
2011/02/16 17:29:18	Pregenerated	LOGIN	GB0R0RDL	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:30:14	Pregenerated	TIME OUT OF RANGE	GB0R0RDL	192.168.1.10	00:1A:92:9F:A4:9B	393 / 344	283.2KB / 57.0KB
2011/02/16 17:47:37	Local Users	LOGIN	test1	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:50:28	Local Users	LOGOUT	test1	192.168.1.10	00:1A:92:9F:A4:9B	467 / 395	348.9KB / 63.3KB
2011/02/16 17:50:52	On-Demand	LOGIN	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:00:32	On-Demand	TIME OUT OF RANGE	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	1265 / 861	1.051MB / 147.7KB
2011/02/16 18:22:00	Guest	LOGIN		192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:32:48	Guest	USE UP		192.168.1.10	00:1A:92:9F:A4:9B	1183 / 1088	702.8KB / 273.5KB
2011/02/16 18:34:06	On-Demand	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:52:57	On-Demand	IDLE TIMEOUT	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	27 / 40	9.1KB / 9.4KB
2011/02/16 18:54:06	On-Demand	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 19:05:03	On-Demand	USE UP	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	1095 / 978	767.4KB / 204.9KB
2011/02/16 19:07:28	Pregenerated	LOGIN	UJTD79G4	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B

Showing 1 to 15 of 15 entries

- ➔ **Date :** Indicate that current event's date and time
- ➔ **Auth Type :** There will shows **6** types of authentication : **Pregenerated**, **On-Demand**, **Local Users**(Local Radius Users), **Remote Radius**, **LDAP** and **Guest**.**Status :** There will show **10** types of status as below :
  - ✓ **LOGIN :** Indicate that the user login system.
  - ✓ **LOGOUT :** Indicate that the user logout system.

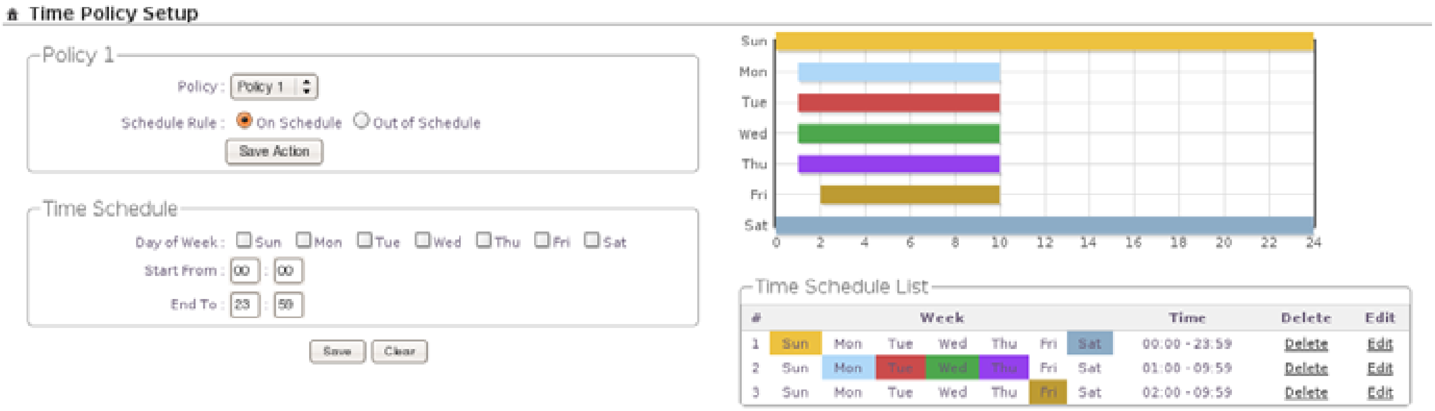
- ✓ **IDLE TIMEOUT :** Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
- ✓ **USE UP :** Indicate that the user's service time is done.
- ✓ **SESSION TIMEOUT :** Indicate that the user session timeout for **Remote Radius**.
- ✓ **VOLUME USE UP :** Indicate that the user's bandwidth is done.
- ✓ **KICK :** Indicate that the system kick out the user.
- ✓ **TIME OUT OF RANGE :** Indicate that the service time of Service Domain is not on schedule.

- ➔ **Passcode/Username :** Indicate that the user's passcode or username.
- ➔ **IP :** Indicate that the user's IP address
- ➔ **MAC :** Indicate that the user's MAC address
- ➔ **Packets In :** Indicate that the current user's packets in.
- ➔ **Bytes In :** Indicate that the current user's bytes in.
- ➔ **Packet Out :** Indicate that the current user's packets out.
- ➔ **Bytes Out : Indicate that the current user's bytes out.**

4.6 Restrain the Users and Sharing Your Internal Service

4.6.1 Configure Time Policy

Administrator can define time policy for IP Filtering, MAC Filtering and Virtual Server. There are 10 policy can be defined. Please click on **Advance** -> **Time Policy** to enter **Time Policy Setup** page.



Time Policy Setup

Policy 1

Policy : Policy 1

Schedule Rule : ● On Schedule ○ Out of Schedule

Save Action

Time Schedule

Day of Week : □Sun □Mon □Tue □Wed □Thu □Fri □Sat

Start From : 00 : 00

End To : 23 : 59

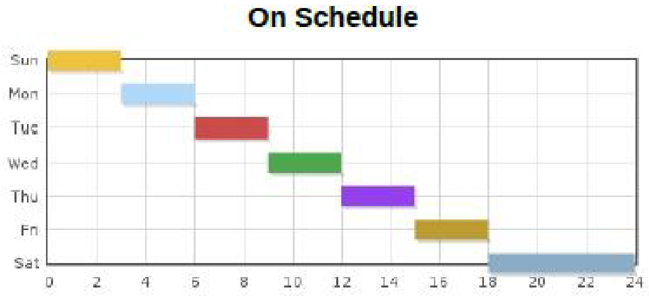
Save Clear

Time Schedule List

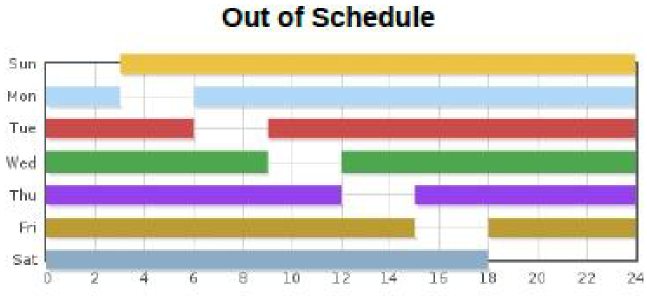
#	Week							Time	Delete	Edit
1	Sun	Mon	Tue	Wed	Thu	Fri	Sat	00:00 - 23:59	Delete	Edit
2	Sun	Mon	Tue	Wed	Thu	Fri	Sat	01:00 - 09:59	Delete	Edit
3	Sun	Mon	Tue	Wed	Thu	Fri	Sat	02:00 - 09:59	Delete	Edit

- ■ **Policy :** There are **10** Policy can be selected.
- ■ **Schedule Rule :** Select desired schedule for this policy.
- ■ **Time Schedule :** Select desired day of week and time period for this policy.

Below depicts an example for “On Schedule” and “Out of Schedule”



On Schedule

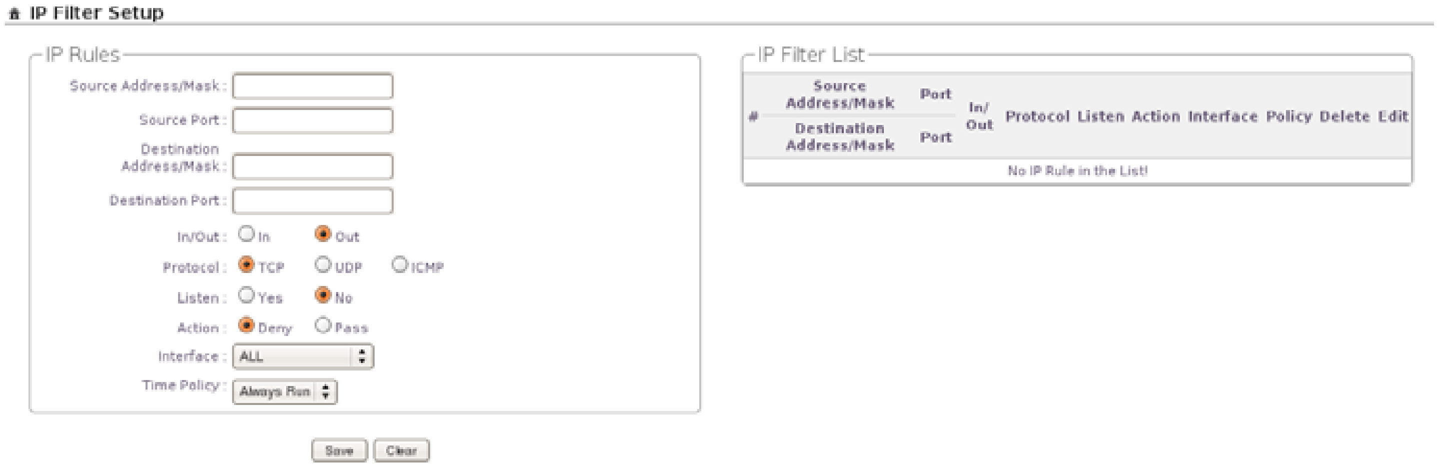


Out of Schedule

Click “**Save**” button to add schedule to policy. There are **10** schedule maximum allowed in the each time policy. All schedule can be **edited** or **removed** in the each time policy. Click ***Reboot*** button to activate your changes.

4.6.2 IP Filter

The administrator can setting IP Filter via this page, Please click on **Advance -> IP Filter** and follow the below setting.



IP Filter Setup

IP Rules

Source Address/Mask :
Source Port :
Destination Address/Mask :
Destination Port :
In/Out : ○ In ● Out
Protocol : ● TCP ○ UDP ○ ICMP
Listen : ○ Yes ● No
Action : ● Deny ○ Pass
Interface : ALL
Time Policy : Always Run

IP Filter List

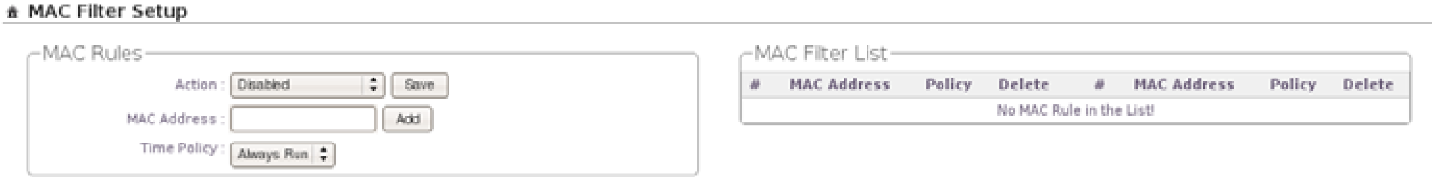
#	Source Address/Mask Destination Address/Mask	Port Port	In/Out	Protocol	Listen	Action	Interface	Policy	Delete	Edit
No IP Rule in the List!										

- **Source Address/Mask :** Enter the desired source IP address and netmask; the mask must be a plain number, i.e. 192.168.100.10/32
- **Source Port :** The source port(s) required for this rule. A single port may be given, or a range may be given as ***start:end*** , which will match all ports from *start* to *end*, inclusive.
- **Destination Address/Mask :** Enter the desired destination IP address and netmask; the mask must be a plain number, i.e. 192.168.1.10/32
- **Destination Port :** The destination port(s) required for this rule. A single port may be given, or a range may be given as ***start:end*** , which will match all ports from *start* to *end*, inclusive.
- **In/Out :** This option used for specialized packet alteration. The system support In (INPUT : for packets coming into the interface itself) or Out (FORWARD : for altering packets being routed through the interface)
- **Protocol :** This option allows you to select protocol type. The system support TCP, UDP or ICMP.
- **Listen :** Enable ***Yes*** to match TCP packets only with the SYN flag.
- **Active :** Enter ***Deny*** to DROP specialized packet; ***Pass*** to ACCET the specialized packet
- **Interface :** Select specified interface where filtering of the incoming /passing-through packets is processed
- **Time Policy :** Select specified time period for this rule.

Click "**Save**" button to add IP filter rule to List. There are **20** rules maximum allowed in this IP Filter List. All rules can be **edited** or **removed** on the List. Click ***Reboot*** button to activate your changes.

4.6.3 MAC Filter

The administrator can setting MAC Filter via this page, Please click on **Advance -> MAC Filter** and follow the below setting.



MAC Filter Setup

MAC Rules

Action : Disabled

MAC Address :

Time Policy : Always Run

MAC Filter List

#	MAC Address	Policy	Delete	#	MAC Address	Policy	Delete
No MAC Rule in the List!							

- **Action :** Select the desired access control rule; the options are "Only **Deny List MAC**", "**Only Allow List MAC**" or "**Disable**".

  define certain clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – **Access Control Type** is set to **Allow**.

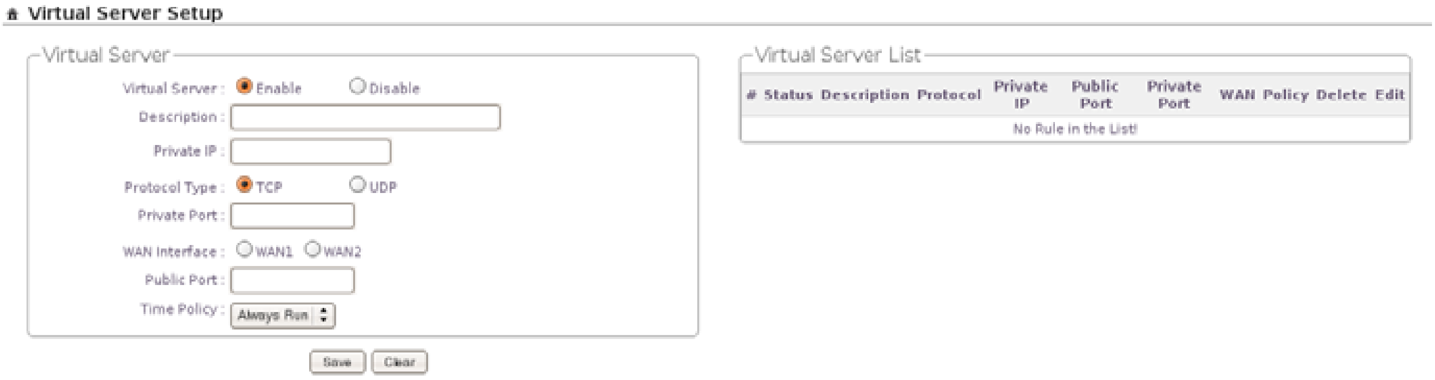
  define certain clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients – **Access Control Type** is set to **Reject**.

- **MAC Address :** Enter MAC address in this field. There are maximum **20** clients users allowed in this MAC address list.
- **Time Policy :** Select specified time period for this rule.

Click "**Save**" button to add MAC filter rule to List. There are maximum **20** rules allowed in this MAC Filter List. All rules can **removed** on the List. Click ***Reboot*** button to activate your changes.

4.6.4 Virtual Server (Port/ IP Forwarding)

A certain area in the network can be exposed to the Internet in a limited and controlled way for on-line game or video conferencing via this page. Please ensure the internal port to be used is not occupied by other applications. Please click on **Advance -> Virtual Server** and follow the below setting.



Virtual Server Setup

Virtual Server

Virtual Server : ● Enable ○ Disable

Description :

Private IP :

Protocol Type : ● TCP ○ UDP

Private Port :

WAN Interface : ○ WAN1 ○ WAN2

Public Port :

Time Policy : Always Run

Virtual Server List

#	Status	Description	Protocol	Private IP	Public Port	Private Port	WAN	Policy	Delete	Edit
No Rule in the List!										

- **Virtual Server :** Check ***Enable*** button to activate this rule, and ***Disable*** to deactivate.
- **Description :** Enter appropriate text to denote name of the Virtual server.
- **Private IP :** The corresponding IP address of the LAN port used for the respected service. Enter the LAN IP address of the assigned host.
- **Protocol Type :** The communication protocol of session. Select an appropriate protocol type, either TCP or UDP protocol.
- **Private Port :** The private port(s) required for this rule. A single port may be given, or a range may be given as ***start:end*** , which will match all ports from *start* to *end*, inclusive.
- **WAN Interface :** Select specified WAN interface where forwarding of incoming packets is processed
- **Public Port :** The public port(s) required for this rule. A single port may be given, or a range may be given as ***start:end*** , which will match all ports from *start* to *end*, inclusive.
- **Time Policy :** Select specified time period for this rule.

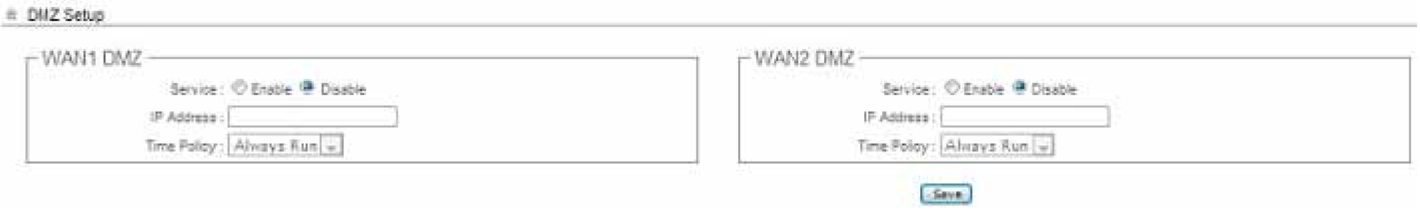
> The Private Port and Public Port can be different, but the port range need the same.
> example : Public Port is 10 to 20, the Private Port can be 30 to 40 or other 10 ports range.

Click "**Save**" button to add Virtual Server rule to List. There are maximum **20** rules allowed in this List. All rules can be **edited** or **removed** on the List. Click ***Reboot*** button to activate your changes.

4.6.5 DMZ

The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. *DMZ* is commonly used with the *NAT* functionality as an alternative for the *Virtual Server* (*IP* / *Port Forwarding)* while makes all the ports of the host network device be visible from the external network side.

Please click on **Advance -> DMZ** and follow the below setting.



DMZ Setup

WAN1 DMZ

Service : ○ Enable ● Disable

IP Address :

Time Policy : Always Run

WAN2 DMZ

Service : ○ Enable ● Disable

IP Address :

Time Policy : Always Run

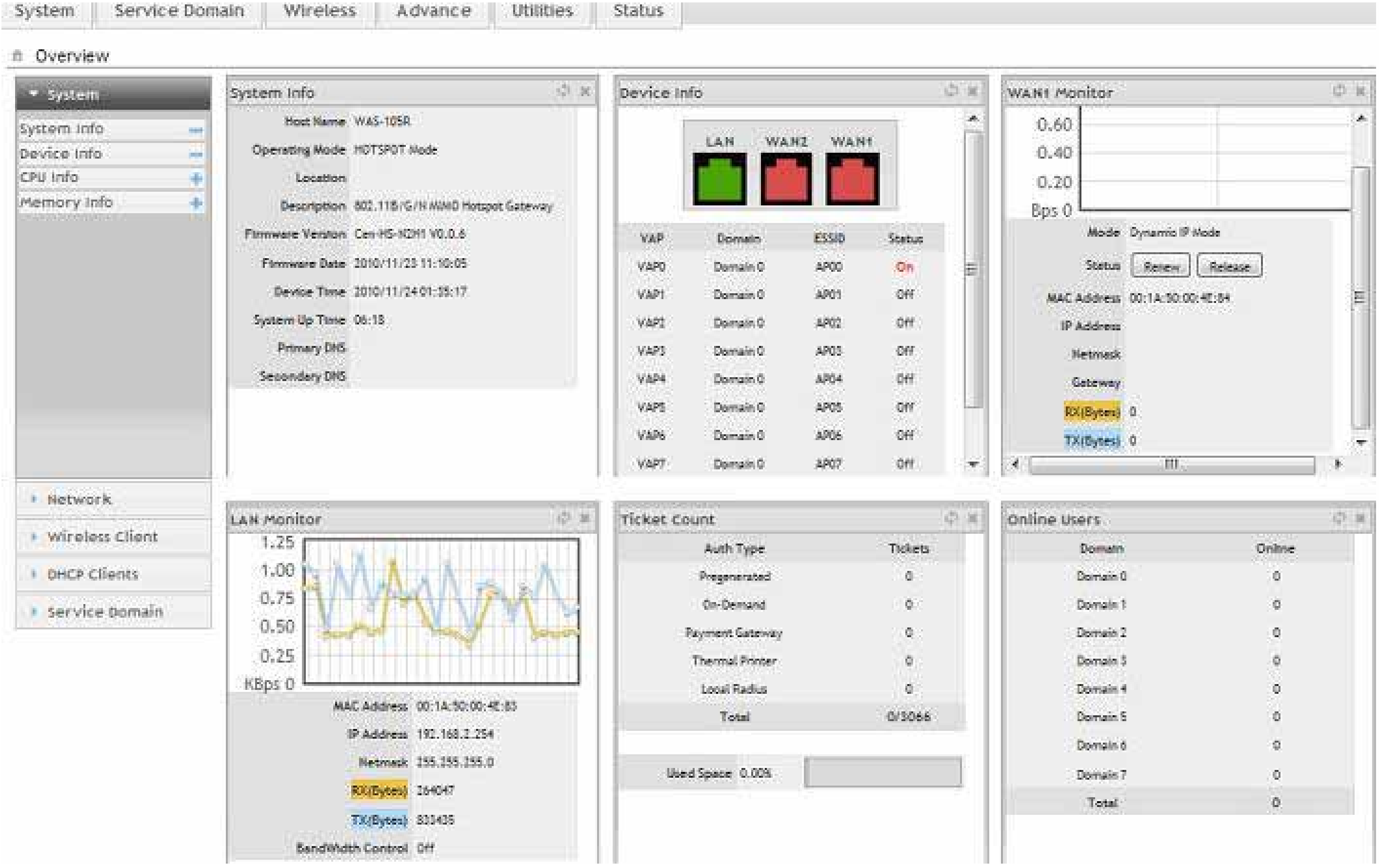
- **DMZ :** Check ***Enable*** button to activate this function, and ***Disable*** to deactivate.
- **IP Address :** Enter the IP address of the computer or server to be used as DMZ host; only one DMZ host can be activate at any time period.
- **Time Policy :** Select specified time period for this rule.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.7 Observer the Status

4.7.1 Overview

Detailed information on **System**, **Network**, **Wireless Client**, **DHCP Clients** and **Service Domain** can be reviewed via this page.



System Info

Host Name	WAS-105R
Operating Mode	HOTSPOT Mode
Location	
Description	802.11B/G/N MIMO Hotspot Gateway
Firmware Version	Cen-HS-N2H1 V0.0.6
Firmware Date	2010/11/23 11:10:05
Device Time	2010/11/24 01:35:17
System Up Time	06:18
Primary DNS	
Secondary DNS	

Device Info

VAP	Domain	ESSID	Status
VAP0	Domain 0	AP00	On
VAP1	Domain 0	AP01	Off
VAP2	Domain 0	AP02	Off
VAP3	Domain 0	AP03	Off
VAP4	Domain 0	AP04	Off
VAP5	Domain 0	AP05	Off
VAP6	Domain 0	AP06	Off
VAP7	Domain 0	AP07	Off

WAN1 Monitor

Mode	Dynamic IP Mode
Status	Renew Release
MAC Address	00:1A:50:00:4E:84
IP Address	
Netmask	
Gateway	
RX(Bytes)	0
TX(Bytes)	0

LAN Monitor

MAC Address	00:1A:50:00:4E:83
IP Address	192.168.2.254
Netmask	255.255.255.0
RX(Bytes)	264047
TX(Bytes)	833435
BandWidth Control	Off

Ticket Count

Auth Type	Tickets
Pregenerated	0
On-Demand	0
Payment Gateway	0
Thermal Printer	0
Local Radius	0
Total	0/5066

Used Space 0.00%

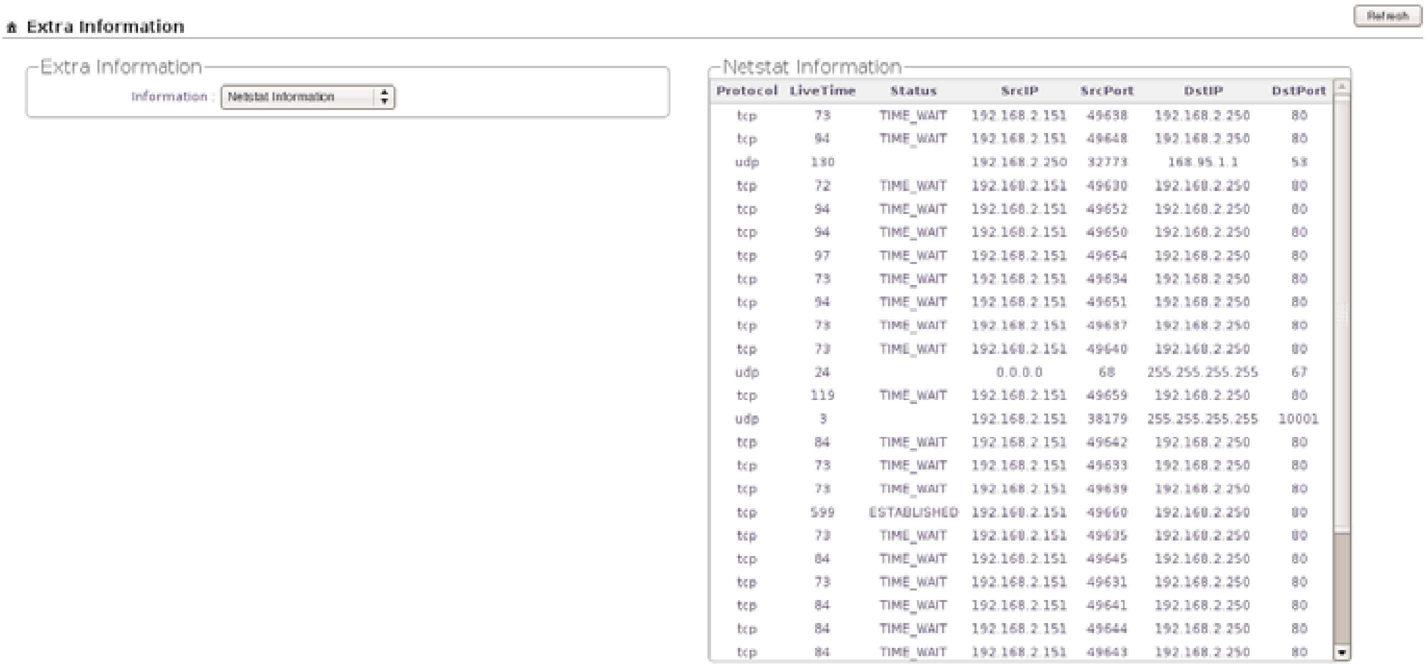
Online Users

Domain	Online
Domain 0	0
Domain 1	0
Domain 2	0
Domain 3	0
Domain 4	0
Domain 5	0
Domain 6	0
Domain 7	0
Total	0

- **System Information :** Display the information of the system.
- **Networking Information :** Display the information of the network.
- **Wireless Client Information** : Display the information of the wireless clients.
- **DHCP Clients Information :** Display the information of the DHCP clients.
- **Service Domain Information :** Display the information of the Service Domain.

4.7.2 Extra Info

Administrator could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “**Refresh**” button is used to retrieve latest table information.

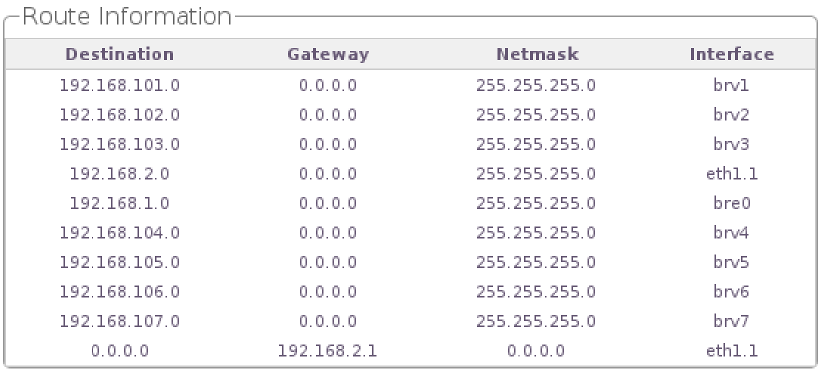


Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	73	TIME_WAIT	192.168.2.151	49638	192.168.2.250	80
tcp	94	TIME_WAIT	192.168.2.151	49648	192.168.2.250	80
udp	130		192.168.2.250	32773	168.95.1.1	53
tcp	72	TIME_WAIT	192.168.2.151	49630	192.168.2.250	80
tcp	94	TIME_WAIT	192.168.2.151	49652	192.168.2.250	80
tcp	94	TIME_WAIT	192.168.2.151	49650	192.168.2.250	80
tcp	97	TIME_WAIT	192.168.2.151	49654	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49634	192.168.2.250	80
tcp	94	TIME_WAIT	192.168.2.151	49651	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49637	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49640	192.168.2.250	80
udp	24		0.0.0.0	68	255.255.255.255	67
tcp	119	TIME_WAIT	192.168.2.151	49659	192.168.2.250	80
udp	3		192.168.2.151	38179	255.255.255.255	10001
tcp	84	TIME_WAIT	192.168.2.151	49642	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49633	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49639	192.168.2.250	80
tcp	599	ESTABLISHED	192.168.2.151	49660	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49635	192.168.2.250	80
tcp	84	TIME_WAIT	192.168.2.151	49645	192.168.2.250	80
tcp	73	TIME_WAIT	192.168.2.151	49631	192.168.2.250	80
tcp	84	TIME_WAIT	192.168.2.151	49641	192.168.2.250	80
tcp	84	TIME_WAIT	192.168.2.151	49644	192.168.2.250	80
tcp	84	TIME_WAIT	192.168.2.151	49643	192.168.2.250	80

- **Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the *connection track list* should show-up. NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status*, *Source/Destination IP address* and *Port.*

- **Route Information :** Select “**Route Information**” on the drop-down list to display route table.

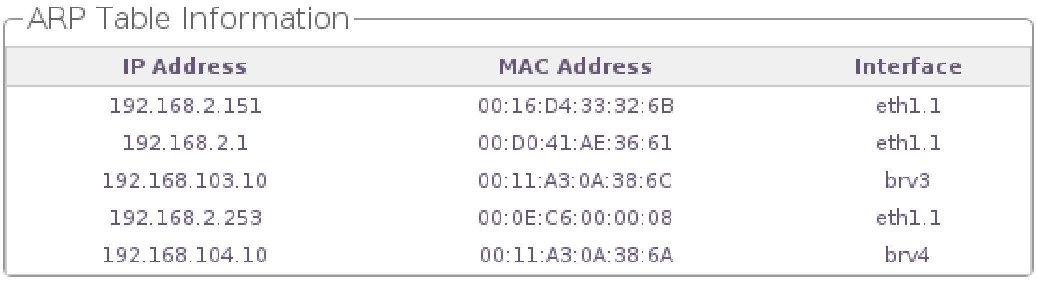
  WAS-105R could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.



Destination	Gateway	Netmask	Interface
192.168.101.0	0.0.0.0	255.255.255.0	brv1
192.168.102.0	0.0.0.0	255.255.255.0	brv2
192.168.103.0	0.0.0.0	255.255.255.0	brv3
192.168.2.0	0.0.0.0	255.255.255.0	eth1.1
192.168.1.0	0.0.0.0	255.255.255.0	bre0
192.168.104.0	0.0.0.0	255.255.255.0	brv4
192.168.105.0	0.0.0.0	255.255.255.0	brv5
192.168.106.0	0.0.0.0	255.255.255.0	brv6
192.168.107.0	0.0.0.0	255.255.255.0	brv7
0.0.0.0	192.168.2.1	0.0.0.0	eth1.1

- **ARP Table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

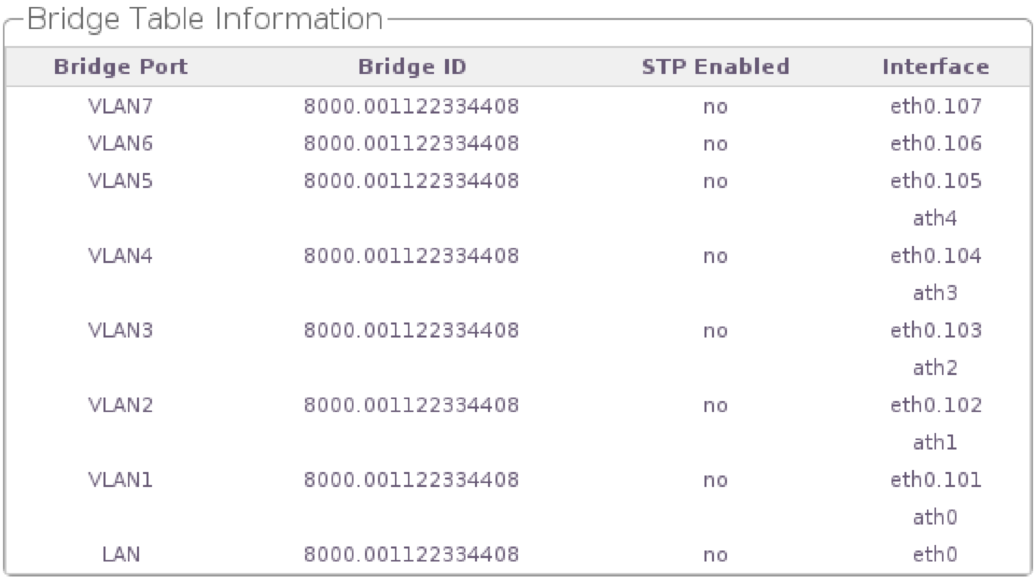


ARP Table Information

IP Address	MAC Address	Interface
192.168.2.151	00:16:D4:33:32:6B	eth1.1
192.168.2.1	00:D0:41:AE:36:61	eth1.1
192.168.103.10	00:11:A3:0A:38:6C	brv3
192.168.2.253	00:0E:C6:00:00:08	eth1.1
192.168.104.10	00:11:A3:0A:38:6A	brv4

- **Bridge Table Information :** Select “**Bridge Table Information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, eth0.vlan_tag, ath0~ath7).



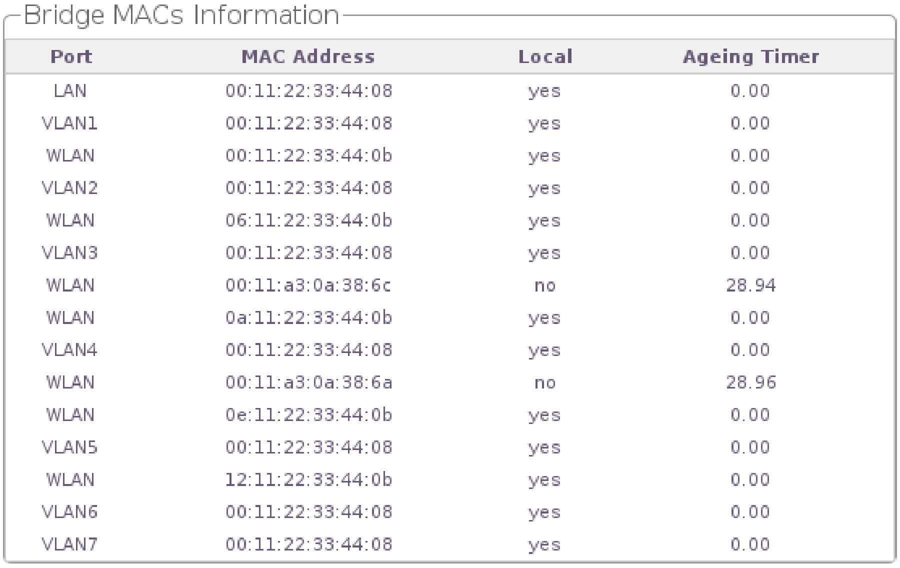
Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
VLAN7	8000.001122334408	no	eth0.107
VLAN6	8000.001122334408	no	eth0.106
VLAN5	8000.001122334408	no	eth0.105 ath4
VLAN4	8000.001122334408	no	eth0.104 ath3
VLAN3	8000.001122334408	no	eth0.103 ath2
VLAN2	8000.001122334408	no	eth0.102 ath1
VLAN1	8000.001122334408	no	eth0.101 ath0
LAN	8000.001122334408	no	eth0

- **Bridge MACs Information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

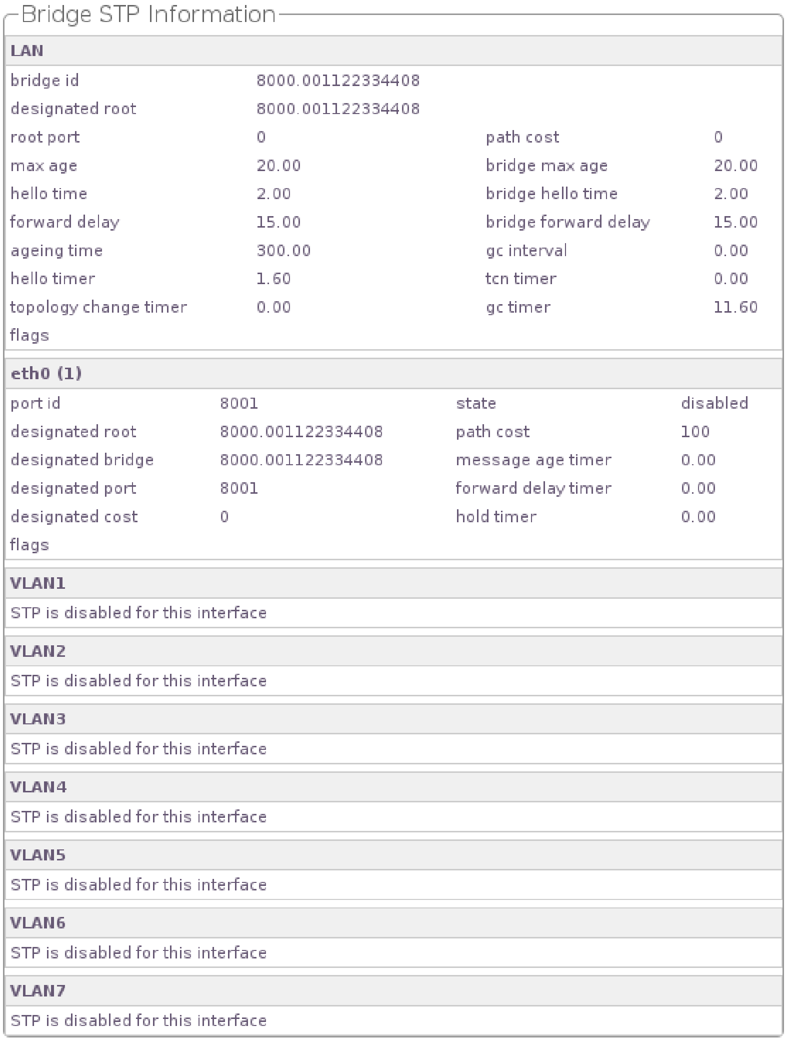
Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:11:22:33:44:08	yes	0.00
VLAN1	00:11:22:33:44:08	yes	0.00
WLAN	00:11:22:33:44:0b	yes	0.00
VLAN2	00:11:22:33:44:08	yes	0.00
WLAN	06:11:22:33:44:0b	yes	0.00
VLAN3	00:11:22:33:44:08	yes	0.00
WLAN	00:11:a3:0a:38:6c	no	28.94
WLAN	0a:11:22:33:44:0b	yes	0.00
VLAN4	00:11:22:33:44:08	yes	0.00
WLAN	00:11:a3:0a:38:6a	no	28.96
WLAN	0e:11:22:33:44:0b	yes	0.00
VLAN5	00:11:22:33:44:08	yes	0.00
WLAN	12:11:22:33:44:0b	yes	0.00
VLAN6	00:11:22:33:44:08	yes	0.00
VLAN7	00:11:22:33:44:08	yes	0.00

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

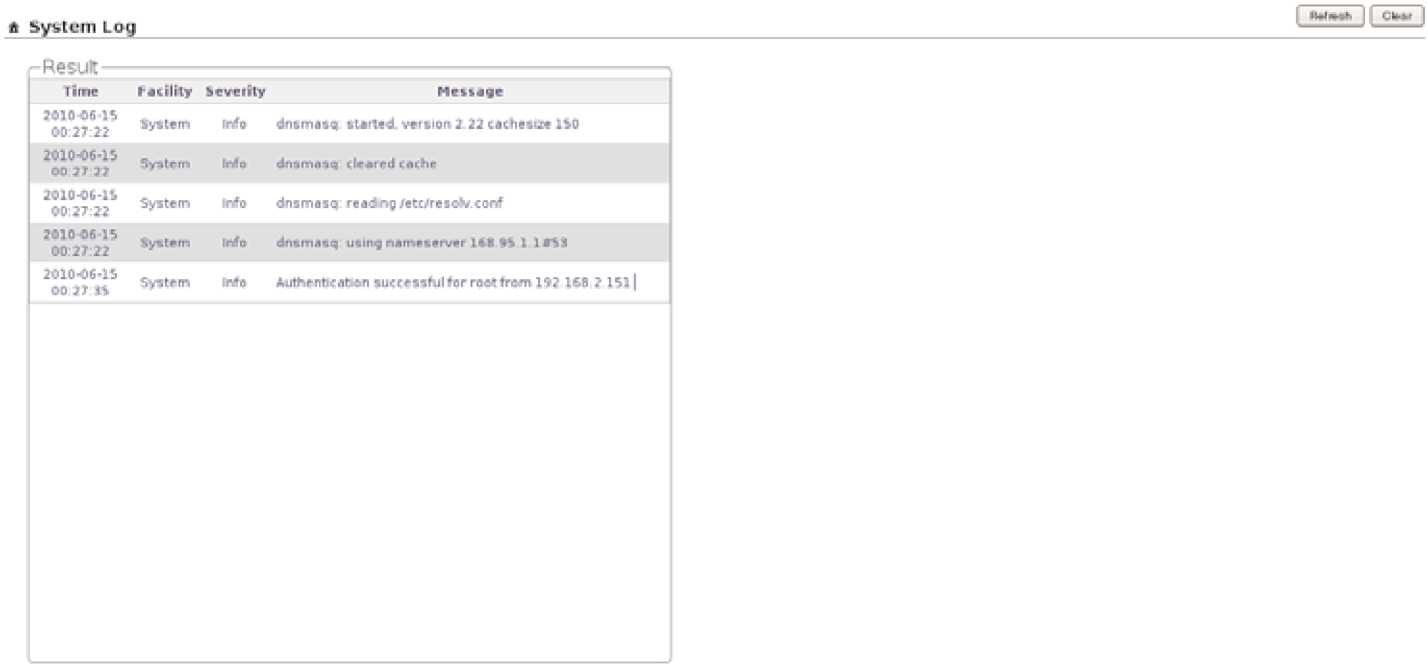


Bridge STP Information

LAN			
bridge id	8000.001122334408		
designated root	8000.001122334408		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00	gc interval	0.00
hello timer	1.60	tcn timer	0.00
topology change timer	0.00	gc timer	11.60
flags			
eth0 (1)			
port id	8001	state	disabled
designated root	8000.001122334408	path cost	100
designated bridge	8000.001122334408	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			
VLAN1			
STP is disabled for this interface			
VLAN2			
STP is disabled for this interface			
VLAN3			
STP is disabled for this interface			
VLAN4			
STP is disabled for this interface			
VLAN5			
STP is disabled for this interface			
VLAN6			
STP is disabled for this interface			
VLAN7			
STP is disabled for this interface			

4.7.3 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



Time	Facility	Severity	Message
2010-06-15 00:27:22	System	Info	dnsmasq: started, version 2.22 cachesize 150
2010-06-15 00:27:22	System	Info	dnsmasq: cleared cache
2010-06-15 00:27:22	System	Info	dnsmasq: reading /etc/resolv.conf
2010-06-15 00:27:22	System	Info	dnsmasq: using nameserver 168.95.1.1#53
2010-06-15 00:27:35	System	Info	Authentication successful for root from 192.168.2.151

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such “System” or “User”
- **Severity :** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message :** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Appendix A. Web GUI valid Characters

Table A Web GUI Valid Characters

Block	**Field**	**Valid Characters**
LAN/VLAN	VLAN Tag	0-4094
	IP Address	A.B.C.D IP Format
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	A.B.C.D IP Format
	Hostname	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
Bandwidth Control	Total Max. Upload/Download	0-102400, 0 is unlimited, default is 512
	Individual Upload/Download	0-102400, 0 is unlimited, default is 512
	Group Upload/Download	0-102400, 0 is unlimited, default is 512
	Session Limit per IP	10-500, 0 is unlimited
DHCP Server	Start/End IP	A.B.C.D IP Format
	DNS1/DNS2 IP	A.B.C.D IP Format
	WINS IP	A.B.C.D IP Format
	Domain	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Lease Time	600-99999999, default is 86400
WAN	Manual MAC Address	12 HEX characters
	IP Address	A.B.C.D IP Format
	IP Netmask	128.0.0.0 ~ 255.255.255.255
	IP Gateway	A.B.C.D IP Format
	PPTP Server	A.B.C.D IP Format
	My WAN IP	A.B.C.D IP Format
	My WAN IP Netmask	128.0.0.0 ~ 255.255.255.252
	Hostname	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	User name	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Password	
	MTU	576 ~ 1492
	Primary/Secondary DNS	A.B.C.D IP Format

DDNS	Hostname	Length : Up to 32 0-9, A-Z, a-z @ - _ .
	User Name	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Password	

Table A   Web GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
Management	System Name	Length : 1-32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	Length : Up to 45 chars Space
	Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Port	1 ~ 65535
	Port	1 ~ 65535
	IP Address/ Domain	A.B.C.D IP Format or Domain
	IP Address to Ping	A.B.C.D IP Format
	Ping Interval	60~3600; default is 300
	Startup Delay	60~3600; default is 300
	Failure Count To Reboot	1~99; default is 3
SNMP	RO/ RW community	Length : 1-32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW user	Length : 1-31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =

Block	**Field**	**Valid Characters**
	Community	Length : 1-32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	A.B.C.D IP Format
General Setup	Aggregation Frames	2-64, default is 32
	Aggregation Size	1024-65535, default is 50000
Advanced Setup	Beacon Interval	40 ~ 3500
	DTIM Interval	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347

Table A Web GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
Virtual AP Setup	ESSID	Length : 1-31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII characters
	Group Key Update Period	>=10 seconds, default is 600
	Master Key Update Period	>= 10 seconds, default is 86400
	WEP Key Update Period	>=0 seconds, default is 300, 0 is disable
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	A.B.C.D IP Format
	Radius Port	1 ~ 65535
	Shared Secret	1 ~ 64 characters
	EAP Reauth Period	>= 0 seconds; 0 is disable, default is 3600
WDS Setup	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII chars
	Peer's MAC Address	12 HEX chars
	Description	Up to 32 characters Space
IP Filter	Source/Destination Address	A.B.C.D IP Format
	Source/Destination Mask	0 ~ 32
	Source/Destination Port	1 ~ 65535
MAC Filter	MAC address	MAC Format; 12 HEX characters
Virtual Server	Description	Up to 32 characters
	Private IP	A.B.C.D IP Format

Block	**Field**	**Valid Characters**
	Private/Public Port	1 ~ 65535
DMZ	IP Address	A.B.C.D IP Format
Time Policy	Start From / End To	Time Format : hh:mm Start From < End To
Service Domain	Login Timeout	1~60; default is 10
	Redirect URL	URL Format
	Guest Count Limit	1~100; default is 5
	Guest Time	1~720; default is 10

Table A Web GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
Pregenerated Tickets	File ID	1 ~ 32767
	Price	1-7 digit number : xxxxx.xx
	Currency	1~3 letters characters
	Quantity of Tickets	1 ~ 3069
	Passcode Length	8 ~ 31, default is 8
	Description	Up to 32 characters Space
	Time Quota	1 ~ 366x24x60 , default is 60
	Volume Quota	Default 10; Max is 102400
	Effective Start/ End Time	Date / Time Format : MM/DD/YYYY HH:MM Start Time < End Time
Billing Plan	Plan Name	Up to 32 characters
	Price	1-7 digit number : xxxxx.xx
	Currency	1~3 letters characters
	Passcode Length	8 ~ 31, default is 8
	Wireless ESSID	Up to 100 characters Space
	Wireless Key	Up to 100 characters Space
	Description	Up to 100 characters Space
	Time Quota	1 ~ 366x24x60 , default is 60
	Volume Quota	Default 10; Max is 102400
Thermal Printer	IP Address	A.B.C.D IP Format
	Command Port	1 ~ 65535, default is 5000
	New Lock Password	4-8 digit number
	Confirm Lock Password	4-8 digit number
	Balance Date	Time format : HH:MM
	Description	Up to 32 characters Space
Local Radius	Username	Length : 4-16 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` . =
	Password	Length : 4-16 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` . =
	MAC Address	MAC Format; 12 HEX characters
	Description	Up to 32 characters Space

Table A Web GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
Remote Radius	Primary/Secondary Server IP	A.B.C.D IP Format
	Authentication/Account Port	1 ~ 65535
	Secret Key	1-64 characters
LDAP	Server IP	A.B.C.D IP Format
	Port	1 ~ 65535
	Identity	Length : 1-16 0-9, A-Z, a-z @-_.
	Password	1-16 characters
	Base DN	1-64 characters
	Account Attribute	1-64 characters
Walled Garden	Walled Name	4-32 characters Space
	IP Address/ Domain	A.B.C.D IP Format or Domain
	Homepage	URL Format
	Description	32 characters Space
Notification	Sender From	E-mail Format
	SMTP Server	A.B.C.D IP Format or Domain
	Port	1-65535, default is 25
	Username	Length : 1-64 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Password	Length : 1-64 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Receiver E-mail	E-mail Format
	Sending Interval	10-4200, default is 1440
	IP	A.B.C.D IP Format

Appendix B. System Manager Privileges

There are three system management accounts for maintaining the system; namely, the **root**, **admin** and **operator** accounts are with different levels of privileges. The root manager account is empowered with full privilege to Read & Write while the admin manager account is Read only.

The following table display admin and operator account’s privileges.

Main Menu	Sub Menu	Group	Admin Privilege	0perator Privilege
System	WAN		None	None
	WAN Traffic		None	None
	LAN/VLAN		None	None
	DDNS		None	None
	Management	System Information	Read	None
		Root Password	Read	None
		Admin Password	Read & Write	None
		Operator Password	Read & Write	None
		Login Methods	Read	None
	Time Server		None	None
	SNMP		None	None
Service Domain	Service Domain		Read & Write	None
	Authentication – Management		Read & Write	None
	Authentication – Pregenerated		Read & Write	None
	Authentication – OnDemand	Billing Plan Setup	Read & Write	None
		Create Accounts	Read & Write	Read & Write
		Payment Gateway	Read & Write	Read & Write
		Thermal Printer Setup	Read & Write	Read & Write
		Billing Plan Report	Read & Write	Read & Write
	Authentication – Local Radius		Read & Write	None
	Authentication – Remote Radius		Read & Write	None
	Authentication – LDAP		Read & Write	None
	Walled Garden		Read & Write	None
	Notification		Read & Write	None
	Online Users		Read & Write	Read & Write
	Log Info		Read & Write	Read & Write
Wireless	General		Read & Write	None
	Advanced		Read & Write	None
	Virtual AP		Read & Write	None
	Associated Clients		Read & Write	None
	WDS Status		Read & Write	None
Advance	DMZ		Read & Write	None
	IP Filter		Read & Write	None
	MAC F ter		Read & Write	None
	Virtua Server		Read & Write	None
	Time Policy		Read & Write	None
Profile Settings	Backup Settings	Read & Write	None	
	Restore Settings	Read & Write	None	
	Reset to Default	Read & Write	None	
System Upgrade		Read & Write	None	
Network Utility		Read & Write	None	
Format Database		Read & Write	None	
Reboot		Read & Write	None	

Appendix C. Create PayPal Business Account

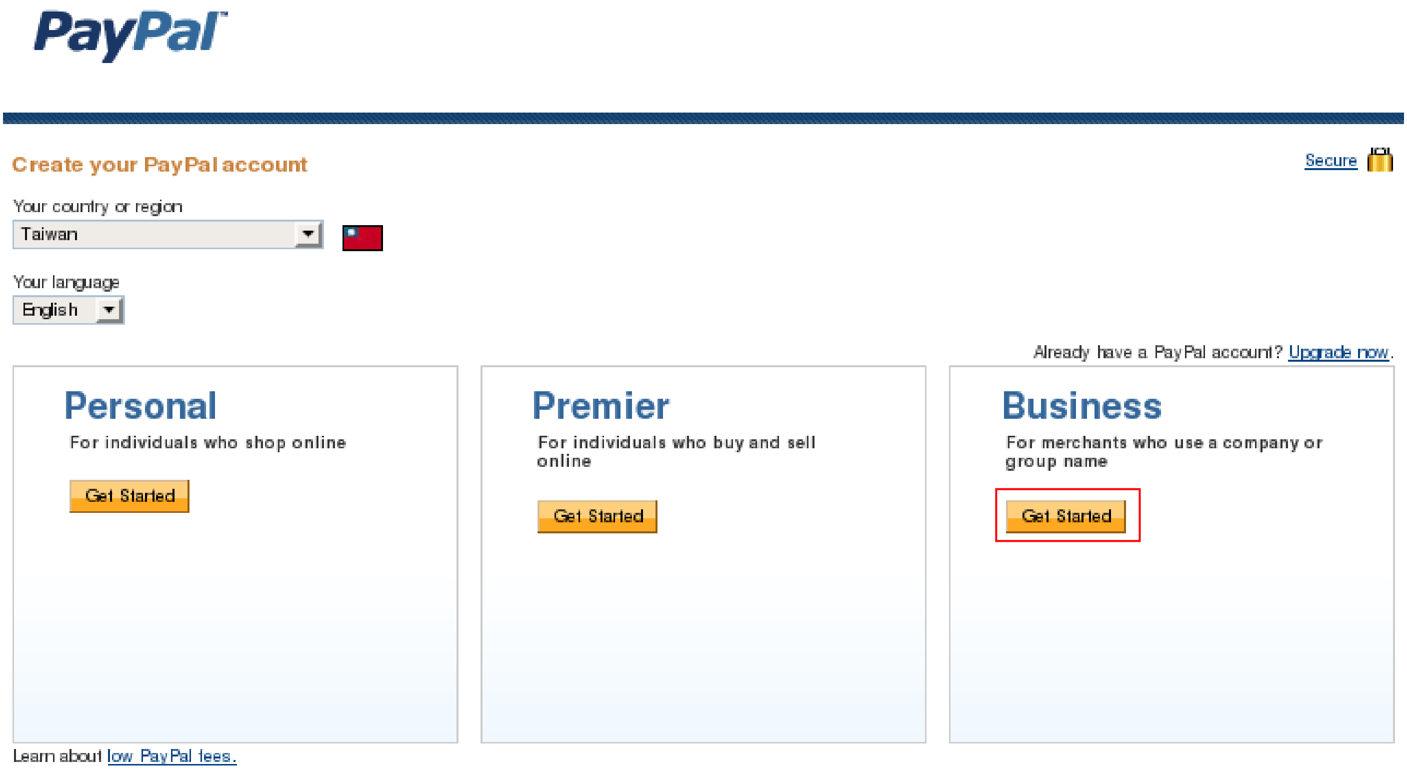
This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access using their PayPal accounts or credit cards.

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

Sign Up Process :

Step 1 : Sign up for a PayPal **Business Account** and Login.

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


Create your PayPal account

Your country or region: Taiwan

Your language: English

Already have a PayPal account? Upgrade now.

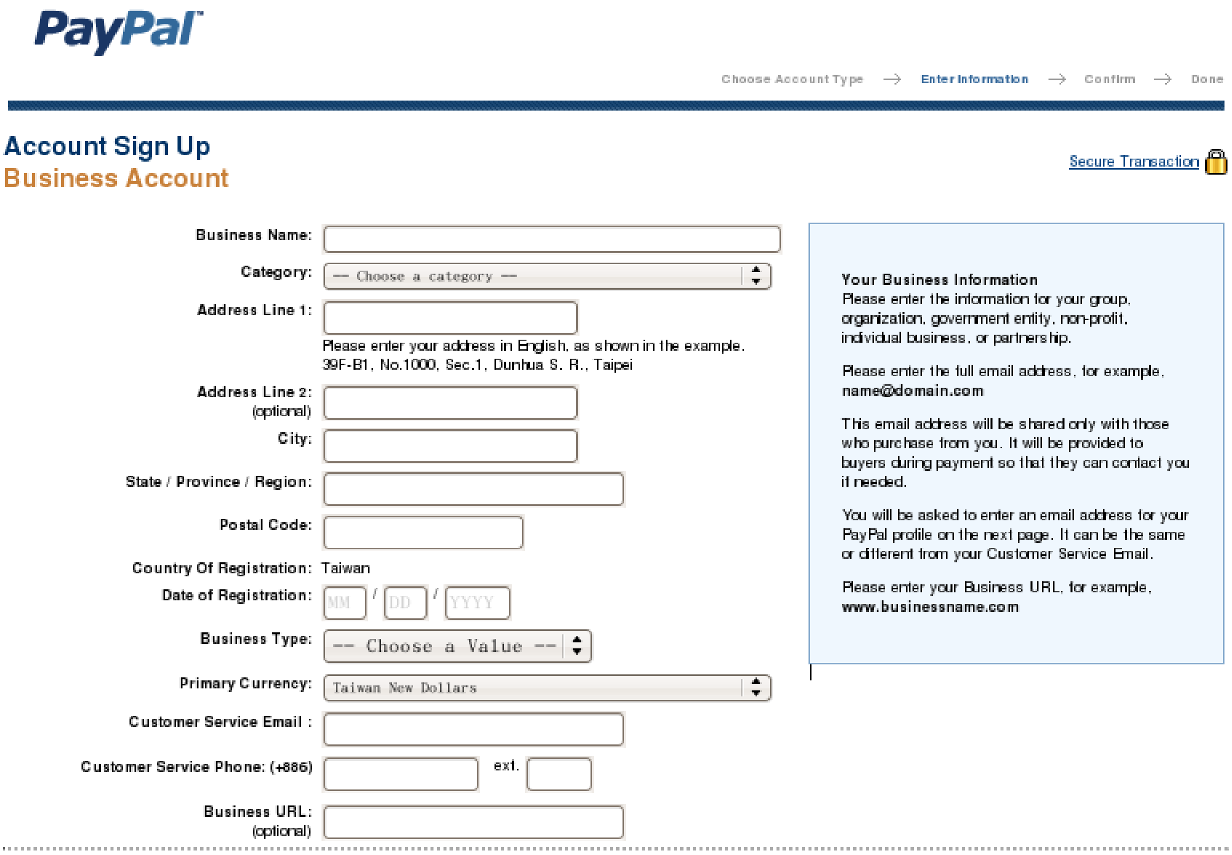
Personal – For individuals who shop online – Get Started

Premier – For individuals who buy and sell online – Get Started

Business – For merchants who use a company or group name – Get Started

Learn about low PayPal fees.

Click ***Get Started*** button to create **PayPal Business Account** on Business field, the Account Sign Up page will appear.



Account Sign Up
Business Account

Business Name:

Category: -- Choose a category --

Address Line 1:

Please enter your address in English, as shown in the example.
39F-B1, No.1000, Sec.1, Dunhua S. R., Taipei

Address Line 2: (optional)

City:

State / Province / Region:

Postal Code:

Country Of Registration: Taiwan

Date of Registration: MM / DD / YYYY

Business Type: -- Choose a Value --

Primary Currency: Taiwan New Dollars

Customer Service Email :

Customer Service Phone: (+886) ext.

Business URL: (optional)

Your Business Information
Please enter the information for your group, organization, government entity, non-profit, individual business, or partnership.

Please enter the full email address, for example, **name@domain.com**

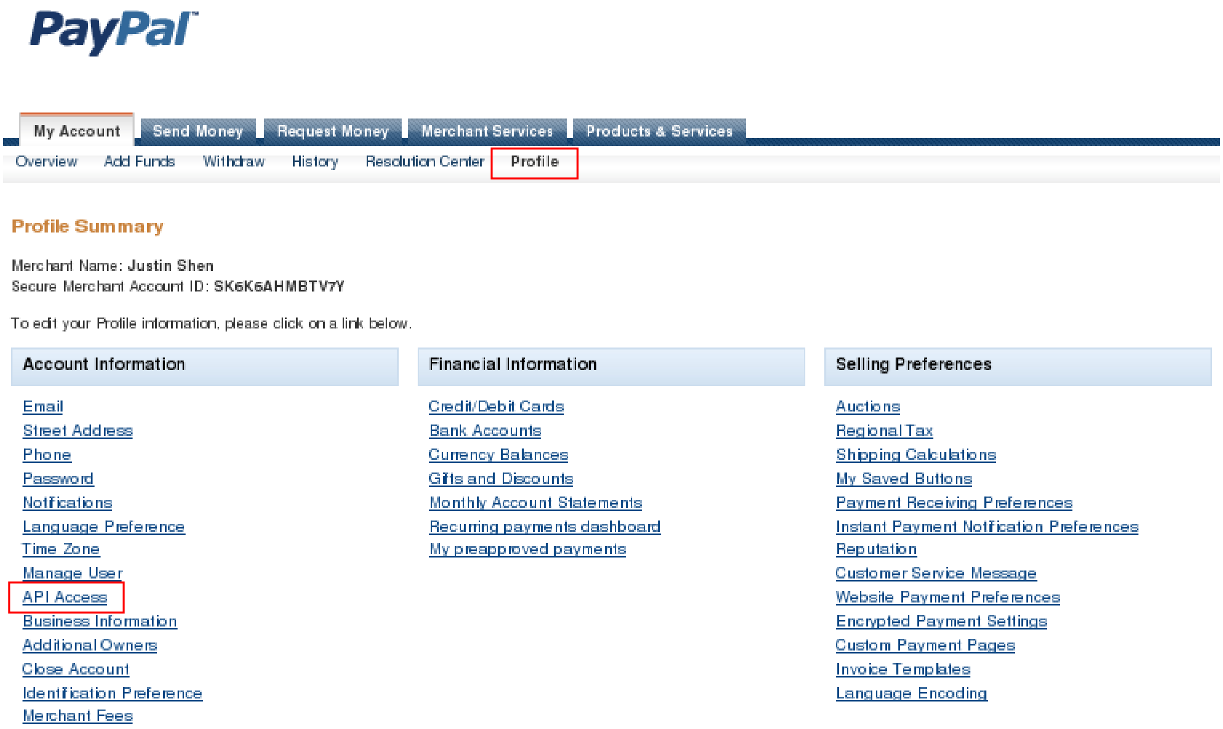
This email address will be shared only with those who purchase from you. It will be provided to buyers during payment so that they can contact you if needed.

You will be asked to enter an email address for your PayPal profile on the next page. It can be the same or different from your Customer Service Email.

Please enter your Business URL, for example, **www.businessname.com**

Step 2 : Edit **NECESSARY** settings in “**API Access**”

Please click on **Profile** -> **API Access** in the **Account Information**.



Profile Summary

Merchant Name: **Justin Shen**
Secure Merchant Account ID: **SK6K6AHMBTV7Y**

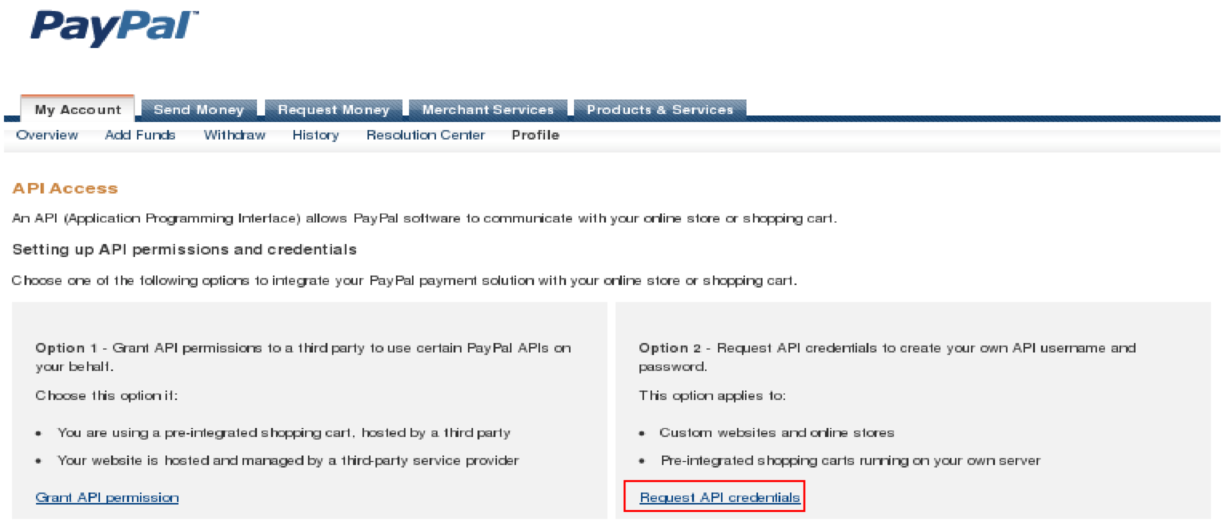
To edit your Profile information, please click on a link below.

Account Information
- Email
- Street Address
- Phone
- Password
- Notifications
- Language Preference
- Time Zone
- Manage User
- API Access
- Business Information
- Additional Owners
- Close Account
- Identification Preference
- Merchant Fees

Financial Information
- Credit/Debit Cards
- Bank Accounts
- Currency Balances
- Gifts and Discounts
- Monthly Account Statements
- Recurring payments dashboard
- My preapproved payments

Selling Preferences
- Auctions
- Regional Tax
- Shipping Calculations
- My Saved Buttons
- Payment Receiving Preferences
- Instant Payment Notification Preferences
- Reputation
- Customer Service Message
- Website Payment Preferences
- Encrypted Payment Settings
- Custom Payment Pages
- Invoice Templates
- Language Encoding

After click API Access on Account Information, the API Access setting will appear. Click “**Request API credentials**” in **Option 2 – Request API credentials to create your own API username and password**.



API Access

An API (Application Programming Interface) allows PayPal software to communicate with your online store or shopping cart.

Setting up API permissions and credentials

Choose one of the following options to integrate your PayPal payment solution with your online store or shopping cart.

Option 1 - Grant API permissions to a third party to use certain PayPal APIs on your behalf.

Choose this option if:

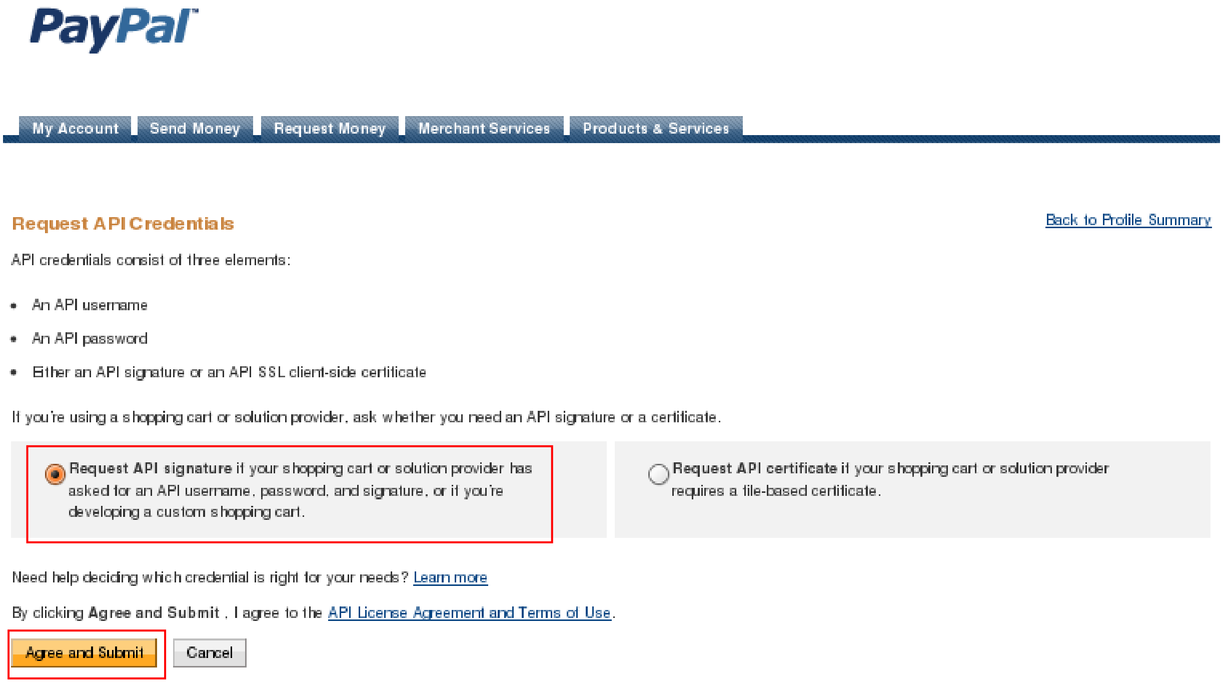
- You are using a pre-integrated shopping cart, hosted by a third party
- Your website is hosted and managed by a third-party service provider

Option 2 - Request API credentials to create your own API username and password.

This option applies to:

- Custom websites and online stores
- Pre-integrated shopping carts running on your own server

Select **Request API signature** and click “**Agree and Submit**” button to generate **API username**, **API password**, and **API signature**.



Request API Credentials

API credentials consist of three elements:

- An API username
- An API password
- Either an API signature or an API SSL client-side certificate

If you're using a shopping cart or solution provider, ask whether you need an API signature or a certificate.

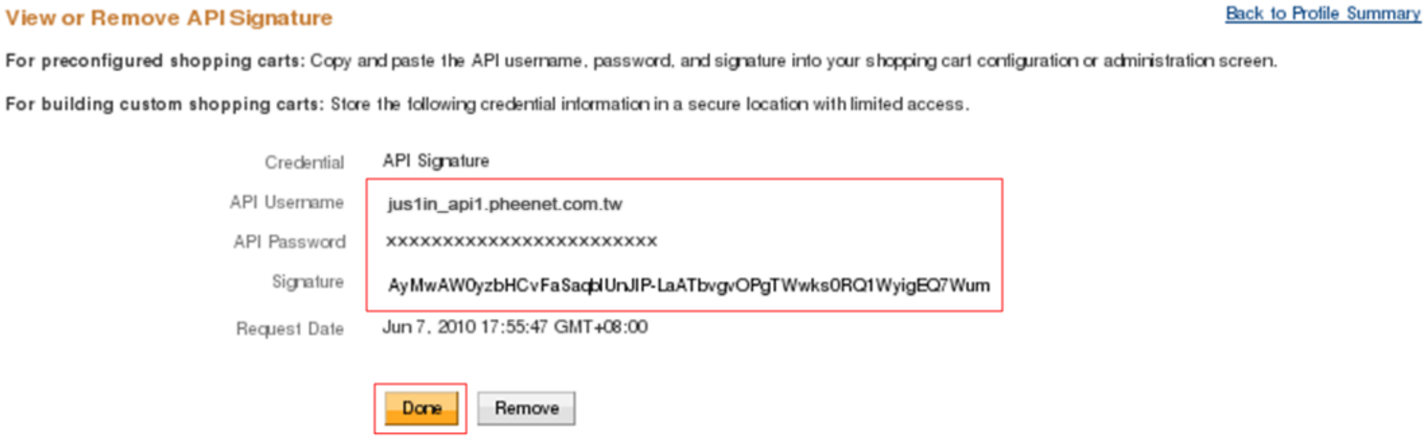
● Request API signature if your shopping cart or solution provider has asked for an API username, password, and signature, or if you're developing a custom shopping cart.

○ Request API certificate if your shopping cart or solution provider requires a file-based certificate.

Need help deciding which credential is right for your needs? Learn more

By clicking Agree and Submit , I agree to the API License Agreement and Terms of Use.

The **API Username**, **API Password** and **Signature** will generated. Click “**Done**” button to finish process.



View or Remove API Signature

Back to Profile Summary

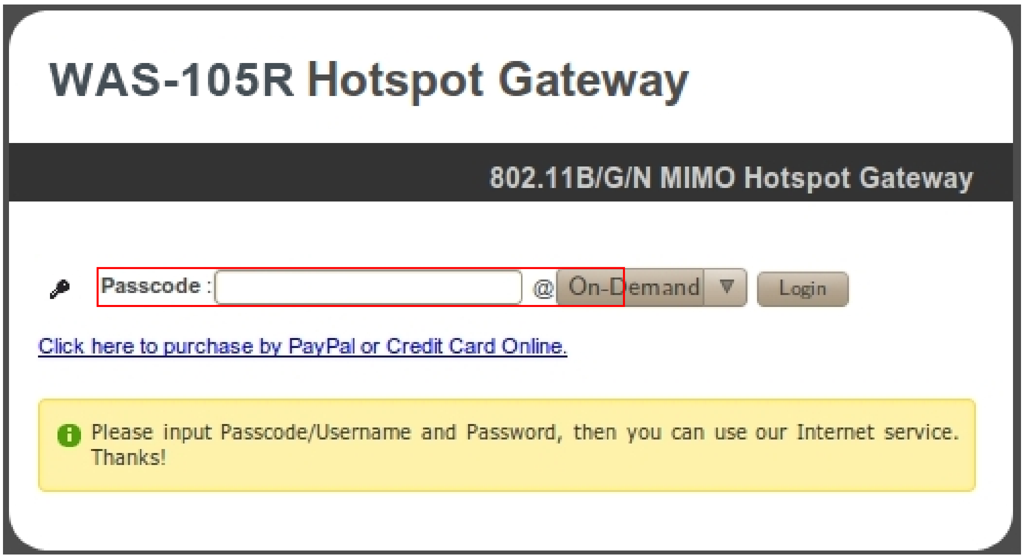
For preconfigured shopping carts: Copy and paste the API username, password, and signature into your shopping cart configuration or administration screen.

For building custom shopping carts: Store the following credential information in a secure location with limited access.

Credential	API Signature
API Username	jus1in_api1.pheenet.com.tw
API Password	xxxxxxxxxxxxxxxxxxxxxxxx
Signature	AyMwAW0yzbHCvFaSaqbIUnJIP-LaATbvgvOPgTWwks0RQ1WyigEQ7Wum
Request Date	Jun 7, 2010 17:55:47 GMT+08:00

Appendix D. Examples of Making Payments for End Users

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



WAS-105R Hotspot Gateway

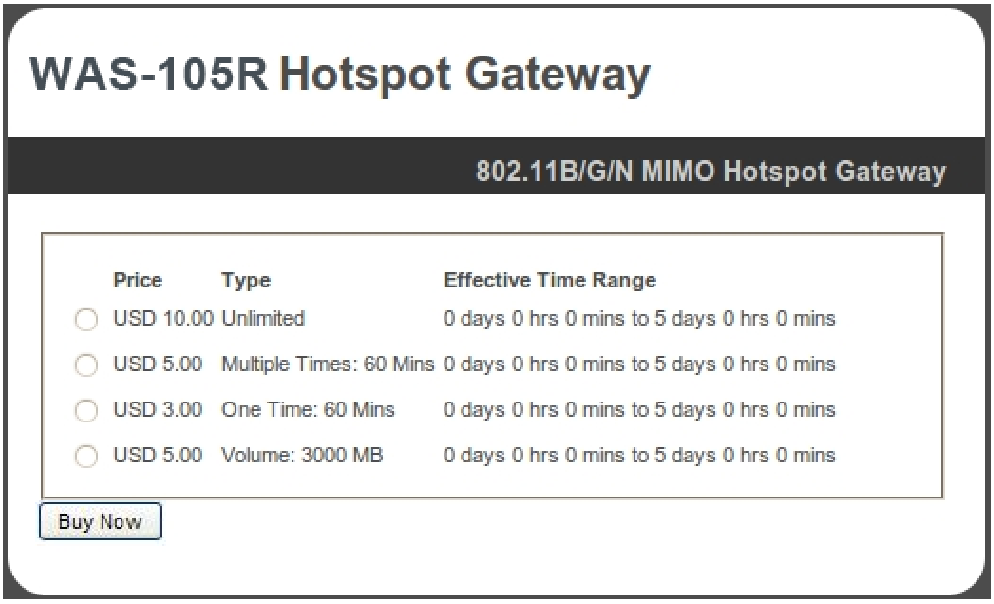
802.11B/G/N MIMO Hotspot Gateway

Passcode : @ On-Demand ▼ Login

Click here to purchase by PayPal or Credit Card Online.

Please input Passcode/Username and Password, then you can use our Internet service. Thanks!

Step 2 : Select service package and Click ***Buy Now*** button to send out this transaction. There will be a connecting message as below.

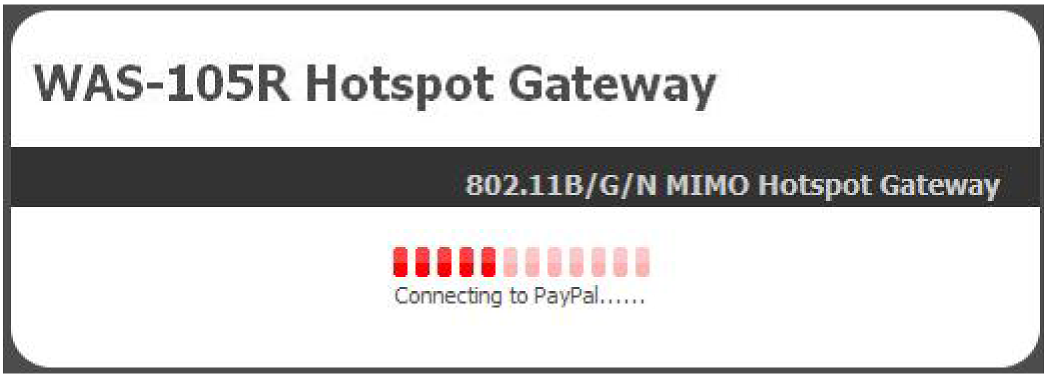


WAS-105R Hotspot Gateway

802.11B/G/N MIMO Hotspot Gateway

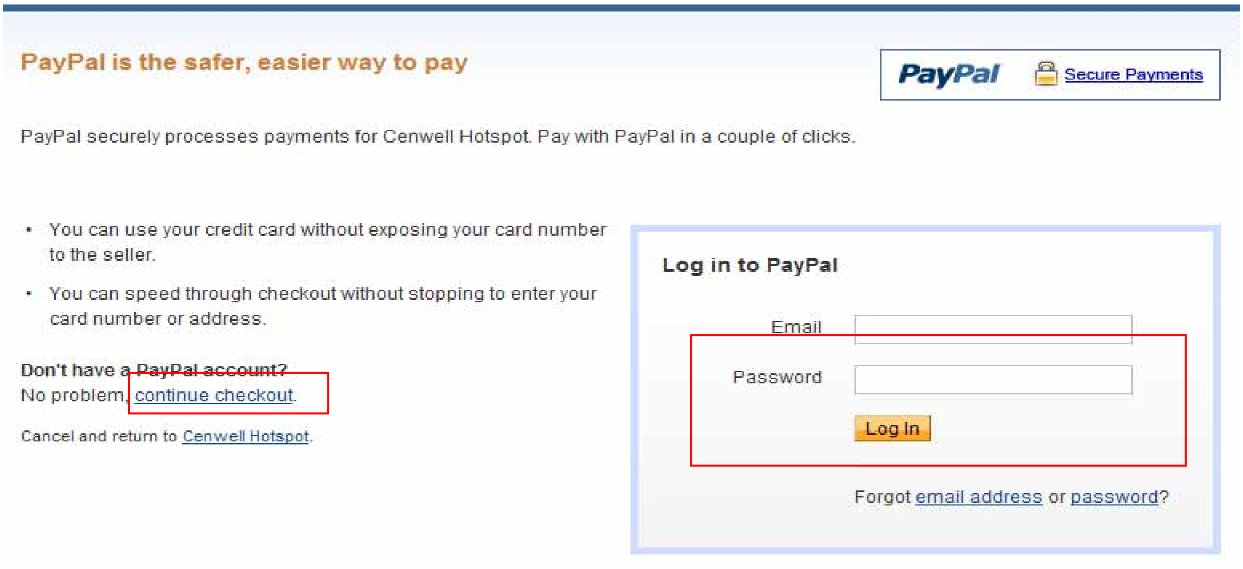
	Price	Type	Effective Time Range
○	USD 10.00	Unlimited	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins
○	USD 5.00	Multiple Times: 60 Mins	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins
○	USD 3.00	One Time: 60 Mins	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins
○	USD 5.00	Volume: 3000 MB	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins

Buy Now



Connecting to PayPal......

Step 3 : You will be redirected to PayPal website to complete the payment process. You can pay service fee via Paypal account or use your credit card (Click "**continue checkout**" hyperlinks)



PayPal is the safer, easier way to pay

PayPal securely processes payments for Cenwell Hotspot. Pay with PayPal in a couple of clicks.

- You can use your credit card without exposing your card number to the seller.
- You can speed through checkout without stopping to enter your card number or address.

Don't have a PayPal account?
No problem, continue checkout.

Cancel and return to Cenwell Hotspot.

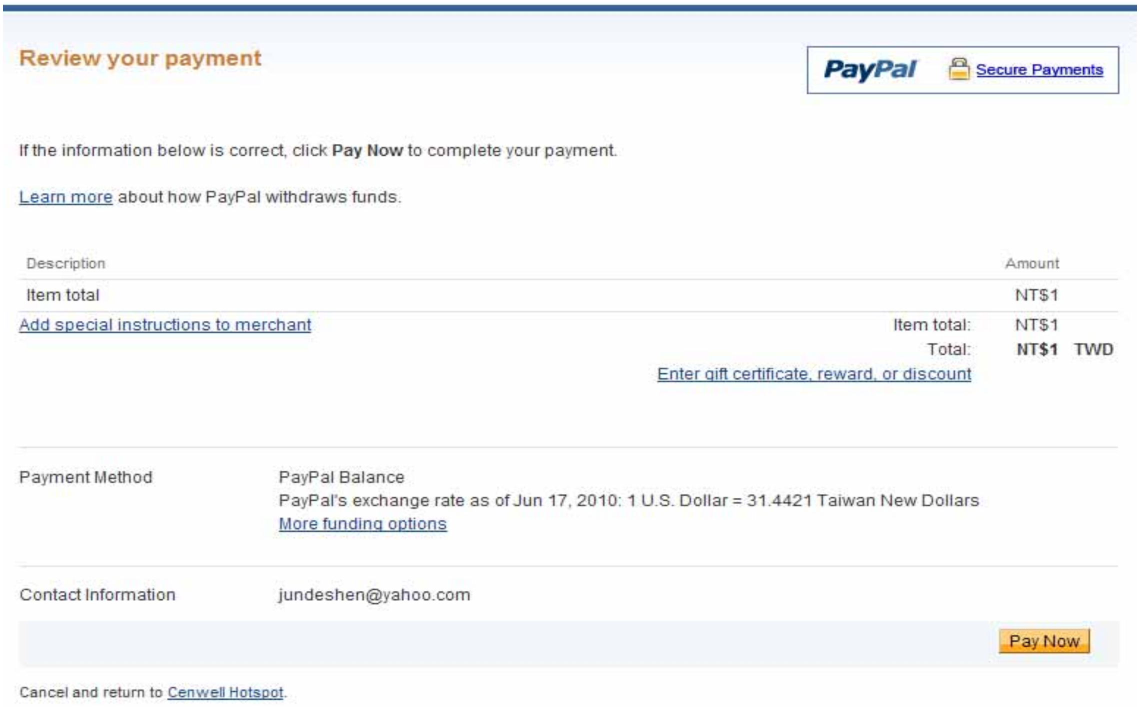
Log in to PayPal

Email

Password

Forgot email address or password?

Step 4 : After login Paypal The payment information will appear. Click ***Pay Now*** button to get passcode.



Review your payment

If the information below is correct, click **Pay Now** to complete your payment.

Learn more about how PayPal withdraws funds.

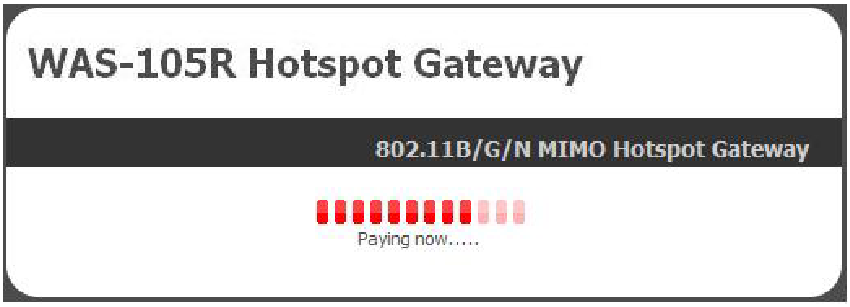
Description	Amount
Item total	NT$1
Add special instructions to merchant Item total: Total: Enter gift certificate, reward, or discount	NT$1 **NT$1** TWD

Payment Method: PayPal Balance
PayPal's exchange rate as of Jun 17, 2010: 1 U.S. Dollar = 31.4421 Taiwan New Dollars
More funding options

Contact Information: jundeshen@yahoo.com

Cancel and return to Cenwell Hotspot.

Step 5 : After clicking ***Pay Now*** button, the process of paying confirm will appear. **Please don't close this window**.

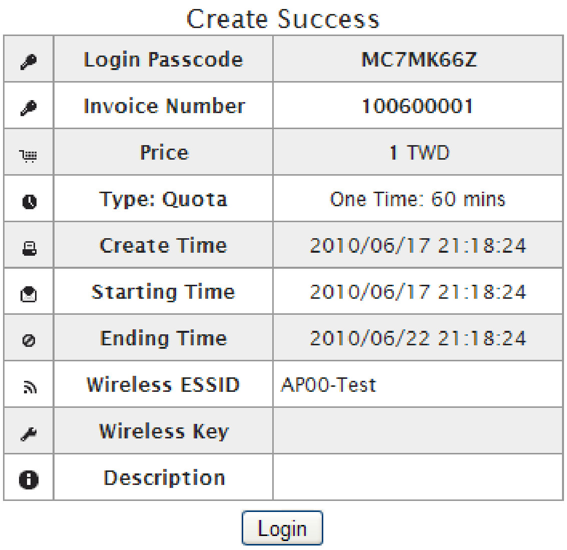


WAS-105R Hotspot Gateway

802.11B/G/N MIMO Hotspot Gateway

Paying now.....

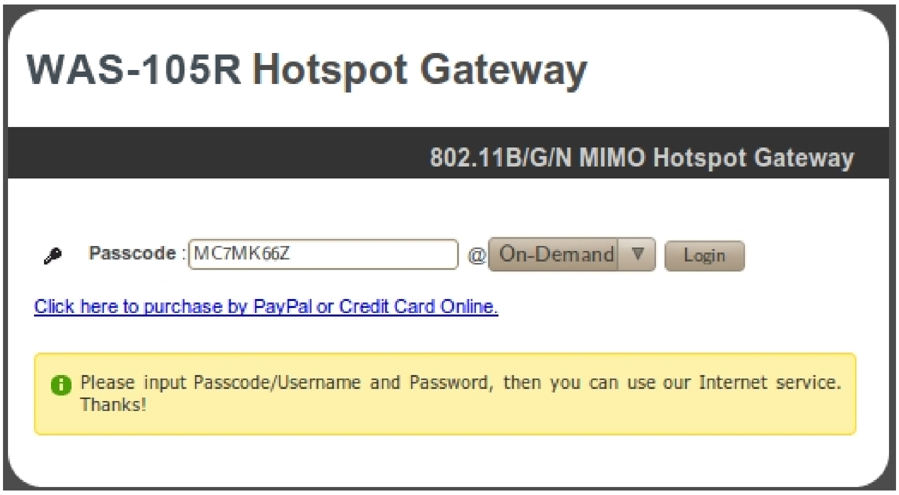
Step 6 : After paying confirm, the system will create **Passcode** for end users login. Click ***Login*** button to enter Login page. (Write down your "**Login Passcode"** before you click ***Login*** button)



Create Success

Login Passcode	MC7MK66Z
Invoice Number	100600001
Price	1 TWD
Type: Quota	One Time: 60 mins
Create Time	2010/06/17 21:18:24
Starting Time	2010/06/17 21:18:24
Ending Time	2010/06/22 21:18:24
Wireless ESSID	AP00-Test
Wireless Key	
Description	

Step 7 : Input generated passcode and click ***Login*** button to login Internet Service.



WAS-105R Hotspot Gateway

802.11B/G/N MIMO Hotspot Gateway

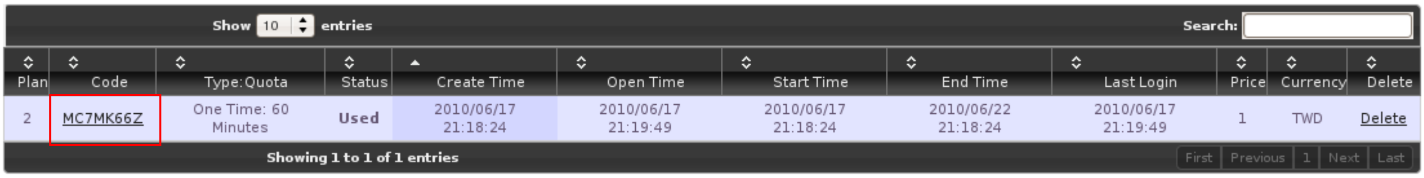
Passcode : MC7MK66Z @ On-Demand

Click here to purchase by PayPal or Credit Card Online.

Please input Passcode/Username and Password, then you can use our Internet service. Thanks!

Appendix E. Issue Refund for PayPal

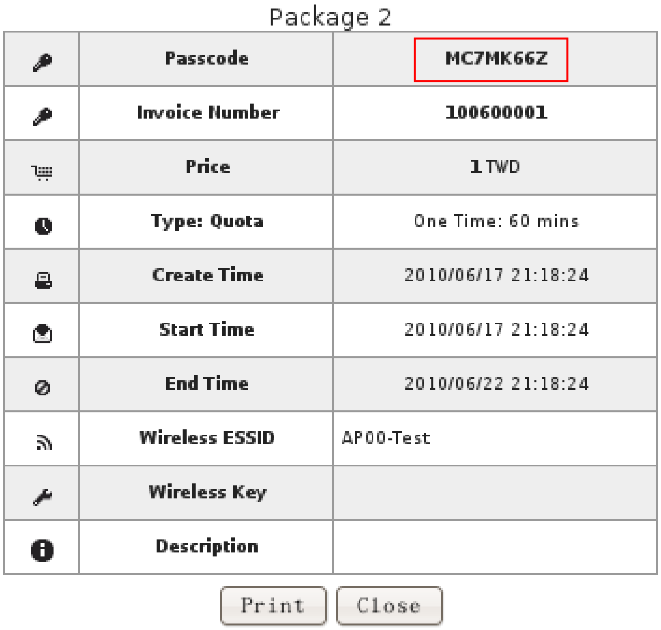
Step 1 : Click on **Service Domain -> Authentication -> On-Demand -> Payment Gateway Setup**, and then click ***Information*** button on the Billing Plan Setup List to enter **Payment Gateway Information** page. Click on selected passcode's hyperlinks for viewing this ticket's **Invoice Number**



Show 10 entries Search:

Plan	Code	Type:Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
2	MC7MK66Z	One Time: 60 Minutes	Used	2010/06/17 21:18:24	2010/06/17 21:19:49	2010/06/17 21:18:24	2010/06/22 21:18:24	2010/06/17 21:19:49	1	TWD	Delete

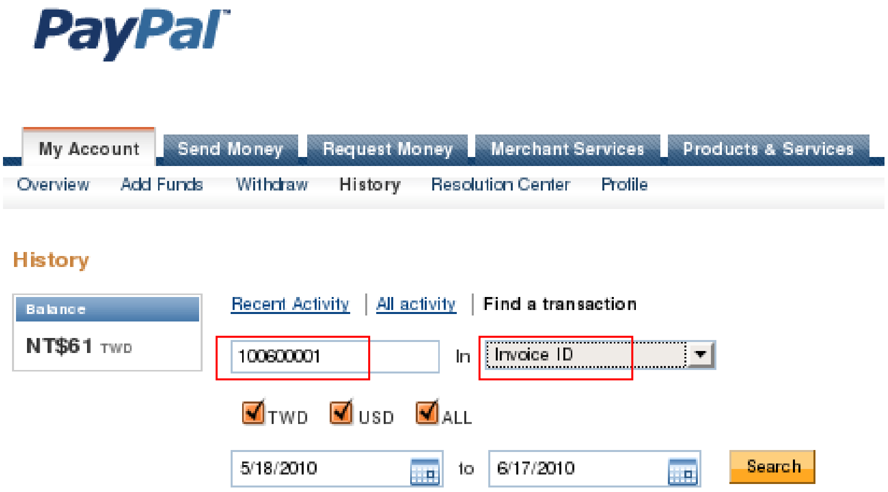
Showing 1 to 1 of 1 entries



Package 2

	Passcode	MC7MK66Z
	Invoice Number	100600001
	Price	1 TWD
	Type: Quota	One Time: 60 mins
	Create Time	2010/06/17 21:18:24
	Start Time	2010/06/17 21:18:24
	End Time	2010/06/22 21:18:24
	Wireless ESSID	AP00-Test
	Wireless Key	
	Description	

Step 2 : Please login in PayPal, and click on **History -> Find a transaction**. Then enter ***Invoice Number*** in “**Invoice ID**” and specify the time period for search. Click ***Search*** button to view the transaction details.

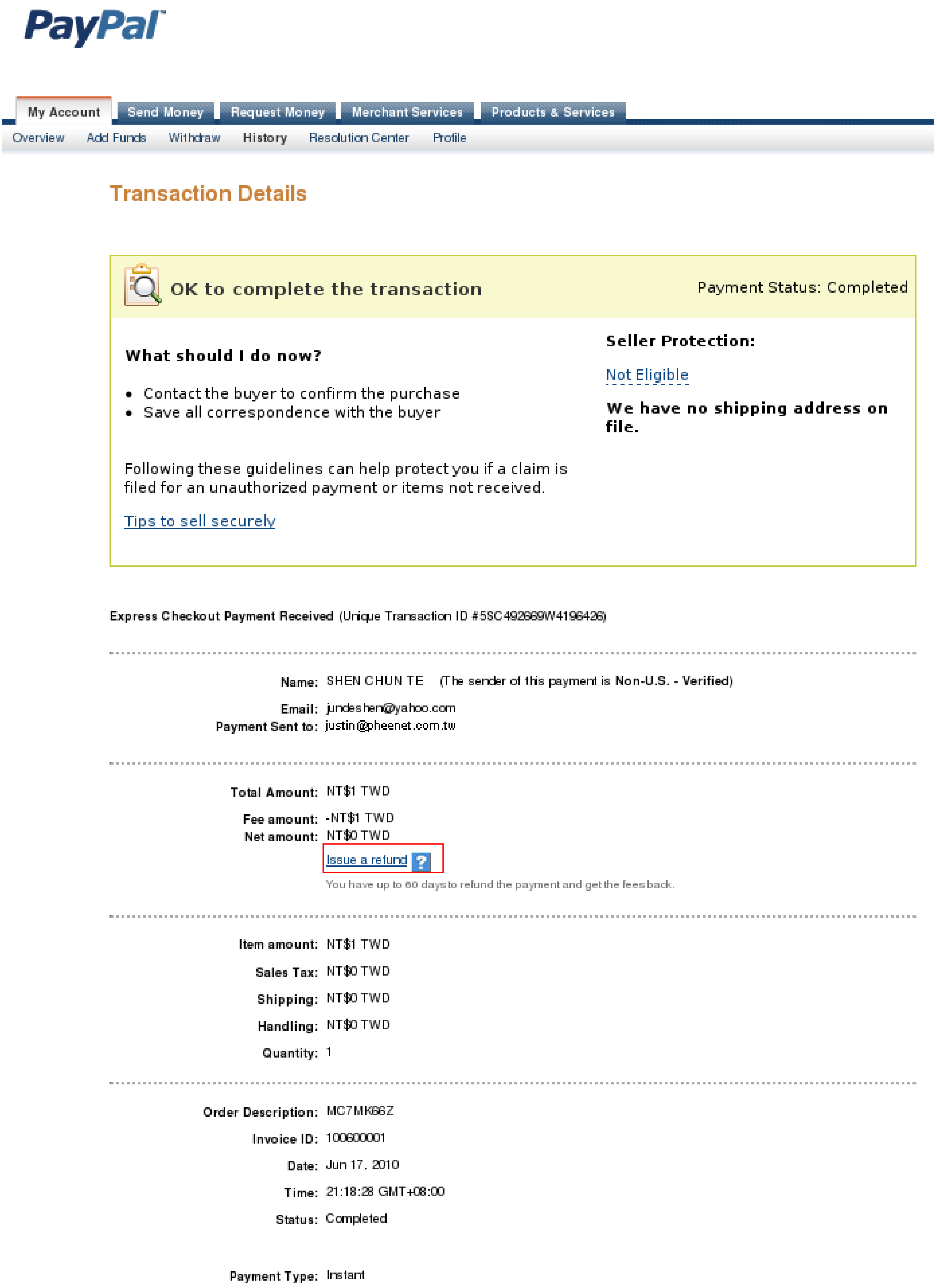


100600001 In Invoice ID

☑ TWD ☑ USD ☑ ALL

5/18/2010 to 6/17/2010

Step 3 : View the transaction detail and click “**Issue a refund**”.



Transaction Details

OK to complete the transaction

Payment Status: Completed

What should I do now?

- Contact the buyer to confirm the purchase
- Save all correspondence with the buyer

Following these guidelines can help protect you if a claim is filed for an unauthorized payment or items not received.

Tips to sell securely

Seller Protection:

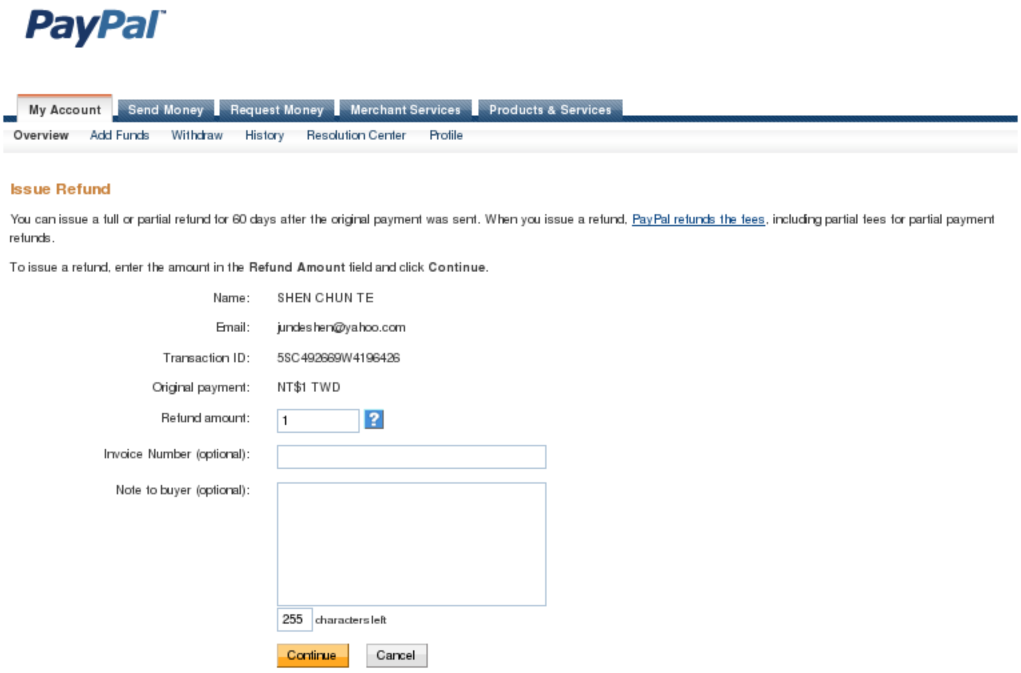
Not Eligible

We have no shipping address on file.

Express Checkout Payment Received (Unique Transaction ID #5SC492669W4196426)

Name:	SHEN CHUN TE (The sender of this payment is **Non-U.S. - Verified**)
Email:	jundeshen@yahoo.com
Payment Sent to:	justin@pheenet.com.tw
Total Amount:	NT$1 TWD
Fee amount:	-NT$1 TWD
Net amount:	NT$0 TWD
	Issue a refund ? You have up to 60 days to refund the payment and get the fees back.
Item amount:	NT$1 TWD
Sales Tax:	NT$0 TWD
Shipping:	NT$0 TWD
Handling:	NT$0 TWD
Quantity:	1
Order Description:	MC7MK66Z
Invoice ID:	100600001
Date:	Jun 17, 2010
Time:	21:18:28 GMT+08:00
Status:	Completed
Payment Type:	Instant

Step 4 : Click ***Continue*** button to next page.



Issue Refund

You can issue a full or partial refund for 60 days after the original payment was sent. When you issue a refund, PayPal refunds the fees, including partial fees for partial payment refunds.

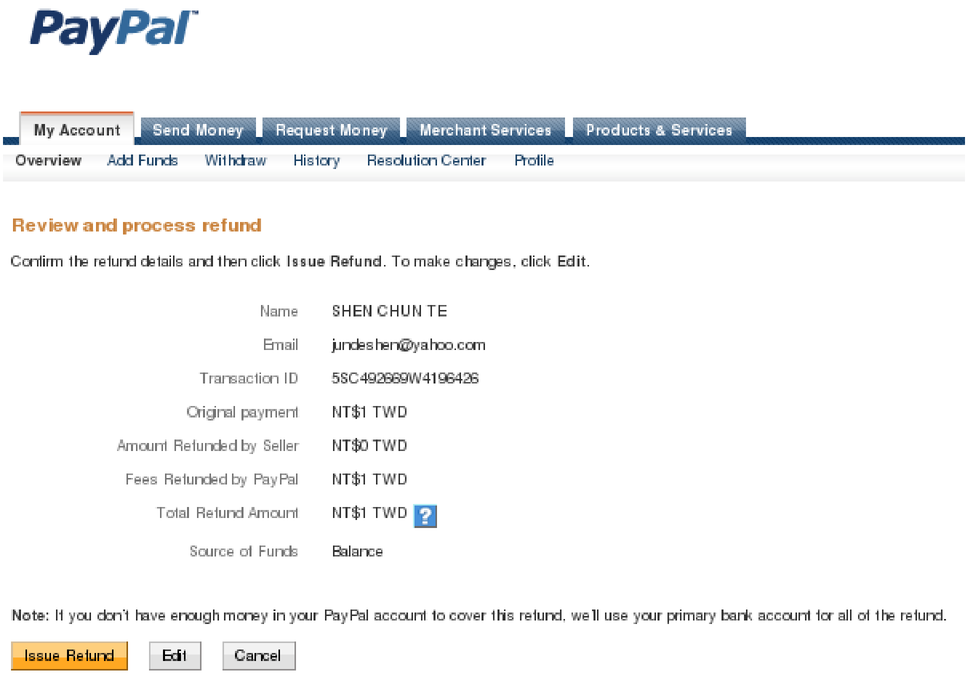
To issue a refund, enter the amount in the **Refund Amount** field and click **Continue**.

Name:	SHEN CHUN TE
Email:	jundeshen@yahoo.com
Transaction ID:	5SC492669W4196426
Original payment:	NT$1 TWD
Refund amount:	1 ?
Invoice Number (optional):	
Note to buyer (optional):	

255 characters left

Continue Cancel

Step 5 : Click ***Issue Refund*** button to refund this payment.



Review and process refund

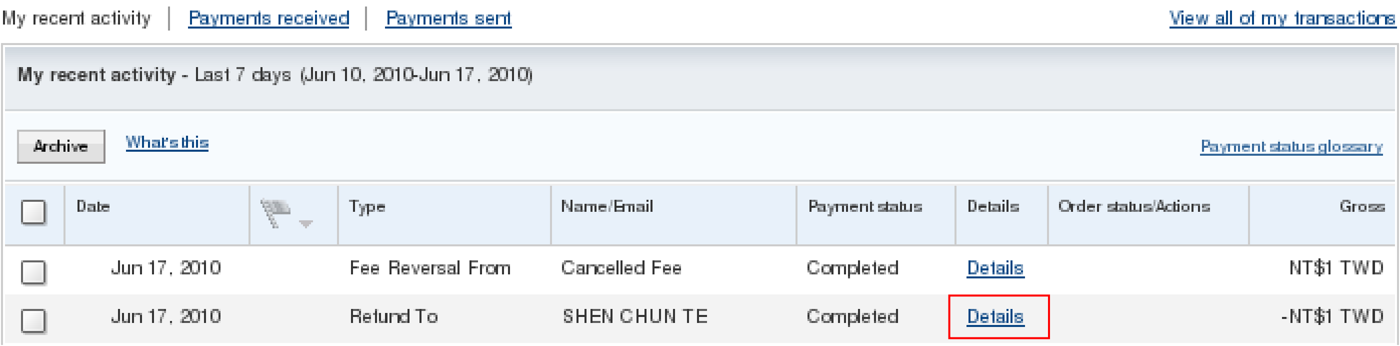
Confirm the refund details and then click **Issue Refund**. To make changes, click **Edit**.

Name	SHEN CHUN TE
Email	jundeshen@yahoo.com
Transaction ID	5SC492669W4196426
Original payment	NT$1 TWD
Amount Refunded by Seller	NT$0 TWD
Fees Refunded by PayPal	NT$1 TWD
Total Refund Amount	NT$1 TWD ?
Source of Funds	Balance

Note: If you don't have enough money in your PayPal account to cover this refund, we'll use your primary bank account for all of the refund.

Issue Refund Edit Cancel

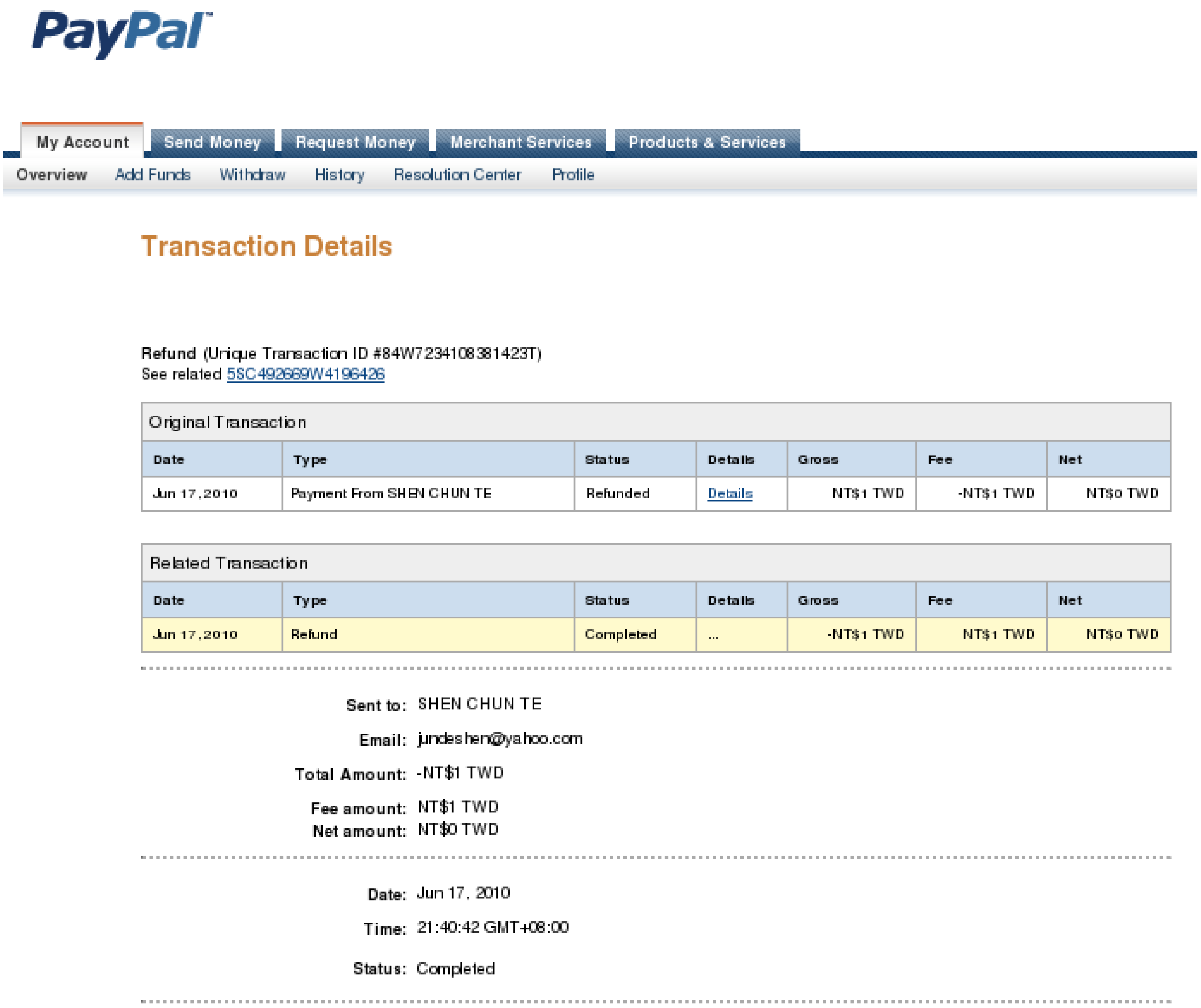
Step 6 : Go **My Account**, and verify **Transaction Details**.



My recent activity | Payments received | Payments sent
View all of my transactions
Archive
What's this
Payment status glossary

My recent activity - Last 7 days (Jun 10, 2010-Jun 17, 2010)

□	Date		Type	Name/Email	Payment status	Details	Order status/Actions	Gross
□	Jun 17, 2010		Fee Reversal From	Cancelled Fee	Completed	Details		NT$1 TWD
□	Jun 17, 2010		Refund To	SHEN CHUN TE	Completed	Details		-NT$1 TWD



Transaction Details

Refund (Unique Transaction ID #84W7234108381423T)
See related 5SC492669W4196426

Original Transaction

Date	Type	Status	Details	Gross	Fee	Net
Jun 17,2010	Payment From SHEN CHUN TE	Refunded	Details	NT$1 TWD	-NT$1 TWD	NT$0 TWD

Related Transaction

Date	Type	Status	Details	Gross	Fee	Net
Jun 17,2010	Refund	Completed	...	-NT$1 TWD	NT$1 TWD	NT$0 TWD

Sent to:	SHEN CHUN TE
Email:	jundeshen@yahoo.com
Total Amount:	-NT$1 TWD
Fee amount:	NT$1 TWD
Net amount:	NT$0 TWD

Date:	Jun 17, 2010
Time:	21:40:42 GMT+08:00
Status:	Completed