PheeNet

Network Access Control Gateway / Controller

User's Manual Ver.1.0.0 *WMS-308N*

Table of Contents

Chapter 1. Before You Start

1.1 Preface

The WMS-308N is a full-featured Network Access Control Gateway / Controller that aggregates up to 120 access points (APs), built-in 5000 local accounts/ on-demand accounts and delivers centralized control and security for wireless deployments.

The WMS-308N is designed for applications in which a compact, cost-effective"all-in-one" networking solution is required. The WMS-308N included a policy forced firewall, Intelligent Dual-WAN Load balance, Wireless LAN controller, IP sharing, and 4-Port Giga Ethernet switch in a desktop-mount enclosure. This device centrallized configuration and management model enables the controllers to be deployed, monitored, and controlled without local IT staff.

1.2 Package Contents

- WMS-308N x 1
- CD-ROM (With User Manual and QIG) x 1
- Power Adapter DC 12V 1.5A x 1
- RJ-45 Ethernet Cable 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

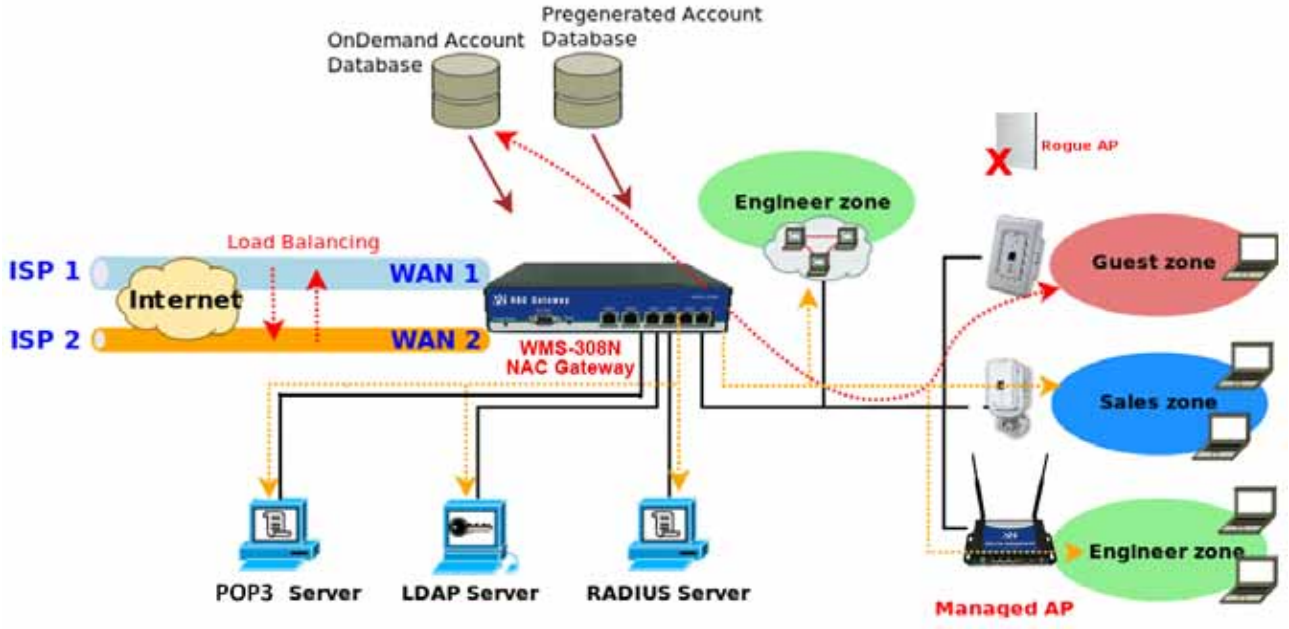
2.1 Introduction of WMS-308N

The WMS-308N – 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 environments. One single WMS-308N can serve up to 500 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 the owners set up public access services without extra RADIUS server.

2.2 System Concept

WMS-308N Network Access Gateway / 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, and 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

➢ Access Point Management and Support

➔ WMS-308N Network Access Gateway / Controller Support

- Max: 120 Access Points per Controller
- Max: 500 wireless client per Controller
- Provide Local Account : 5000

➔ AP Management – Control - Monitoring

- **Centralized AP Management**
  - ✓ AP Group management –maintain a set of setting templates that simplify the task to assign the same setting to multiple APs
  - ✓ AP-Automatic configuration and provisioning by WMS-308N
  - ✓ Locally maintained configuration profiles for managed APs
  - ✓ Auto discovery for managed APs
  - ✓ Automatic recovery of APs in case of system failure
  - ✓ Central firmware Upgrade-Select multiple APs and upgrade their firmware at the same time , including bulk upgrade
  - ✓ Remote Firmware upgrade
  - ✓ Zero Configuration technology to restore defective AP's setting onto the replacement AP
- **Central AP Control**
  - ✓ Provides MAC address Control list of client stations for each managed APs
  - ✓ Access Filter
  - ✓ Time-based AP access control
  - ✓ Single UI for upgrading and restoring managed APs' firmware
  - ✓ WLAN Partition – if enabled, WLAN clients are not allowed to exchange data through the AP (WAP-854NP, WAP-954GP, WAP-1954NP, WAP-1954NP-C, CPE-2010G / CPE-2000GN-1, WLO-15814N / WLO-15802N, WLO-12400N / WLO-12410N)
  - ✓ Max allowed APs
  - ✓ Support Roaming – Intra-Switch , Inter-band , Inter-Switch
- **Central AP Monitoring**
  - ✓ Monitor AP Status
  - ✓ The number of associated clients to the AP
  - ✓ The AP RF information
  - ✓ Associated Station List
  - ✓ Monitoring IP List
  - ✓ Load balancing based on number of users
  - ✓ Load balancing based on utilization

- ✓ AP User Statistic – Maintain all wireless clients connection history and depict statics in diagrams
- ✓ Support Monitor IP on third-party APs
- ✓ System alarms and status reports on managed APs
- ✓ Topology Monitor-list monitored device; periodically updates devices' status
- ✓ AP life check-real time tracking monitors APs status (AP Health Checking)
- ✓ Provide centralized remote management via HTTP/SNMP interface
- ✓ SYSLOG support including remote servers

➔ Radio Resource Management

- Automatic Channel Assignment and power setting for controlled APs
- Simultaneous air monitoring and end user service
- Self-healing coverage based on dynamic RF condition
- Dense deployment options for capacity optimizations
- Multiple BSSID per Radio: 8
- Hot Standby at AP mode (supports fail-over as a standby AP)
- Load Balance with another available AP (Real-time users limitation)
- Radio Management
- Coverage interference detection

➔ Wireless Encryption

- WPA personal and enterprise
- WPA2 personal and enterprise
- AES(CCMP): 128bit (FIP-197)
- WEP40/64 and 104/128-bit
- TKIP: RC4-40
- SSL and TLS: RC4 128-bit and RSA1024 and 2048 bit
- EAP-TLS, EAP-TTL/MSCHAPv2

➔ Wireless Security

- IEEE802.1X network login user authentication (EAP-MD5/TLS/TTLs)
- EAP over LAN (EAPoL) transport with PEAP and EAP-TLS authentication
- RADIUS server authentication (RFC2618)
- IEEE802.1X user authentication of controller management on controller Telnet and console sessions
- Multiple access privilege levels
- Hierarchical management and password protection for management interface
- EAP offload for AAA server scalability and survivability
- Stateful 802.1X authentication for standalone APs
- SSID and Location based authentication
- Multi-SSID support for operation of Multiple WLANs
- Simultaneous Centralized and distributed WLAN support

➔ Identity –Based Security

- 802.1X Authentication with WPA,WAP2 and 802.11i
- Local Accounts of 802.1X Authentication

- Support RADIUS /LDAP/POP3 for AAA server
- User Name and encryption key binding for strong network identity creation
- Local User Data Base for AAA fail-over protection

➔ **Wireless Roaming Support**

- Inter AP roaming
- Fast roaming
- L2 roaming

➢ User Management

➔ Support 500 simultaneous authentication users

➔ Max 5000 Pregenerated/ On-Demand/ Local RADIUS/ authentication users

➔ Users Session Management

➔ Configurable user Black list (with schedule)

➔ Allows MAC address and user identity binding for local user authentication

➔ Authentication methods supported: Pregenerated/ On-Demand, Local RADIUS, LDAP, and Remote RADIUS and POP3

➔ SSL protected login portal page

➔ Session and account expiration control

➔ User Log and traffic statistic notification via automatically email service

➔ Session limit control

➔ 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

➢ Service Domain

➔ Integrating with WAP-854NP/ WAP-954GP and other PheeNet products to have Service Domain feature and each Service Domain can have its own settings:

➔ The network is divided into maximum of 8 groups, each defined by VLAN Tag

➔ Each Domain has its own **(1) login portal page (2) authentication options (3) LAN/VLAN 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

➔ Types of authentication options (Local, POP3, RADIUS, LDAP, On-Demand and Pregenerated)

➔ Web login/ logout/ redirected page (customizable)

➔ Default Policy

- NAT or Route Mode
- Specific Route (WAN1 or WAN2 , or a specified gateway)
- Login schedule
- Bandwidth (max/min)

➢ Authentication

- ➔ Authentication : single sign-on (SSO) client with authentication integrated into the local authentication environment through local/domain, LDAP, RADIUS, POP3, MAC authentication
- ➔ 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 user identity binding for local user authentication
- ➔ No. Of Registered RADIUS Servers: 2
- ➔ Support MAC control list (ACL)
- ➔ Support Multiple Login service on one Accounts
- ➔ Support auto-expired guest accounts
- ➔ Users can be divided into user groups
- ➔ Each group (role) may get different network policies in different service zones
- ➔ Max simultaneous user session (TCP/UDP) limit
- ➔ Export/Import local users list to/from a text file
- ➔ Web-based Captive Portal for SSL browser-based authentication
- ➔ Authentication type
  - ■ IEEE802.1X (EAP, LEAP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-MD5)
- ➔ RFC2865 RADIUS Authentication
- ➔ RFC3579 RADIUS Support for EAP
- ➔ RFC3748 Extensible Authentication Protocol
- ➔ MAC Address authentication
- ➔ Web-based captive portal authentication

➢ Authorization

Authorization: access control to network resource such as protected network with Intranet, Internet, bandwidth, VPN, and full stateful packet firewall

➢ Accounting

- ➔ Provides billing plans for Pregenerated accounts
- ➔ Provides billing plans for On-Demand accounts
- ➔ Enables session expiration control for On-Demand accounts by time (hour) and data volume (MB)
- ➔ Detailed per-user traffic history based on time and data volume for both local and on-demand accounts
- ➔ Support local RADIUS and external RADIUS server
- ➔ Contain 10 configurable billing plans for on-demand accounts
- ➔ Support credit card billing system by PayPal
- ➔ Support automatic email network traffic history

➢ Dual WAN

- ➔ Load Balancing
  - ■ Outbound Fault Tolerance
  - ■ Outbound load balance

- Multiple Domain Support
- By Traffic

➔ Bandwidth Management by individual and distribution on different network(Service Domain)

➔ WAN Connection Detection

➢ Firewall

➔ Built-in DoS attack protection

➔ Inspection Full stateful packet filter

➔ Access Control List

➔ Multiple Domain Support

➔ Active Firewall Session – 16,000

➢ Network

➔ Support NAT or Router Mode

➔ Support Static IP, Dynamic IP (DHCP Client), PPPoE and PPTP on WAN connection

➔ DHCP Server per Interface; Multiple DHCP Networks

➔ 802.3 Bridging

➔ Proxy DNS/Dynamic DNS

➔ IP/Port destination redirection

➔ DMZ server mapping

➔ Virtual server mapping

➔ H.323 pass-through

➔ Built-in with DHCP server

➔ Support Static Routing

➔ Support RIP and OSPF Dynamic Routing

➔ Binding VLAN with Ethernet interface

➔ Support MAC Filter

➔ Support IP Filter

➔ Support Layer-7 protocol Filter and Web Content Filter

➔ Support Walled garden (free surfing zone)

➔ Support MAC-address and IP –address pass through

➔ **Support IP Plug and Play (IP PnP)**

➢ System Administration

➔ Three administrator accounts

➔ Provide customizable login and logout portal page

➔ CLI access (Remote Management) via Telnet and SSH

➔ Remote firmware upgrade (via the Web)

➔ Utilities to backup and restore the system configuration

➔ Full Statistics and Status Reporting

➔ Real-time traffic monitoring

➔ Ping Watchdog

➢ Network Management

- ➔ Event Syslog
- ➔ Status monitoring of on-line users
- ➔ IP-based monitoring of network devices
- ➔ Interface connection status
- ➔ Support Syslog for diagnosing and troubleshooting
- ➔ User traffic history logging
- ➔ User's session log can be sent to Syslog server
- ➔ Remote Syslog reporting to external server
- ➔ Traffic Analysis and Statistics
- ➔ SNMP v1, v2c, v3
- ➔ SNMP Traps to a list of IP Addresses
- ➔ Support MIB-II
- ➔ NTP Time Synchronization
- ➔ Administrative Access : HTTP / HTTPS

WMS-308N Hardware Specifications	
Base Platform	32-bit , MIPS24K Processor
CPU Clock Speed	680 MHz
Serial Port	1 (DB-9)
USB Port	1 (Optional 3G interface radio with major brands – ODM only)
Reset Switch Built-in	Push-button momentary contact switch
Ethernet Configuration	10/100/1000 BASE-TX auto-negotiation Ethernet port x 6 (RJ-45 connector) WAN * 2 LAN * 4
DRAM	On board : 256Mbytes
Flash	On board : 32 Mbytes
CF Socket	1 (reserved for option)
Built-In LED Indicators	1 * Power ; 1 * Status, 1 * Net Status (This is for AP management, when system can't detect managed AP)
Environmental & Mechanical Characteristics	
Operating Temperature	0 °C ~ 55 °C
Storage Temperature	-20 °C ~ 75 °C
Operating Humidity	10% to 80% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Power Supply	110 – 220V AC Power; 12 VDC, 1.5A input.
Unit Dimensions	243 x 150 x 45.5 (mm) (Width x Depth x Height)
Unit Weight	1.4 Kg
Form Factor	Wall Mountable , Metal case
Certifications	FCC/CE

Chapter 3. Base Installations

3.1 Installations

3.1.1 System Requirements

- Standard 10/100/1000Base 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/Status :**

   ➔ **LED Green ON** indicates power on, **OFF** indicates power off.

   ➔ When system restart, **LED Amber** will flash **three** times after system up.

   ➔ **LED Amber ON** indicate the Flash is busy(For example, format database, create or delete accounts...etc)

2. **Console :** The serial RS-232 DB9 cable attaches here.
3. **Reset :** Press and hold the button for more than **10** seconds until Power/Status **LED Amber FLASH** to reset the system to default configurations. After you release button, the **LED Amber will ON** and system's database will be formatted until **LED Green ON** to restart system.
4. **WAN1/WAN2 :** Two WAN ports are available on the system. **LED Green ON** indicates **10/100**-Mbps link is established on the port. **LED Amber ON** indicates **1000**-Mbps link is established on the port.
5. **LAN :** Clients devices connect to WMS-308N via LAN ports

Rear Panel

1. **Power SOCKET (12V DC) :** Attach the power socket here.

3.1.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of WMS-308N

1. Place the WMS-308N at a best location.

The best location for WMS-308N is usually at the center of your wireless network.

2. Connect WMS-308N to your outbound network device.

Connect one end of the Ethernet cable to the WAN1/WAN2 port of WMS-308N 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 WMS-308N to your network device.

Connect one end of the Ethernet cable to LAN port of WMS-308N 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. Connect the DC power adapter to the WMS-308N power socket on the rear panel.

Please only use the power adapter supplied with the WMS-308N package. Using a different power adapter may damage this system

Now, the hardware installation is completed.

To double verify the wired connection between WMS-308N 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 port of WMS-308N. An IP address will be assigned to the PC automatically via the WMS-308N.

2. Launch a web browser to access the web GUI of WMS-308N by entering "**http://192.168.2.254**" in the address field.

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.

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.x 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 WMS-308N

  Username : **root**

  Password : **default**

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

  Username : **admin**

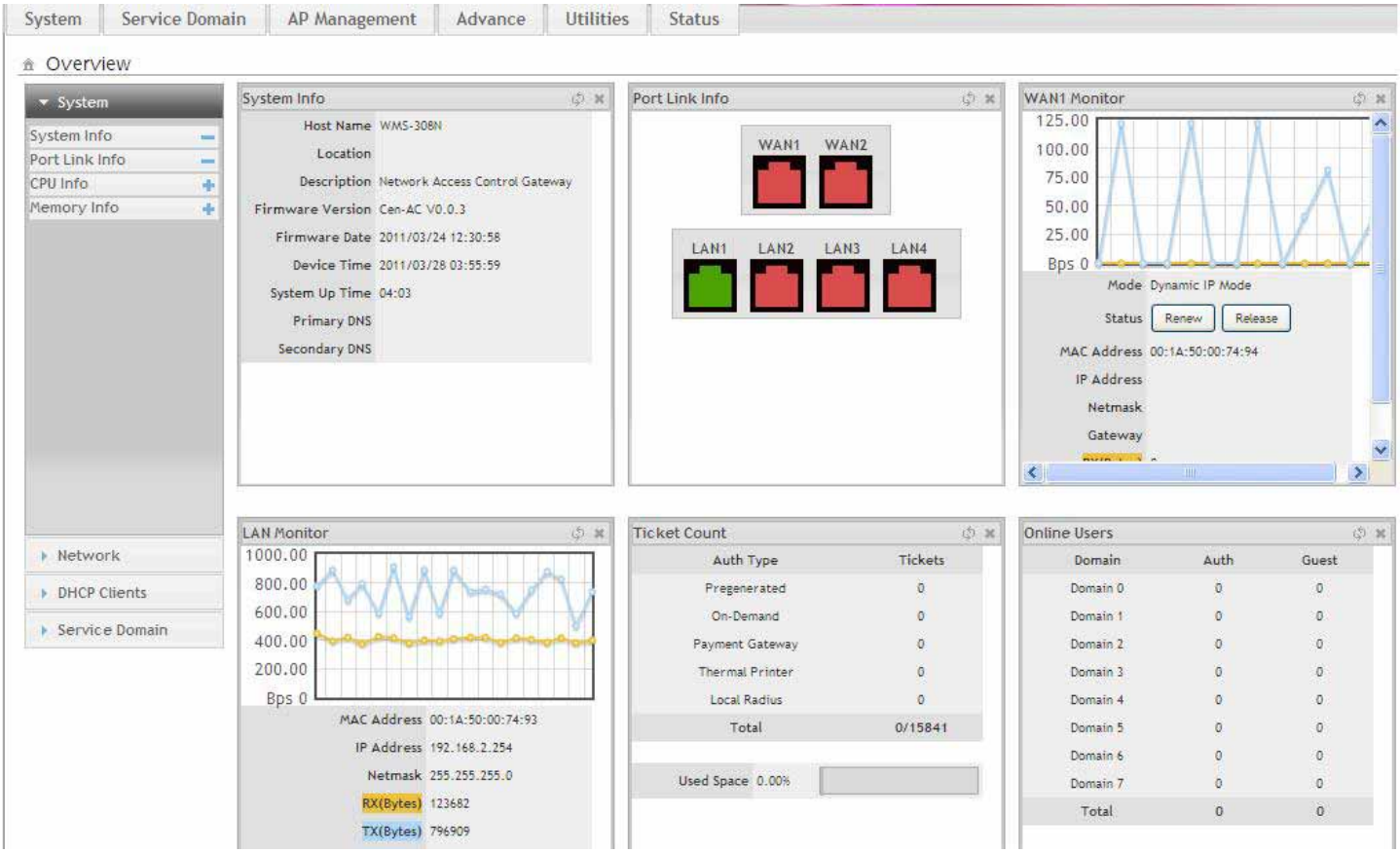
  Password : **admin**

- 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.



3.2.2 Quick Configuration

WMS-308N 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. WMS-308N 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.

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

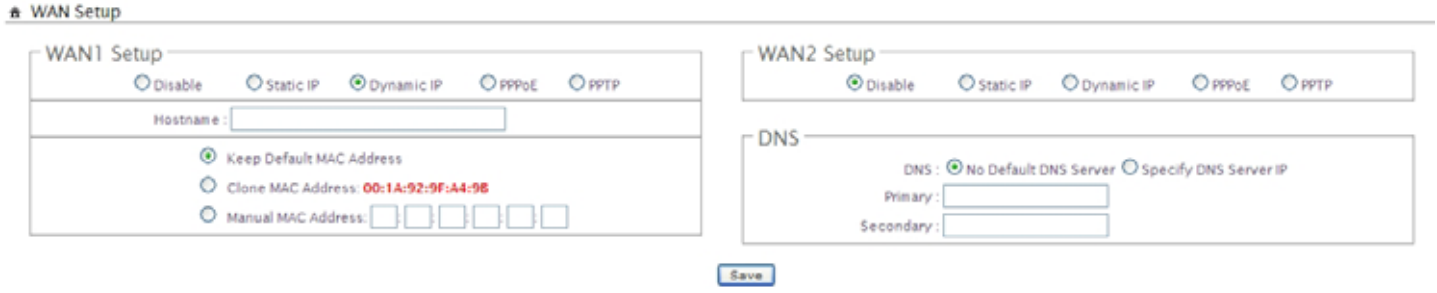
Step 2 : Select Connection Type for WAN1 Port and Set DNS Server

➔ 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.

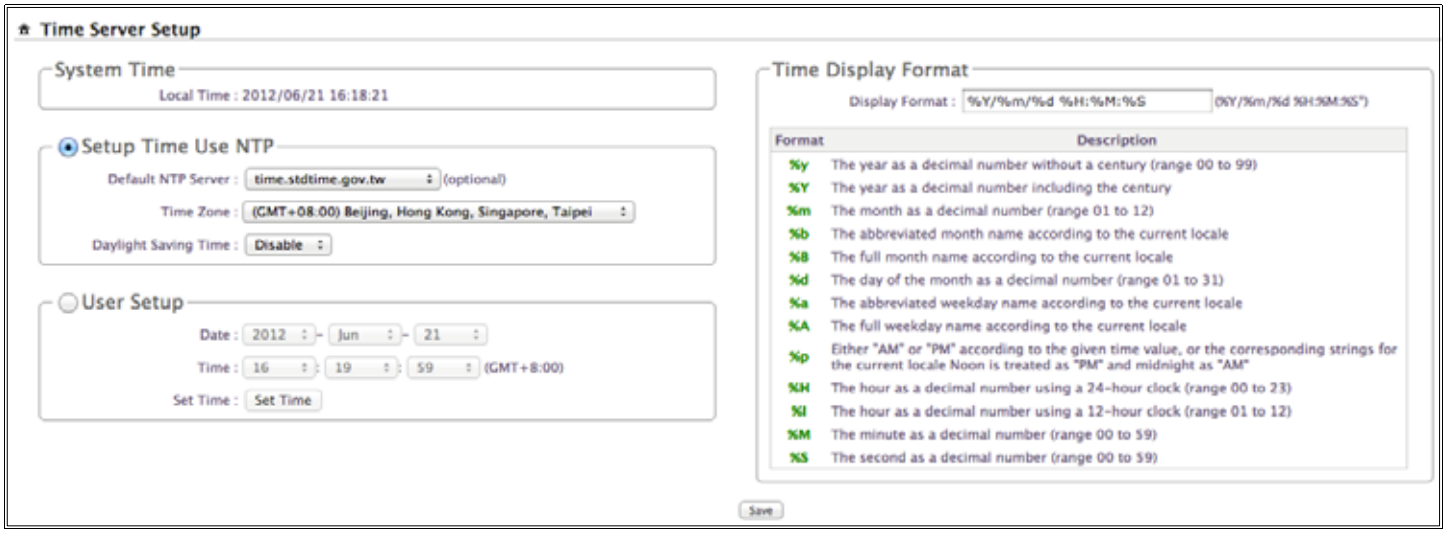
➔ Click ***Save*** button.



Step 3 : Choose System's Time

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

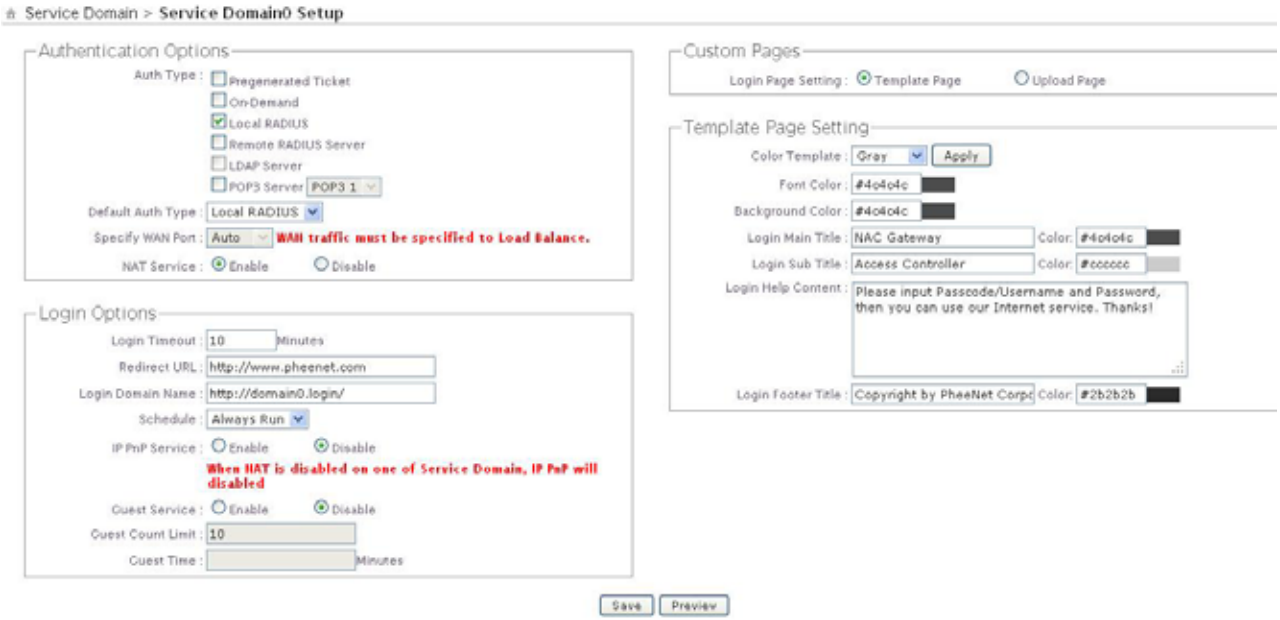
➔ Select the appropriate setting and Click ***Save*** button.



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

Step 4 : Select Authentication Type for Service Domain

➔ Click **Service Domain** → **Service Domain0**, the Service Domain0 Setup page will appear, for each Service Domain, authentication type can be selected in ***Pregenerated Ticket***, ***On-Demand***, ***Local RADIUS***, ***Remote RADIUS Server***, ***LDAP Server*** and ***POP3***, and select one authentication type for Default Auth Type. Below depicts an example for **Local RADIUS**.

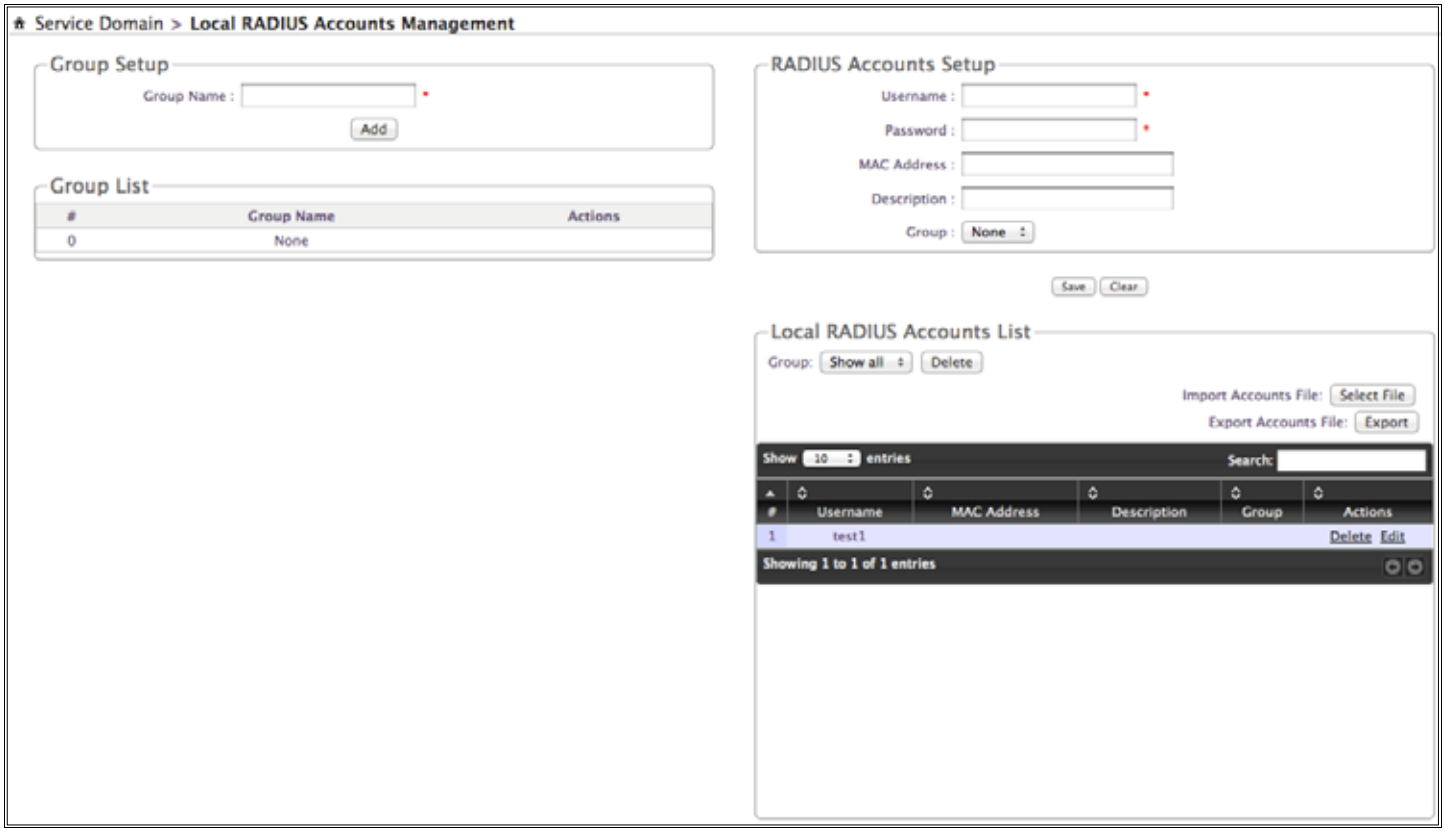


➔ Select ***Local Radius*** for Service Domain0's Authentication Type.

➔ Click ***Save*** button.

Step 5 : Add Local Radius Accounts

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

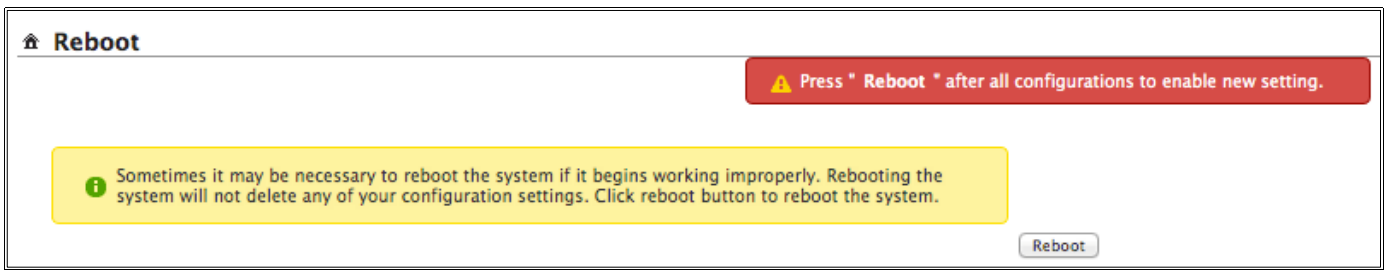


➔ A new account can be added into the Local Radius Database. To add a account here, enter the Username (e.g. **test1**), Password (e.g. **11111**), MAC Address(optional, to specify the valid MAC address of this account) and Description.

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

Step 6 : Restart WMS-308N

➔ Click ***Reboot*** button to start 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:

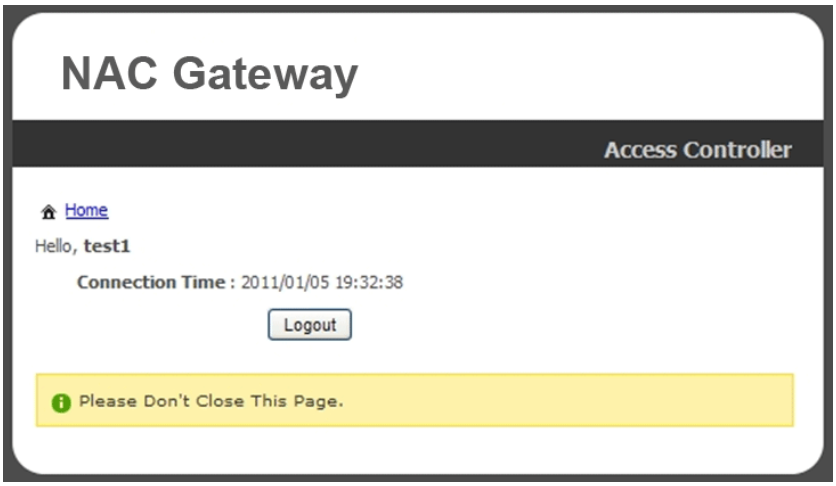
Step :

1. Connect a client device (e.g. Notebook) with wireless interface to scan the configured ESSID of WMS-308N (e.g. **AP00**) and get associated with this ESSID.
2. The client device will obtain an IP address automatically via DHCP from WMS-308N. Open a web browser on a client device, access any URL, and then the Domain0's **User Login Page** will appear.

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 WMS-308N and has been authenticated by the system. Now, you are connected the network and Internet!



Chapter 4. Web Interface Configuration

WMS-308N provides functions as stated below where they can be configured via a user-friendly web based interface.

OPTION	System	Service Domain	AP Management	Advanced	Utilities	Status
Function	WAN	Service Domain	Device Discovery	DMZ	Profile Setting	Overview
	WAN Traffic	Authentication	Batch Setup Management	IP Filter	Firmware Upgrade	Extra Info
	LAN	Privilege List	Group Setup Management	MAC Filter	Network Utility	Event Log
	DDNS	Walled Garden	Traffic Monitor	Virtual Server	USB Storage Setup	
	Management	Notification	Group Status	Blacklist	Format Database	
	Time Server	Online Users	Rogue AP Detection	IP Routing	Reboot	
	SNMP	Log Info	Website Monitor	Time Policy		

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 WMS-308N to the external Network

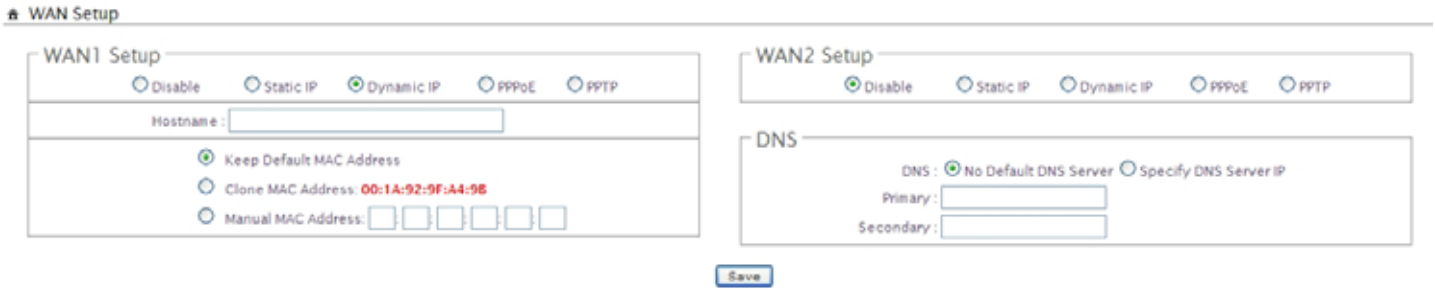
4.1.1 Network Requirement

Basically, in general network environment, the main role of WMS-308N is a Gateway. It manages the entire network from internal network to Internet.

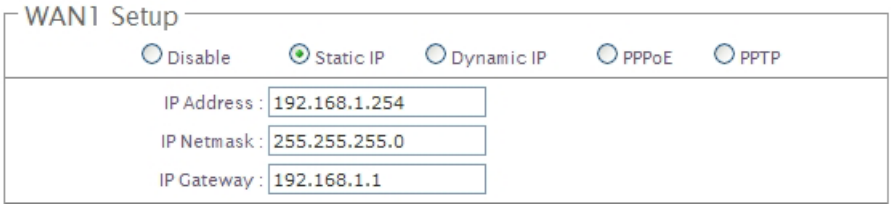
Then, the first step is to prepare an Internet connection from your ISP and connect it to the WAN or WAN2 port of WMS-308N.

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.



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



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

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

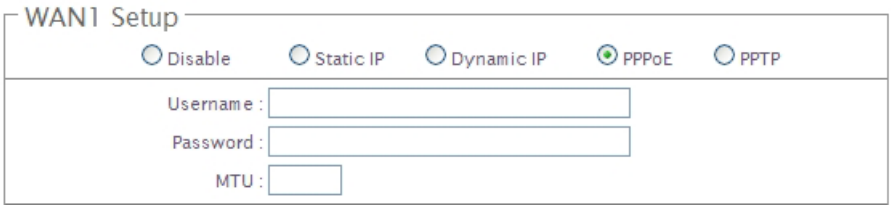
➔ **IP Gateway :** The IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. WMS-308N will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the WMS-308N'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 WMS-308N is connected to a network with the presence of a PPPoE server.

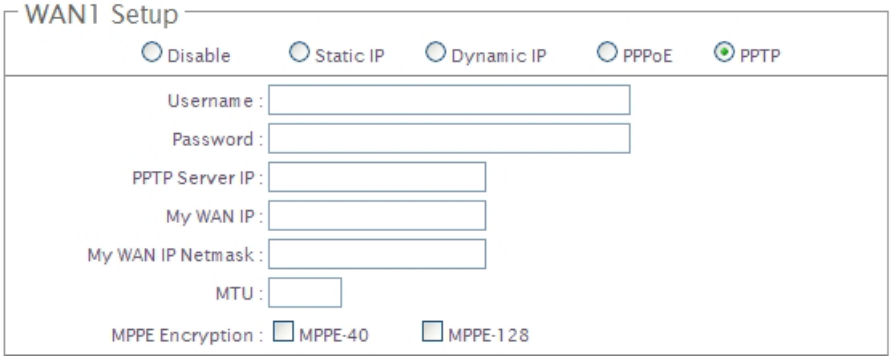


  ➔ **User Name :** Enter User Name for PPPoE connection

  ➔ **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.



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

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

  ➔ **PPTP Server IP :** 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 :** Select “No Default DNS Server” or “Specify DNS Server IP” option 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.

Change these settings as described here and 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).

- **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 WMS-308N 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 WMS-308N 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.

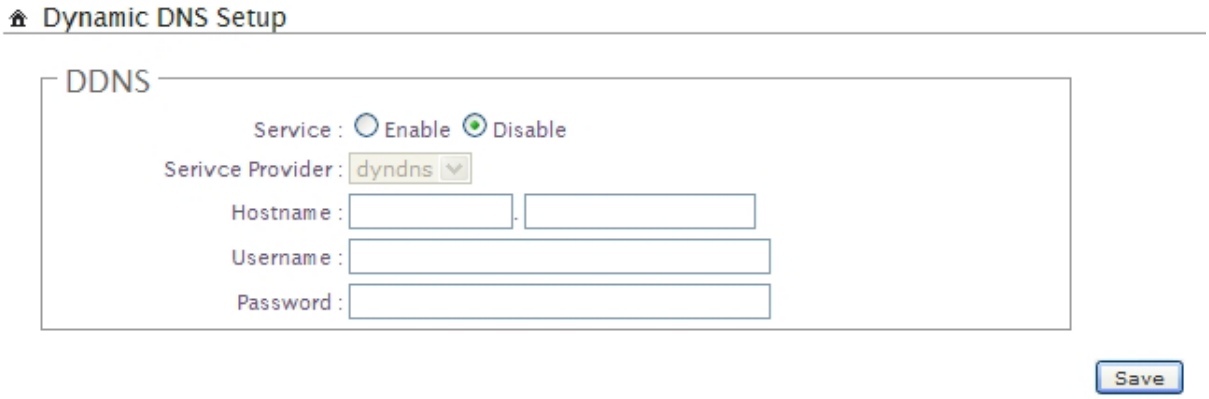
If "Connection Detection" is **disabled** and the PHY's connection status shows **Red**(Status → Port Link Info). the system will detect PHY on every **5** seconds. When system detect failure **1** times, the traffic of package will routed via **Secondary** WAN Interface. When Primary WAN Interface detect **1** time success, the traffic of package will routed via **Primary** WAN Interface.

If "Connection Detection" is **disabled** and the PHY's connection is **Green**(Status → Port Link Info), the system will detect remote Gateway IP address of Primary WAN on every **5** seconds. When system detect failure **3** times, the traffic of package will routed via **Secondary** WAN Interface. When Primary WAN Interface detect **1** time success, the traffic of package will routed via **Primary** WAN Interface.

Change these settings as described here and 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.

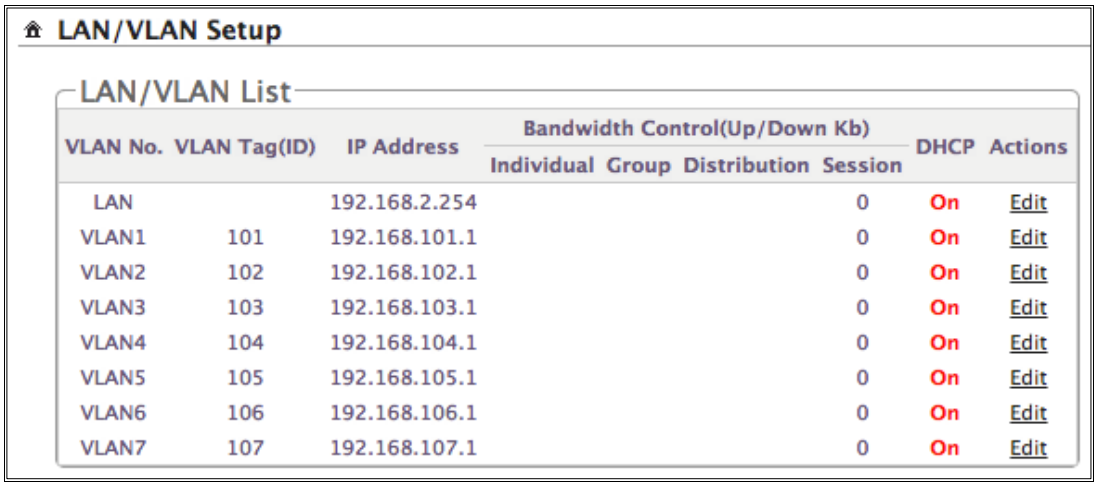


- **Service:** By default, it's "**Disable**". To "**Enable**" to activate this function. Each time your IP address for WAN is changed, the information will be updated to DDNS service provider automatically.
- **Service Provider:** Select the correct Service Provider from the drop-down list, here included are *dyndns*, *dhs*, *ods* and *tzo* embedded in the WMS-308N.
- **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.

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

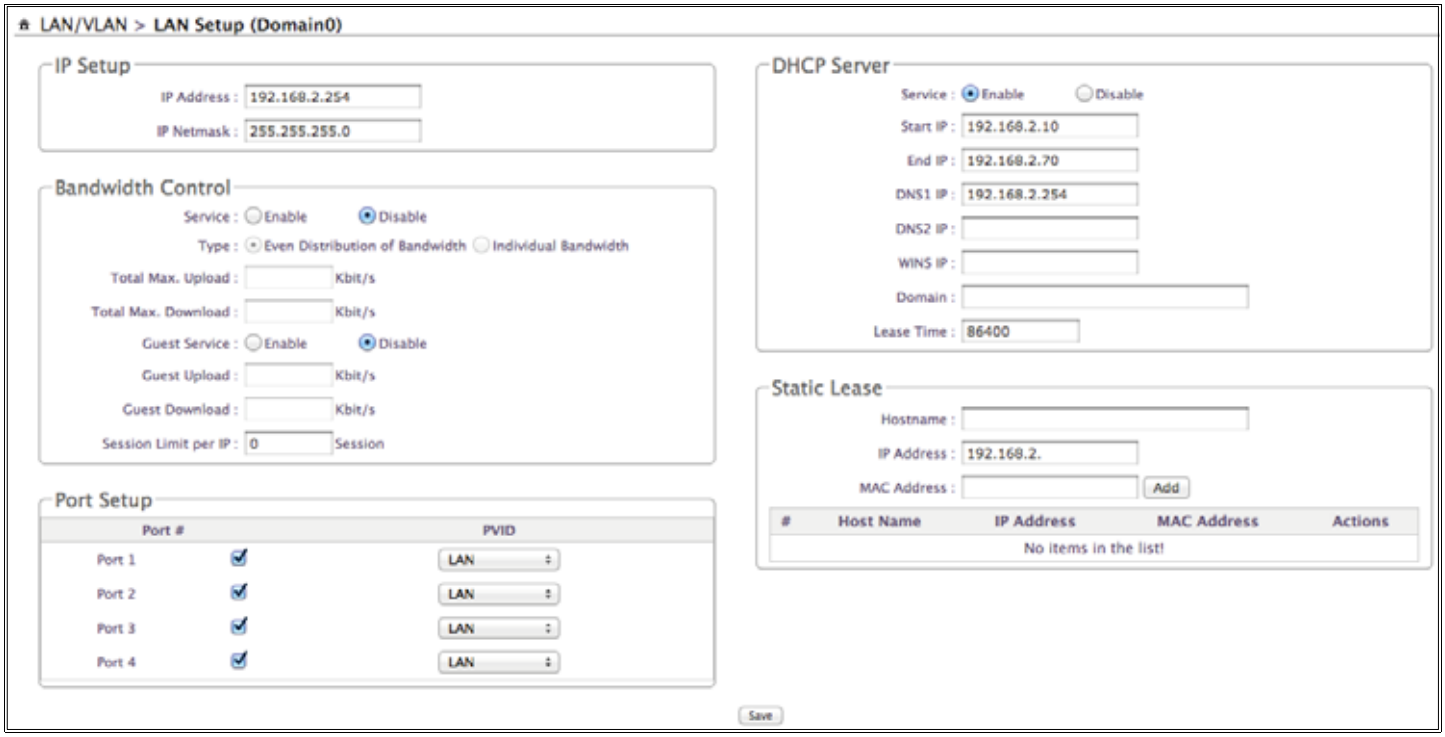
4.1.5 Configure Local(LAN/VLAN) Network

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.



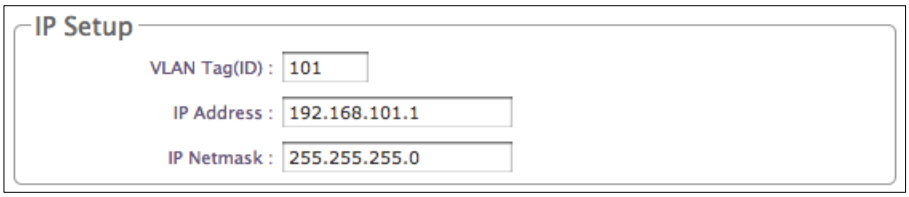
VLAN No.	VLAN Tag(ID)	IP Address	Bandwidth Control(Up/Down Kb)				DHCP	Actions
			Individual	Group	Distribution	Session		
LAN		192.168.2.254				0	On	Edit
VLAN1	101	192.168.101.1				0	On	Edit
VLAN2	102	192.168.102.1				0	On	Edit
VLAN3	103	192.168.103.1				0	On	Edit
VLAN4	104	192.168.104.1				0	On	Edit
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

- **VLAN No. :** Denote the system's VLAN port.
- **VLAN Tag(ID) :** Denote the VLAN tag of the respective VLAN port. Only for VLAN1 ~ VLAN7
- **IP Address :** Denote the IP address of the respective LAN/VLAN port.
- **Individual :** Denote the Individual Max. Upload/Download of the respective LAN/VLAN port.
- **Group :** Denote the Group Upload/Download of the respective LAN/VLAN port.
- **Distribution :** Denote the Distribution Upload/Download of the respective LAN/VLAN port.
- **Session :** Denote the Session of the respective LAN/VLAN port.
- **DHCP :** Denote the DHCP server status of the respective LAN/VLAN.
- **Actions :** Click this option to configure LAN/VLAN's settings, the setup page should be appear. Below depicts an example for **LAN**..



- **IP Setup :**

  ➔ **VLAN Tag(ID) :** Virtual LAN, the system supports **7** tagged VLAN port (VLAN1 ~ VLAN7). The valid values are from **1** to **4094**. The default VLAN1's tag ~ VLAN7's tag are from 101 to 107



Some system and VLAN switch do not support VLAN tag 1

  ➔ **IP Address :** The IP address of the LAN/VLAN port; The default LAN's IP address as **192.168.2.254**, and 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 activate bandwidth control service.

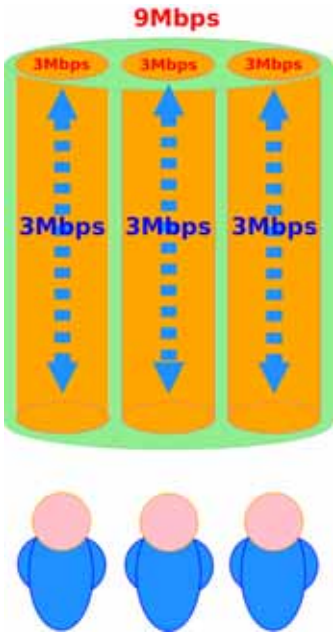
  ➔ **Type :** Enable the desire option among "**Even Distribution of Bandwidth**" or "**Individual Bandwidth**".

  ➔ **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.

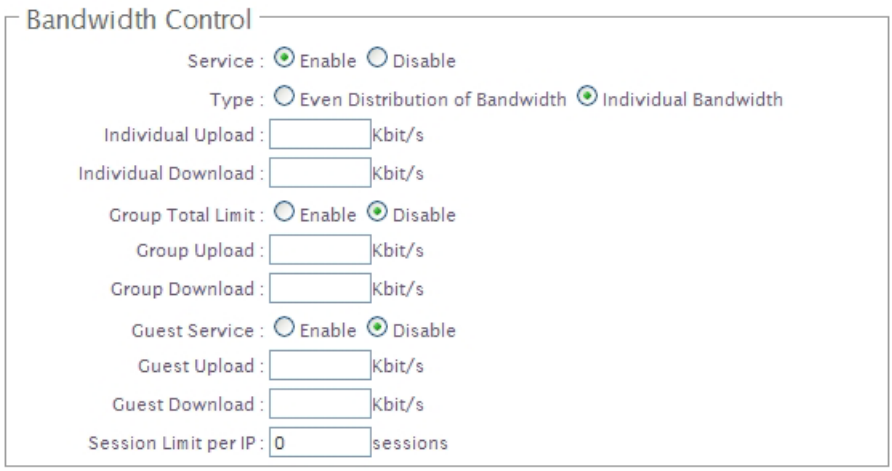
  ✓ **Total Max. Upload :** The Total Max. Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited,

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



➔ **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.

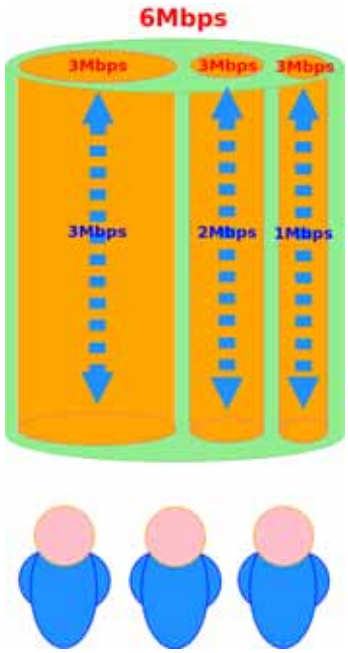


✓ **Individual Upload :** The Individual Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

✓ **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
- **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.

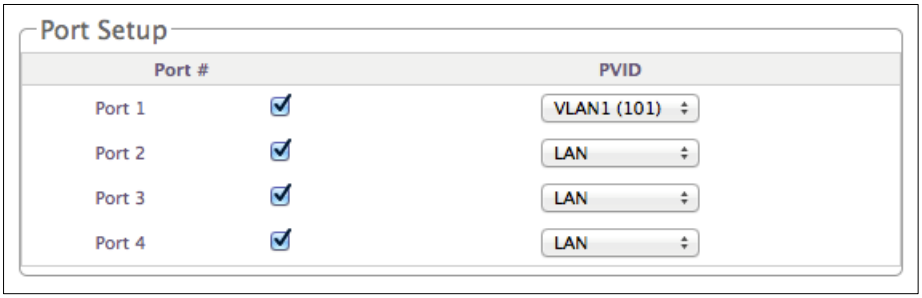
✓ **Guest Upload :** The Guest Upload is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

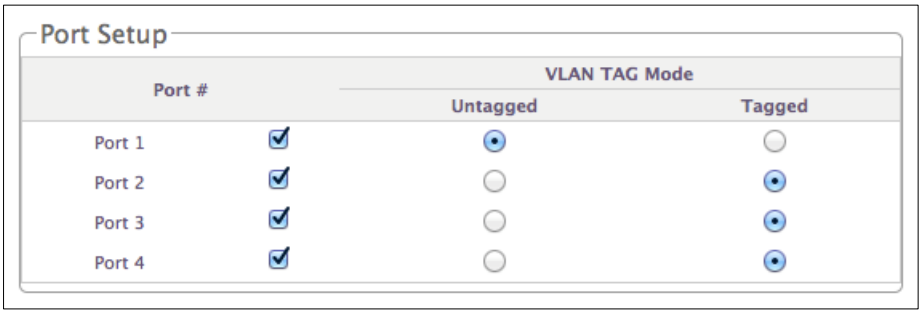
✓ **Guest Download :** The Guest Download is in the range of **0~102400** Kbit/s, 0 indicates unlimited, default is **512** Kbit/s

➔ **Session Limit per IP :** The number of sessions is in the range of **10~500**, 0 indicates unlimited, default is **0**.

■ **Port Setup :** The port setup is different between LAN and VLAN Setup page. On the LAN Setup page, the system manager can set each port's PVID. On the VLAN# Setup page, the system manager can set tagged or untagged on each port.

Please note that the VLAN's port was set to untagged, the port need set PVID instead of port. For example, if you need untagged's clients connect to **Server Domain1**(**VLAN1**) via **Port 1**, the Port 1 need set to Port-based VLAN. The Port 1 need enabled and select PVID in **VLAN1** on **LAN Setup** page, then the Port 1 select **Untagged** in VLAN TAG Mode on **VLAN1 Setup** page.





➔ **Port :** Indicate the system's RJ-45 interface port. By default; it's enabled. To disable to unactivated LAN's or VLAN's port.

➔ **PVID :** Port VID, Select desired default VLAN ID on the respective port, all untagged packets arriving at the device are tagged with the port PVID.

➔ **VLAN TAG Mode :** Select **Tagged** or **Untagged** on the respective port.

■ **DHCP Server :**

➔ **Service :** 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 WMS-308N.

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

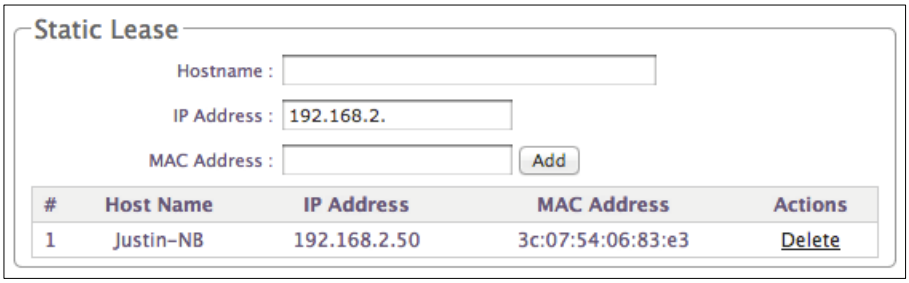
DNS2 server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

➔ **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.

- **Static Lease :** If you want a computer or device to always have the same IP address assigned, you can create a static lease. The system will assign the IP address only to that computer or device. There are maximum **50** rules allowed in this list.
  - **Hostname :** Enter the hostname of the computer or device.
  - **IP Address :** Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.
  - **MAC Address :** Enter the MAC address of the computer or device.
  - **Actions :** Click an action button to perform the appropriate action.
    - **Delete :** Click this button to remove the lease for a specific LAN device and free an entry in the lease table.

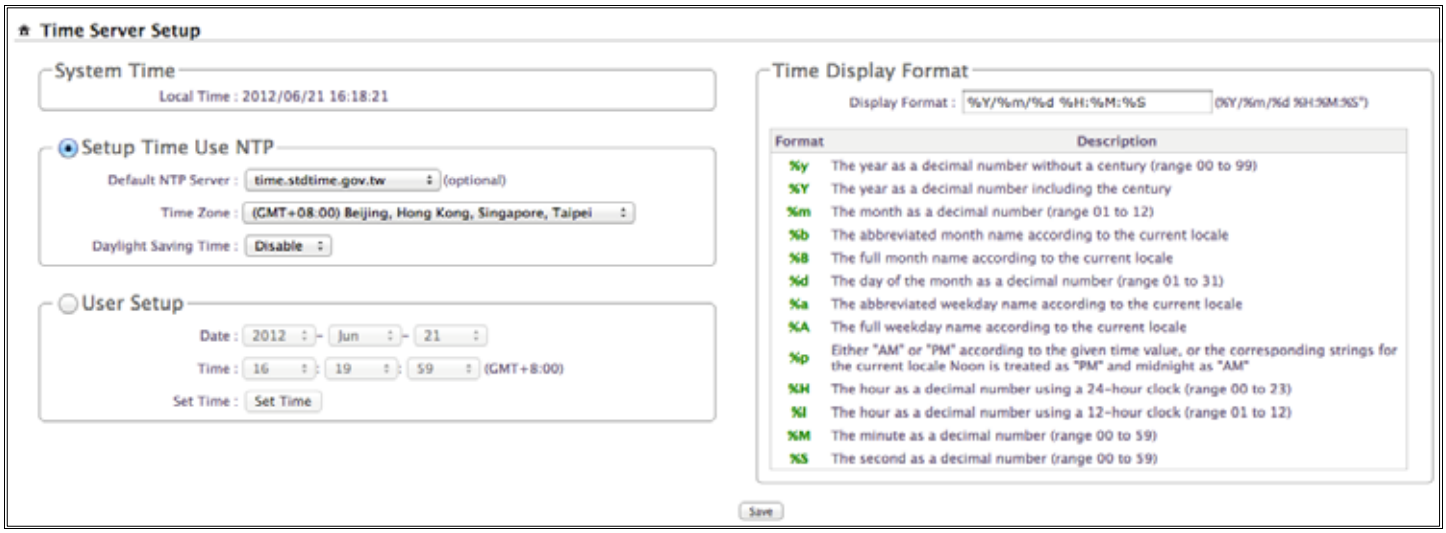


➔ Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2 Manage the System

4.2.1 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 :** Denote 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.

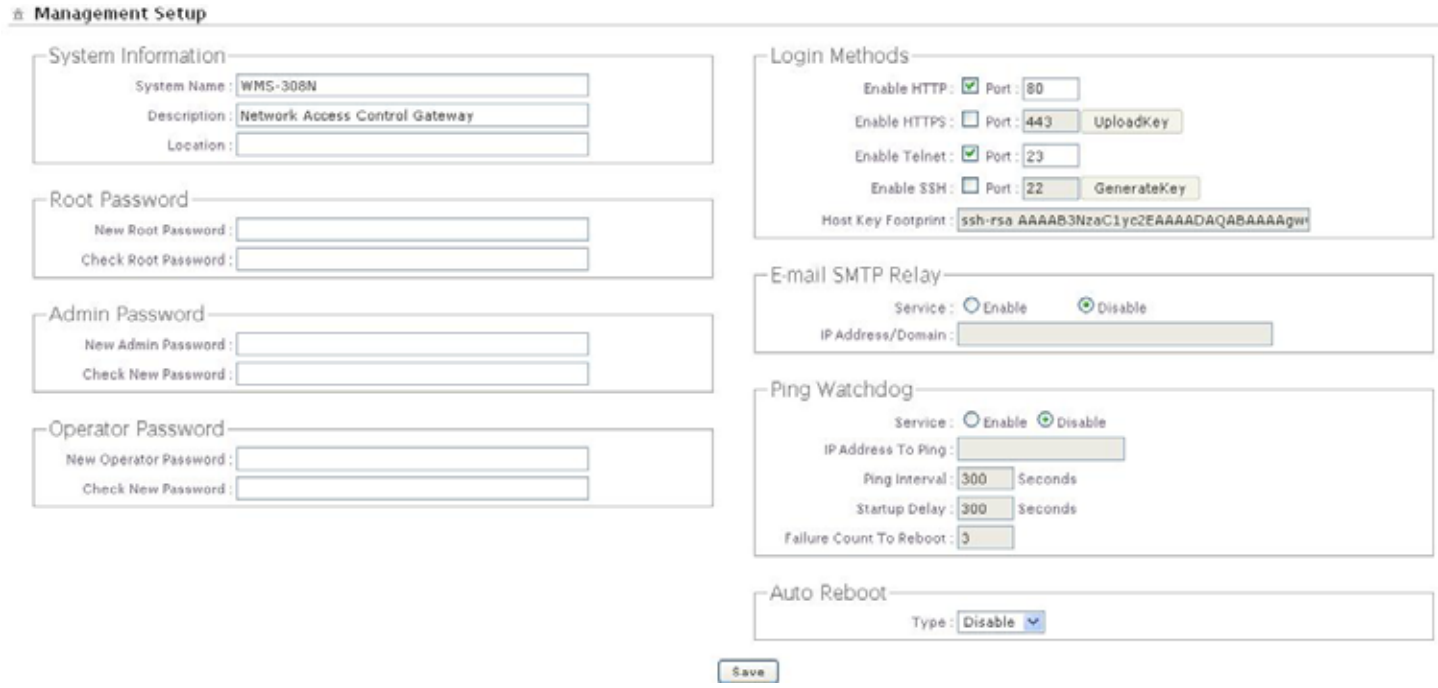
If Time server setting selected in “Setup Time User NTP”, please verify system's Default Gateway and DNS setting first.

- **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

4.2.2 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 :** 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 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.

The configure of SMTP server can't set encryption and authentication. The IP address of SMTP server can't set on LAN's subnet.

恩

- **Ping Watchdog :** The ping watchdog sets the WMS-308N 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 WMS-308N 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.

  ➔ **Service :** Click ***Enable*** to activated 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.

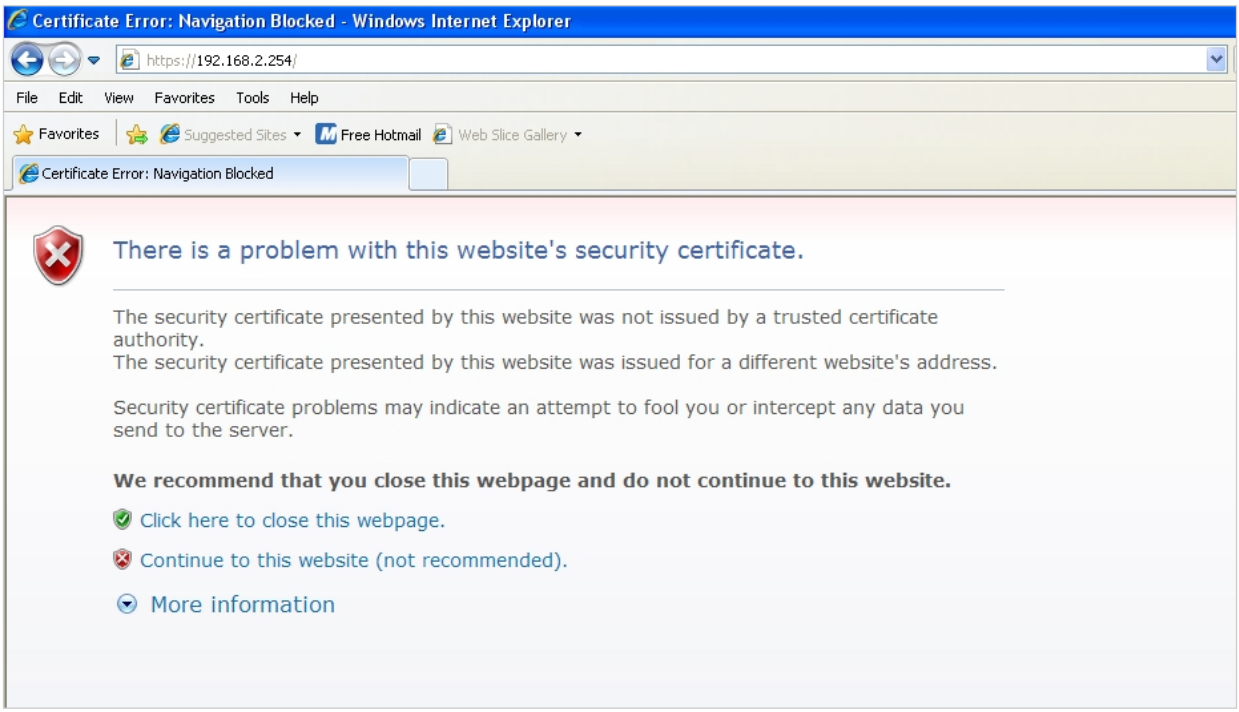
- ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device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

■ **Auto Reboot :**

- ➔ **Type :** There are four types can be selected : **Disable**, **Daily**, **Weekly** or **Monthly**, choose either the daily , weekly or monthly in your specify time to restart system

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 WMS-308N's GUI (https://192.168.2.254). There will be a “Certificate Error”, because the browser treats WMS-308N as an illegal website.



Click “***Continue to this website***” to access the WMS-308N's GUI. The WMS-308N's Home page will be appear.

4.2.3 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.

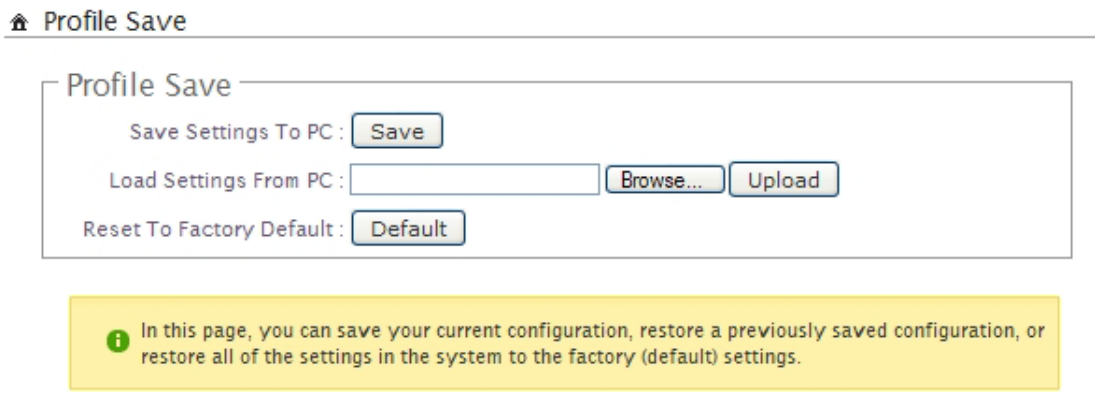
- **SNMP v2c Enable :** Check to enable SNMP v2c.
  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.
- **SNMP v3 Enable :** Check to enable SNMP v3.

  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.

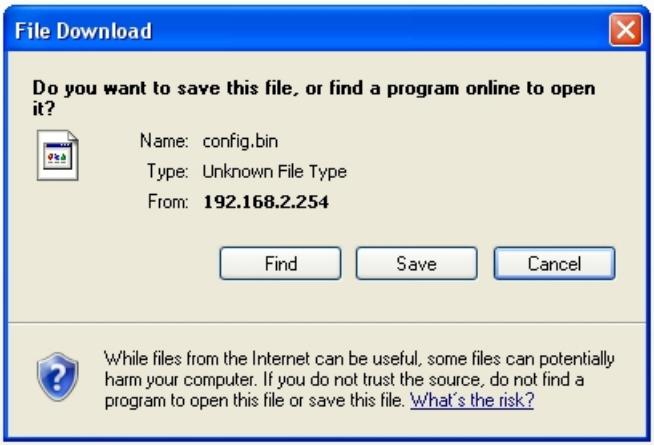
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2.4 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.



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



- **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.

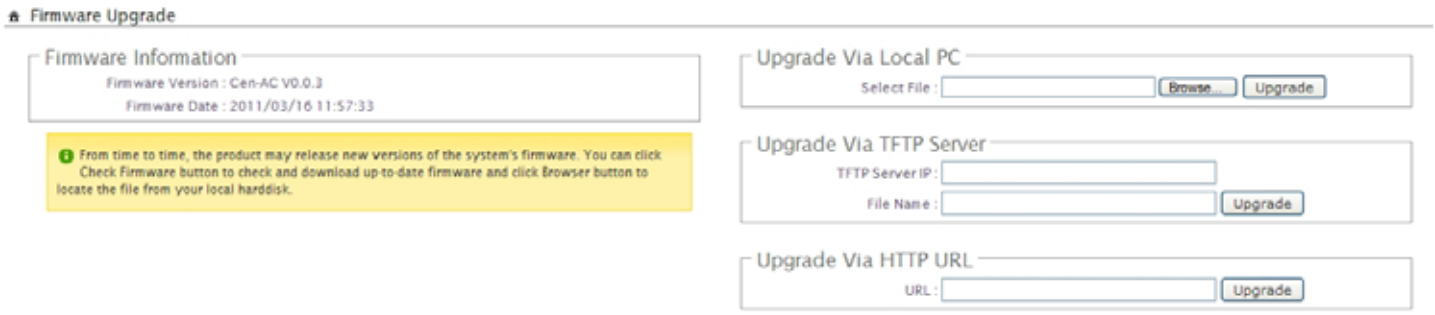
- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings. The system will **restart** after uploading configuration and database.

1. Do not interrupt during Profile upload or Reset to Default including power on/off as this may damage system.
2. While Profile upload or Reset to Default, the Power/Status Green LED will change to Amber LED.

4.2.5 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. It might take a few minutes before the upgrade process completes and the system needs to be restarted to activate the new firmware.

Please click on **Utilities** → **Firmware Upgrade** and follow the below setting.



- **Upgrade Via Local PC :** Click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.
- **Upgrade Via TFTP Server :** Enter TFTP Server IP address and firmware file, and then click Upgrade button to upgrade.
- **Upgrade Via HTTP URL :** Enter URL address(example : http://192.168.2.10/xxx.bin), and then click Upgrade button to upgrade.

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.

4.2.6 Network Utility

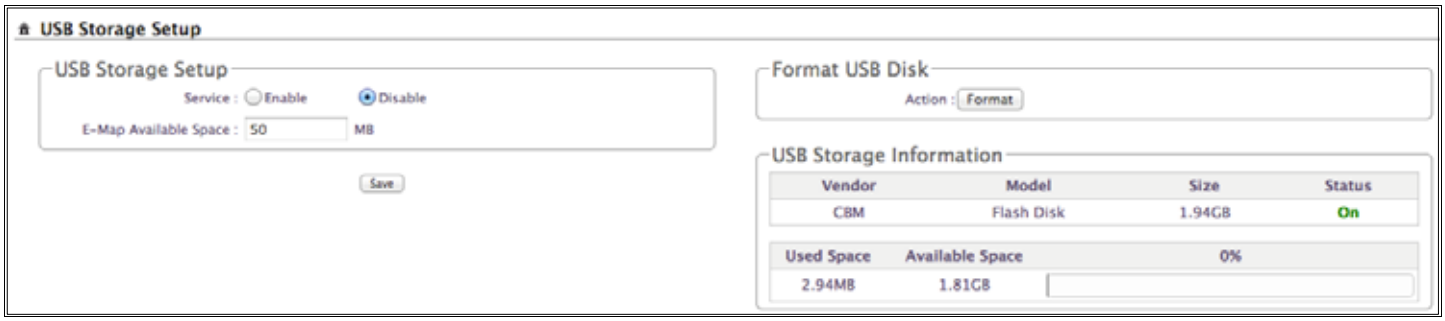
The administrator can diagnose network connectivity via the PING utility.

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

- **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 WMS-308N 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.
- **Lookup IP :** This utility will covert a host or domain name into IP address. The test is started using the **Start** button, click **Stop** button to stopped test
  - ➔ **Domain :** Specifies the host or domain for converting
  - ➔ **Count :** By default, it's 10 and the range is from 1 to 99. It indicates number of converting test.

4.2.7 USB Storage Setup

This function allows administrator to setup USB storage device for save more e-map, custom portal login page and managed AP's profile. Please click on **Utilities** → **USB Storage Setup** and follow the below setting.



- **USB Storage Setup :** Select **Enable** Service to activate USB storage function. The **Upload File Space Size** is in the range of **10~100** MB, default is **50** MB. This space size is for e-map, custom portal login page and managed AP's profile
- **Format USB Disk :** Click ***Format*** button to format USB storage device.

If you want to copy e-map, custom portal page and managed AP's profile to external USB storage, you must click **Format** button first, then **Enable** USB Storage Service.

- **USB Storage Information :** Show detail informations of USB storage device. If the status shows Off, you should click ***Format*** button to activated.

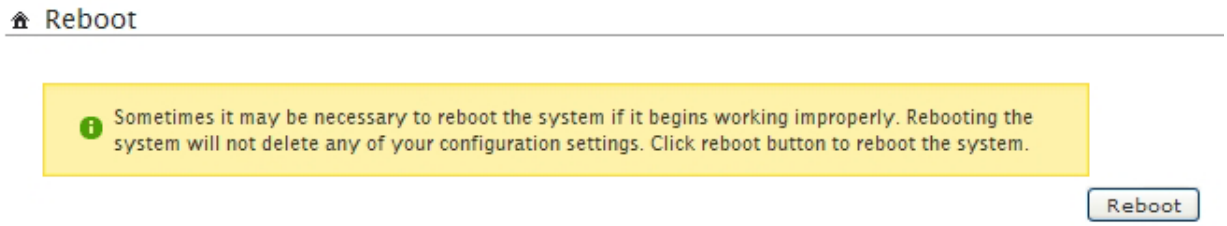
4.2.8 Format Database

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

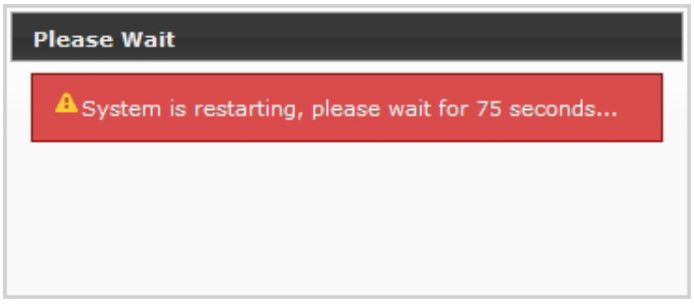
1. Do not interrupt during format database including power on/off as this may damage system.
2. While system format database, the Power/Status **Green** LED will change to **Amber** LED.

4.2.8 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. Please click on **Utilities** → **Reboot**
- ✓ and follow the below setting.



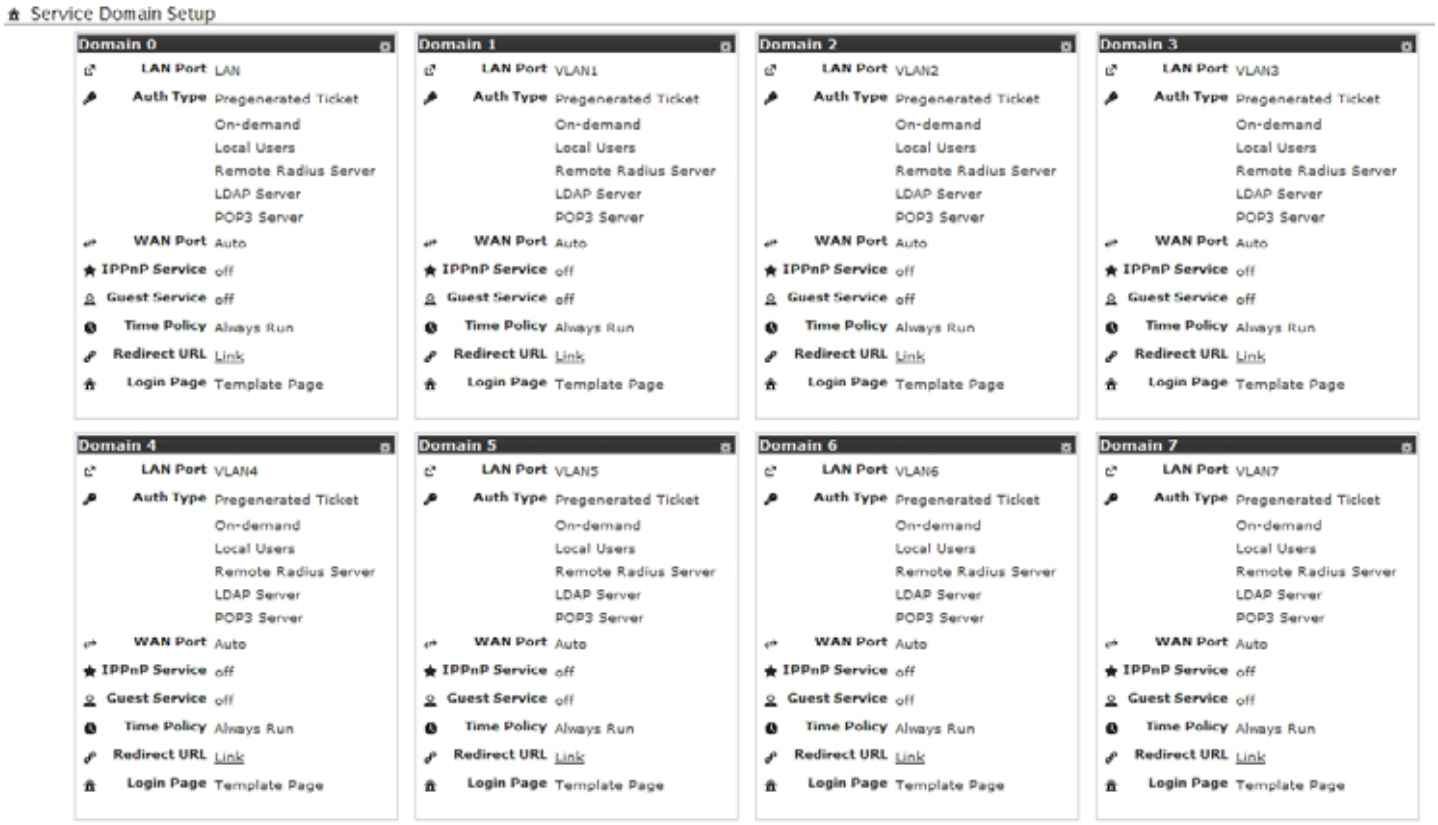
A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



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

4.3 Access To External Network With Service Domain

WMS-308N supports **8** Service Domain, administrator can quickly setup via this page.

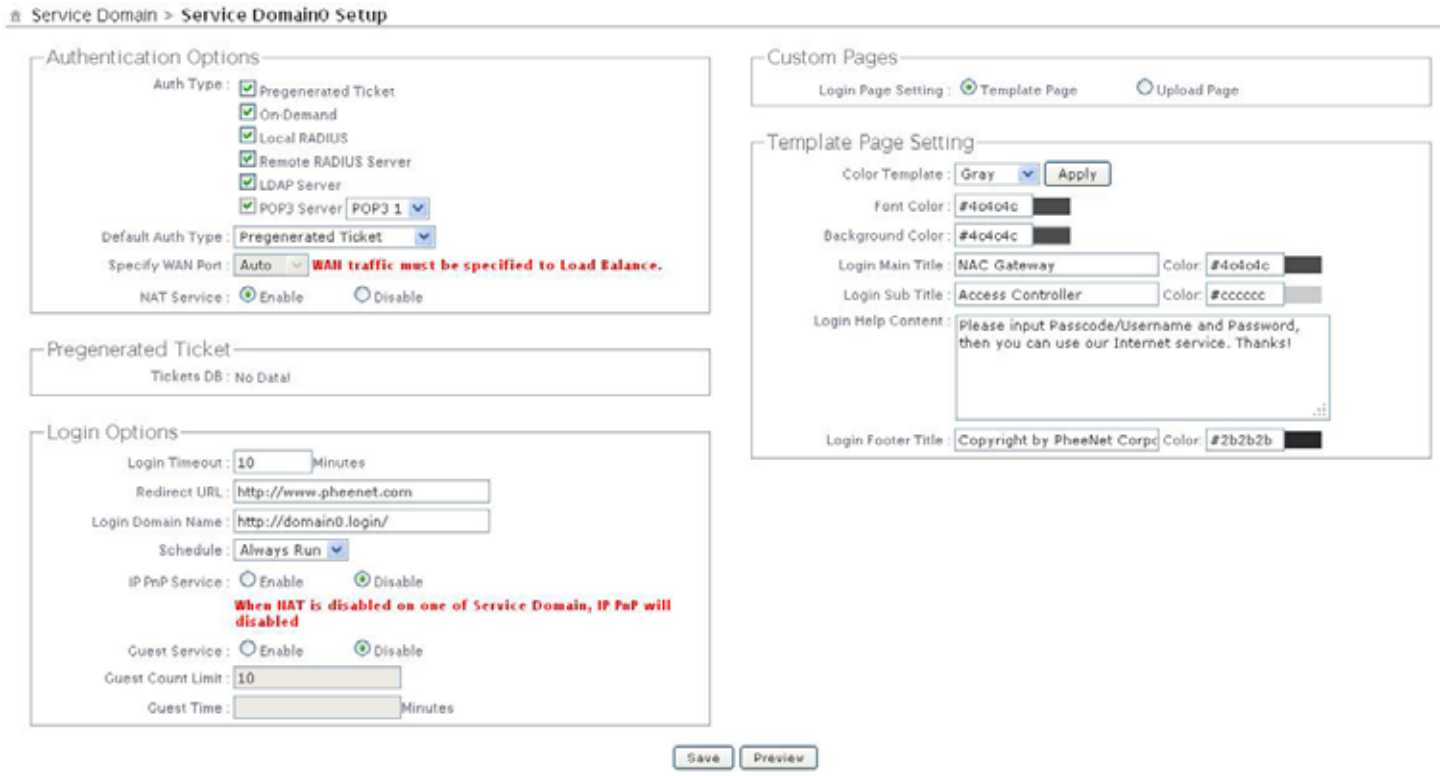


- **LAN Port :** The bonding interface for the respective Service Domain
- **Auth Type :** The authentication type for the respective Service Domain. There are **Six** types : Pregenereated Ticket. On-demand, Local Users, Remote Radius Server, LDAP and POP3.
- **WAN Port :** Denote the outgoing traffic for the respective Service Domain.
- **IPPnP Service :** Denote status of IP PnP service for the respective Service Domain.
- **Guest Service :** Denote status of Guest service for the respective Service Domain.
- **Schedule :** Denote the schedule of authentication service on the respective Service Domain.
- **Redirect URL :** The redirect URL for this Login page of Service Domain.
- **Login Page :** Denote the custom page for this Service Domain. There are two types : **Template** page or Upload page
- **:** Click tools icon on the top-right corner of each Domain settings window, the Service Domain page will pop-up.

4.3.1 Configure Service Domain

Administrator can configure Service Domain with different authentication service type, specified outgoing traffic, 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 :** Select authentication type for the respective Service Domain. The system supports multiple authentication in the respective 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 the respective Service Domain.
  - ➔ **Specify WAN Port :** By default, it's "**Auto**"; Select desired WAN port for the respective Service Domain, the clients will connect to Internet via specific outgoing WAN port.

This function only activate on **Load Balance Mode** on WAN Traffic page.

  - ➔ **NAT Service :** By default, it's "**Enable**" to activated NAT service. To ***Disable*** to unactivated NAT service.
- **Pregenerated Ticket :** When Pregenerated Tickets selected in Auth Type field, the Tickets DB will appear. Select desired tickets database for Pregenerated authentication after creating the tickets database on the

Pregenerated Tickets page(See **Section 4.3.2.2**).

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

  ➔ **Login Timeout :** 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.

  ➔ **Redirect URL:** Enter the specified website to redirect, when users log in successfully, the pop-up page will directed to the specified URL.

  ➔ **Login Domain Name :** Enter the specified URL to display login page. If you close the login page and cause you can't click Logout button to stop service, you can enter specified URL on browser to display login page.

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

  ➔ **IP PnP Service :** IP Plug and Play, the WMS-308N 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 WMS-308N.

IP PnP only supports on **NAT** mode

  ➔ **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.

  ✓ **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.

  疪 **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*.

- **Custom Pages :** 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.

```
<meta name="apple-mobile-web-app-capable" content="yes" /><!--Auto Login for Apple's product-->
<meta names="apple-mobile-web-app-status-bar-style" content="black" /><!--Auto Login for Apple's product-->

<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 ** ** content

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

You only can modify , here is define CSS content for ** **

```
.ad{
    float: left;
    display: inline=block;
    text-align: center;
```

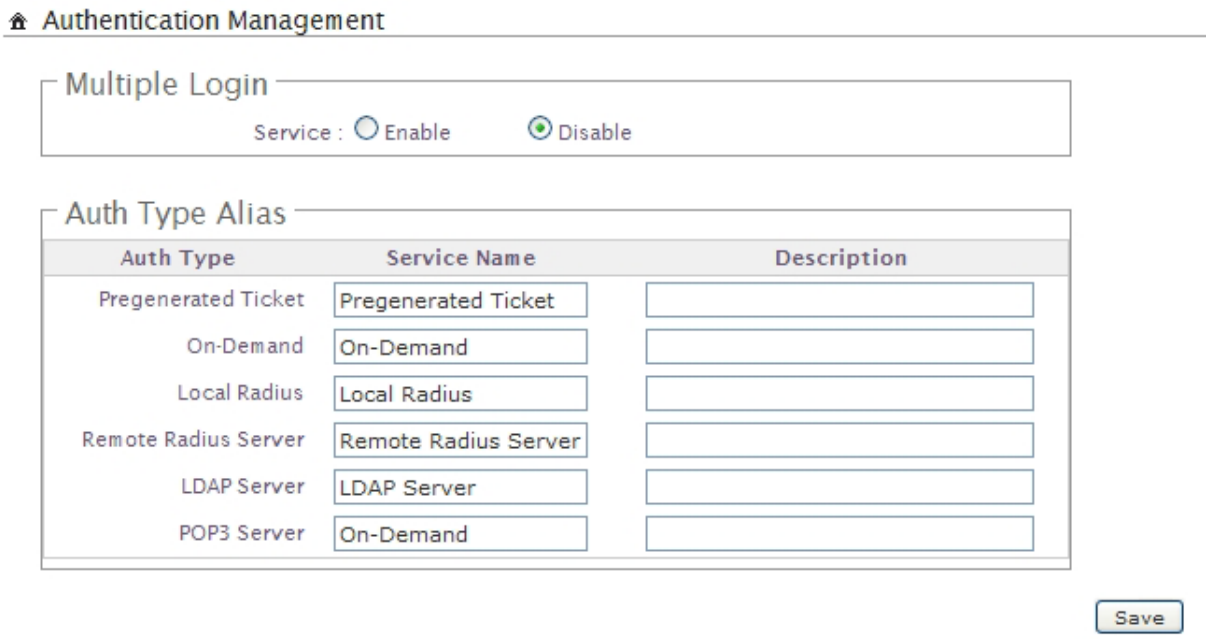
```
    width: 100px;
    margin: 5px;
    padding: 5px;
    background: #fff;
    font-size: 14px;
    font-weight: bold;
}

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

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

4.3.2 Configure Authentication

WMS-308N support **6** types of authentication : ***Pregenerated Tickets***, ***On-Demand Users***, ***Local RADIUS Accounts***, ***Remote RADIUS Server*** and ***Remote LDAP Server*** and ***POP3***. This section depicts to configure the settings for pregenerated tickets, on-demand users and authentication server. If authentication does not selected, the clients can access Internet without authentication.

4.3.2.1 Authentication Management

The WMS-308N 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.

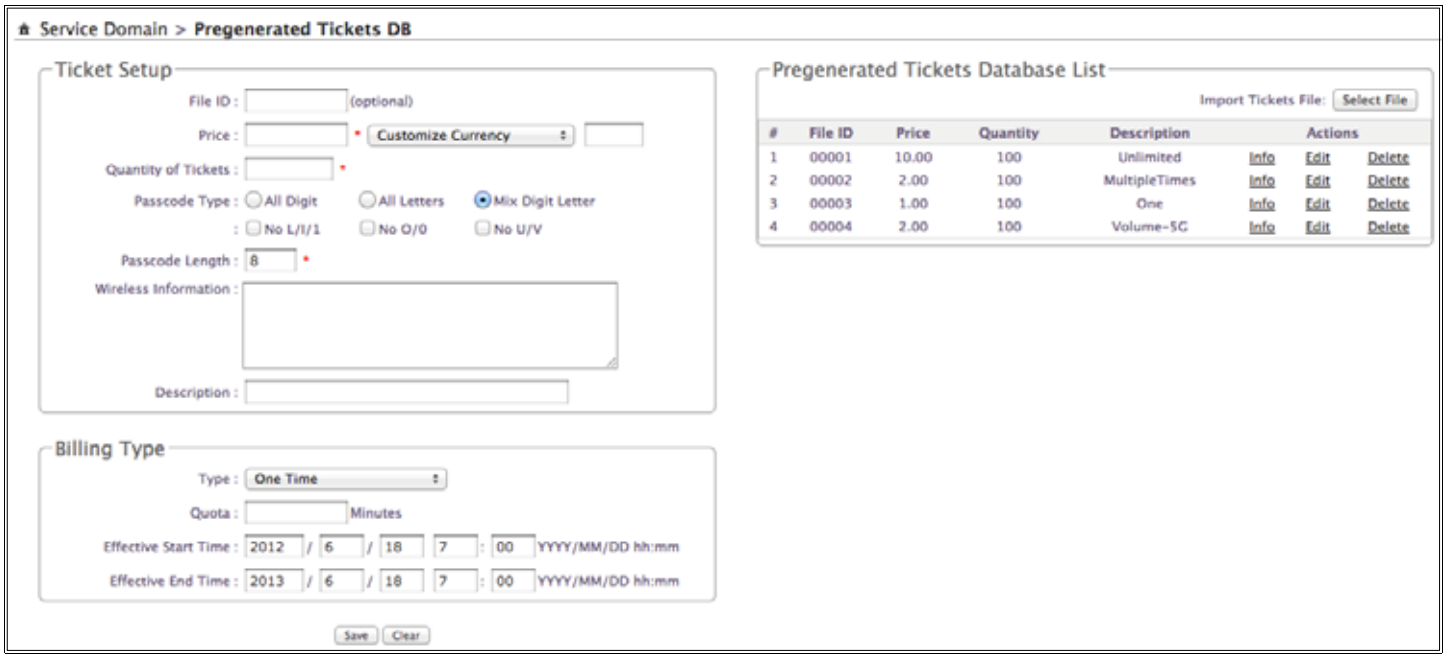


- **Multiple Login :** Click ***Enable*** button to activate multiple login service, and Disable to inactivate multiple login service.
- **Auth Type :** Denote authentication type of the system.
- **Service Name :** Enter desired alias name of the respective authentication type on login page.
- **Description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

4.3.2.2 Configure Pregenerated Tickets

This section is for administrators to pregenerated authentication tickets for entire external Network. There are four types of 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.



- **Ticket Setup :**
  - ➔ **File ID :** Enter the **8 hex digit** number for identifying tickets database, this setting is optional, If you don't specified file ID, the system will automatically generate
  - ➔ **Price :** The price charged for this tickets databases
  - ➔ **Currency :** Select currency from drop-down list or enter customize currency 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 Digit Letter**. 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
  - ➔ **Wireless Information :** Specify desired wireless information for this tickets database
  - ➔ **Description :** Enter the tickets databases description
- **Billing Type :**
  - ➔ **Type :** There are different billing policies for this tickets database : **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)

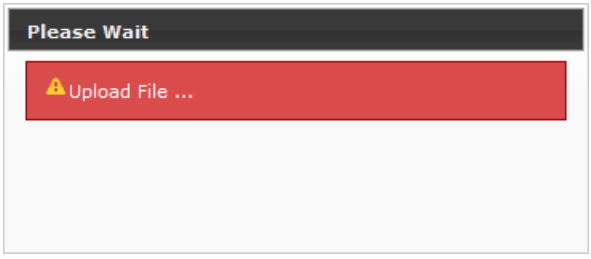
➔ **Effective Starting Time :** Specify desired effective starting time for this tickets database

➔ **Effective Ending Time :** Specify desired effective ending time for this tickets database.

Click ***Save*** button for create database of ticket .

➔ **Pregenerated Tickets Database List :** Shows all created ticket of database in the list

➔ **Import Tickets File :** Click this to upload the tickets of database. Click ***Select File*** button to select the file for the tickets upload. The "**Upload File ...**" message will appear.



➔ **File ID :** Denote the identity number of the database

➔ **Price :** Denote the price of ticket in the database

➔ **Description :** Denote the additional information of database

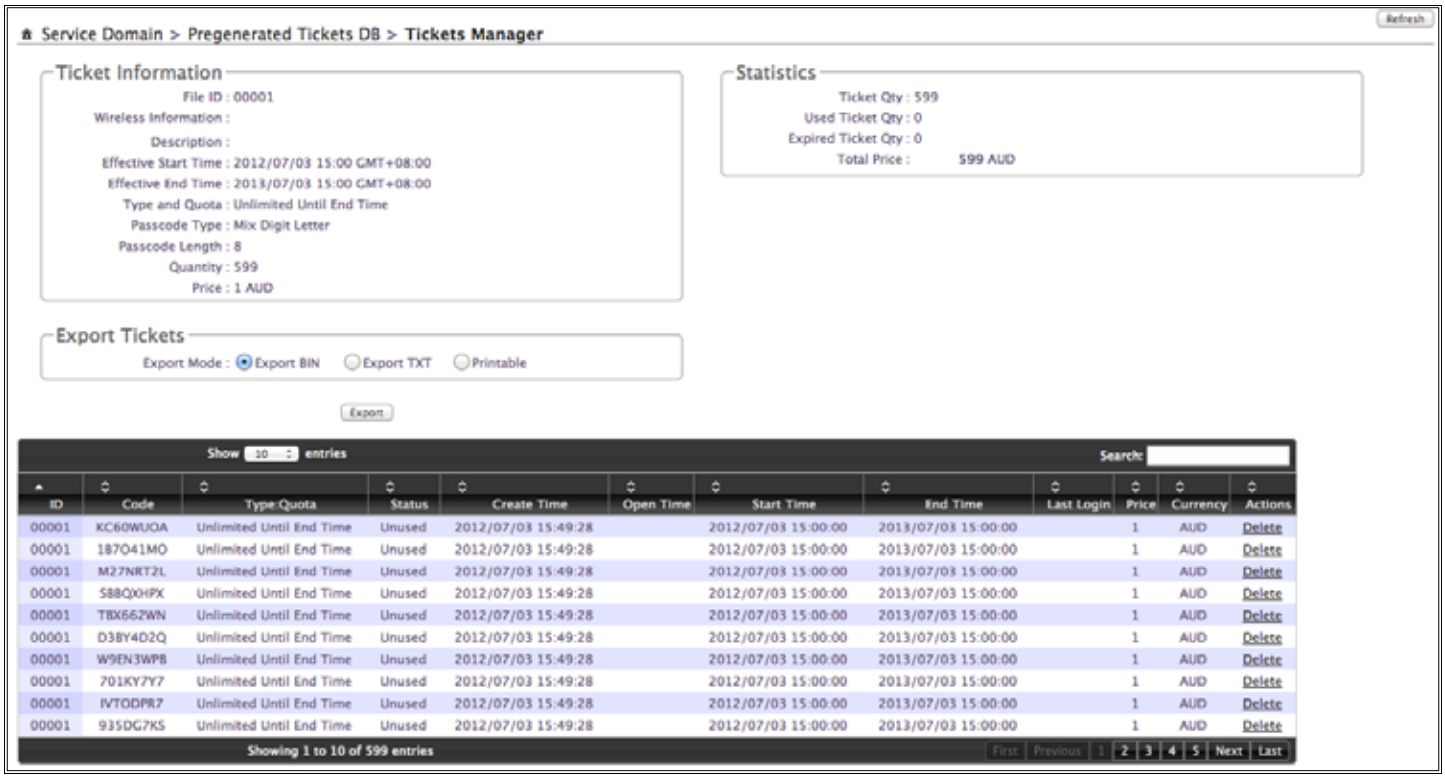
➔ **Actions :** Click an action button to perform the appropriate action.

✓ **Info :** Click this option to view information of each tickets database.

✓ **Edit :** Click this option to edit **Wireless Information** and **Description** in selected tickets database.

✓ **Delete :** Click this option to delete selected tickets database.

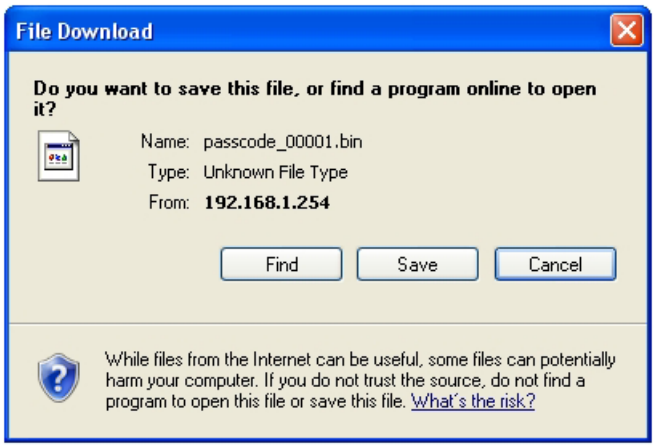
Below depicts an example for information of Pregenerated tickets databases when you click **Info** option



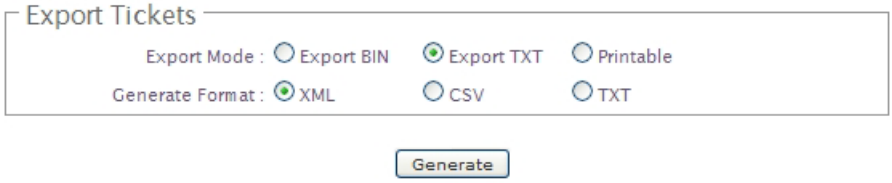
- **Ticket Information :** Show the ticket information in this database
  - ➔ **File ID :** Denote the identity number of the database
  - ➔ **Wireless Information :** Denote the wireless information on the ticket
  - ➔ **Description :** Denote additional information on the ticket
  - ➔ **Effective Starting Time :** Denote the effective starting time on the ticket
  - ➔ **Effective Ending Time :** Denote the effective ending time on the ticket
  - ➔ **Type and Quota :** Denote the billing type and service quota on the ticket
  - ➔ **Passcode Type :** Denote the passcode type on the ticket
  - ➔ **Passcode Length :** Denote the passcode length on the ticket
  - ➔ **Quantity :** Denote the quantity of ticket in this database
  - ➔ **Price :** Denote the price charged on the ticket
- **Statistic :** Show the statistics of information in this database
  - ✓ **Ticket Qty :** Denote the quantity of created ticket in this database
  - ✓ **Used Ticket Qty :** Denote the quantity of used ticket in this database
  - ✓ **Expired Ticket Qty :** Denote the quantity of expired ticket in this database
  - ✓ **Total Price :** Denote the total ticket's price and currency in this database

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

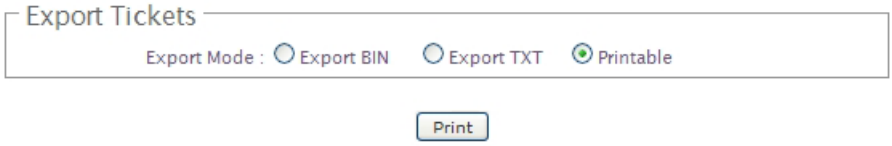
  ➔ **Export BIN :** The administrator can backup ticket database or copy to other WMS-308N. Click ***Export*** button, the ticket databases (***FileID_passcode.bin***) will be download from system. Below depicts an example for exporting tickets database.



  ➔ **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.



  ➔ **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.

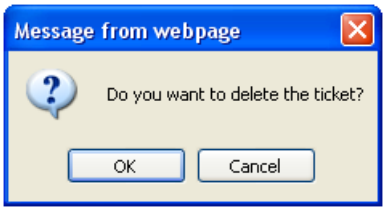


Below depicts an example for printable tickets

Passcode	FGKLVDTB	Passcode	LZHS1Q14	Passcode	LCNG2UZW	Passcode	630MUO2P
Price	10.00 USD	Price	10.00 USD	Price	10.00 USD	Price	10.00 USD
Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00
End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00
Wirless ESSID		Wirless ESSID		Wirless ESSID		Wirless ESSID	
Passcode	K3QGGJ7H	Passcode	YO90UAKF	Passcode	NNC5IBH4	Passcode	EX68L9XM
Price	10.00 USD	Price	10.00 USD	Price	10.00 USD	Price	10.00 USD
Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00	Start Time	2011/01/06 17:00:00
End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00	End Time	2011/02/06 17:00:00
Wirless ESSID		Wirless ESSID		Wirless ESSID		Wirless ESSID	

➔ **Tickets List :** Show all tickets in this database

- ➔ **File ID :** Denote the identity number of the database
- ➔ **Code :** User can used Passcode of ticket for access Internet
- ➔ **Type/Quota :** Denote the billing type and service quota on this ticket
- ➔ **Status :** Denote the status of ticket. There three types of status : **Unused**, **Used** and **Expired**
- ➔ **Create Time :** Denote the ticket create time
- ➔ **Open Time :** Denote the time of the first time used on this ticket
- ➔ **Start Time :** Denote effective starting time on this ticket
- ➔ **End Time :** Denote effective ending time on this ticket
- ➔ **Last Login :** Denote the last login time on this ticket
- ➔ **Price :** Denote the price of the charged on this ticket.
- ➔ **Currency :** Denote the currency of the charged on this ticket
- ➔ **Actions :** Click an action button to perform the appropriate action.
  - ✓ **Delete :** Click this option to remove ticket from this billing plan. When administrator click this option, the alert message will appear as below.



Click ***Refresh*** button to reload the page.

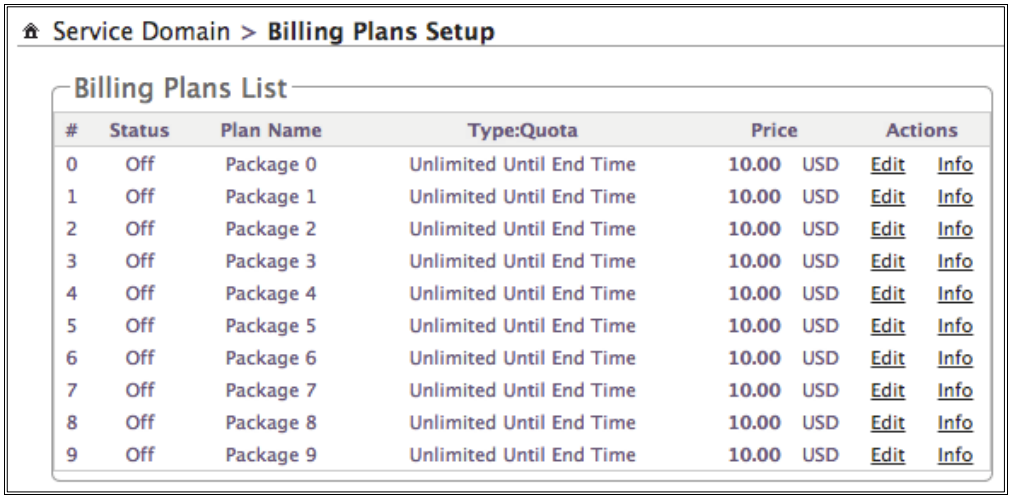
After you login system via Pregenerated authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)

If Timer Page doesn't appear in the browser, please enter "http(s)://domain0.login" to open Timer Page.(see section 4.3.1)

4.3.2.3 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**.

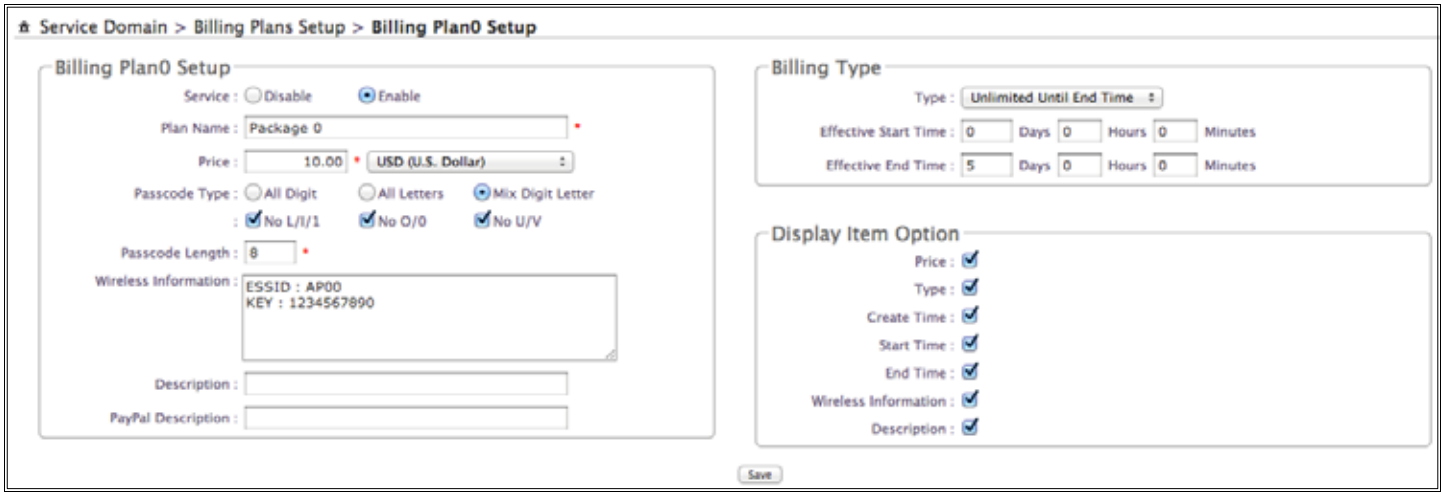
Click on **Service Domain -> Authentication -> On-Demand**, then the Billing Plans List page will appears.



- **Status :** Denote the current status of billing plan.
- **Plan Name :** Denote the name of billing plan
- **Type/Quota :** Denote the billing type and quota of billing plan
- **Price :** Denote the price charged of billing plan
- **Actions :** Click an action button to perform the appropriate action.
  - ➔ **Edit :** Click this option to edit the respective billing plan. There are **10** billing plans can be edited.
  - ➔ **Info :** Click this option to view accounts list and information of the respective billing plan.

4.3.2.3.1 Create Billing Plans

Click on **Service Domain** → **Authentication** → **On-Demand**, and click ***Edit*** option on **Billing Plans List**, the **Billing Plan Setup** page will appear.



- **Billing Plan Setup**
  - ➔ **Service :** 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 and currency for this billing plan

> The **Paypal** payment gateway does not support "**Customize Currency**" option..

  - ➔ **Passcode Type :** There are different passcode type for this billing plan: **All Digit**, **All Letters**, **Mix Digit Letter**. Select All Letters or Mix Digit Letter, 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 Information :** Enter the wireless information for this billing plan.
  - ➔ **Description :** Enter any additional information that will appear at the bottom of the receipt.
  - ➔ **Paypal Description :** Enter any additional information that will appear at the list of the login page.

- **Billing 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)

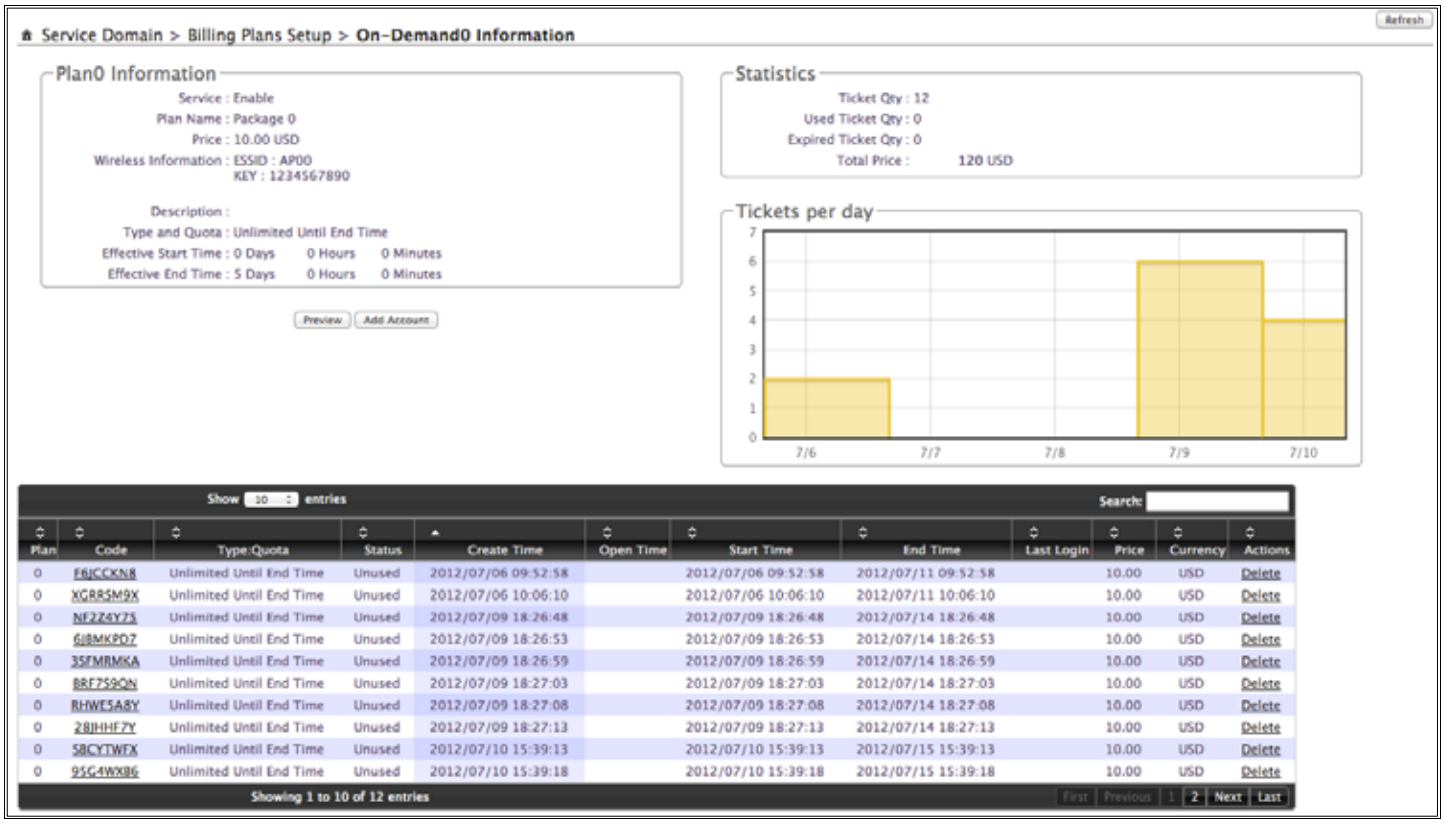
- ➔ **Effective Starting Time :** Specify desired effective starting time for this billing plan.
- ➔ **Effective Ending Time :** Specify desired effective ending time for this billing plan.

- **Display Item Option :** Select desired display item for ticket

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

4.3.2.3.2 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.



- **Plan Information :** Show plan information for this billing plan
  - ➔ **Service :** Denote the current status of billing plan
  - ➔ **Plan Name :** Denote the plan name of billing plan
  - ➔ **Price :** Denote the price charged of billing plan
  - ➔ **Wireless Information :** Denote the wireless information of billing plan
  - ➔ **Description :** Denote additional information of billing plan
  - ➔ **Type and Quota :** Denote billing type and service quota of billing plan
  - ➔ **Effective Starting Time :** Denote effective starting time of billing plan
  - ➔ **Effective Ending Time :** Denote effective ending time of billing plan

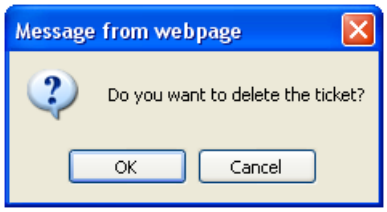
Click ***Preview*** button to preview ticket in the billing plan. Below depicts an example for previewing ticket. Click ***Close*** button to close window.

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

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

- **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

- **Tickets per day :** Show the bar chart of quantity of the ticket in this billing plan
- **Tickets List :** Show tickets information
  - ➔ **Plan :** Denote the billing plan on this ticket
  - ➔ **Code :** User can used Passcode of ticket for access Internet
  - ➔ **Type/Quota :** Denote the billing type and service quota on this ticket
  - ➔ **Status :** Denote the current status on this ticket. There three types of status : **Unused**, **Used** and **Expired**
  - ➔ **Create Time :** Denote the time of create on this ticket
  - ➔ **Open Time :** Denote the time of the first time used on this ticket
  - ➔ **Start Time :** Denote effective starting time on this ticket
  - ➔ **End Time :** Denote effective ending time on this ticket
  - ➔ **Last Login :** Denote the last login time on this ticket
  - ➔ **Price :** Denote the price of the charged on this ticket
  - ➔ **Currency :** Denote the currency of the charged on this ticket
  - ➔ **Actions :** Click an action button to perform the appropriate action.
    - ✓ **Delete :** Click this option to remove ticket from this billing plan. When administrator click this option, the alert message will appear as below.



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

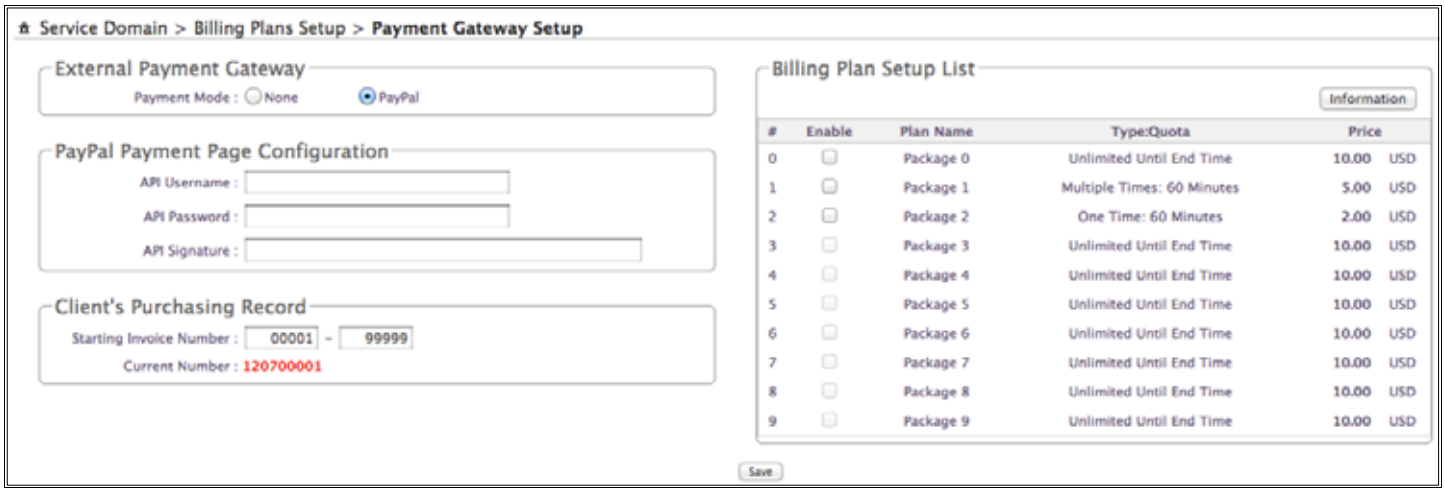
The list only shows generate of the ticket by clicking **Add Account** button

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)://domain0.login" to open Timer Page.(see section 4.3.1)

4.3.2.3.3 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.



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.

The **Paypal** payment gateway does not support "**Customize Currency**" option on Billing Plan.

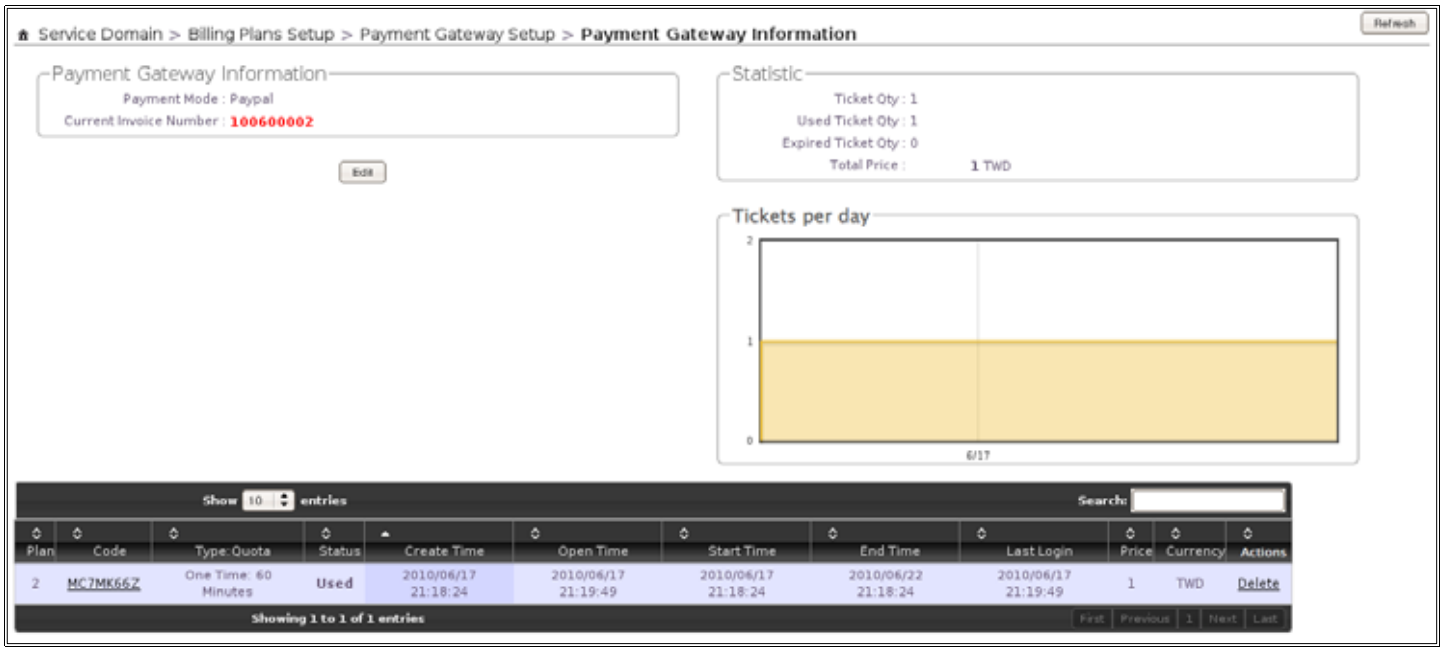
After opening a PayPal Business Account, the merchant should find the "**API Signature**" of this PayPal account to continue "External Payment Gateway Setup".

- **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.
- **Billing Plan Setup List** :
  - ➔ **Enable :** Select specified the billing plan for this payment gateway.
  - ➔ **Plan Name :** Denote the name of billing plan.

➔ **Type/Quota :** Denote the billing type and quota of billing plan

➔ **Price :** Denote the price charged of billing plan

➔ **Information :** Click this button to view accounts information for PayPal.



■ **Payment Gateway Information :** Show current ticket's invoice number.

Click ***Edit*** button to enter **Payment Gateway Setup** page

■ **Statistic :** Shows on-demand users statistic information for this billing plan via payment gateway created

➔ **Ticket Qty :** Denote quantity of created ticket from payment gateway

➔ **Used Ticket Qty :** Denote quantity of used ticket from payment gateway

➔ **Expired Ticket Qty :** Denote quantity of expired ticket from payment gateway

■ **Total Price :** Denote total ticket's price and currency from payment gateway

■ **Tickets per day :** Show the bar chart of quantity of the ticket from payment gateway

■ **Tickets List :** Show tickets information

➔ **Plan :** Denote the billing plan on this ticket

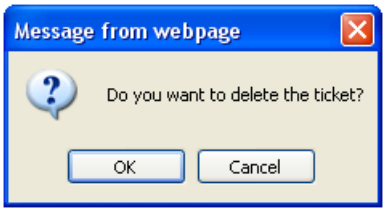
➔ **Code :** User can used Passcode of ticket for access Internet

➔ **Type/Quota :** Denote the billing type and service quota on this ticket

➔ **Status :** Denote the current status on this ticket. There three types of status : **Unused**, **Used** and **Expired**

➔ **Create Time :** Denote the time of create on this ticket

- ➔ **Open Time :** Denote the time of the first time used on this ticket
- ➔ **Start Time :** Denote effective starting time on this ticket
- ➔ **End Time :** Denote effective ending time on this ticket
- ➔ **Last Login :** Denote the last login time on this ticket
- ➔ **Price :** Denote the price of the charged on this ticket.
- ➔ **Currency :** Denote the currency of the charged on this ticket
- ➔ **Actions :** Click an action button to perform the appropriate action.
  - ✓ **Delete :** Click this option to remove ticket from this billing plan. When administrator click this option, the alert message will appear as below.



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

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

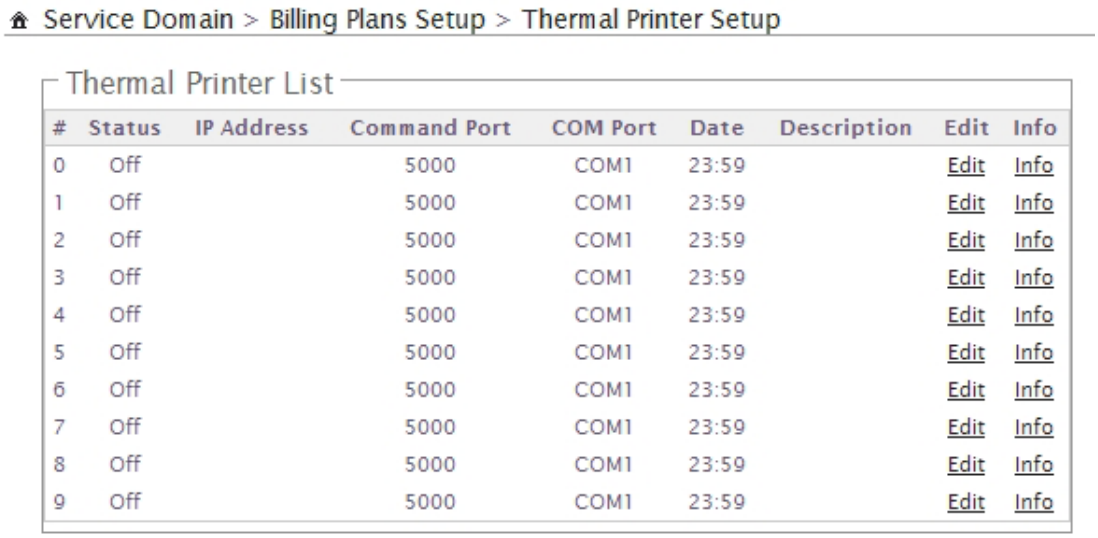
After you login system via **On-Demand** authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)

If Timer Page doesn't appear in the browser, please enter "http(s)://domain0.login" to open Timer Page.(see section 4.3.1)

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

4.3.2.3.4 Configure Thermal Printer

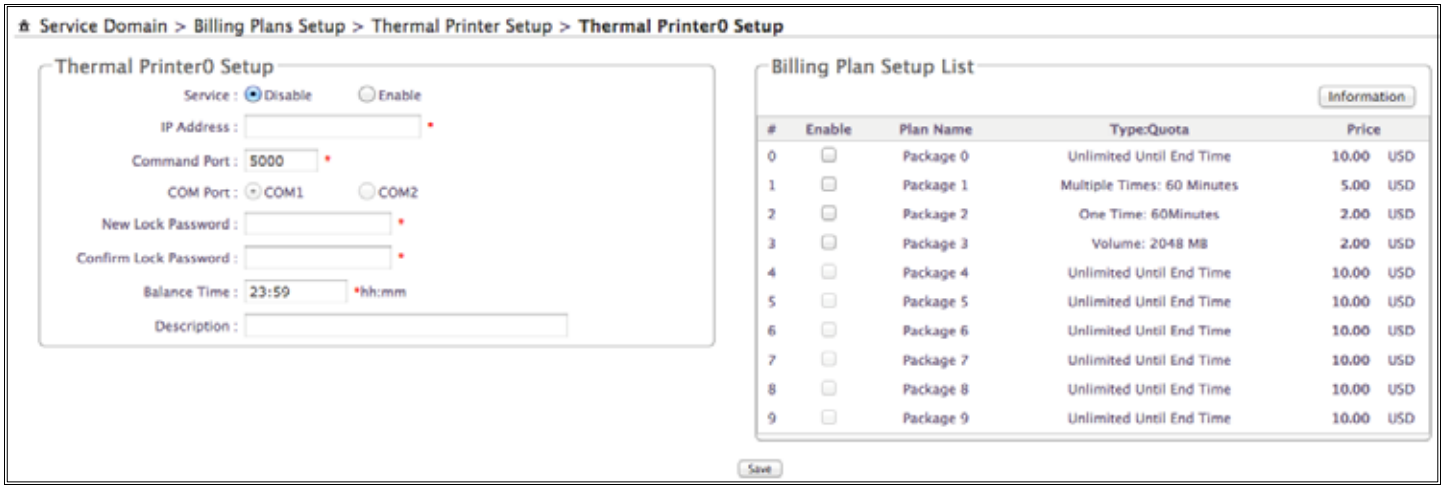
WMS-308N can generate ticket of on-demand users manually or automatically from Thermal Printer. Please click on **Service Domain -> Authentication -> On-Demand -> Thermal Printer Setup** to enter the **Thermal Printer List** page. In the Thermal Printer List page. Administrator may configure Thermal Printer setting and generate tickets manually and delete tickets.



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

- **Status :** Denote the current status of thermal printer
- **IP Address :** Denote the IP address of SR-120X serial server
- **Command Port :** Denote the command port of SR-120X serial server
- **COM Port :** Denote the COM port of SR-120X serial server to connect to thermal printer
- **Date :** Denote balance date of thermal printer
- **Description :** Denote the additional information of thermal printer
- **Actions :** Click an action button to perform the appropriate action.
  - **Edit :** Click this option to edit the respective settings of thermal printer. There are **10** thermal printer can be edited. Each thermal printer can specified billing plan
  - **Info :** Click this option to view accounts list and information of the respective billing plan from thermal printer created

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



■ **Thermal Printer Setup :**

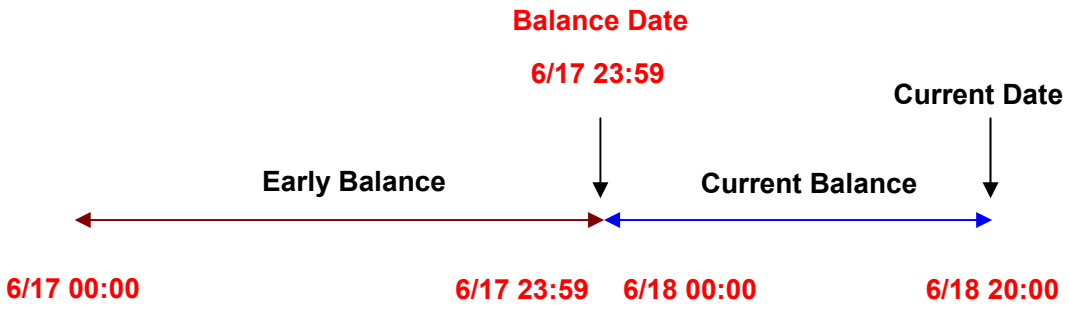
➔ **Service :** By default, it's "**Disable**". To "**Enable**" to activate this function.

➔ **IP Address :** Enter the IP address of SR-120X serial server

➔ **Command Port :** Enter the command port of SR-120X serial server

➔ **COM Port :** Select the COM port of SR-120X serial server to connect to thermal printer

➔ **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

■ **Billing Plan Setup List** :

➔ **Enable :** Select specified the billing plan for this thermal printer

➔ **Plan Name :** Denote the name of billing plan

➔ **Type/Quota :** Denote the billing type and quota of billing plan

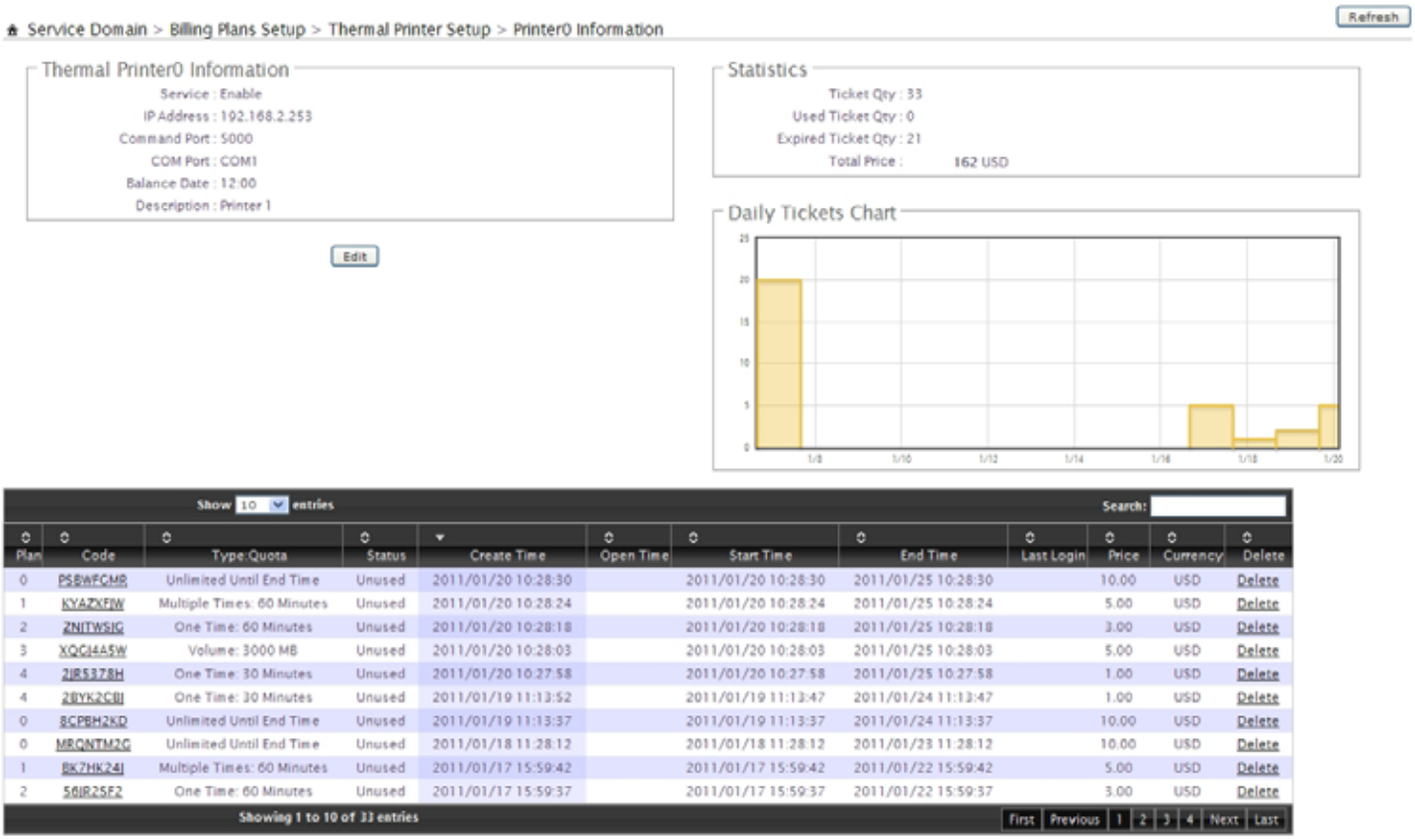
➔ **Price :** Denote the price charged of billing plan

➔ **Information :** Click this button to view accounts information for PayPal.

After configuring thermal printer general setting, administrator must select specified 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.



➔ **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.

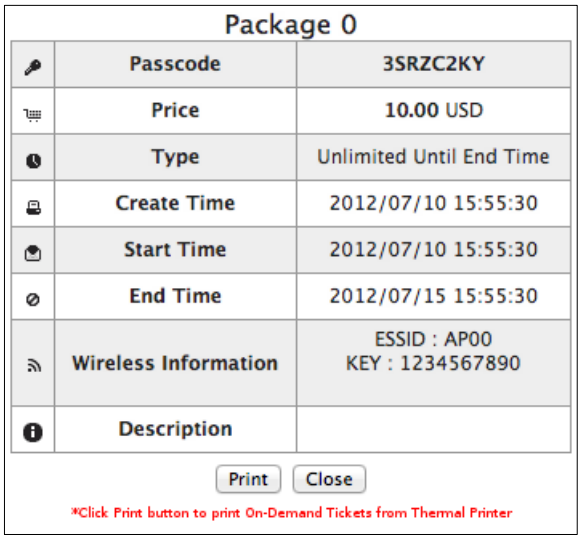
➔ **Total Price :** Denote total ticket's price and currency in this Thermal Printer.

■ **Tickets per day :** Show the bar chart of quantity of the ticket from thermal printer.

■ **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.



➔ **Type/Quota :** Denote the billing type and service quota on this ticket

➔ **Status :** Denote the current status on this ticket. There three types of status : **Unused**, **Used** and **Expired**

➔ **Create Time :** Denote the time of create on this ticket

➔ **Open Time :** Denote the time of the first time used on this ticket

➔ **Start Time :** Denote the effective starting time on this ticket

➔ **End Time :** Denote the effective ending time on this ticket

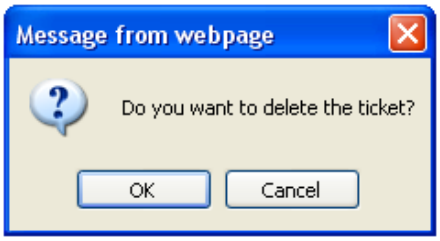
➔ **Last Login :** Denote the last login time on this ticket

➔ **Price :** Denote the price of the charged on this ticket.

➔ **Currency :** Denote the currency of the charged on this ticket

➔ **Actions :** Click an action button to perform the appropriate action

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



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

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

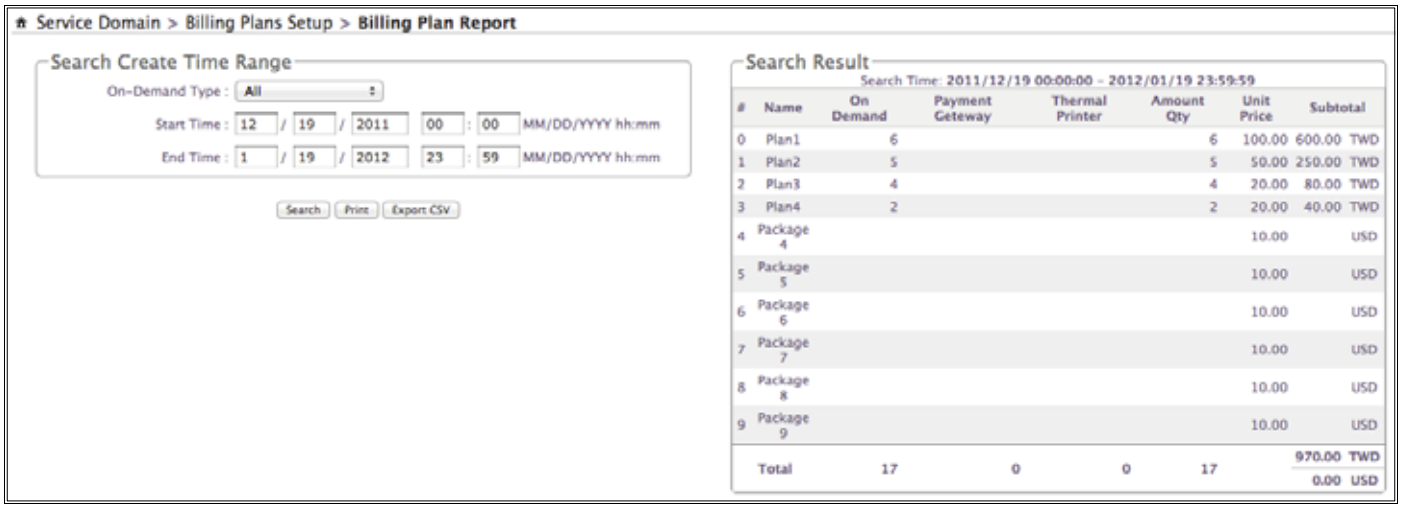
After you login system via **On-Demand** authentication, the timer page will appear. Don't close Timer page(Because the ***Logout*** button on this page)

If Timer Page doesn't appear in the browser, please enter "http(s)://domain0.login" to open Timer Page.(see section 4.3.1)

4.3.2.3.5 Billing Plan Report

Click on **Service Domain -> Authentication -> On-Demand** to enter the **Billing Plans Report** page.

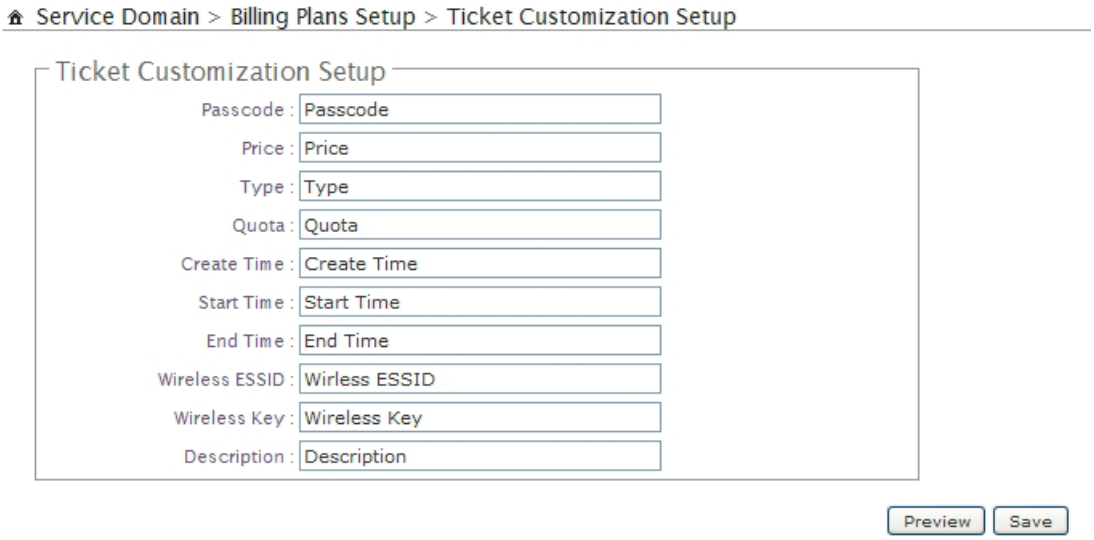
Administrator can get a complete report or a report of a particular period.



- **Search Create Time Range**
  - **On-Demand Type :**There are **four** type can be selected : **ALL**, **Manually Create**, **Payment Gateway** and **Thermal Printer**.
  - **Start Time :** Specify desired search starting time
  - **End Time :** Specify desired search ending time
- **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.
- **Export CSV :** Administrator can download billing plan report to PC.
- **Search Result :** Shows search result of the specified time range
  - ➔ **Search Time :** Denote the specified search time range
  - ➔ **Name :** Denote the name of billing plan
  - ➔ **On-Demand :** Denote the quantity of ticket from manually created
  - ➔ **Payment Gateway :** Denote the quantity of ticket from payment gateway created
  - ➔ **Thermal Printer :** Denote the quantity of ticket from thermal printer created
  - ➔ **Amount Qty :** Denote total quantity of created ticket of billing plan
  - ➔ **Unit Price :** Denote the unit price of billing plan
  - ➔ **Subtotal :** Denote the total price of billing plan
  - ➔ **Total :** Denote the total price and quantity on all billing plan

4.3.2.3.6 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.

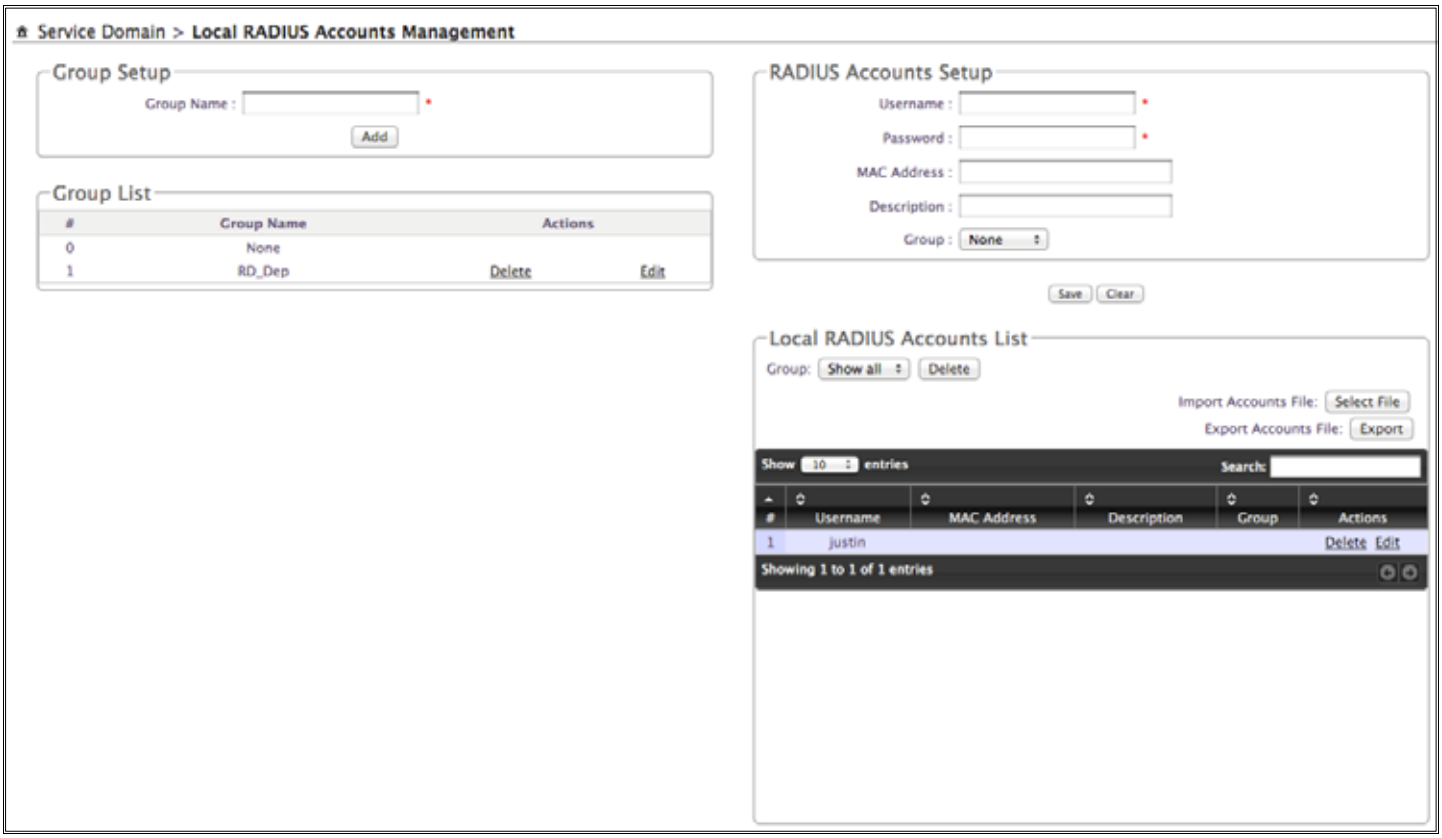


Change these settings as described here and click ***Save*** button to save your changes. Click ***Preview*** button to preview ticket in the **Billing Plan 0**. Below depicts an example for previewing ticket. Click ***Close*** button to close window.

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

4.3.2.4 Configure Local Radius Accounts

WMS-308N 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.



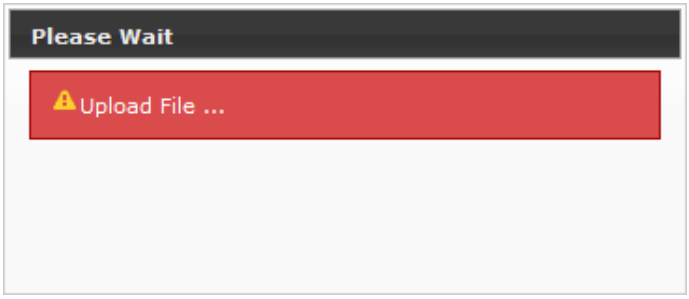
- **Group Setup :** Enter the specified name on group and click ***Add*** button to create. Up to **20** groups can added.
- **Group List :** Display all of groups in the list, click ***Delete*** option to remove group name and all of the accounts in this group will be removed, click ***Edit*** option to change group name.
- **RADIUS Accounts Setup :**
  - ➔ **Username :** Enter the username of account on local RADIUS authentication. **4-16** alphanumeric and specify characters supported.
  - ➔ **Password :** Enter the password of account on local RADIUS authentication. **4-16** alphanumeric and specify characters supported.
  - ➔ **MAC Address :** Enter the MAC address of account on local RADIUS authentication.(**optional**)
  - ➔ **Description :** Enter appropriate text to denote this account.
  - ➔ **Group :** Select the specified group on local RADIUS authentication, default is None.

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

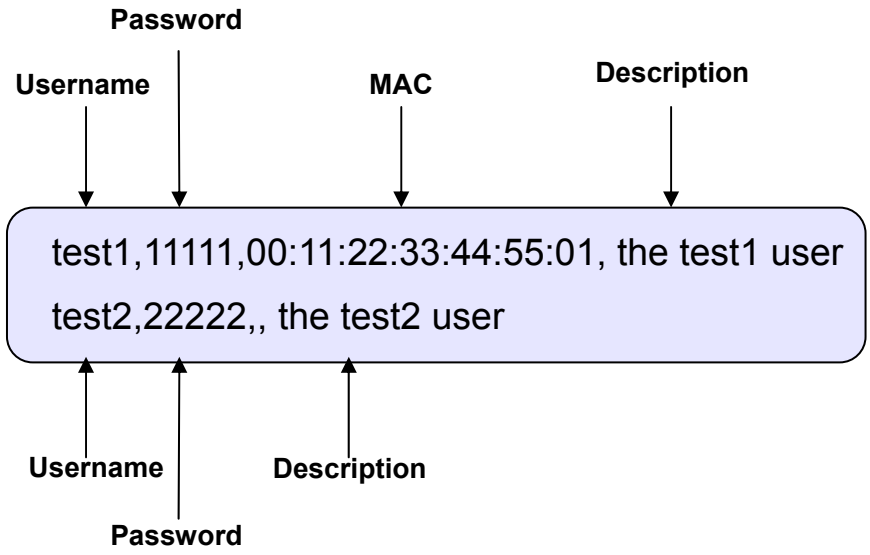
■ **Local RADIUS Accounts List :**

➔ **Delete :** Select the specified group and click ***Delete*** button to remove accounts of the specified group.

➔ **Import Accounts File :** Select the specified group on **Group** option and click ***Select File*** button to select the text file for uploading the accounts of the specified group. The "**Upload File ...**" message will appear.



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 process will fail. Below depicts an example for text file.

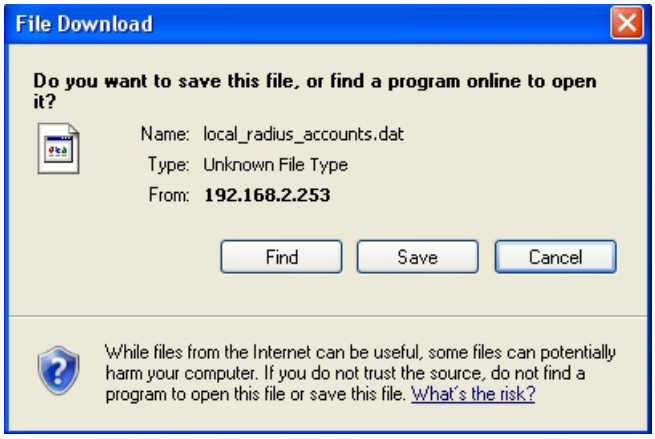


恩

The same Username account can't exist on different groups, the Group option only for convenient management.

恩

➔ **Export Accounts File :** Select the specified group on **Group** option and click ***Export*** button to save accounts of the specified group to PC. The "File Download" window will appear..

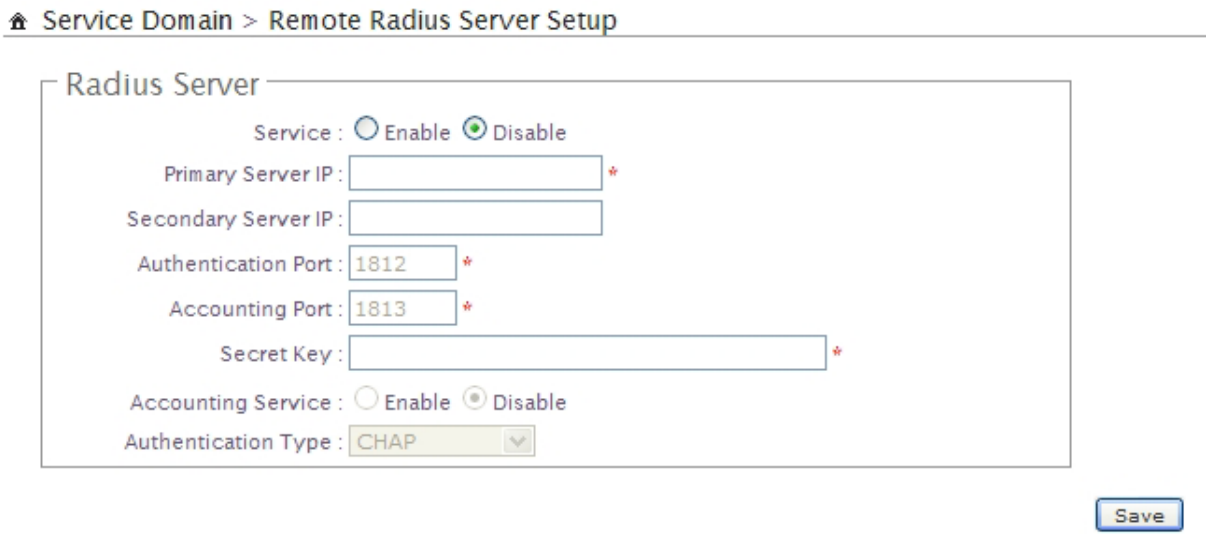


- **Search :** Enter a keyword to be searched in the text field and all matching the keyword will be listed.
- **Username :** Denote the username of account on local RADIUS authentication
- **MAC Address :** Denote the MAC address of account on local RADIUS authentication
- **Description :** Enter appropriate text to denote this account
- **Group :** Denote the specified of account on local RADIUS authentication
- **Actions :** Click an action button to perform the appropriate action.
  - ➔ **Delete :** Click this option to remove the specified account.
  - ➔ **Edit :** Click this option to edit the specified account

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

4.3.2.5 Configure Remote Radius Server

WMS-308N provide remote Radius server authentication. Please click on **Service Domain** -> **Authentication** -> **Remote Radius Server**, the page of **Remote Radius Server Setup** will appear

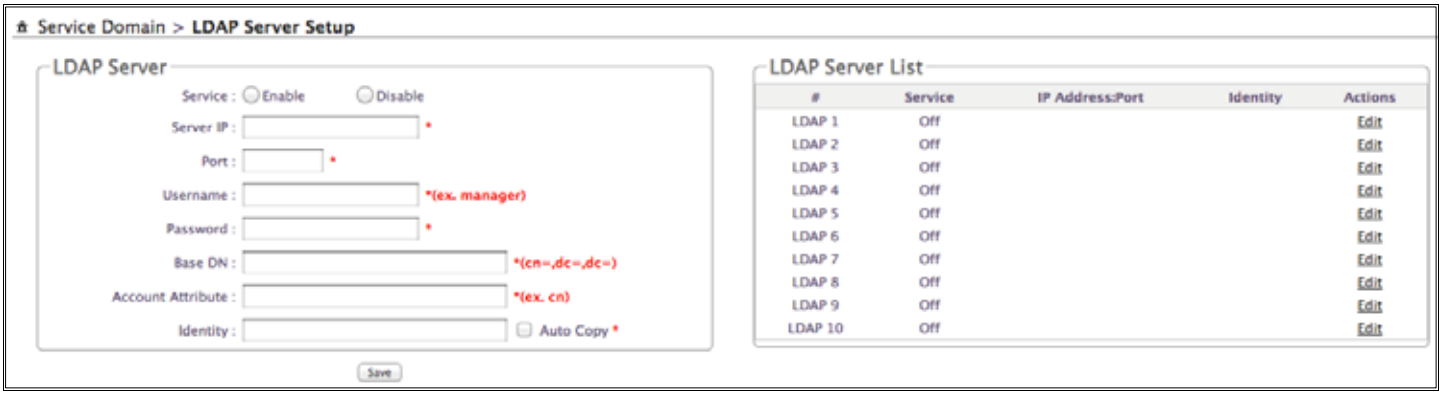


- **Service :** By default, it's "**Disable**". To "**Enable**" to activate this function.
- **Primary/Secondary Server IP :** Enter the IP address of the Authentication RADIUS server.
- **Authentication Port :** The port number used by Authentication RADIUS server. Use the default **1812** or enter 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

4.3.2.6 Configure LDAP Server

WMS-308N provide remote LDAP server authentication. Up to **10** remote LDAP server can be configured. Please click on **Service Domain** → **Authentication** → **LDAP**, the page of **LDAP Server Setup** will appear



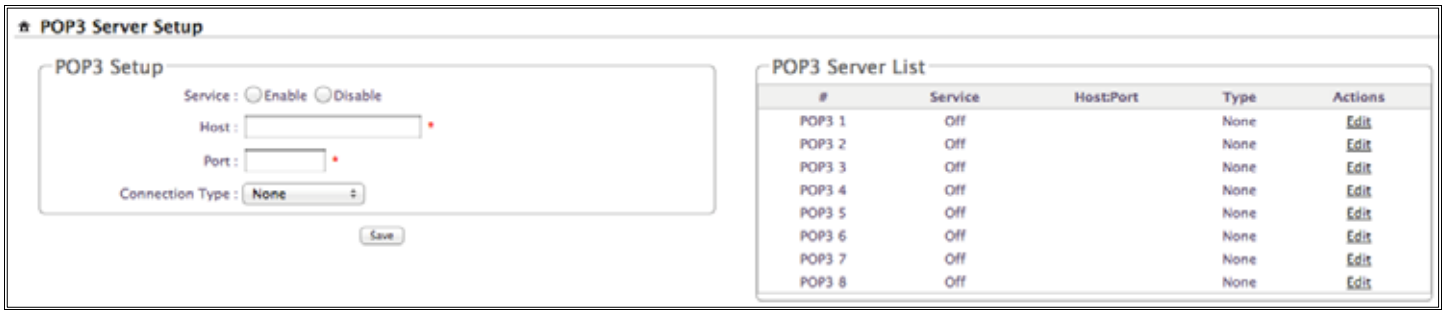
Click **Edit** option to configure LDAP server on the **LDAP Server List**.

- **LDAP Server**
  - ➔ **Service :** By default, it's "**Disable**". To "**Enable**" to activate this function.
  - ➔ **Server IP :** Enter the IP address of the external LDAP server.
  - ➔ **Port :** Enter the Port of the external LDAP server, default port is **389**.
  - ➔ **Username :** Enter the Administrator's username to access to the external LDAP server
  - ➔ **Password :** Enter the Administrator's Password to access to the external LDAP server
  - ➔ **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 external LDAP server.
  - ➔ **Identity :** Enter the Administrator's Identity to access directory service. Click on **Auto Copy**, the system will automatically generate identity
- **LDAP Server List**
  - ➔ **Service :** Denote the current status of LDAP server
  - ➔ **IP Address/Port :** Denote the IP address and port number to connect to the external LDAP server
  - ➔ **Identity :** Denote the Administrator's Identity to access to the external LDAP server
  - ➔ **Actions :** Click an action button to perform the appropriate action.
    - ✓ **Edit :** Click this option to edit the respective billing plan. There are **10** LDAP server can be edited.

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

4.3.2.7 Configure POP3 Server

The system supports authentication by an external POP3 authentication server. Up to **8** POP3 server can be configured. Please click on **Service Domain** → **Authentication** → **POP3,** the page of **POP3 Server Setup** will appear.



Click "**Edit**" to configure POP3 server on the **POP3 Server List**.

- **POP3 Setup**
  - ➔ **Service :** By default, it's "**Disable**". To "**Enable**" to activate this function.
  - ➔ **Host :** Enter the Domain/IP address of the external POP3 server.
  - ➔ **Port :** Enter the authentication port of the external POP3 server. (The default is **110**)

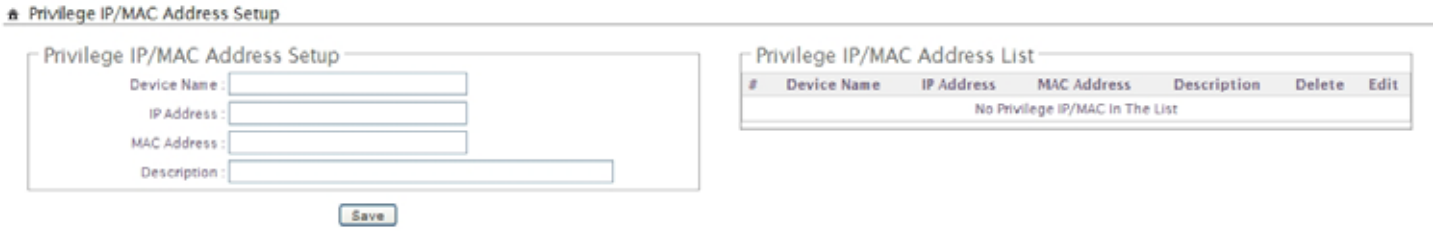
> Sometimes POP3 server use Port **110** for **STARTTLS** encryption and Port **995** for **SSL/TLS** encryption

  - ➔ **Connection Type :** Some POP3 server need encryption linking for authentication. The system provides "**STARTTL**" and "**SSL/TLS**" encryption for external POP3 server
- **POP3 Server List**
  - ➔ **Service :** Denote the current status of POP3 server
  - ➔ **Host/Port : D**enote the Host/IP address and port number to connect to external POP3 server
  - ➔ **Type :** Denote the encryption type to connect to external POP3 server
  - ➔ **Actions :** Click an action button to perform the appropriate action.
    - ✓ **Edit :** Click this option to edit the respective billing plan. There are **8** POP3 server can be edited.

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

4.3.3 Configure Privilege List

This function provides local device can access Internet without authentication. If there are some workstations belonging WMS-308N that need to access to network without authentication, enter the IP or MAC address of these workstations in this list. Up to **50** rules can be defined in this list. Please click on **Service Domain** → **Privilege IP/MAC Address**, the page of **Privilege IP/MAC Address Setup** will appear.



- **Privilege IP/MAC Address Setup**
  - ➔ **Device Name :** Enter the name of the workstation
  - ➔ **IP Address :** Enter the IP address(or **IP address/Mask**) of the workstation. Permitting specific IP addresses to have network access rights without going through standard authentication process
  - ➔ **MAC Address :** Enter the MAC address of the workstation. Permitting specific MAC addresses to have network access rights without going through standard authentication process
  - ➔ **Description :** Enter appropriate text to denote this workstation

Click ***Save*** button to add new rule, all of rules can be **edited** and **deleted.**

- **Privilege IP/MAC Address List**
  - ➔ **Device Name :** Denote the name of workstation.
  - ➔ **IP Address :** Denote the IP address(or **IP address/Mask**) of workstation
  - ➔ **MAC Address :** Denote the MAC address of workstation.
  - ➔ **Description :** Enter appropriate text to denote this workstation
  - ➔ **Actions :** Click an action button to perform the appropriate action.
    - ✓ **Delete :** Click this option to remove the specified item
    - ✓ **Edit :** Click this option to edit the specified item

4.3.4 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** rules 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.

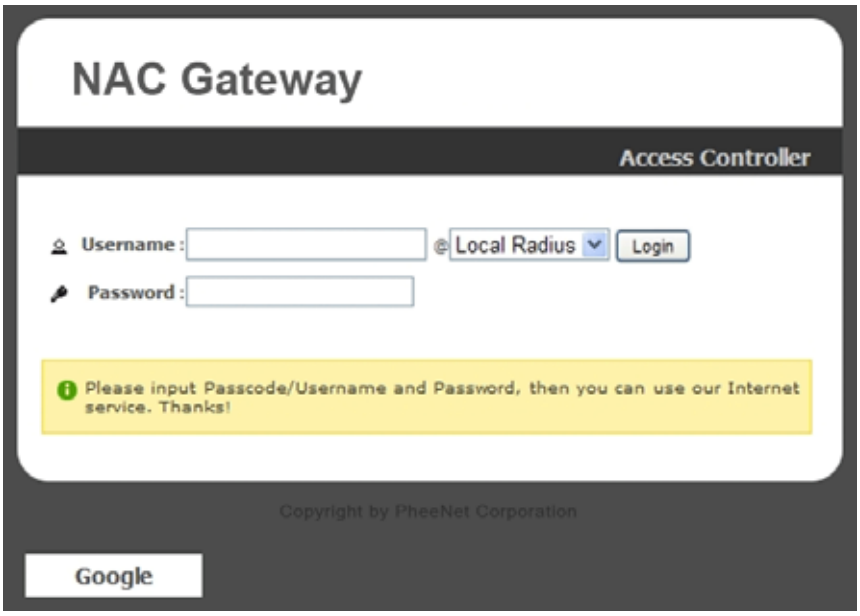
- **Walled Garden**
  - ➔ **Name :** Enter a descriptive name for this rule for identifying purposes
  - ➔ **IP Address/Domain :** Enter the IP address/Domain of the workstation.
  - ➔ **Homepages :** Enter the MAC address of the workstation.
  - ➔ **Description :** Enter appropriate text to denote this workstation

Click ***Save*** button to add new rule, all of rules can be **edited** and **deleted**

- **Walled Garden List**

1. **Name :** Denote the name of workstation
2. **IP Address/Domain :** Denote the IP address(or **IP address/Mask**) of workstation
3. **Actions :** Click an action button to perform the appropriate action.
   - **Delete :** Click this option to remove the specified item
   - **Edit :** Click this option to edit the specified item

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


NAC Gateway
Access Controller
Username :
@Local Radius
Login
Password :
Please input Passcode/Username and Password, then you can use our Internet service. Thanks!
Copyright by PheeNet Corporation
Google

4.3.5 Configure Notification

WMS-308N can automatically send the notification of **Traffic Log**, **On-Demand Log**, **Session Log**, **Monitor AP Report** and **AP Status** to 3 particular E-mail addresses. The notification of AP Status is triggered by the event when a managed APs becomes unreachable during "**Auto Download Profile Interval**" period. A trial email is provided by the system for validation. The system also supports recording System Log, On-Demand User Log and Session Log via remote Syslog servers. Please click on **Service Domain** -> **Notification**, the page of **Notification E-mail Setup** will appear and enter the related information and select the desired items and then apply the settings.

- **SMTP Server Setup :** There are two SMTP Server supported, when two SMTP servers enabled, the system use SMTP 1 for primary SMTP server and SMTP 2 for backup SMTP server.
  - ➔ **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)

Sometimes SMTP server use Port **587** for **TLS** encryption and Port **465** for **SSL** encryption

  - ➔ **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) . For Billing Plan Report, the send interval between **1** and **24** hours.

➔ **Billing Report Time :** The start time of sending e-mail. For example : the Billing Report Time is 14:00 and Sending Interval is 6 hours, the system will send report on 20:00.

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

■ **Syslog Setup :** There are 3 types of Syslog supported : **Syslog Log**, **On-Demand User Log** and **Session Log**. Enter the specify IP address and Port number to sent report.

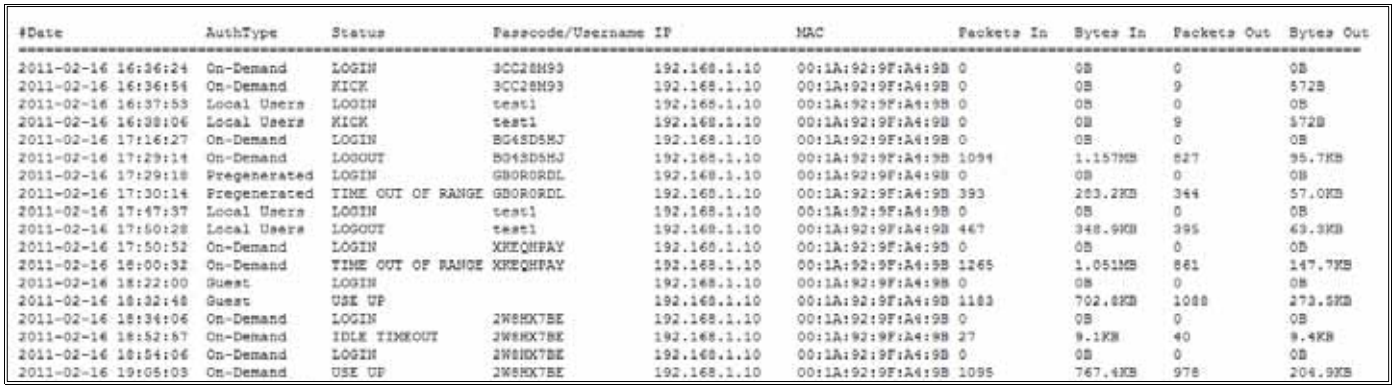
The all history log are saved in the DRAM, if you restart system, the all of history log will empty.

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

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
2011-02-16 16:36:24	On-Demand	LOGIN	3CC28N93	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 16:36:54	On-Demand	KICK	3CC28N93	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	9	572B
2011-02-16 16:37:53	Local Users	LOGIN	test1	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 16:38:06	Local Users	KICK	test1	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	9	572B
2011-02-16 17:16:27	On-Demand	LOGIN	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 17:29:14	On-Demand	LOGOUT	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	1094	1.157MB	827	95.7KB
2011-02-16 17:29:18	Pregenerated	LOGIN	GBORORDL	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 17:30:14	Pregenerated	TIME OUT OF RANGE	GBORORDL	192.168.1.10	00:1A:92:9F:A4:9B	393	283.2KB	364	57.0KB
2011-02-16 17:47:37	Local Users	LOGIN	test1	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 17:50:28	Local Users	LOGOUT	test1	192.168.1.10	00:1A:92:9F:A4:9B	467	348.9KB	395	63.3KB
2011-02-16 17:50:52	On-Demand	LOGIN	XKEQNPAY	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 18:00:32	On-Demand	TIME OUT OF RANGE	XKEQNPAY	192.168.1.10	00:1A:92:9F:A4:9B	1265	1.051MB	861	147.7KB
2011-02-16 18:22:00	Guest	LOGIN		192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 18:32:48	Guest	USE UP		192.168.1.10	00:1A:92:9F:A4:9B	1183	702.8KB	1088	273.5KB
2011-02-16 18:34:06	On-Demand	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 18:52:57	On-Demand	IDLE TIMEOUT	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	27	9.1KB	40	9.4KB
2011-02-16 18:54:06	On-Demand	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 19:05:03	On-Demand	USE UP	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	1095	767.4KB	978	204.9KB

➔ **Date :** Denote the current event's date and time

➔ **Auth Type :** There will shows **7** types of authentication : **Pregenerated**, **On-Demand**, **Local Users**(Local RADIUS Users), **Remote RADIUS**, **LDAP**, **POP3** and **Guest**.

➔ **Status :** There will show **10** types of status as below :

- ✓ **LOGIN :** Denote the user login to the hotspot service
- ✓ **LOGOUT :** Denote the user logout to the hotspot service
- ✓ **IDLE TIMEOUT :** Denote the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
- ✓ **USE UP :** Denote the quota of time of user is over
- ✓ **SESSION TIMEOUT :** Denote the user session timeout for connecting to remote RAIDUS
- ✓ **VOLUME USE UP :** Denote the quota of volume of user is over
- ✓ **KICK :** Denote the system kick out the user.
- ✓ **TIME OUT OF RANGE :** Denote the service time out of range

➔ **Passcode/Username :** Denote the user's passcode or username

➔ **IP :** Denote the user's IP address

➔ **MAC :** Denote the user's MAC address

➔ **Packets In :** Denote the current user's packets in

➔ **Bytes In :** Denote the current user's bytes in

➔ **Packet Out :** Denote the current user's packets out

➔ **Bytes Out :** Denote the current user's bytes out

■ **On-Demand Log :**

As shown in the following figure, each line is traffic history record consisting of 15 fields : **Date**, **Location**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out**, **Start Time**, **End Time, Plan**, **Payment Type** and **Cost**

#Date	Location	Status	Passcode/Username	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Start Time	End Time	Plan	Payment Type	Cost
2012-02-13 14:19:27		ADD OD ACCOUNT	QEJ6GNG9	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:19:27	2012-02-18 14:19:27	Plan 3	Cash	USD 2.00
2012-02-13 14:19:37		ADD OD ACCOUNT	KPE3YG6S	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:19:37	2012-02-18 14:19:37	Plan 3	Cash	USD 2.00
2012-02-13 14:19:45		ADD OD ACCOUNT	Z7CWKZ73	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:19:45	2012-02-18 14:19:45	Plan 3	Cash	USD 2.00
2012-02-13 14:19:53		ADD OD ACCOUNT	XMMN9W7C	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:19:53	2012-02-18 14:19:53	Plan 3	Cash	USD 2.00
2012-02-13 14:20:24		ADD OD ACCOUNT	F4E7CHCS	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 14:20:43		ADD OD ACCOUNT	J8DYNBTM	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:20:43	2012-02-18 14:20:43	Plan 0	Cash	USD 10.00
2012-02-13 14:37:24		LOGIN	XMMN9W7C	192.168.3.10	E4:CE:8F:4B:C2:9E	0	0B	0	0B	2012-02-13 14:19:53	2012-02-18 14:19:53	Plan 3	Cash	USD 2.00
2012-02-13 14:42:46		VOLUME USE UP	XMMN9W7C	192.168.3.10	E4:CE:8F:4B:C2:9E	146258	201.165MB	80276	3.376MB	2012-02-13 14:19:53	2012-02-18 14:19:53	Plan 3	Cash	USD 2.00
2012-02-13 14:43:42		LOGIN	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	0	0B	0	0B	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 14:55:54		IDLE TIMEOUT	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	15119	20.684MB	8054	355.3KB	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:04:13		LOGIN	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	0	0B	0	0B	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:05:02		LOGOUT	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	1549	1.723MB	1295	145.5KB	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:05:52		LOGIN	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	1	52B	2	104B	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:15:56		KICK	F4E7CHCS	192.168.3.10	E4:CE:8F:4B:C2:9E	3799	2.008MB	4879	577.6KB	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:15:56		DELETE OD ACCOUNT	F4E7CHCS	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 14:20:24	2012-02-18 14:20:24	Plan 2	Cash	USD 2.00
2012-02-13 15:17:47		ADD OD ACCOUNT	6C6RW3FC	0.0.0.0	00:00:00:00:00:00	0	0B	0	0B	2012-02-13 15:17:47	2012-02-18 15:17:47	Plan 1	Cash	USD 5.00

- ➔ **Date :** Denote the current event's date and time
- ➔ **Location :** Denote the current device's location
- ➔ **Status :** There will show **10** types of status as below :
  - ✓ **LOGIN :** Denote the user login to the hotspot service
  - ✓ **LOGOUT :** Denote the user logout to the hotspot service
  - ✓ **IDLE TIMEOUT :** Denote the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
  - ✓ **USE UP :** Denote the quota of time of user is over
  - ✓ **VOLUME USE UP :** Denote the quota of volume of user is over
  - ✓ **KICK :** Denote the system kick out the user
  - ✓ **TIME OUT OF RANGE :** Denote the service time out of range
  - ✓ **ADD OD ACCOUNT :** Denote the system add On-Demand user account
  - ✓ **DELETE OD ACCOUNT :** Denote the system delete On-Demand user account
- ➔ **Passcode/Username :** Denote the user's passcode or username
- ➔ **IP :** Denote the user's IP address
- ➔ **MAC :** Denote the user's MAC address
- ➔ **Packets In :** Denote the current user's packets in
- ➔ **Bytes In :** Denote the current user's bytes in
- ➔ **Packet Out :** Denote the current user's packets out
- ➔ **Bytes Out :** Denote the current user's bytes out
- ➔ **Start Time :** Denote the start time on this users
- ➔ **End Time :** Denote the end time on this users

➔ **Plan :** Denote the current user's billing plan

➔ **Payment Type :** Denote the current payment type, there were show **Cash** or **PayPal**

➔ **Cost :** Denote the current service charge

- **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:A4:9E
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:A4:9E
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:A4:9E
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:A4:9
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:A4:9E
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:A4:9E
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:A4:9
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:A4:9
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:A4:9
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:A4:9
```

- **Billing Report :** The log

~ 2012/02/14 11:00:00

#	Name	On Demand	Payment Gateway	Thermal Printer	Amount	Qty	Unit Price	Subtotal	
0	Plan1	19	0	0	19	10.00	190.00	USD	
1	Plan2	10	0	0	10	5.00	50.00	USD	
2	Plan3	8	0	0	8	2.00	16.00	USD	
3	Plan4	10	0	0	10	2.00	20.00	USD	
4	Package 4	0	0	0	0	0.00	0.00	USD	
5	Package 5	0	0	0	0	0.00	0.00	USD	
6	Package 6	0	0	0	0	0.00	0.00	USD	
7	Package 7	0	0	0	0	0.00	0.00	USD	
8	Package 8	0	0	0	0	0.00	0.00	USD	
9	Package 9	0	0	0	0	0.00	0.00	USD	
		47	0	0	47				
							276.00	USD	

- **Monitor IP Report :** The log record unreachable monitor IP report. As shown in the following figure, each line is a Monitor IP report record consisting of **Date**, **Time**, **URL.**

```
2012/08/06 13:42:41  http://192.168.2.60  offline
2012/08/06 13:42:44  http://192.168.2.61  offline
2012/08/06 13:42:47  http://192.168.2.64  offline
2012/08/06 13:44:08  http://192.168.2.60  offline
2012/08/06 13:44:10  http://192.168.2.61  offline
2012/08/06 13:44:13  http://192.168.2.64  offline
```

- **AP Status :** The log record unreachable managed APs or detect rogue AP. As shown in the following figure for unreachable, each line is a AP Status record consisting of **Date**, **Time**, **Host Name**, **IP address** , **MAC address**

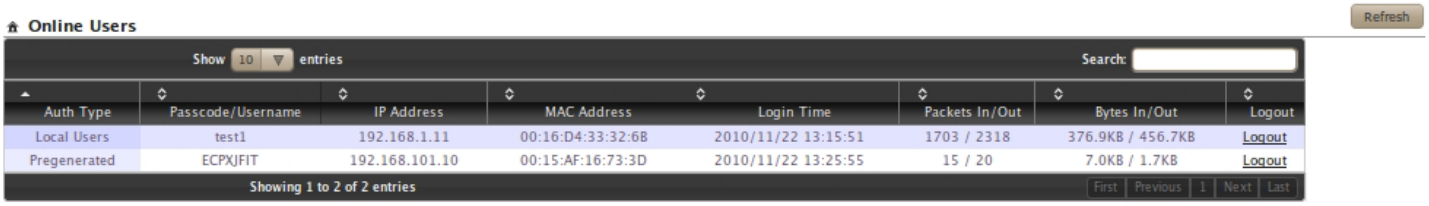
```
2012/08/06 12:38:39   AP952X  192.168.2.61   00026FC7CA60   offline
2012/08/06 12:38:39   AP952X  192.168.2.64   0011A31B3ED9   offline
2012/08/06 12:38:42   AP952X  192.168.2.60   00212F2F0CAB   offline
```

As shown in the following figure for detecting rogue AP, each line is a AP Status record consisting of **Date**, **Time**, **ESSID** , **MAC address**

```
2012/06/25 08:29:12   Rogue AP Detection:   Test_AP(00:21:2f:2f:0c:a6)
```

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

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

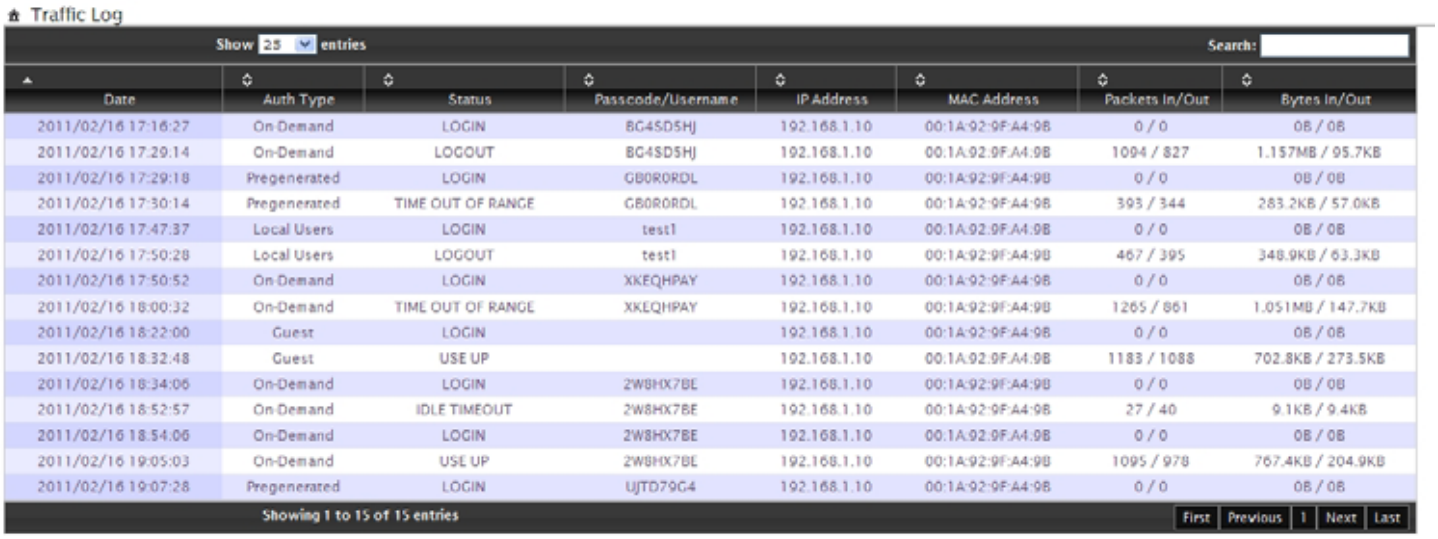
4.3.7 Log Information

The WMS-308N can record authentication traffic history or On-Demand event 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.

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**.



➔ **Date :** Denote 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 :** Denote the user login to the hotspot service
- ✓ **LOGOUT :** Denote the user logout to the hotspot service
- ✓ **IDLE TIMEOUT :** Denote the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
- ✓ **USE UP :** Denote the quota of time of user is over
- ✓ **SESSION TIMEOUT :** Denote the user session timeout for connecting to remote RAIDUS
- ✓ **VOLUME USE UP :** Denote the quota of volume of user is over
- ✓ **KICK :** Denote the system kick out the user
- ✓ **TIME OUT OF RANGE :** Denote the service time out of rangeule.

➔ **Passcode/Username :** Denote the user's passcode or username.

➔ **IP :** Denote the user's IP address

➔ **MAC :** Denote the user's MAC address

➔ **Packets In :** Denote the current user's packets in.

➔ **Bytes In :** Denote the current user's bytes in.

➔ **Packet Out :** Denote the current user's packets out.

➔ **Bytes Out :** Denote the current user's bytes out.

■ **On-Demand Log :**

As shown in the following figure, each line is traffic history record consisting of 14 fields : **Date**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out**, **Start Time**, **End Time**, **Plan**, **Payment Type** and **Cost**

➔ **Date :** Denote current event's date and time

➔ **Status :** There will show **10** types of status as below :

- ✓ **LOGIN :** Denote the user login to the On-Demand service
- ✓ **LOGOUT :** Denote the user logout to the on-demand service
- ✓ **IDLE TIMEOUT :** Denote the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
- ✓ **USE UP :** Denote the quota of time of user is over
- ✓ **VOLUME USE UP :** Denote the quota of volume of user is over
- ✓ **KICK :** Denote the system kick out the user.
- ✓ **TIME OUT OF RANGE :** Denote the service time out of range.

- ✓ **ADD OD ACCOUNT :** Denote the system add user account on On-Demand service
- ✓ **DELETE OD ACCOUNT :** Denote the system remove user account on on-demand service

On-Demand Log

Show 25 entries Search:

Date	Status	Passcode/Username	IP Address	MAC Address	Packets In/Out	Bytes In/Out	Start Time	End Time	Plan	Payment Type	Cost
2012/02/13 14:19:27	ADD OD ACCOUNT	QEJ6GNG9	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:19:27	2012/02/18 14:19:27	3	Cash	USD 2.00
2012/02/13 14:19:37	ADD OD ACCOUNT	KPE3YG6S	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:19:37	2012/02/18 14:19:37	3	Cash	USD 2.00
2012/02/13 14:19:45	ADD OD ACCOUNT	Z7CWKZ73	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:19:45	2012/02/18 14:19:45	3	Cash	USD 2.00
2012/02/13 14:19:53	ADD OD ACCOUNT	XMMN9W7C	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:19:53	2012/02/18 14:19:53	3	Cash	USD 2.00
2012/02/13 14:20:24	ADD OD ACCOUNT	F4E7CMCS	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 14:20:43	ADD OD ACCOUNT	J8DYNBTM	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:20:43	2012/02/18 14:20:43	0	Cash	USD 10.00
2012/02/13 14:37:24	LOGIN	XMMN9W7C	192.168.3.10	E4:CE:8F:4B:C2:9E	0 / 0	0B / 0B	2012/02/13 14:19:53	2012/02/18 14:19:53	3	Cash	USD 2.00
2012/02/13 14:42:46	VOLUME USE UP	XMMN9W7C	192.168.3.10	E4:CE:8F:4B:C2:9E	146258 / 80276	201.165MB / 3.376MB	2012/02/13 14:19:53	2012/02/18 14:19:53	3	Cash	USD 2.00
2012/02/13 14:43:42	LOGIN	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	0 / 0	0B / 0B	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 14:55:54	IDLE TIMEOUT	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	15119 / 8054	20.684MB / 355.3KB	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:04:13	LOGIN	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	0 / 0	0B / 0B	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:05:02	LOGOUT	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	1549 / 1295	1.723MB / 145.5KB	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:05:52	LOGIN	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	1 / 2	52B / 104B	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:15:56	KICK	F4E7CMCS	192.168.3.10	E4:CE:8F:4B:C2:9E	3799 / 4879	2.008MB / 577.6KB	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:15:56	DELETE OD ACCOUNT	F4E7CMCS	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 14:20:24	2012/02/18 14:20:24	2	Cash	USD 2.00
2012/02/13 15:17:47	ADD OD ACCOUNT	6C6RW3FC	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2012/02/13 15:17:47	2012/02/18 15:17:47	1	Cash	USD 5.00
2012/02/13 15:18:21	LOGIN	6C6RW3FC	192.168.3.10	E4:CE:8F:4B:C2:9E	0 / 0	0B / 0B	2012/02/13 15:17:47	2012/02/18 15:17:47	1	Cash	USD 5.00

Showing 1 to 17 of 17 entries First Previous 1 Next Last

- ➔ **Passcode/Username :** Denote the user's passcode or username.
- ➔ **IP :** Denote the user's IP address
- ➔ **MAC :** Denote the user's MAC address
- ➔ **Packets In :** Denote the current user's packets in.
- ➔ **Bytes In :** Denote the current user's bytes in.
- ➔ **Packet Out :** Denote the current user's packets out.
- ➔ **Bytes Out :** Denote the current user's bytes out.
- ➔ **Start Time :** Denote the start time of current service users
- ➔ **End Time :** Denote the end time of current service users
- ➔ **Plan :** Denote the current user's billing plan.
- ➔ **Payment Type :** Denote the current payment type, there were show **Cash** or **PayPal**
- ➔ **Cost :** Denote the current service charge

Click ***Refresh*** button to reload the page.

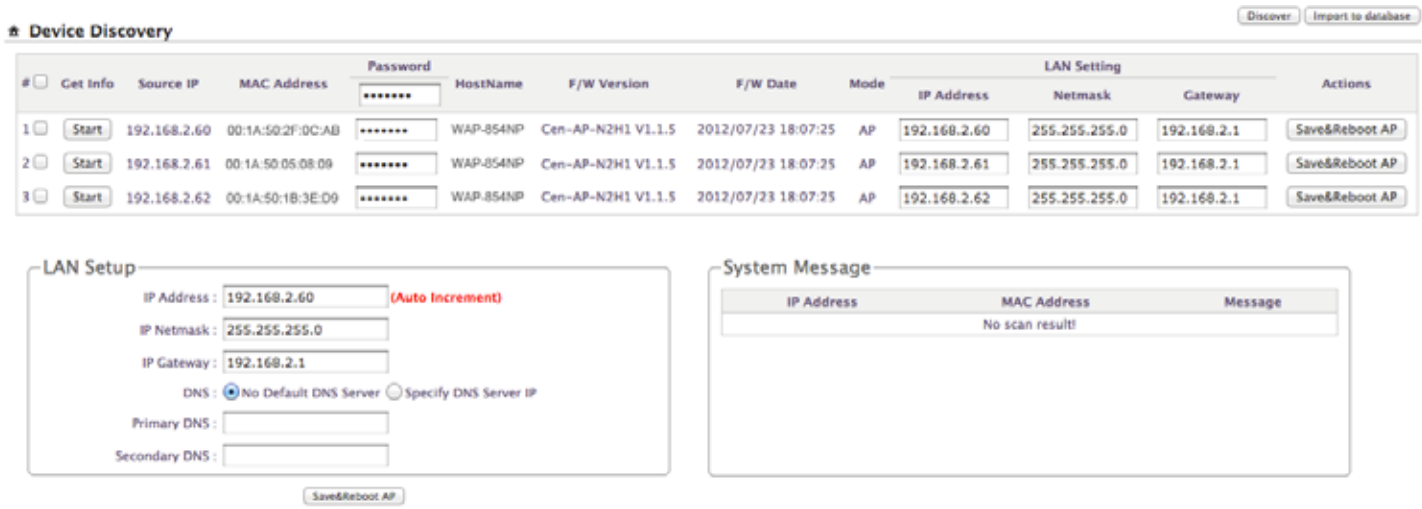
.

4.4 Control your Managed AP

WMS-308N supports to manage up to **120** managed access points (AP), WLAN users are connected to the network via the managed APs, and they can be configured in this section. This section include the following functions : **Device Discovery**, **Profile Management**, **Batch Setup Management**, **Group Setup Management**, **Traffic Monitor, AP Group Status**, **Rogue AP Detection, Notification** and **Website Monitor**.

4.4.1 Discovery Managed AP

Use this function to detect all of managed APs in the local area network by the current discovery process. Each discovered managed APs can configured Password, IP address, Netmask or Gateway. Importing managed APs' profile for Profile Management. Please click on **AP Management** → **Device Discovery**, the **Device Discovery** page will appear.



- **Discover :** Click ***Discover*** button to search managed AP device on your network
- **Get Info :** Click ***Start*** button to get current informations of the selected managed AP. Select desired managed AP and click ***Import to database*** button to import respective managed AP's profile to system, then the success message "**Import to Database**" will be displayed on **System Message** field. Up to **120** managed APs can be imported to system.

> If the managed AP's IP address are the same or already exist in the profile list, the system can't import profile to database, please use LAN Setup to configure different IP address of the respective managed AP before you import profile to system.

- **Source IP :** Denote the current IP address of the respective managed AP.
- **MAC Address :** Denote the current MAC address of the respective managed AP.

Password : Enter the specified the password in the password field of the top of the list and click ***Discover*** button to access managed AP, the system use "**default"** password to access managed AP. If managed AP can't get F/W

Version, F/W Date, Mode and LAN Setting, or display error message "**Error:401 Unauthorized**" on **System Message** field. Enter the correct password on the respective managed AP, and click ***Get Info*** button to get information on the respective managed AP, or click ***Save&Reboot AP*** button to change password of the respective managed AP.

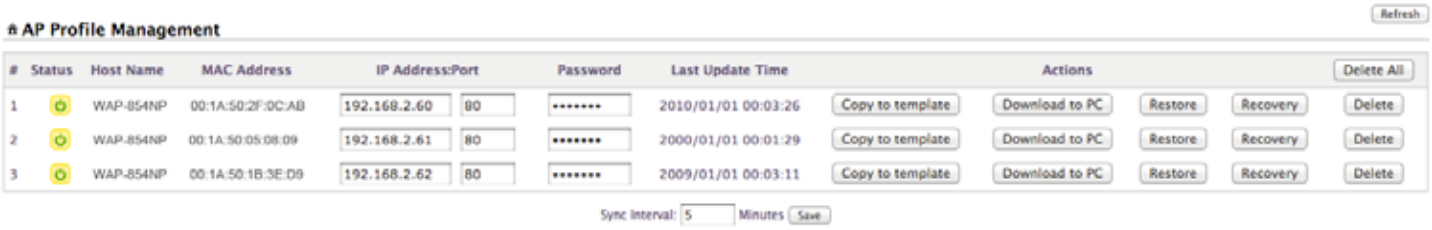
- **HostName :** Denote the current hostname of the respective managed AP.
- **F/W Version :** Denote the current firmware version of the respective managed AP.
- **F/W Date :** Denote the current firmware date of the respective managed AP.
- **Mode :** Denote the current operating mode of the respective managed AP.
- **LAN Setting :** Denote the current LAN setting of the respective managed AP, the respective managed AP can configure LAN setting and click ***Save&Reboot AP*** button to activated setting.
- **LAN Setup :** Assign IP range for specify managed APs on LAN Setup field and click ***Save&Reboot AP*** button to activated.
  - ➔ **IP Address :** Specify **Start** IP address as desired to set up the managed APs. Example : If you select three managed APs and set start IP address to 192.168.2.60, then the three managed APs' IP address range from 192.168.2.60 to 192.168.2.62.
  - ➔ **IP Netmask :** Specify IP netmask as desired to set up the managed APs.
  - ➔ **IP Gateway :** Specify default gateway as desired to set up the managed APs.
  - ➔ **DNS :** Specify primary and secondary DNS server IP as desired to set up the managed APs.
- **System Message :** Display system message for each managed APs after clicking ***Save&Reboot AP***, ***Start***, or ***Import to database*** button
  - ➔ **IP Address :** Denote the current IP address of the respective managed AP.
  - ➔ **MAC Address :** Denote the current MAC address of the respective managed AP.
  - ➔ **Message :** Display the current message of the respective managed AP.
    - ✓ **Error: 401 Unauthorized** – System can't access managed APs after clicking ***Start*** or ***Discover*** button to detect and access managed AP. The correct password must be entered on this field and Click ***Save&Reboot AP*** button to activated setting.
    - ✓ **Error: Device already exist!** – The same IP address or MAC address already exist in the database.
    - ✓ **Change IP: xxx:xxx:xxx:xxx** – System change IP address of the respective managed AP.
    - ✓ **Import to Database** – System import configuration profile of the respective managed AP to flash.
    - ✓ **Error: Profile Download ERROR** – System can't download profile of the respective managed AP, the IP address of managed AP need the same with controller.

Click ***Discover*** button, the system will rescan managed AP.

To support switch discovery, the **WAP-954GP** need use firmware version **2.0.16** or higher; the **WAP-854NP** need use firmware version 1.1.5 or higher; the **CPE-2010G / CPE-2000GN-1** need use firmware version **2.1.6** or higher; the **WLO-15814N / WLO-15802N** need use firmware version **V1.1.8** or higher.

4.4.2 Managed AP's Profiles Management

After administrator import profile of the respective managed AP, the each managed AP's profile will saved in the database of switch and listed status on AP Profile Management page. Up to **120** managed APs can be imported to system. This section provides profiles management of the respective managed AP. Administrator can copy profile to template database, download profile to PC, restore or auto-recovery profile for managed AP. Please click on **AP Management** → **Device Discovery**, the **AP Profile Management** setting field will appear on bottom of **Device Discovery** page.



- **Status :** Denote the current status of the respective managed AP. The following three status :
  - ✓ **On Line :** Denote the current managed AP able detected and accessed
  - ✓ **Off Line :** Denote the current managed AP unable detected and accessed
  - ✓ **Unauthorized** : Denote the current managed AP able detected, but **unable** accessed.

If Status shows **Unauthorized**, it indicates the **Password** is incorrect. You need change correct password and click **Save** button.

  - ✓ **Changed :** Indicate the current managed AP's settings changed. The switch will automatically download profile after the "**Auto Download Profile Interval**".
  - ✓ **Upgrading :** Indicate the system upgrade on current managed AP.

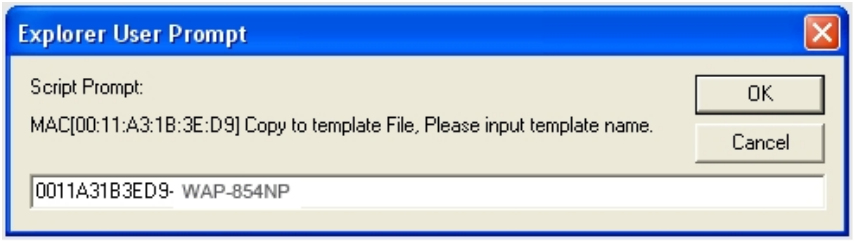
- **Host Name :** Denote the current system name of the respective managed AP.
- **AP MAC Address :** Denote the current MAC address of the respective managed AP.
- **IP Address/Port :** Denote the current LAN IP address and port of the respective managed AP.

If the managed AP's ***IP Address*** and ***Port*** changed after importing profile. Administrator need change IP address and port, then click **Save** button to activated. Otherwise the switch **unable** access managed AP.

- **Password :** The default password is "**default**" while administrator import managed AP's profile. Enter the correct password of the respective managed AP to access.

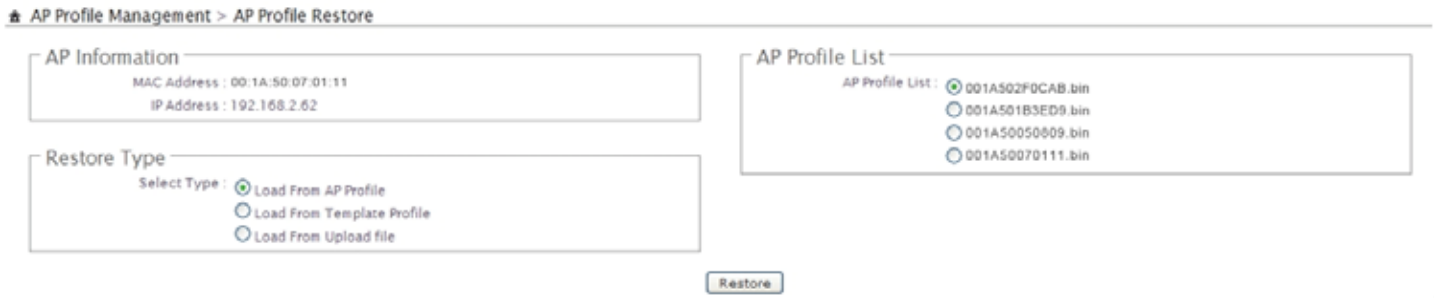
- **Last Update Time :** Denote the last update time of the respective managed AP.
- **Actions :** Click an action button to perform the appropriate action.

✓ **Copy To Template :** Click "**Copy**" button to save profile of the desired managed AP to template database. The alert window should be appear, then enter desired template's name and click **OK** button to save. Below depicts an example for copy profile to template. Template is a mechanism that keep one AP as a standard profile, then other APs can share the same Template without repeatedly keying all the parameters.



➔ **Download To PC :** Click "**Download**" button to save profile of the desired managed AP to local PC.

➔ **Restore :** Click "**Restore**" button to restore profile to managed AP, the AP Profile Restore page will appear.



✓ **AP Information :** Display the MAC and IP address information of the selected managed AP's profile.

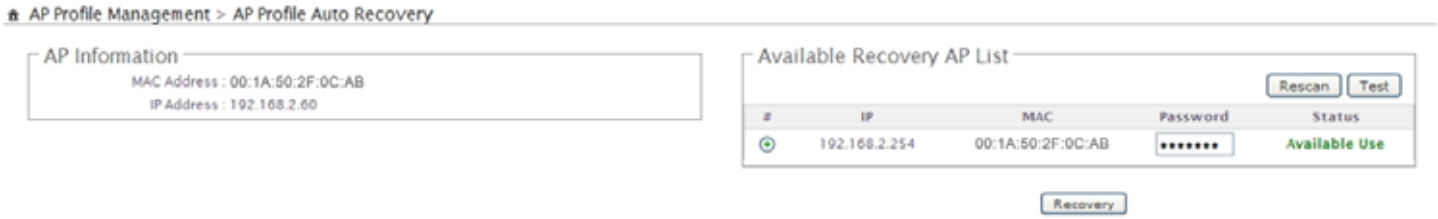
✓ **Restore Type :** Select desired profile type for selected managed AP to restore. The switch supports three types of restore method : **Load From AP Profile**, **Load From Template Profile** and **Load From Upload File**. Click "**Restore**" button to change current managed AP with the selected profile.

◆ **Load From AP Profile :** Select desired profile from AP Profile List. All imported profiles will be on the AP Profile List, the system use MAC address(**12 hex characters**) of the respective managed AP for profile's name.

◆ **Load From Template :** Template is a mechanism that keep one AP as a standard profile, then other APs can share the same Template without repeatedly keying all the parameters. Select desired profile from Template Profile List. All saved template profiles will be on the Template Profile List. Click **Delete** button to remove template file on the list.

- **Load From Upload File :** Select desired profile from local PC.

- **Auto Recovery :** Click "**Recovery**" button to upload profile to new or unlist managed AP, the AP Profile Auto Recovery page will appear.



- ✓ **AP Information :** Display the MAC and IP address informations of the selected managed AP's profile.
- ✓ **Available Recovery AP List :** All of available managed AP will display in the list. These managed APs not yet imported to profile list.
  - ◆ **IP :** Denote the current IP address of the respective available managed AP.
  - ◆ **MAC :** Denote the current MAC address of the respective available recovery AP.
  - ◆ **Password :** The default password is "**default**". Enter the correct password of the respective managed AP to access.
  - ◆ **Status :** Denote the current status of the respective managed AP. If the status shows "**Available Use**", the managed AP can used; if the status shows "**401 Unauthorized**", the managed AP can not accessed. The correct password must be entered on Password field and Click "**Test**" button to access.

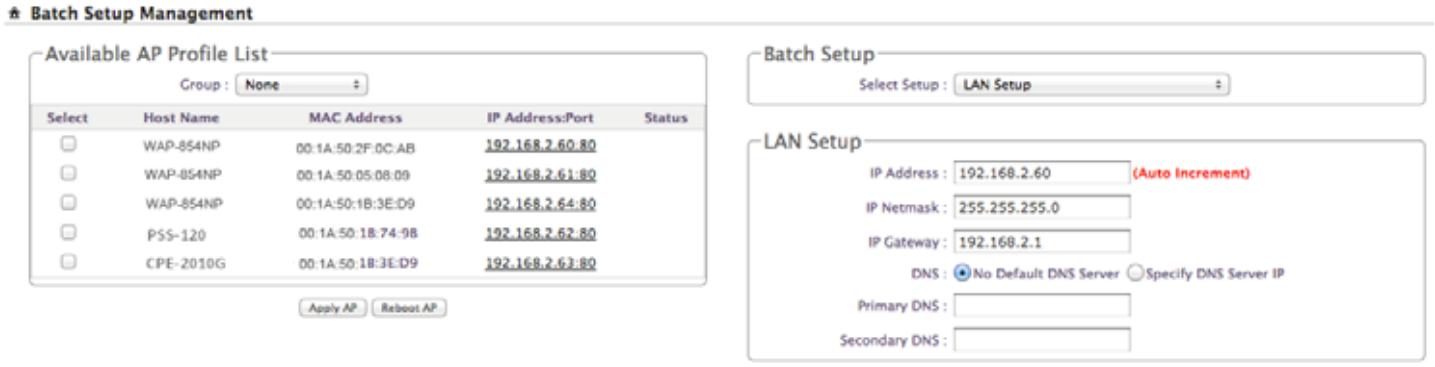
Click ***Rescan*** button to scan available managed AP.

- ➔ **Delete :** Click "**Delete**" button to remove profile on the list.

Sync Interval : The interval in the range of **1~14400** and set in unit of ***minutes***. The default value is **5** minutes. During every interval, the system automatically download profile or configure setting from the respective AP.

4.4.3 Managed AP Batch Setup

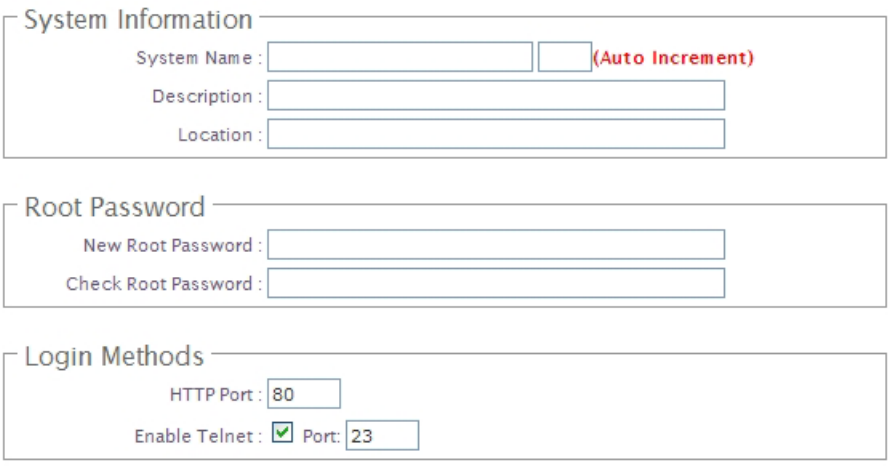
WMS-308N supports batch configuration of the managed APs, for automatically assigning IP addresses from a range of IP addresses to the selected managed APs; for configuring wireless general and security settings to the selected managed APs; for upgrading firmware to the selected managed APs.



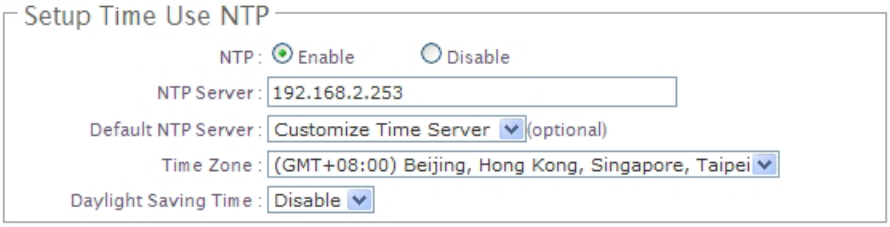
- **Available AP Profile List :** All managed AP's profiles will be displayed on the list.
  - ➔ **Group :** Select a specific group of managed APs for batch configuration.
  - ➔ **Select :** Select desired managed AP for batch configuration.
  - ➔ **Host Name :** Denote the current system name of the respective managed AP.
  - ➔ **AP MAC Address :** Denote the current MAC address of the respective managed AP.
  - ➔ **IP Address :** Denote the current IP address of the respective managed AP.
  - ➔ **Status :** Denote the current status of the respective managed AP after click "**Apply AP**" or "**Reboot AP**" button for batching configuration. The following status : Save LAN/Wireless/VAP Error[Connect Fail(1)], Upgrade Firmware Error[Connect Fail(1)], Upgrade Firmware Error[Firmware Upload ERROR], Save LAN/Wireless/VAP Success, Check Free Memery, Upgrade Firmware Now, Rebooting .

1. To prevent data loss during firmware upgrade, please backup current settings before proceeding.
2. Do not interrupt during firmware upgrade including switch power on/off or unplug RJ-45 cable from PoE port as this may damage managed APs.

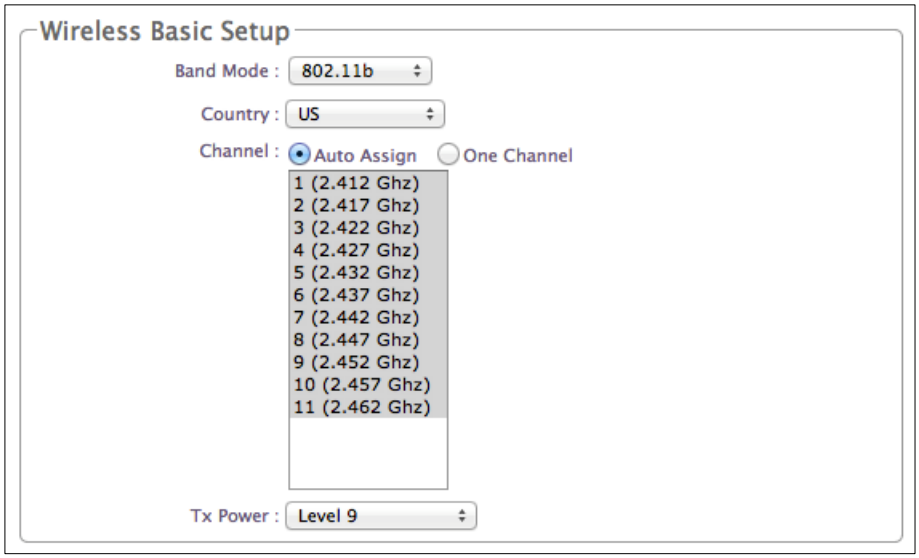
- **Batch Setup :** Select desired for batch configuration, the related setting field will appear.
  - ➔ **LAN Setup :** Specify IP address, Netmask, Gateway and DNS for selected managed APs.
  - ➔ **Management Setup :** Specify desired system information, administrator's password, HTTP's port and Telnet 's port.



➔ **Time Server Setup :** Specify correct Time zone setting for selected managed APs. The default NTP Server is switch's LAN IP address. The local time of managed APs will follow WMS-308N's local time.



➔ **Wireless Basic Setup :** Specify Band, Channel and Tx power for selected managed APs.

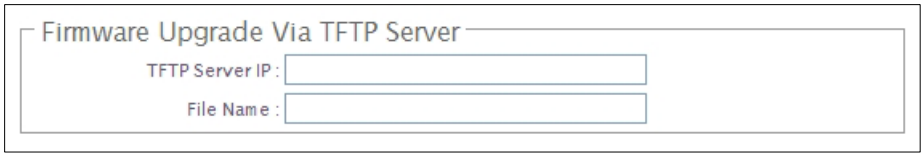


If you configure wireless basic setting for WLO-15814N/WLO-15802N, you need select in **Wireless Basic Setup(WLO-158xx series)** option

➔ **VAP Setup :** Specify **ESSID** and **Security Type** for selected managed APs.

If you configure VAP setting for WLO-15814N/WLO-15802N, you need select in **VAP Setup(WLO-158xx Series)** option

➔ **Firmware Upgrade Via TFTP :** Enter TFTP Server IP address and firmware file, and then click "**Apply AP**" button to upgrade.

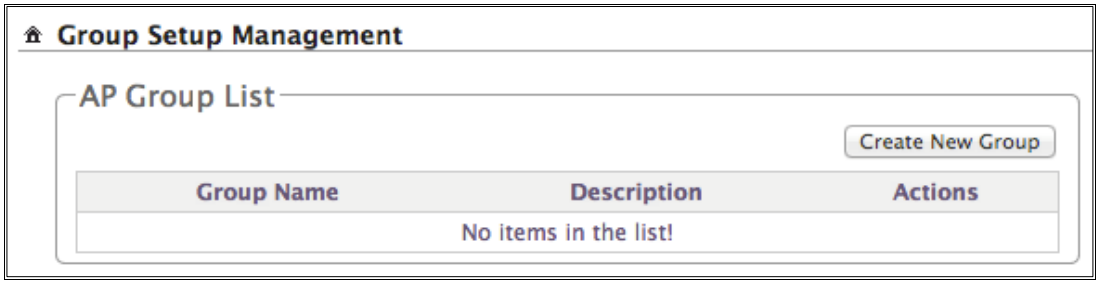


➔ **Upgrade Firmware Via URL :** Enter URL address(example : http://192.168.2.10/xxx.bin), and then click "**Apply AP**" button to upgrade.

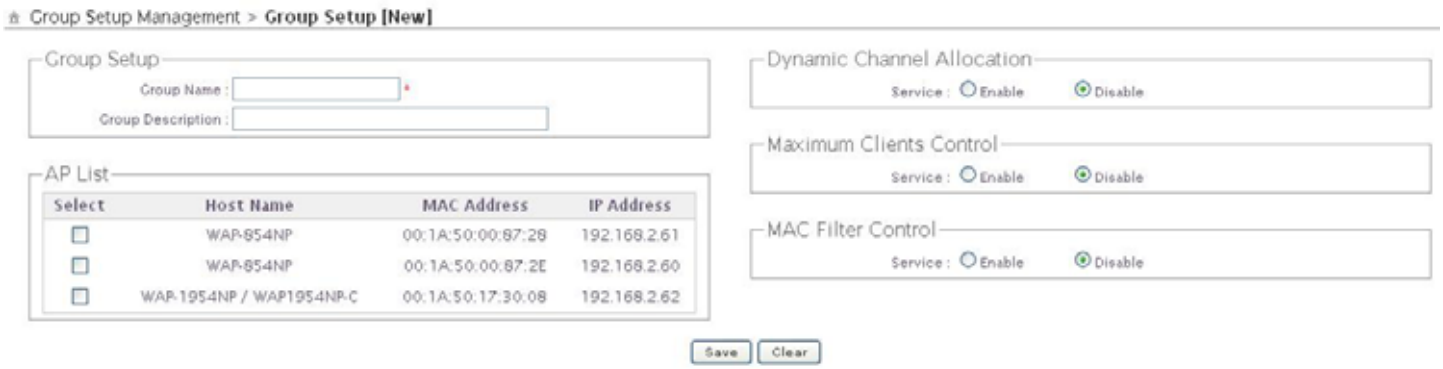
1. To prevent data loss during firmware upgrade, please backup current settings before proceeding.
2. Do not interrupt during firmware upgrade including switch power on/off or unplug RJ-45 cable from PoE port as this may damage managed APs.

4.4.4 Managed AP Group Management

Administrator specify managed APs in the same group, and locate managed APs on the specified map. The switch supports automatically channel assignment and power setting for managed APs, real time wireless clients limitation in the same group managed APs. Please click on **AP Management** → **Group Setup Management**, the **Group Setup Management** page will appear.



- **Create New Group :** Click on ***Create New Group*** button, the group setup page will appear.



➔ **Group Setup :**

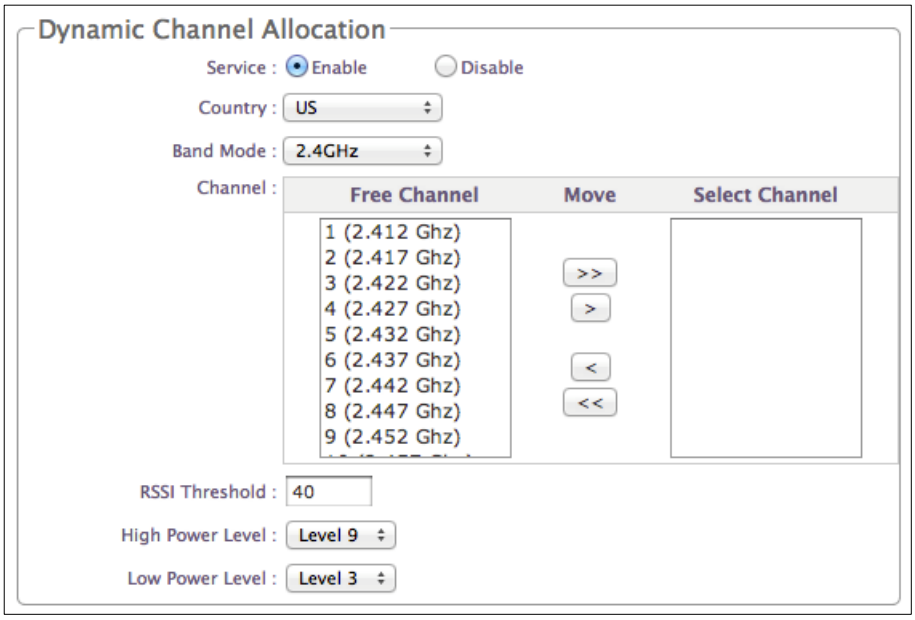
✓ **Group Name :** Specify desired name for group

✓ **Group Description :** Enter appropriate text to denote this group

➔ **AP List :** Select available AP for group

➔ **Dynamic Channel Allocation :** By default, it's "**Disable**". To ***Enable*** to activated dynamic channel allocation function, and select desired channels with specify **RSSI Threshold** and **High/Low Power Level**, the system will automatically assign suitable channel and TX power for group managed APs after the **Sync Interval (Please see section 4.4.2)**. **Figure 4-3** depict flow chart for dynamic channel allocation.

RSSI Threshold **%0** indicates **-95** dbm on WAP-954GP and WAP-854NP; RSSI Threshold **%100** respectively indicates **-35** dbm and **-1** dbm on WAP-954GP and WAP-854NP



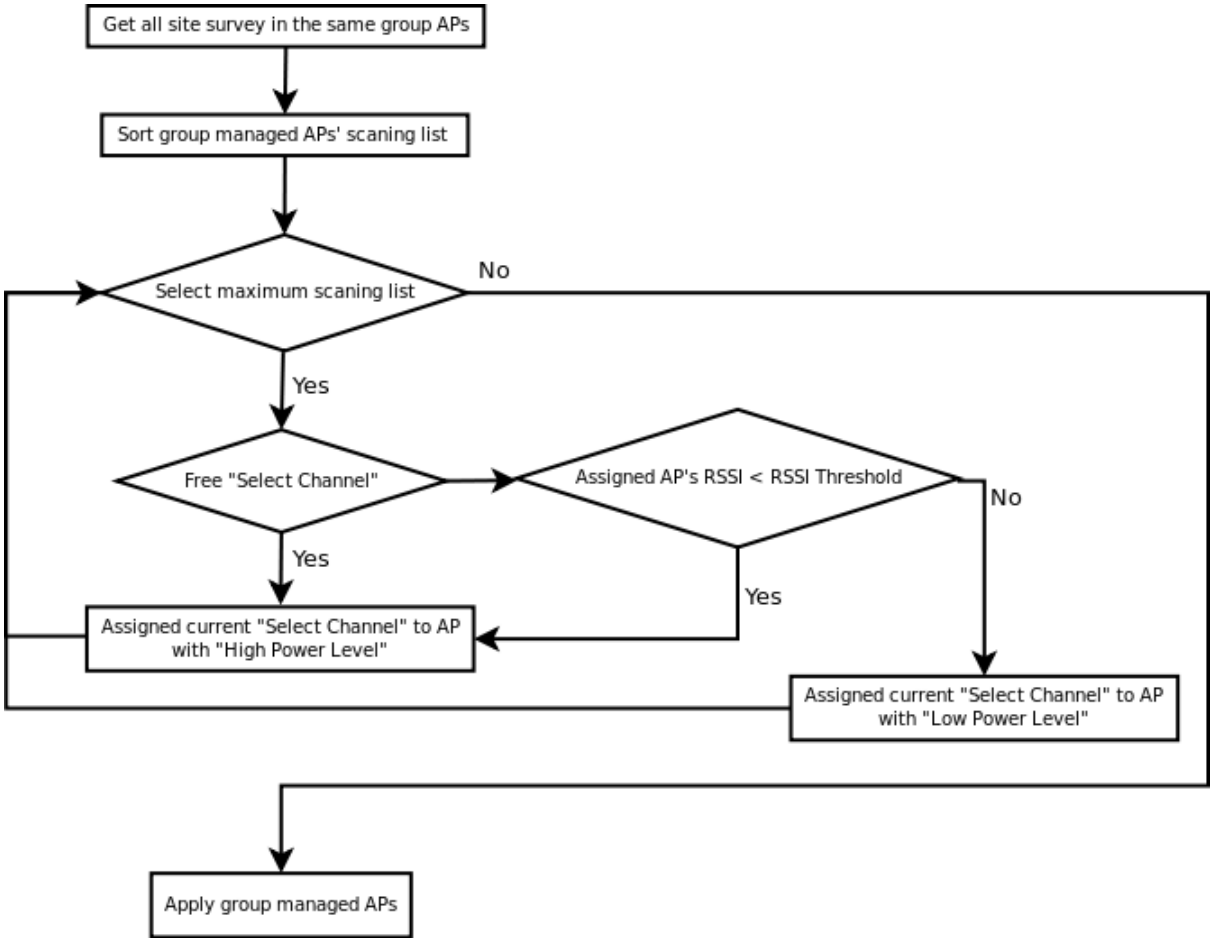
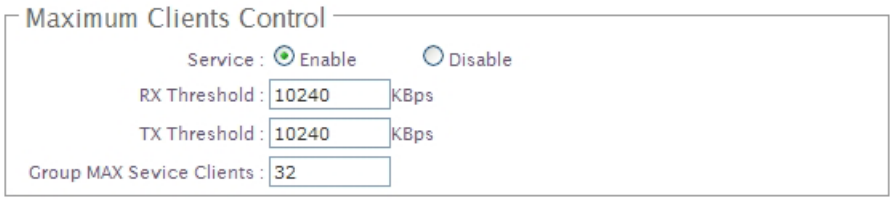


Figure 4-3 Dynamic Channel and Tx Power Allocation Flow Chart

➔ **Maximum Clients Control :** By default, it's "**Disable**". To **Enable** to activated maximum wireless clients limitation in the group, the system will automatically assign maximum clients limitation for group managed APs after the **Sync Interval** (Please see **section 4.4.2**)



- ✓ **Rx Threshold :** Rx Threshold is in the range of **0~120400** and set in unit of *KBps*. The default value is **10240** KBps. Specify desired receive bandwidth for wireless clients limitation in the same group of each managed AP. The wireless clients unable connect to managed AP, when bandwidth of receive achieve limitation.
- ✓ **Tx Threshold :** Tx Threshold is in the range of **0~120400** and set in unit of *KBps*. The default value is **10240** KBps. Specify desired transmit bandwidth for wireless clients limitation in the same group of each managed AP. The wireless clients unable connect to managed AP, when bandwidth of transmit achieve limitation.
- ✓ **Group MAX Service Clients :** Enter maximum number of clients to a desired number in the range of **0~256**. The default value is **32**. For example, while the number of client is set to 32, only 32 clients are allowed to connect with all managed AP in the this group

➔ **MAC Filter Control :** By default, it's "**Disable**". To **Enable** to activate MAC filter control in the same group APs, the system will automatically assign block MAC address of the wireless clients for group managed APs after the **Sync Interval** (Please see **section 4.4.2**)

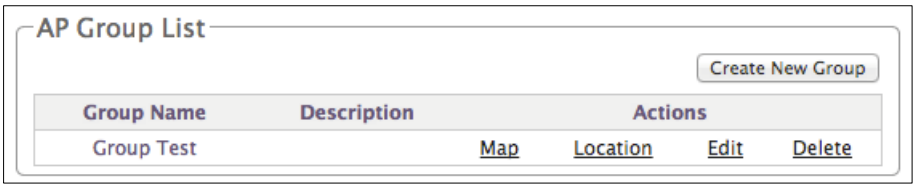
- ✓ **MAC Address :** Enter MAC address in this field. There are maximum **20** clients allowed in this MAC Filter List.

The MAC Address of the wireless clients can be added and removed to the MAC Filter List using the ***Add*** and ***Delete*** button.

You also can add specify MAC address form **Group Online Users** page(Please see **section 4.4.6**).

When these services enabled, the switch will automatically control channel, txpower, maximum clients and MAC filter during every "**Sync Interval**" (Please see **section 4.4.2**).

■ **AP Group List :** Display created group in the list.



➔ **Group Name :** Denote the name of group.

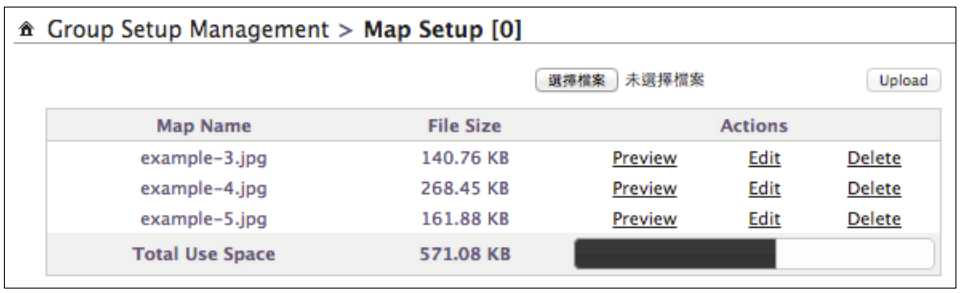
➔ **Description :** Denote the additional description of group.

➔ **Actions :** Click an action button to perform the appropriate action.

✓ **Edit :** Click option to configure settings of the respective group in the list.

✓ **Delete :** Click option to configure settings of the respective group in the list.

✓ **Map :** Use this option to add maps or edit the current map(s). The system supports **JPG**, **JPEG**, **PNG** and **GIF** format.



◆ **Map Name :** Denote the current map's name.

◆ **File Size :** Denote the current map's size

◆ **Actions :** Click an action button to perform the appropriate action.

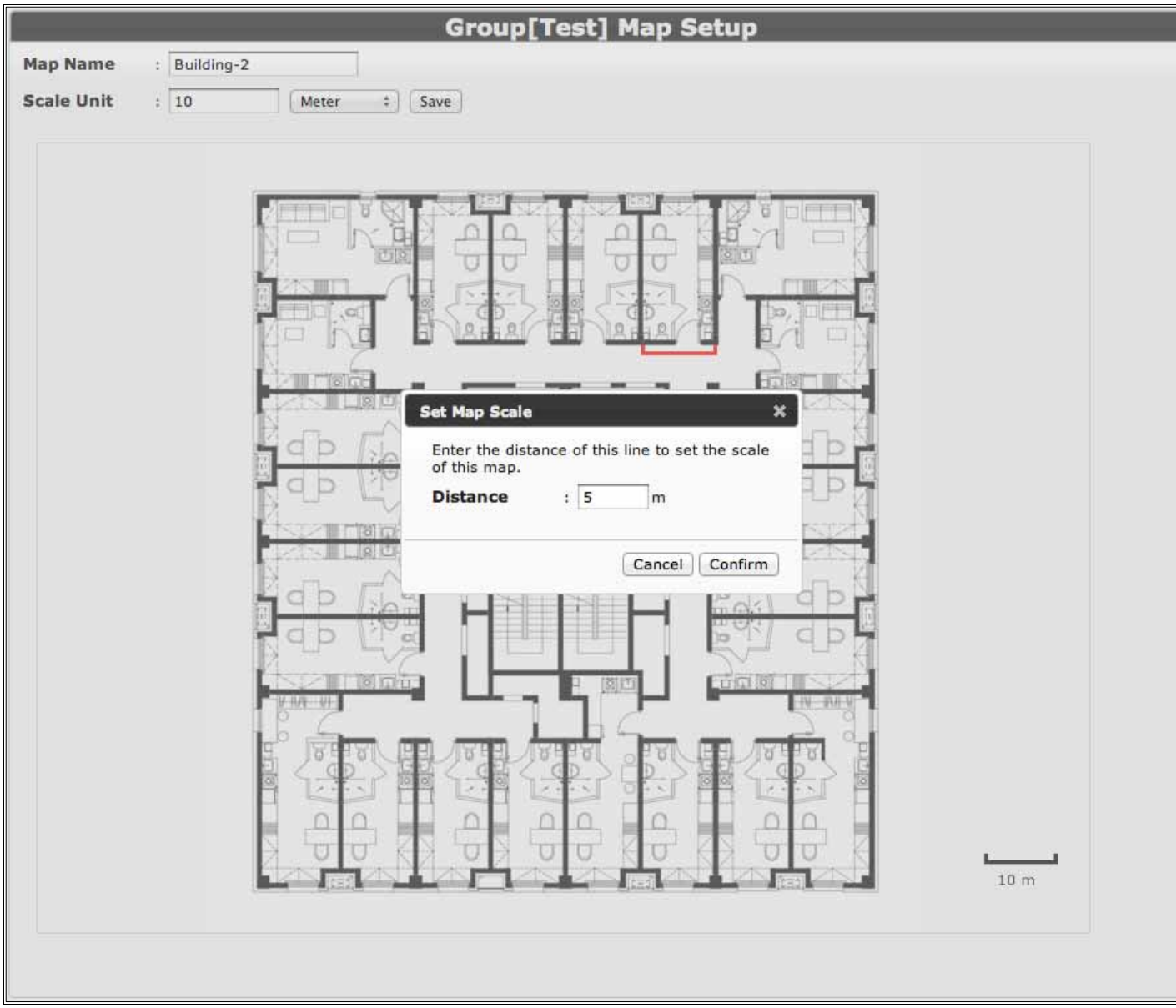
⅄ **Preview :** If multiple maps have been uploaded, you can select which map you want to view using this option.

⅄ **Edit :** Use this option to change map's name and define the scale of the map.

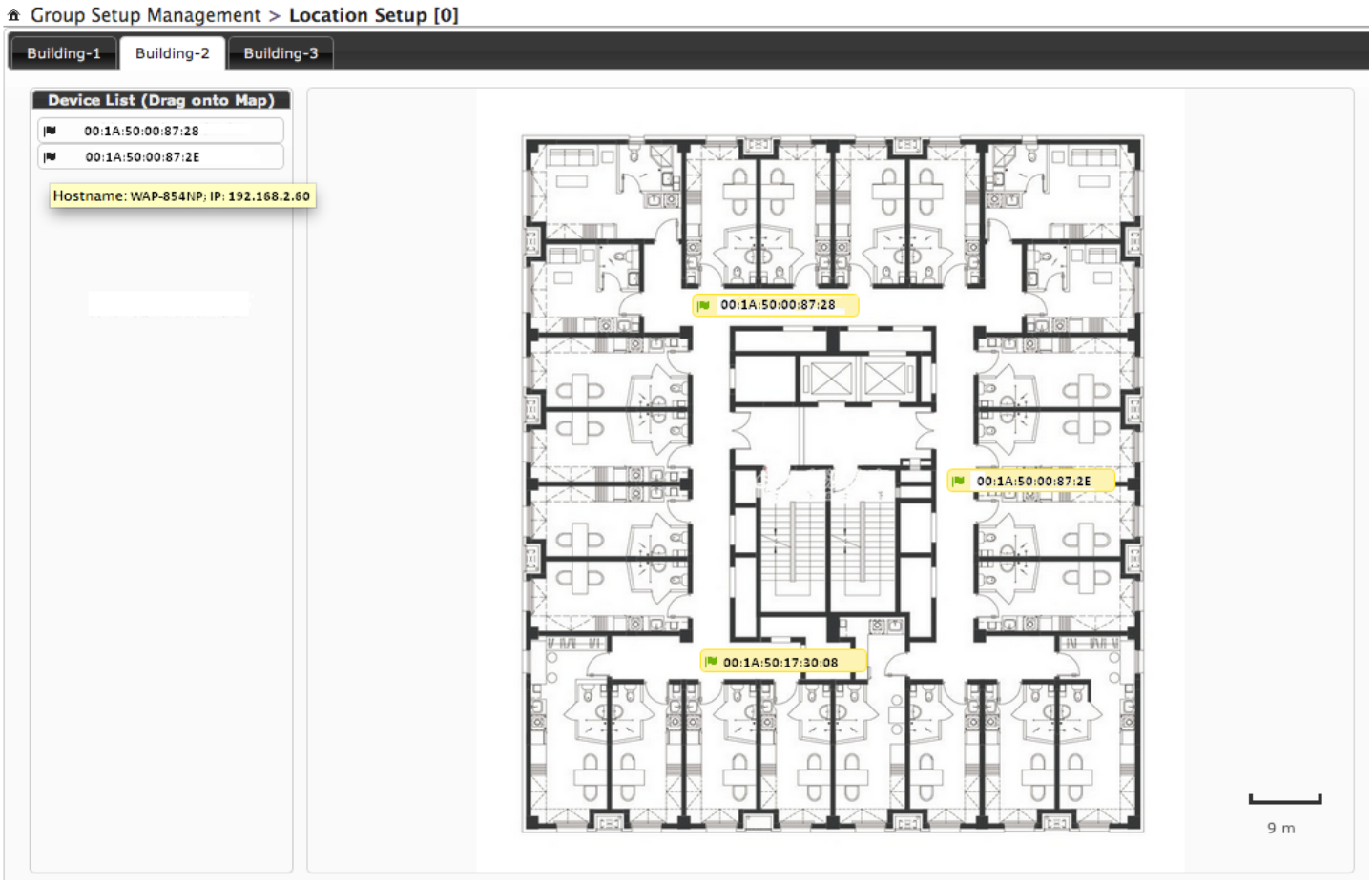
⅄ **Delete :** Use this option to remove map.

- **Total Used Space :** Denote the current used storage space, the total storage is **1MB** for uploading e-map.

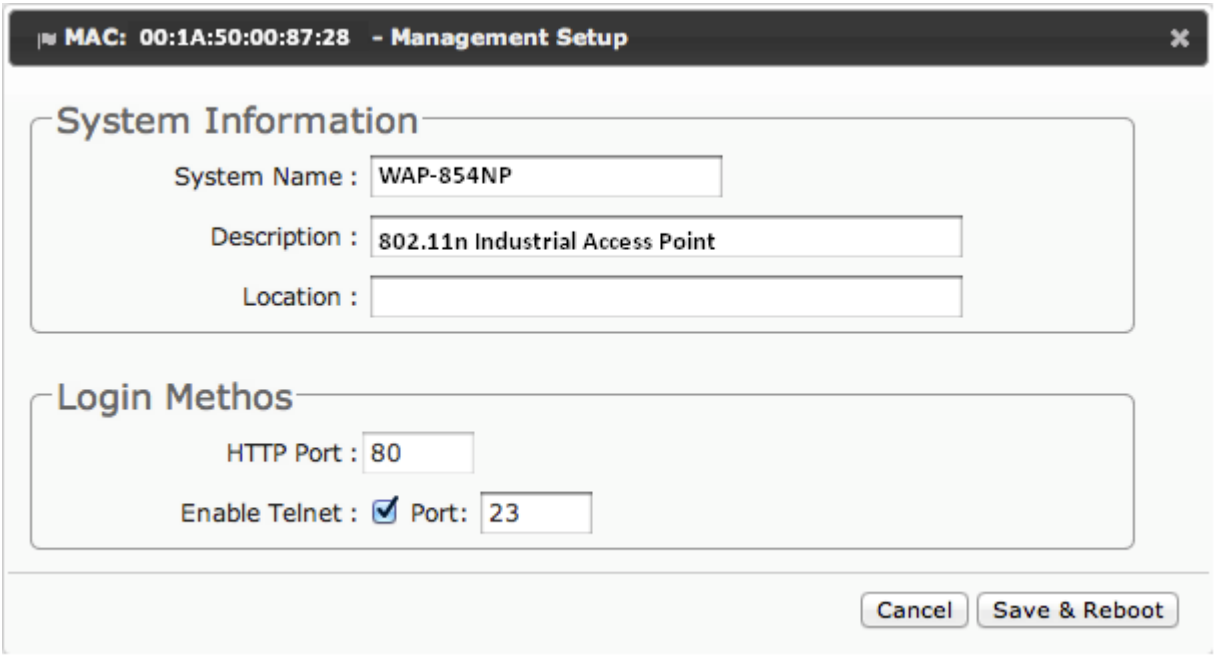
Once you click the Edit link, the Map Setup page will appear. You can change Map Name and Scale Unit. Use your mouse to click and hold to draw a line in the area that you want to use to set the scale of the map, then the Setup Map Scale setting window will popup. Enter the distance that the line represents in the Distance setting field, then lick *Confirm* button to complete, and the new scale value will be displayed at the right-bottom of the map or Scale Unit setting field. The distance is specified in meters by default but you can switch to kilometer, feet or mile using the drop-down selection menu on Scale Unit setting field. Click *Save* button to save your changes



✓ **Location :** Use this option to place managed AP(s) on the map. Drag managed APs icon from the Device List on the left to the appropriate location(s) on the map. Move your mouse on managed APs icon, the Hostname and IP address information will be displayed, as illustrated.



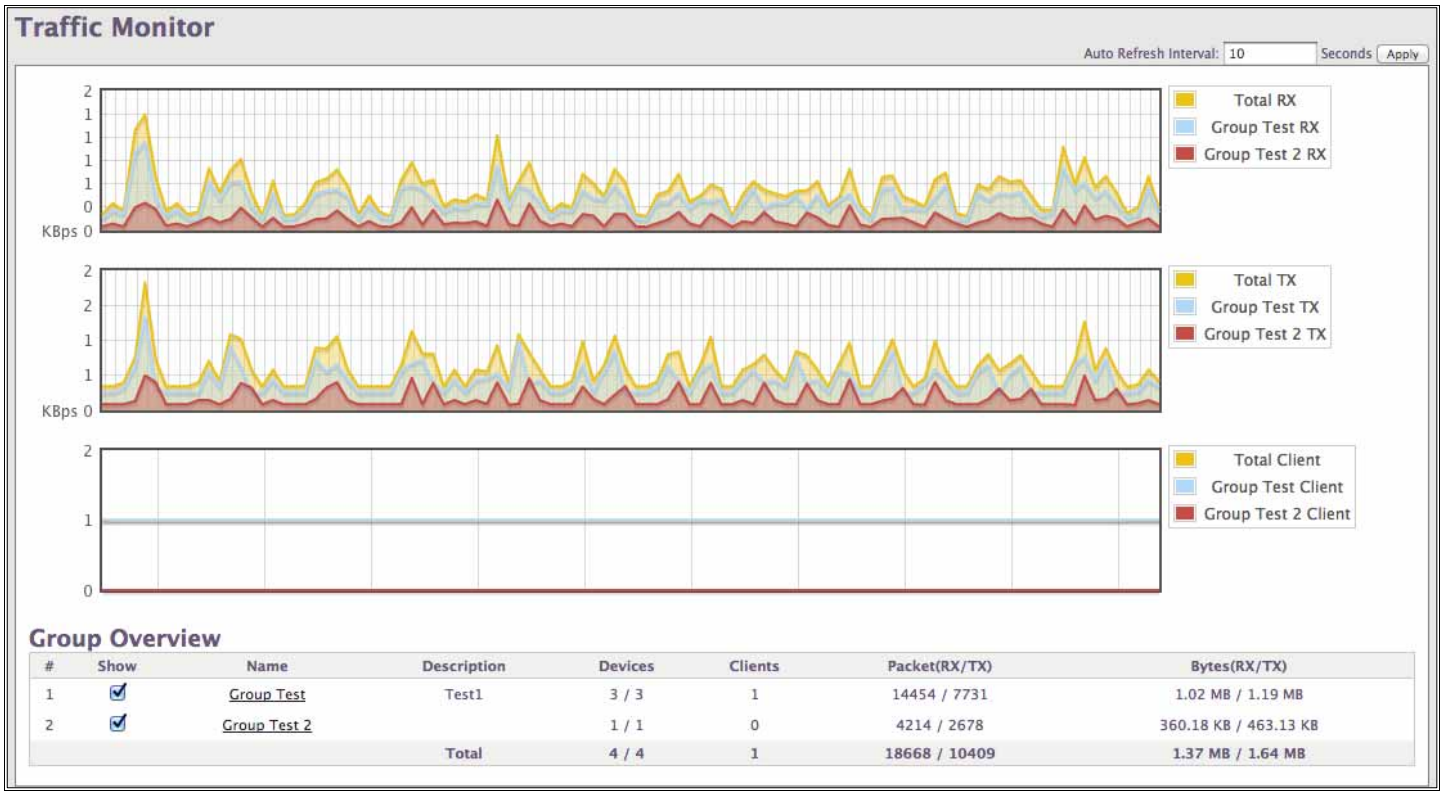
Double click on managed APs icon, the basic management setting page will appear. Specify desired **System Name**, **Description**, **Location**, **HTTP Port** and **Telnet Port**, then click "**Save & Reboot**" button to activate your change on managed APs



4.4.5 AP Group Status

This section provides visual graph of network traffic and online users on real time. Please click on **AP Management** → **Traffic Monitor**, the **Traffic Monitor** page will appear.

.



- **Auto Refresh Interval :** The interval is bigger than **10** and set in unit of ***seconds***. The default value is **10** minutes. During every interval, the system automatically gets network traffic and online users on the respective group or AP.
- **Apply :** Click this button to save changes.
- **Show :** Click this option to add specific group on visual graph of network traffic and online users
- **Name :** Denote the name of the group
- **Description :** Denote the additional information of group
- **Devices :** Denote the current connected AP and total AP in the group
- **Clients :** Denote the number of clients connected to this group
- **Packet(RX/TX) :** Denote the transmitted and received packet of data by the group.
- **Bytes(RX/TX) :** Denote the transmitted and received bytes of data by the group.

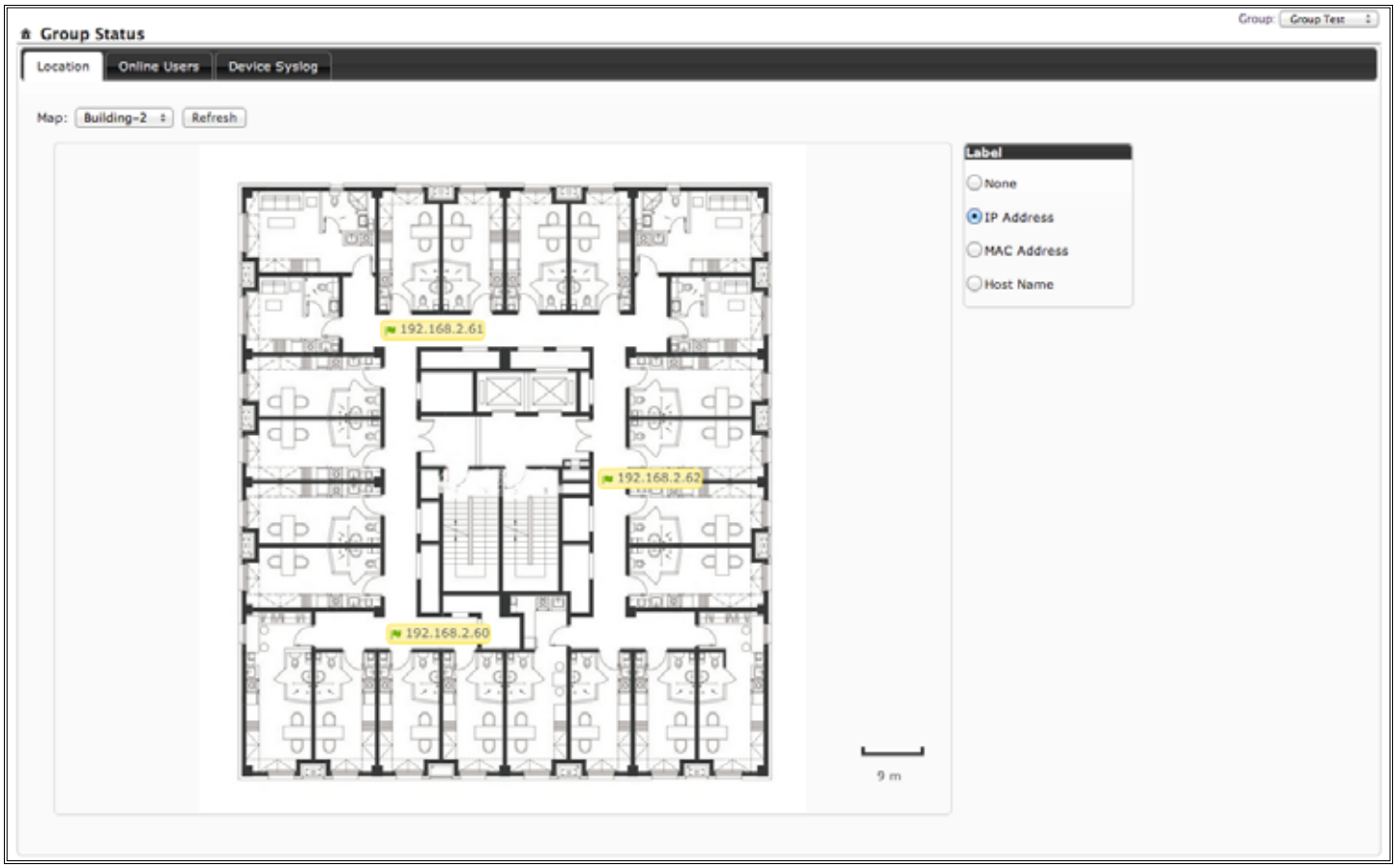
Click specific hyperlinks on Name of Group, the network traffic of managed APs will be displayed, as illustrated.

- **IP Address :** Denote the IP address of the AP.
- **MAC Address :** Denote the MAC address of the AP.
- **F/W Version :** Denote the firmware version of the AP.
- **System Up Time :** Denote the system up time of the AP.
- **Status :** Denote the currently connected status of the AP.
- **Clients :** Denote the number of clients connected to the AP.
- **Packet(RX/TX) :** Denote the transmitted and received packet of data by the AP.
- **Bytes(RX/TX) :** Denote the transmitted and received bytes of data by the AP.
- **Actions :** Click an action button to perform the appropriate action.
  - ➔ **Locate :** Click this button to locate the AP, the LED on the AP will flash so that you can place it in the correct location on the map. The LED will flash around **10** seconds
  - ➔ **Reboot :** Click this button to restart the selected AP

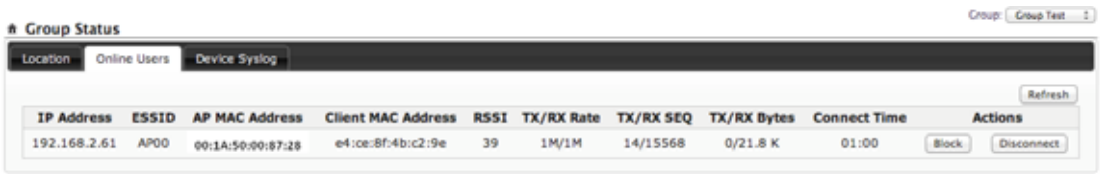
恩

4.4.6 Group Status

This section provides detailed informations of group on **Location**, **Online Users** and **Device Syslog** can be reviewed via this page. Please click on **AP Management** → **Group Status**, the **Group Status** page will appear.



- **Group :** Select a specific group of managed APs to get group status
- **Location :** Show current managed AP's location on the respective group. The **green flag mark** indicates the AP can be accessed and **double click** to view the respective "**System Information**", the **question mark** indicates the AP can not be accessed.
  - ➔ **Map :** If multiple maps have been uploaded, you can select which map you want to view location
  - ➔ **Refresh :** Click this button to reload the page
  - ➔ **Label :** Displays the name applied to the AP on the map.
- **Online Users :** Display a list of users that are connected to the managed AP of the respective group.



➔ **Refresh :** Click this button to reload the page

➔ **IP Address :** Display the IP address of the AP that the client is connected to.

➔ **ESSID :** Display the ESSID of the AP that the client is connected to.

➔ **AP MAC Address :** Display the MAC address of the AP that the client is connected to.

➔ **Client MAC Address :** Display the MAC address of the connected client.

➔ **RSSI :** Display the signal strength from the AP to the client

➔ **TX/RX Rate :** Display the transmitted and received data rate by the client.

➔ **TX/RX SEQ :** Display the transmitted and received sequence of package by the client.

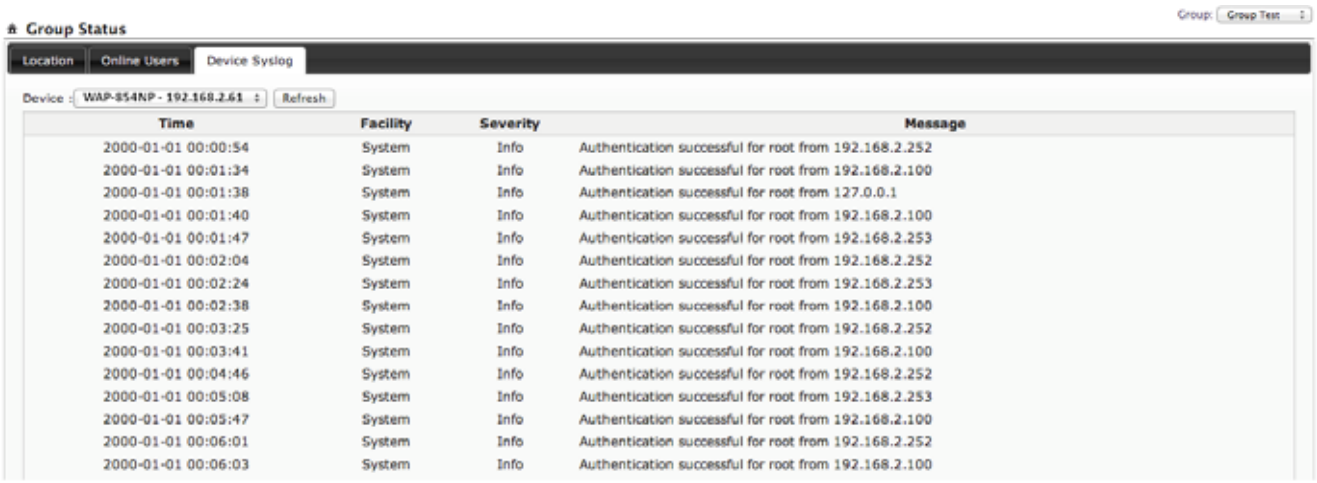
➔ **TX/RX Bytes :** Display the transmitted and received bytes of data by the client.

➔ **Connect Time :** Display the total time the client has been connected for this session

➔ **Actions :** Click an action button to perform the appropriate action.

- ✓ **Block :** Click this button to block a specific client from accessing the AP of the respective group. This will add the client to the MAC Filter List of the respective group.(Please see **section 4.4.4**)
- ✓ **Disconnect :** Click this button to reconnect a specific client from accessing the AP of the respective group.

■ **Devices Syslog :** Display a list of recent events by the AP of the respective group.



➔ **Devices :** Select a specific managed AP to get system log

➔ **Refresh :** Click this button to reload the page

➔ **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.

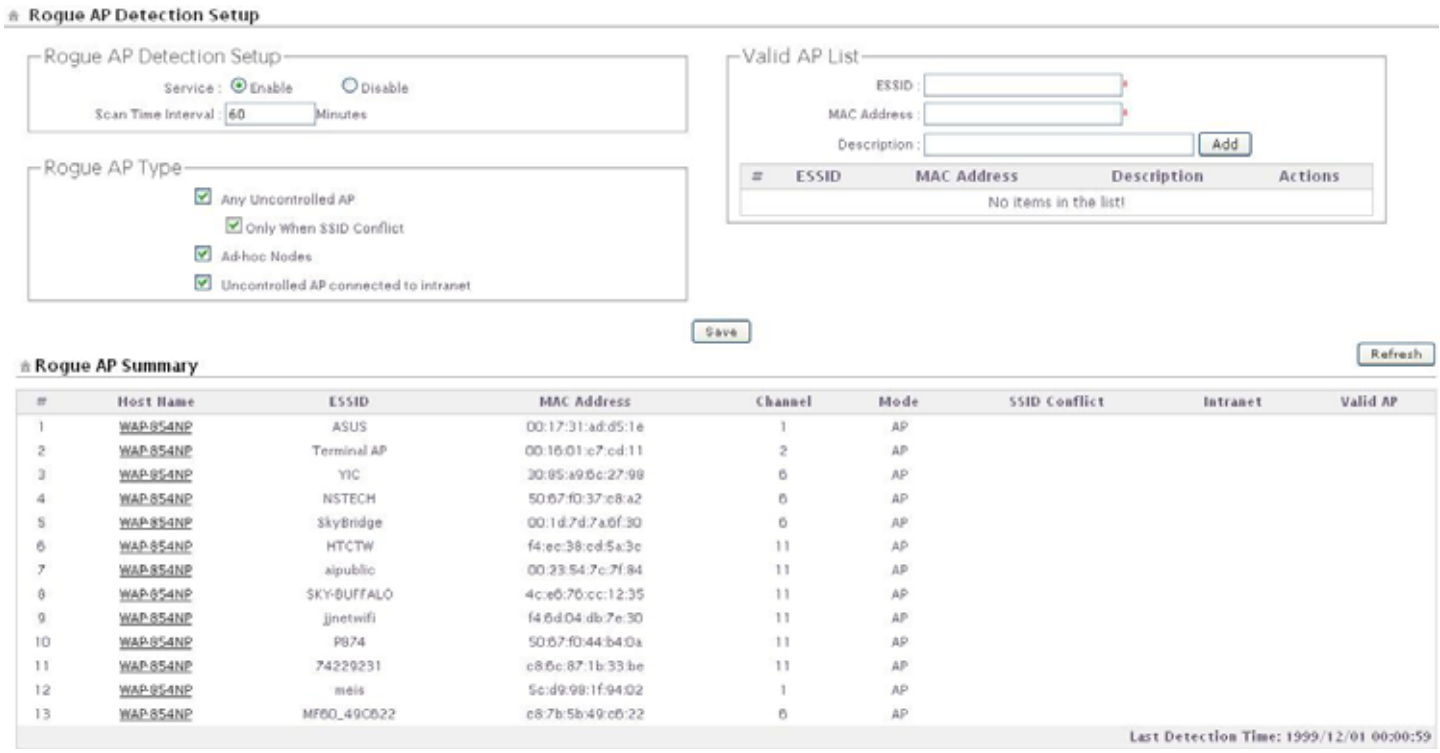
➔ **Message :** Description of the event.

4.4.7 Rogue AP Detection

Wireless networks extend wired networks and increase worker productivity and access to information. However, an unauthorized wireless network presents an additional layer of security concerns. Less thought is put into port security on wired networks, and wireless networks are an easy extension to wired networks.

Therefore, an employee who brings his or her own Access Point (AP) into a well−secured wireless or wired infrastructure and allows unauthorized users access to this otherwise secured network can easily compromise a secure network.

Rogue detection allows the network administrator to monitor and eliminate this security concern. This section provides rogue AP detection, the system can detect the AP is not in the managed AP list. Please click on **AP Management** → **Rogue AP Detection**, the **Rogue AP Detection Setup** page will appear.



- **Rogue AP Detection Setup**
  - ➔ **Service :** By default, it's "**Disable**". To **Enable** to activated rogue detection.
  - ➔ **Scan Time Interval :**The default value is **60** and set in unit of ***minutes***. During every interval, the system will automatically detect rogue AP from the signal coverage of all managed APs
- **Rogue AP Type :** Select what kind of rogue AP is particularly mared into the list.
  - ➔ **Any Uncontrolled AP :** Click this option, the system will find out the rogue AP within the signal coverage of the managed APs
    - ✓ **Only When SSID Conflict :** Click this option, the system only find out the rogue AP with the same ESSID of the all managed AP and particularly mark into the list

- ➔ **Ad-hoc Nodes :** Click this option, the system will find out the Ad-hoc rogue AP within the signal coverage of the managed Aps
- ➔ **Uncontrolled AP connected to intranet :** Click this option, the system will find out the intranet rogue AP within the signal coverage of the managed APs and particularly mark into the list

■ **Valid AP List :** Assign specified uncontrolled AP into the valid list , the system will particularly mark in the Rogue AP Summary.

- ➔ **ESSID :** Enter specified ESSID into the valid list
- ➔ **MAC Address :** Enter specified MAC address of AP into the valid list
- ➔ **Description :** Enter appropriate text to denote this valid AP
- ➔ **Add :** Click this button to add valid AP into the list
- ➔ **Actions :** Click an action button to perform the appropriate action.
  - ◆ **Delete :** Click this button to remove the specified valid AP in the list

■ **Rogue AP Summary :** List all of rogue APs within the signal coverage of the managed APs

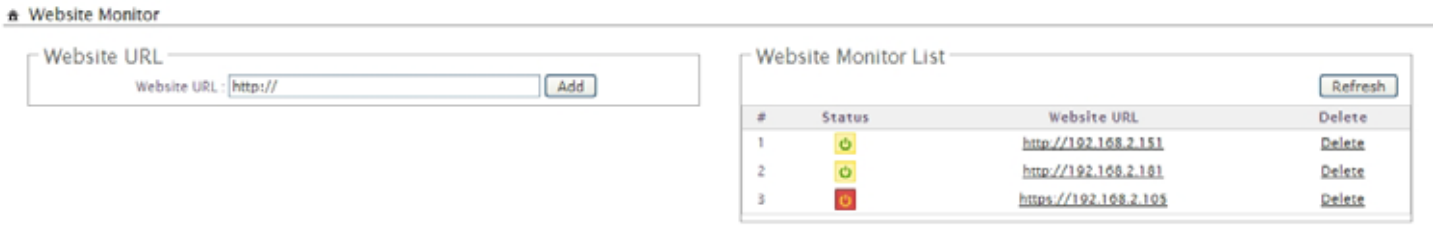
- ➔ **Refresh :** Click this button to reload the page
- ➔ **Host Name :** Denote the current hostname of the managed AP
- ➔ **ESSID :** Denote the current ESSID of the rogue AP
- ➔ **MAC Address :** Denote the current MAC address of the rogue AP
- ➔ **Channel :** Denote the current Channel of the rogue AP
- ➔ **Mode :** Denote the current mode of the rogue AP, there will be **AP** or **Ad-hoc** mode
- ➔ **SSID Conflict :** If the rogue AP matched to "**Only When SSID Conflict**" condition, there will be marked
- ➔ **Intranet :** If the rogue AP matched to "**Uncontrolled AP connected to intranet**" condition, there will be marked
- ➔ **Valid AP :** If the rogue AP is in the Valid AP List, there will be marked

If you want to add valid AP from Rogue AP Summary, move your mouse on specified rogue AP on the list and double-click, the specified rogue AP's ESSID and MAC address will display in the Valid AP List setting field. Click ***Add*** button to add to list.

■ **Last Detection Time :** Denote the last detection time

4.4.6 Website Monitor

WMS-308N will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click Add button and these settings will become effective immediately. Green light means online and red light means offline. The system provides **50** monitor IP address fields on the “Website Monitor List”. Please click on **AP Management** → **Website Monitor**, the **Website Monitor** page will appear.

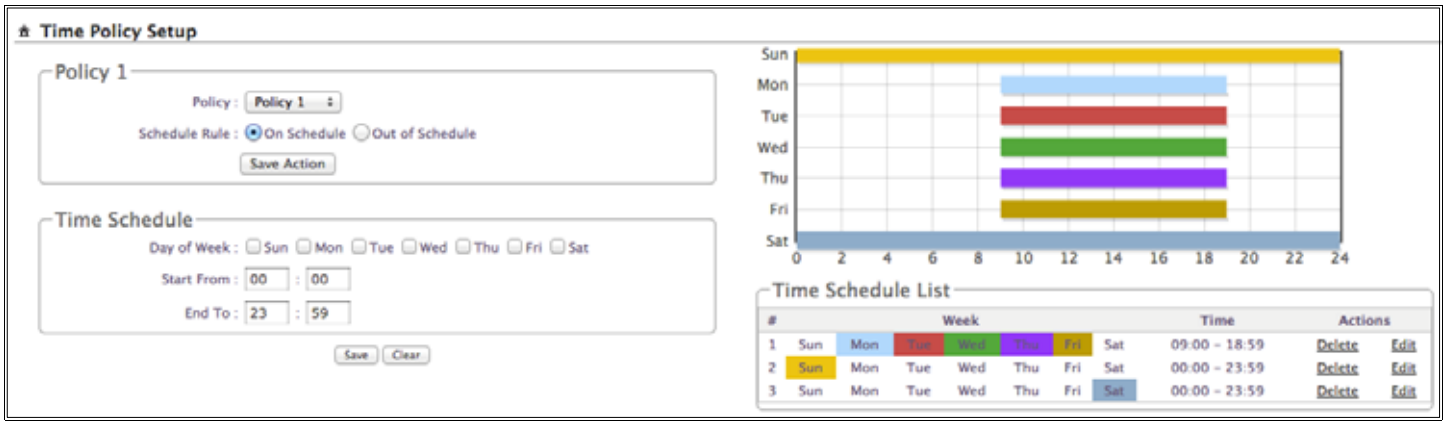


On each monitored item with a WEB server running, administrators may add a link for the easy access by selecting a protocol, http or https, and click the **Add** button. After clicking Add button, the IP address will become a hyperlinks, and administrators can easily access the host by clicking the hyperlinks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

4.5 Restrain the Users and Sharing Your Internal Service

4.5.1 Configure Time Policy

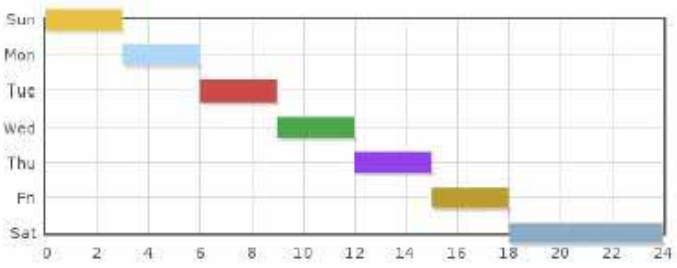
Administrator can define time policy for **Service Domain**, **IP Filtering**, **MAC Filtering** and **Virtual Server**. There are **10** policy can be defined. Please click on **Advance** -> **Time Policy** to enter **Time Policy Setup** page.



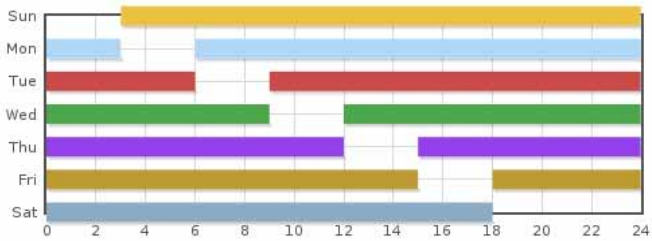
- **Policy :** There are **10** Policy can be selected.
- **Schedule Rule :** Select desired schedule for this policy, click ***Save Action*** button to save Schedule Rule setting
- **Time Schedule :** Select desired day of week and time period for this policy.

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.

4.5.2 IP Filter

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

- **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.
- **Policy :** 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
- **Schedule :** 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.

4.5.3 MAC Filter

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

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

  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.
- **Schedule :** 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.

4.5.4 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.

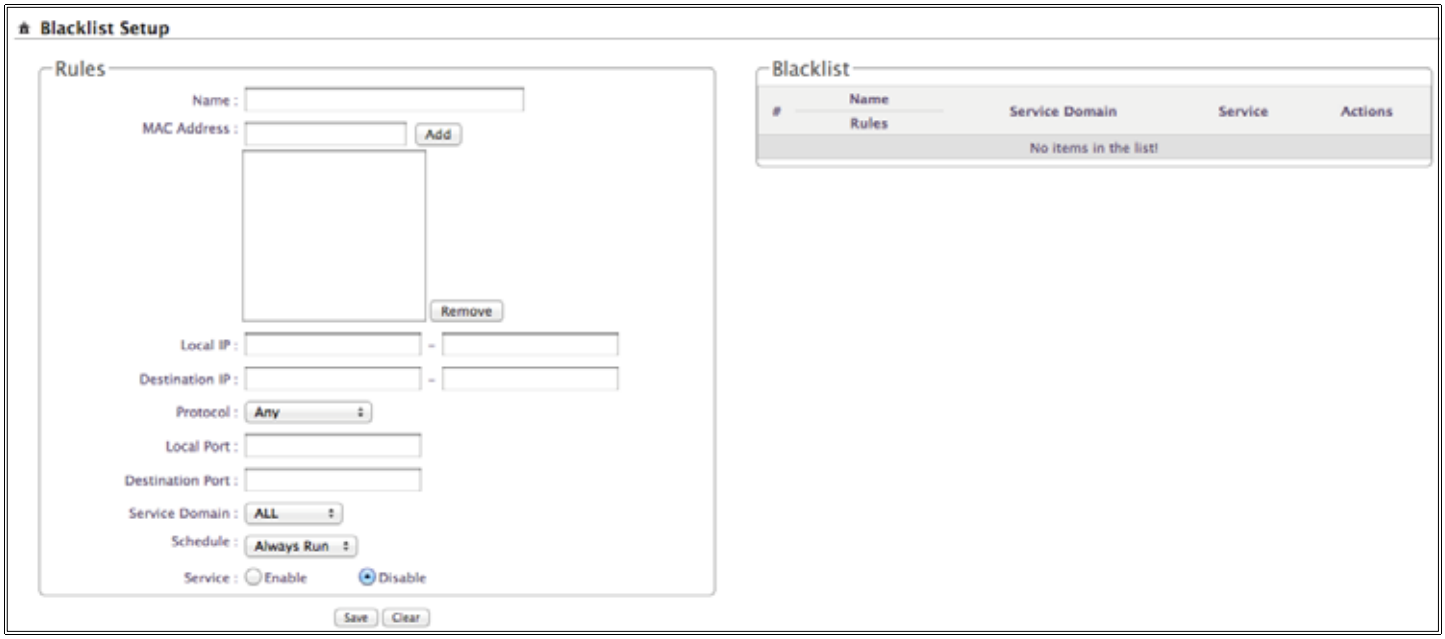
- **Description :** Enter appropriate text to denote this virtual server.
- **Private IP :** The corresponding IP address of the LAN port used for the respected service. Enter the LAN IP address of the assigned host.
- **Protocol Type :** The communication protocol of session. Select an appropriate protocol 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.
- **Schedule :** Select specified time period for this rule.
- **Service :** Check ***Enable*** option to activate this rule, and ***Disable*** to deactivate.

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.

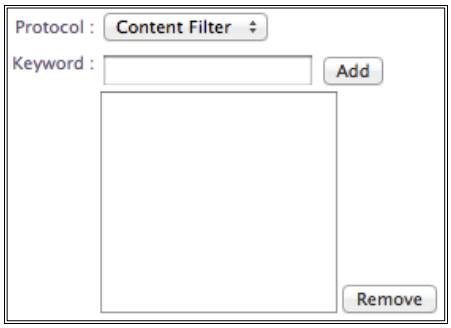
4.5.5 Configure Blacklist

The administrator can add, delete and edit blacklist for uses access. If the system want to deny uses access to specified website, enter the IP address, URL or Keyword of these websites in this list. Up to **20** rules can be defined in this list. Please click on **Service Domain** → **Blacklist**, the page of Blacklist Setup will appear.



- **Name :** Enter a descriptive name for this rule for identifying purposes.
- **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
- **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
- **Protocol :** Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **Content Filter** and **Application**) from drop-down list.

If you want to block websites with specific URL address or using specific keywords, you can select **Content Filter** from drop-down menu, and enter specific URL or keywords in **Keyword** setting field



- **Local Port :** Specify local port(LAN port) range required for this rule
- **Destination Port :** Specify destination port range required for this rule.
- **Service Domain :** Select specified Service Domain for this rule.
- **Schedule :** Select specified time period for this rule.
- **Service :** Check ***Enable*** button to activate this rule, and ***Disable*** to deactivate.

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

4.5.6 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.

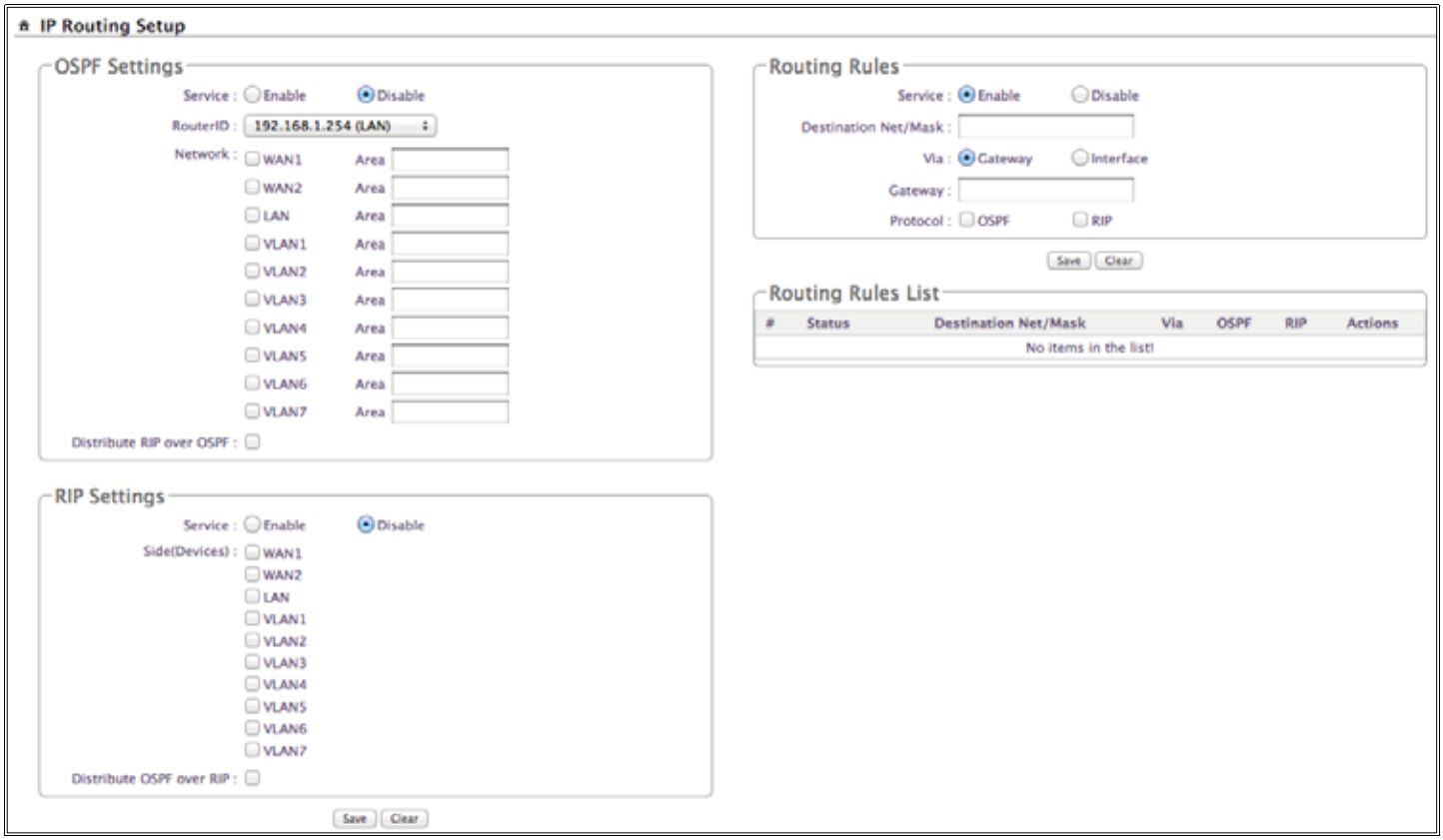
Please click on **Advance -> DMZ** and follow the below setting.

- **Service :** 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.
- **Schedule :** 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.

4.5.7 IP Routing

The IP Routing Settings allows you to configure routing feature in the gateway. The system supports **RIP**(Routing Information Protocol) and **OSPF**(Open Shortest Path First) dynamic routing and allows you to manually configure static network routes. Please click on **Advance -> IP Routing** and follow the below setting.



- **OSPF Settings**
  - ➔ **Service :** By default, it's **Disable**. To **Enable** to activated OSPF routing service.
  - ➔ **Route ID :** The router ID is typically derived by each router from its interface IP address.
  - ➔ **Network :** Specify desired interface **WAN1**, **WAN2**, **LAN** or **VLAN1 ~ VLAN7** for sending and receiving of OSPF packets.
  - ➔ **Area :** Default is **0**, the range is from **0** to **4294967295**.
  - ➔ **Distribute RIP over OSPF :** Allow RIP routes will redistributed into OSPF.
- **RIP Settings**
  - ➔ **Service :** By default, it's **Disable**. To **Enable** to activated RIP routing service.
  - ➔ **Side(Devices) :** Specify desired interface **WAN1**, **WAN2**, **LAN** or **VLAN1 ~ VLAN7** for sending and receiving of RIP packets.
  - ➔ **Distribute OSPF over RIP :** Allow OSPF routes redistributed into RIP..

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

- **Routing Rules :**
  - ➔ **Service :** Click **Enable** to activated static routing.
  - ➔ **Destination Net/Mask :** Specify desired destination IP network address with format of A.B.C.D/M
  - ➔ **Via :** Select a next hop of **Gateway** or **Interface** to the destination IP network.
  - **Protocol :** Set static routing rule to RIP or OSPF network. Select RIP to associate specific network on RIP routing process. Select OSPF to associate specific network with the specified area on OSPF routing process

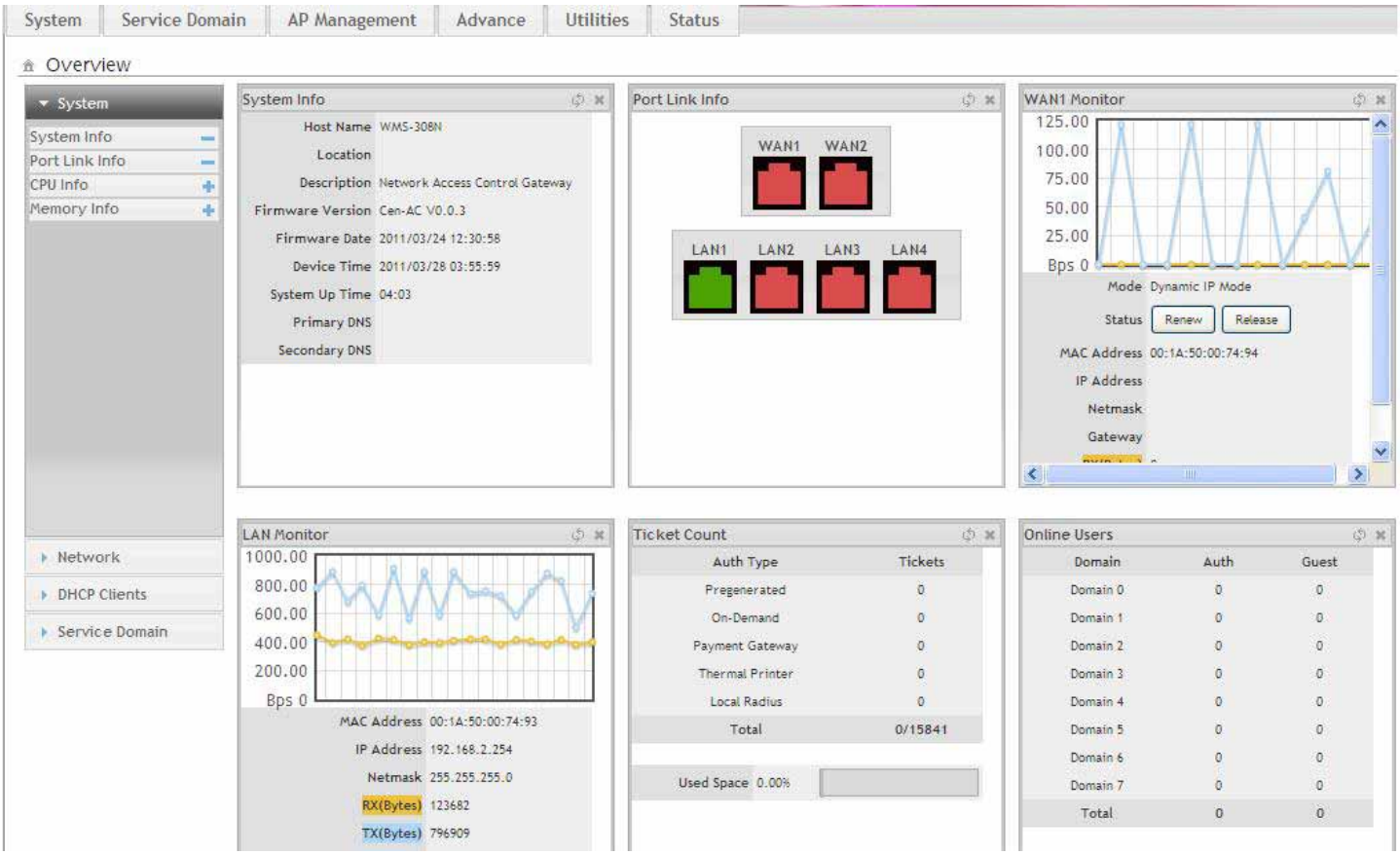
Click "**Save**" button to add Routing rule to List. There are maximum **20** rules allowed in this List. All rules can be **edited** or **removed** on the List. Click ***Reboot*** button to activate your changes.

- **Routing Rules List**
  - ➔ **Status :** Denote the current status of rule
  - ➔ **Destination Net/Mask :** Denote the destination IP network address with mask
  - ➔ **Via :** Denote the next hop of **Gateway** or **Interface** to the destination IP network
  - ➔ **OSPF :** Denote the static routing rule to OSPF
  - ➔ **RIP :** Denote the static routing rule to RIP
  - ➔ **Actions :** Click an action button to perform the appropriate action.
    - ✓ **Edit :** Click this option to edit selected static routing rule
    - ✓ **Delete :** Click this option to delete selected static routing rule

4.6 Observer the Status

4.6.1 Overview

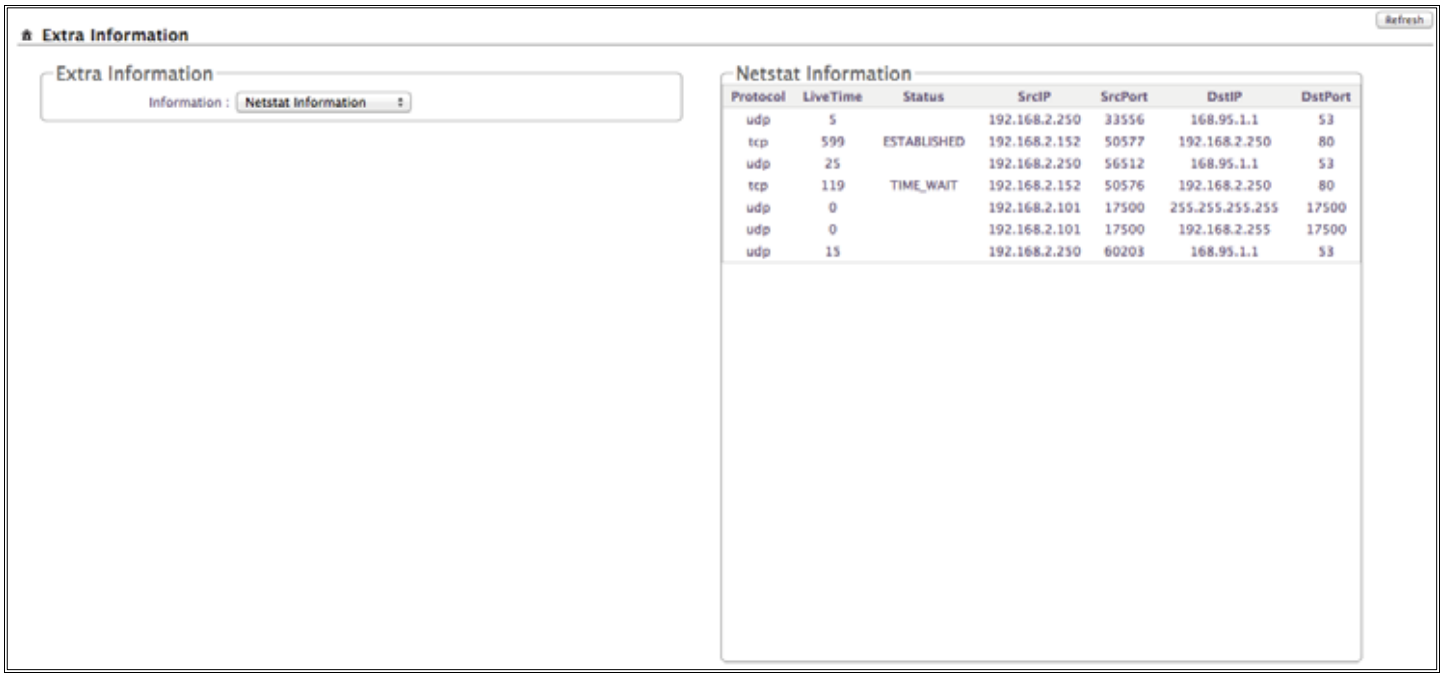
Detailed information on **System**, **Network**, **DHCP Clients** and **Service Domain** can be reviewed via this page.



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

4.6.2 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.



➔ **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.

WMS-308N 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.

Route Information

Destination	Gateway	Netmask	Interface
192.168.101.0	0.0.0.0	255.255.255.0	eth1.101
192.168.102.0	0.0.0.0	255.255.255.0	eth1.102
192.168.103.0	0.0.0.0	255.255.255.0	eth1.103
192.168.2.0	0.0.0.0	255.255.255.0	eth0.1
192.168.1.0	0.0.0.0	255.255.255.0	eth1.0
192.168.104.0	0.0.0.0	255.255.255.0	eth1.104
192.168.105.0	0.0.0.0	255.255.255.0	eth1.105
192.168.106.0	0.0.0.0	255.255.255.0	eth1.106
192.168.107.0	0.0.0.0	255.255.255.0	eth1.107
239.0.0.0	0.0.0.0	255.0.0.0	eth1.0
0.0.0.0	192.168.2.76	0.0.0.0	eth0.1

➔ **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
192.168.2.254	00:11:22:66:88:50	eth0.1
192.168.1.44	00:1A:92:9F:A4:9B	eth1.0

4.6.3 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 :** 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.
- **Refresh :** Click this button to renew the log
- **Clear :** Click this button to clear all the record

Appendix A. Web GUI valid Characters

Table A Web GUI Valid Characters

Block	Field	Valid Characters
LAN/VLAN Setup	VLAN Tag	1-4094
	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
	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
	Start/End IP	A.B.C.D IP Format
	DNS1/DNS2/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
	Hostname	Length : 1-32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	MAC Address	MAC Format
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

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
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	
Management	System Name	Length : 1-32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	Length : Up to 50 characters Space
	Location	Length : Up to 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
	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 ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	Community	Length : 1-32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	A.B.C.D IP Format

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
IPv6 WAN1	Primary/ Secondary DNS	n:n:n:n:n:n:n:n IPv6 Format
	IPv6 Address	n:n:n:n:n:n:n:n IPv6 Format
	Subnet Prefix Length	0~128; default is 64
	Default Gateway	n:n:n:n:n:n:n:n IPv6 Format
	Remote IPv4 Address	A.B.C.D IP Format
	Relay IPv6 Address	n:n:n:n:n:n:n:n IPv6 Format with 0~128 Prefix Length
	Local IPv6 Address	n:n:n:n:n:n:n:n IPv6 Format with 0~128 Prefix Length
	6to4 Address	n:n:n:n:n IPv6 Format
	6to4 Relay	n:n:n:n:n:n:n:n IPv6 Format
IPv6 LAN/VLAN	IPv6 Address	n:n:n:n:n:n:n:n IPv6 Format n:n:n:n:n IPv6 Format for 6to4 WAN Type
	IPv6 Address Range(Start)	n:n:n:n:n:n:n:n IPv6 Format n:n:n:n:n IPv6 Format for 6to4 WAN Type
	IPv6 Address Range(End)	n:n:n:n:n:n:n:n IPv6 Format n:n:n:n:n IPv6 Format for 6to4 WAN Type
	Lease Time	0~9999999; default is 60
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
	Private/Public Port	1 ~ 65535
Blacklist	Name	Length : 1-32 characters Space
	MAC Address	MAC Format
	Local IP/ Destination IP	A.B.C.D IP Format
	Local Port/ Destination Port	1 ~ 65535
	Keyword	Length : 1-64 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
IP Routing	Destination Net/Mask	Net - A.B.C.D IP Format; Mask 0~32
	OSPF Area	0 ~ 4294967295
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

Block	Field	Valid Characters
	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
Authentication Management	Service Name	Length : 1-32 characters Space
	Description	Length : Up to 64 characters Space
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
	Wireless Information	Up to 512 characters
	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 Information	Up to 512 characters
	Description	Up to 100 characters Space
	Paypal 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

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
Local RADIUS	Group	Length : 4-16 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` . =
	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
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
	Username	1-64 characters
	Password	1-16 characters
	Base DN	1-128 characters
	Account Attribute	1-64 characters
	Identity	1-128 characters
POP3	Host	Host name or IP address
	Port	1 ~ 65535
Walled Garden	Walled Name	4-32 characters Space
	IP Address/ Domain	A.B.C.D IP Format or Domain
	Homepage	URL Format
	Description	Up to 32 characters Space
Privilege List	Device Name	4-32 characters
	IP Address	A.B.C.D IP Format or with 0-32 subnet mask
	MAC Address	MAC Format; 12 HEX characters
	Description	Up to 64 characters Space

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
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
	Billing Report Time	hh:mm Time format
	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.

Main Menu	Sub Menu	Group	Admin Privilege	0perator Privilege
System	WAN		None	None
	WAN Traffic		None	None
	LAN/VLAN		Read & Write	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
		SMTP E-Mail Relay	Read	None
		Ping Watchdog	Read	None
		Auto Reboot	Read	None
	Time Server		None	None
	SNMP		None	None
	IPv6 WAN1		None	None
	IPv6 LAN/VLAN		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
	Authentication – POP3		Read & Write	None
	Privilege List		Read & Write	None
	Walled Garden		Read & Write	None
	Notification		Read & Write	None
	Online Users		Read & Write	Read & Write
	Log Info		Read & Write	Read & Write
AP Management	Device Discovery		Read & Write	None
	Batch Setup Management		Read & Write	None
	Group Setup Management		Read & Write	None
	Traffic Monitor		Read & Write	Read & Write
	Group Status		Read & Write	Read & Write
	Rogue AP Detection		Read & Write	None
	Website Monitor		Read & Write	None

Main Menu	Sub Menu	Group	Admin Privilege	0perator Privilege
Advance	DMZ		Read & Write	None
	IP Filter		Read & Write	None
	MAC Filter		Read & Write	None
	Virtual Server		Read & Write	None
	Blacklist		Read & Write	None
	IP Routing		Read & Write	None
	Time Policy		Read & Write	None
Utilities	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

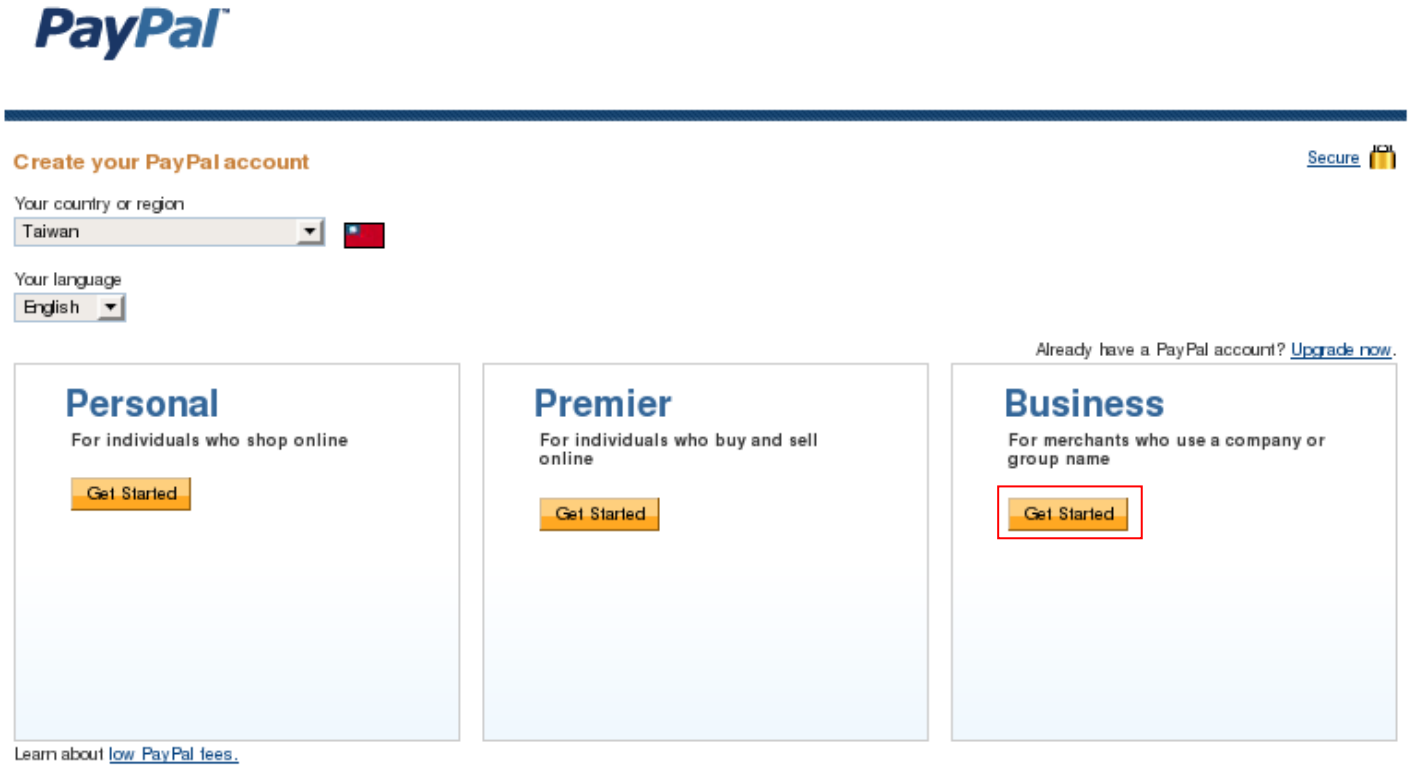
This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access using their PayPal accounts or credit cards.

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

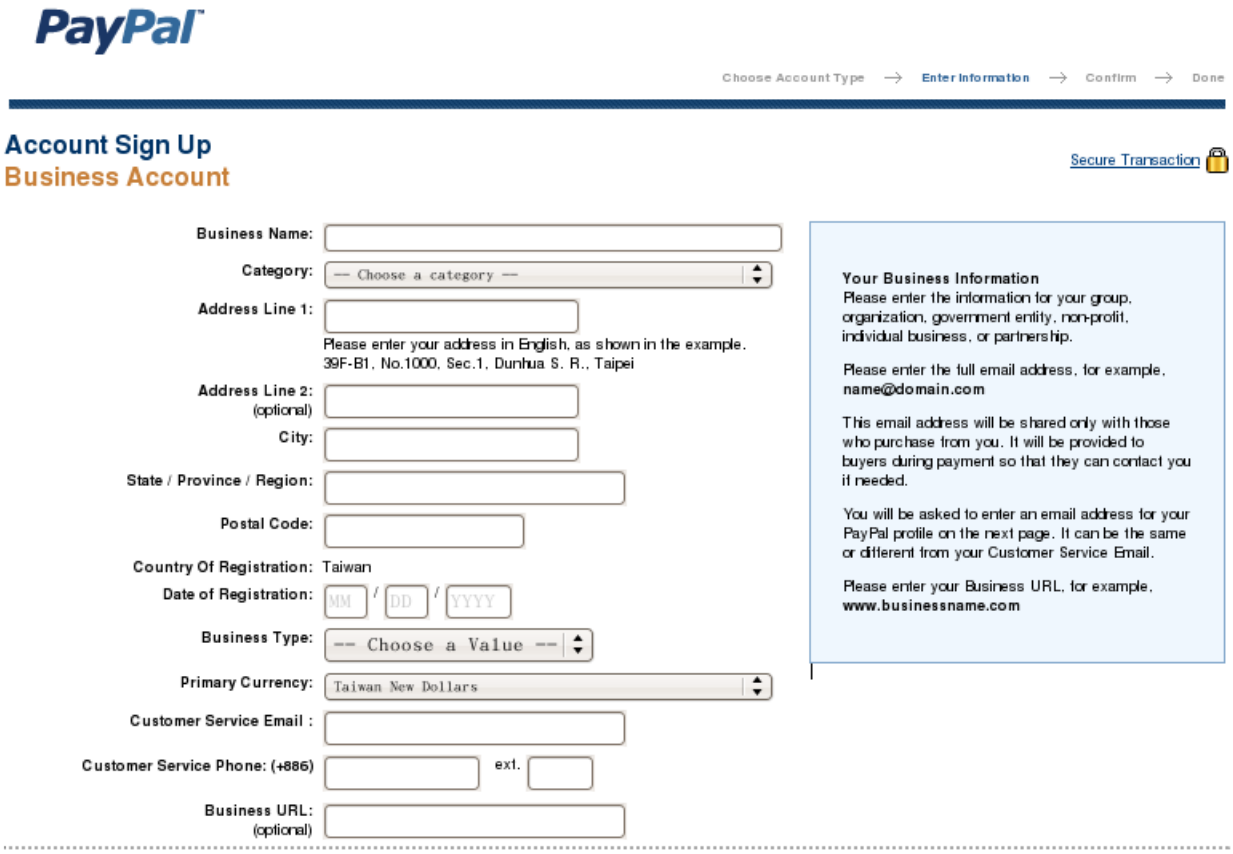
Sign Up Process :

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

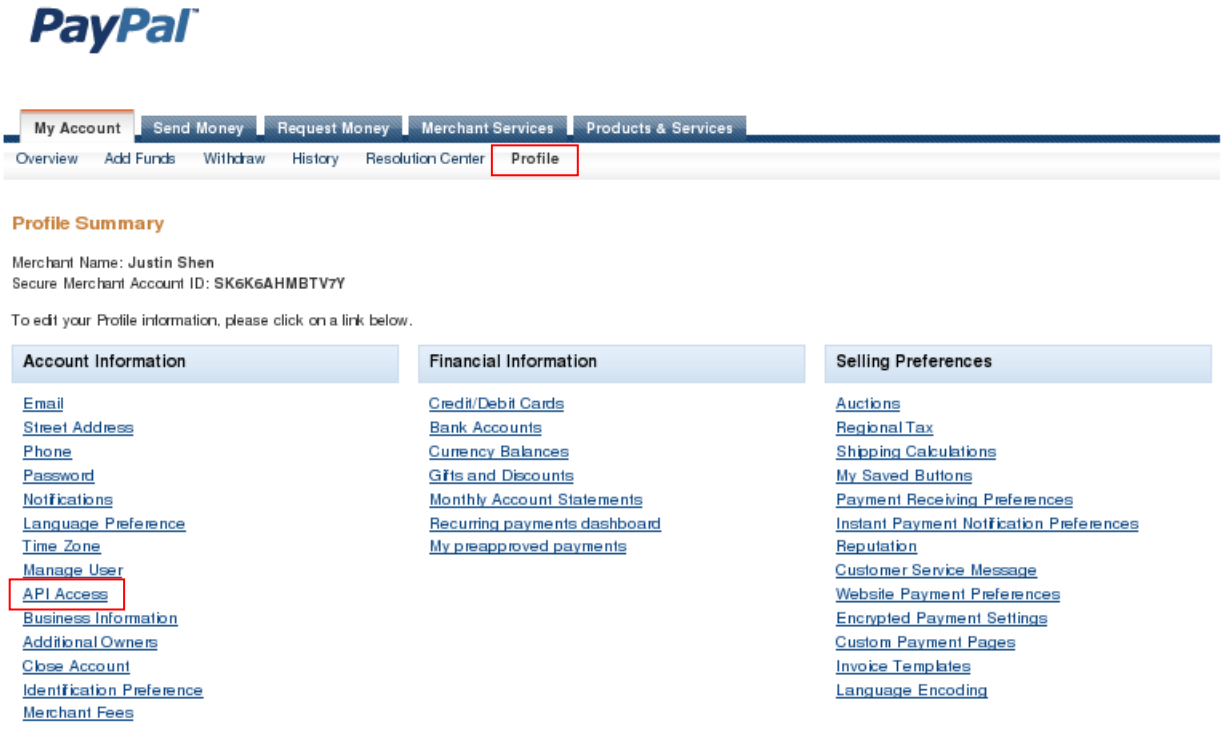


Click ***Get Started*** button to create **PayPal Business Account** on Business field, the Account Sign Up page will appear.

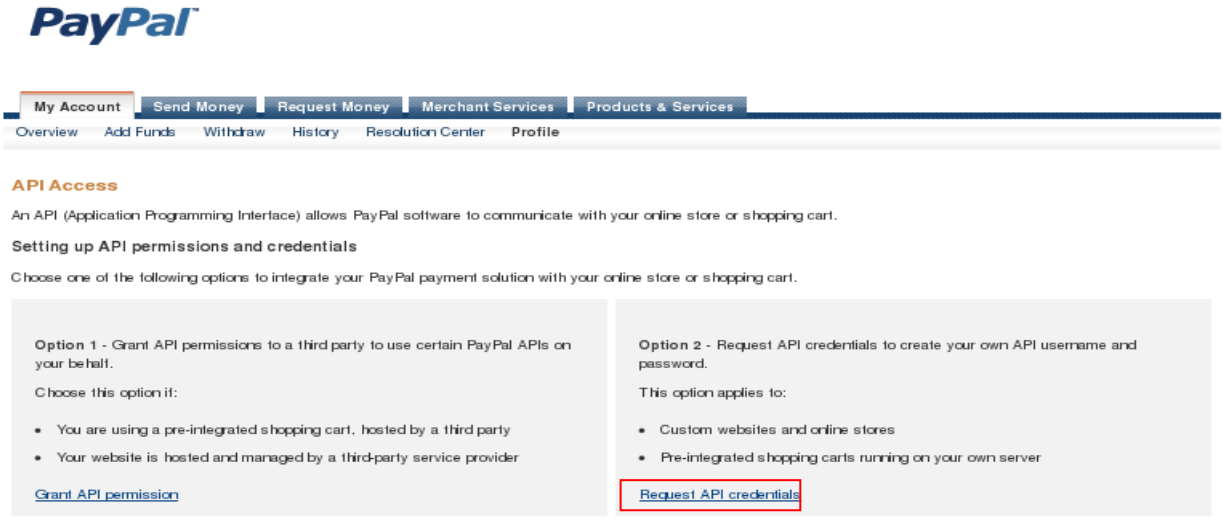


Step 2 : Edit **NECESSARY** settings in "**API Access**"

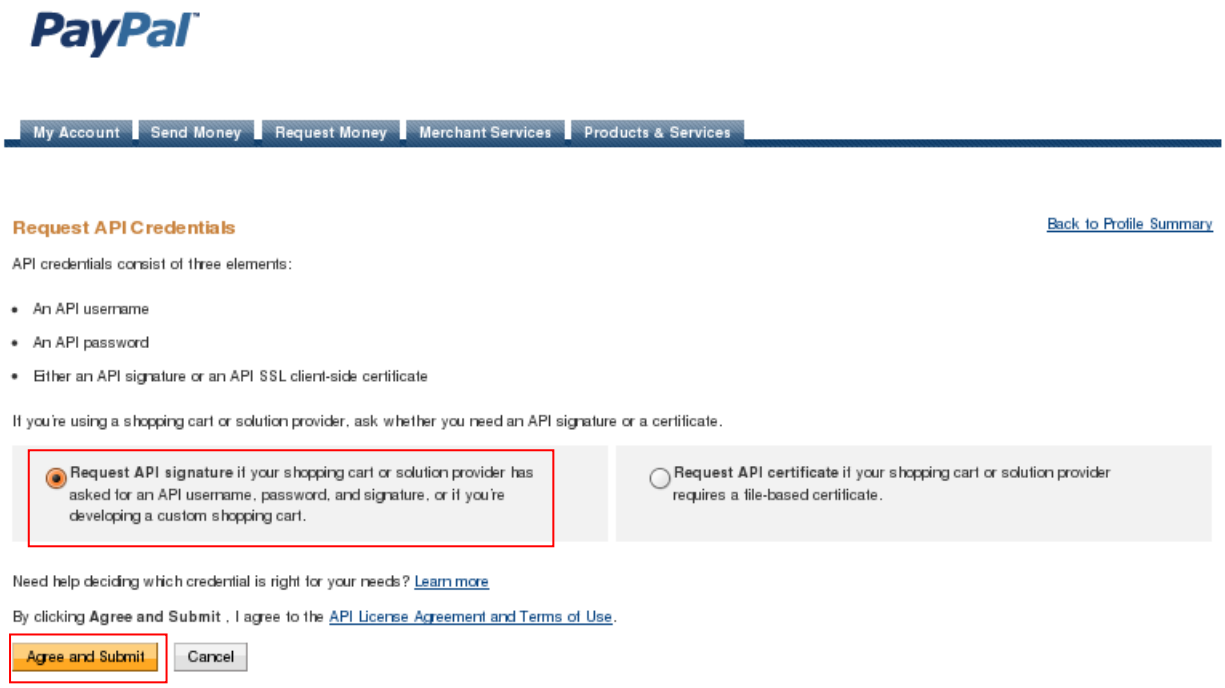
Please click on **Profile** -> **API Access** in the **Account Information**.



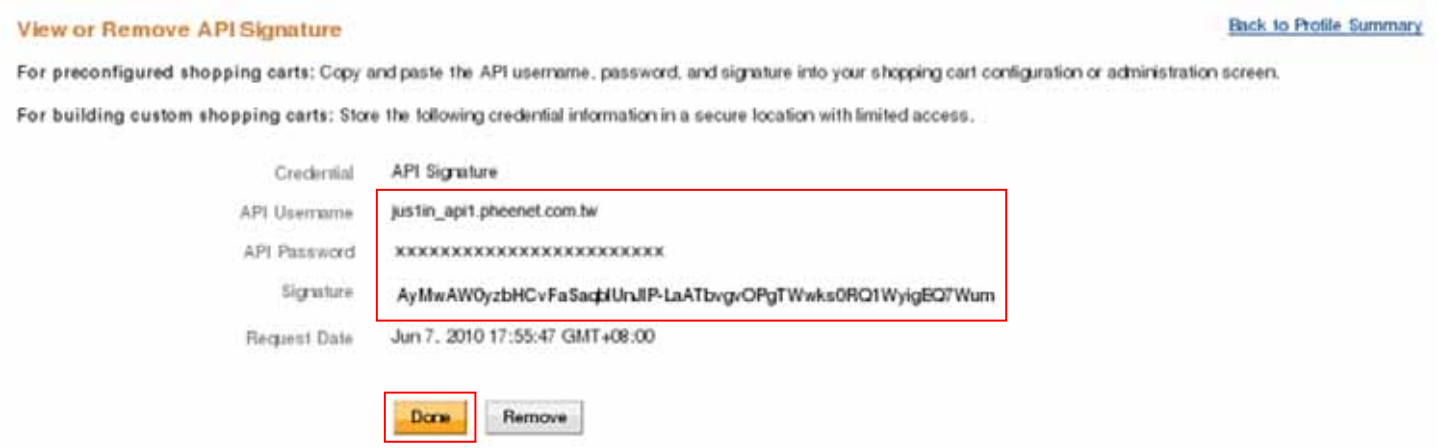
After click API Access on Account Information, the API Access setting will appear. Click "**Request API credentials**" in **Option 2 – Request API credentials to create your own API username and password**.



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

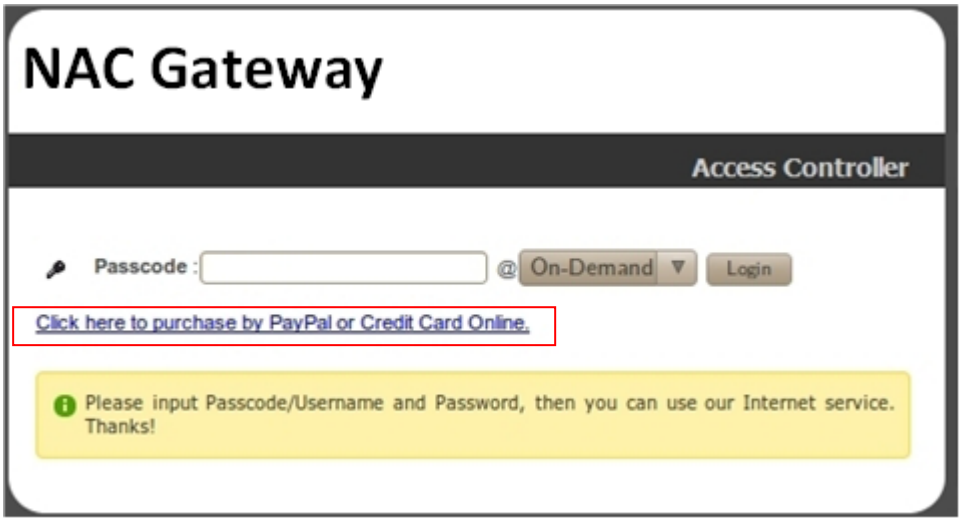


The **API Username**, **API Password** and **Signature** will generated. Click "**Done**" button to finish process.

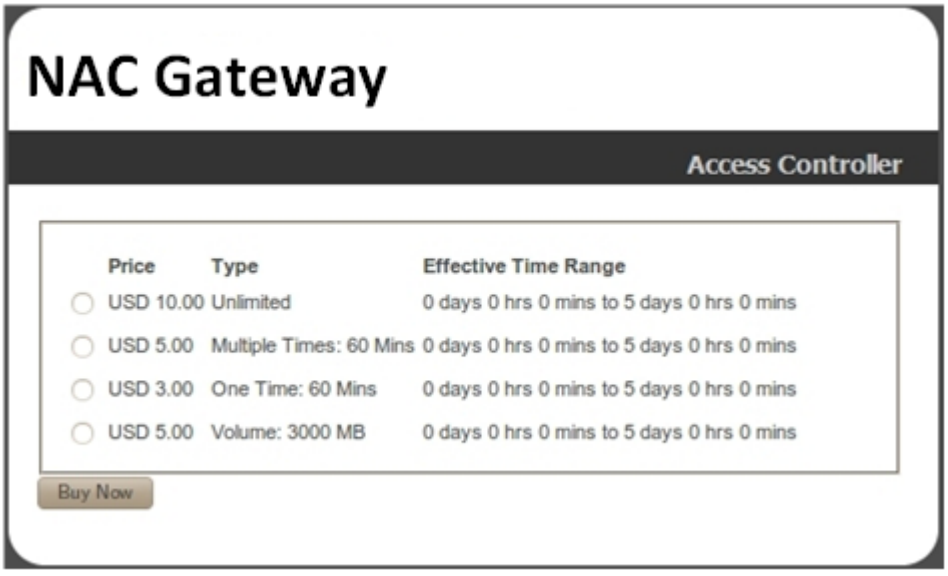


Appendix D. Examples of Making Payments for End Users

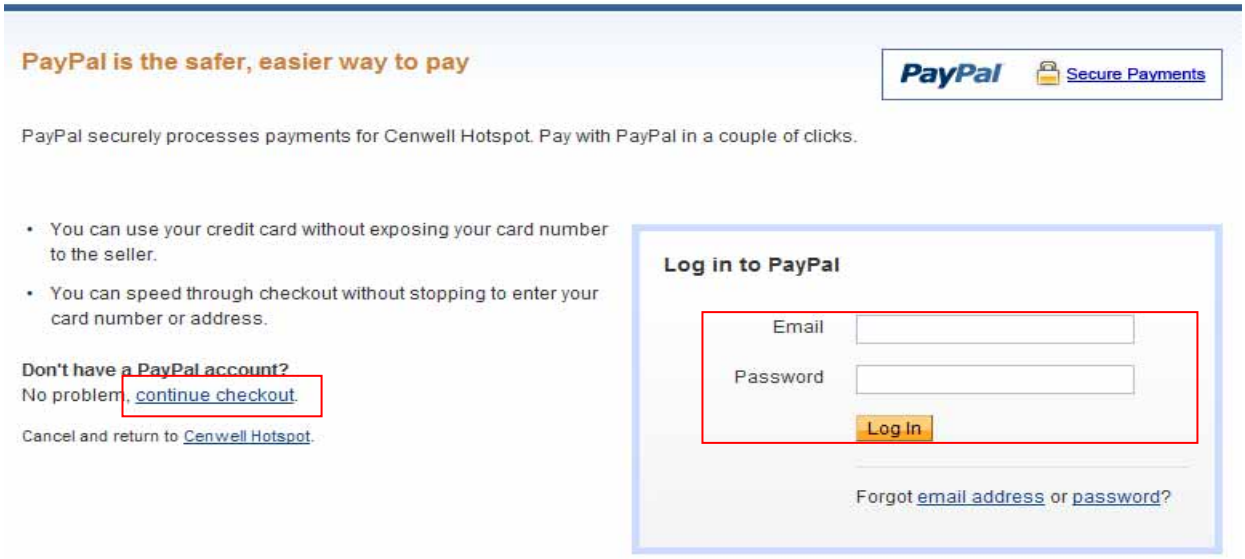
Step 1 : Click the link below the login window to pay for the service by credit card via PayPal.



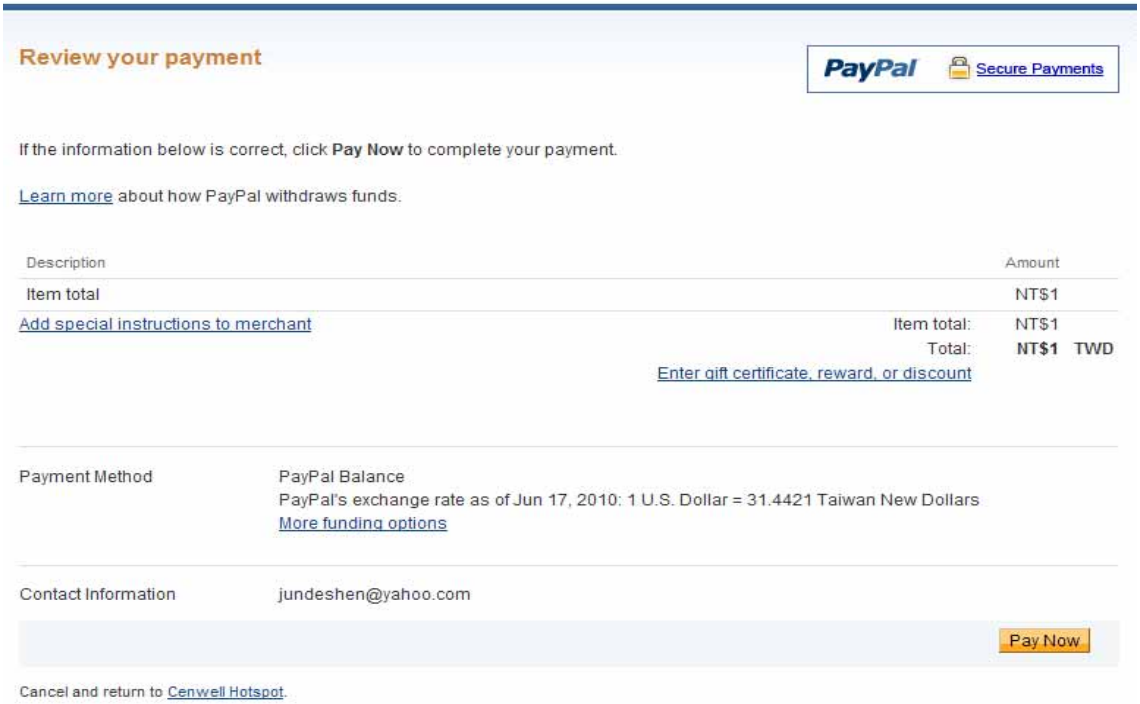
Step 2 : Select service package and Click ***Buy Now*** button to send out this transaction. There will be a connecting message as below.



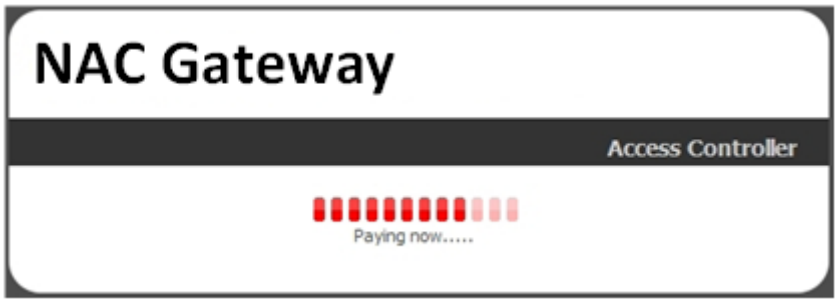
Step 3 : You will be redirected to PayPal website to complete the payment process. You can pay service fee via Paypal account or use your credit card (Click "**continue checkout**" hyperlinks)



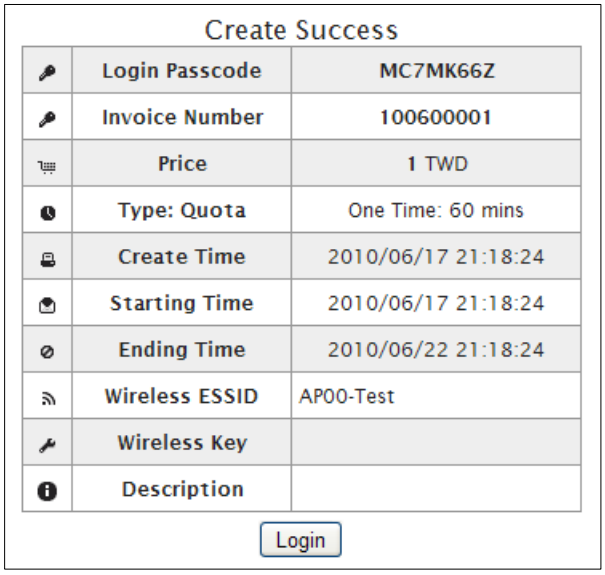
Step 4 : After login Paypal The payment information will appear. Click ***Pay Now*** button to get passcode.



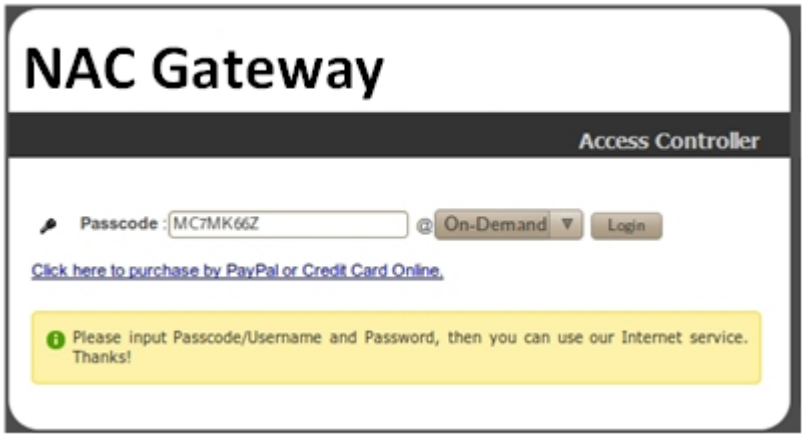
Step 5 : After clicking ***Pay Now*** button, the process of paying confirm will appear. **Please don't close this window**.



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)

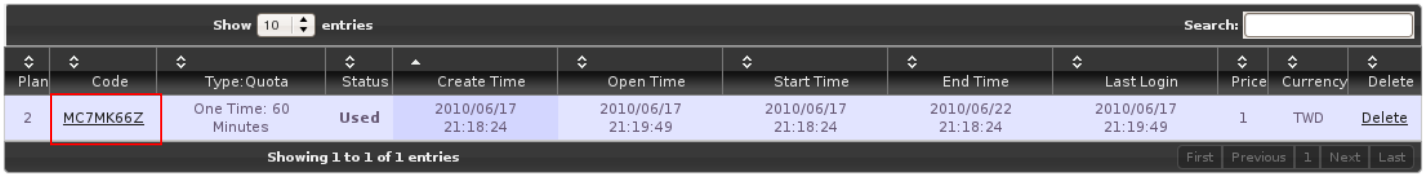


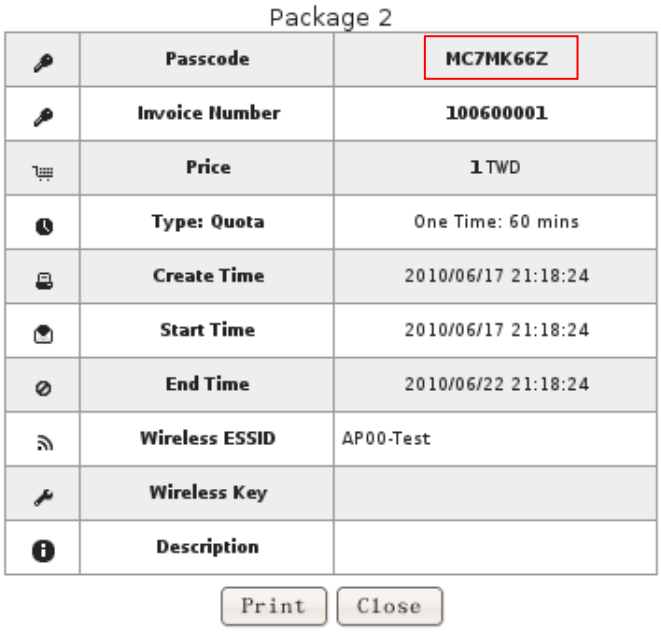
Step 7 : Input generated passcode and click ***Login*** button to login Internet Service.



Appendix E. Issue Refund for PayPal

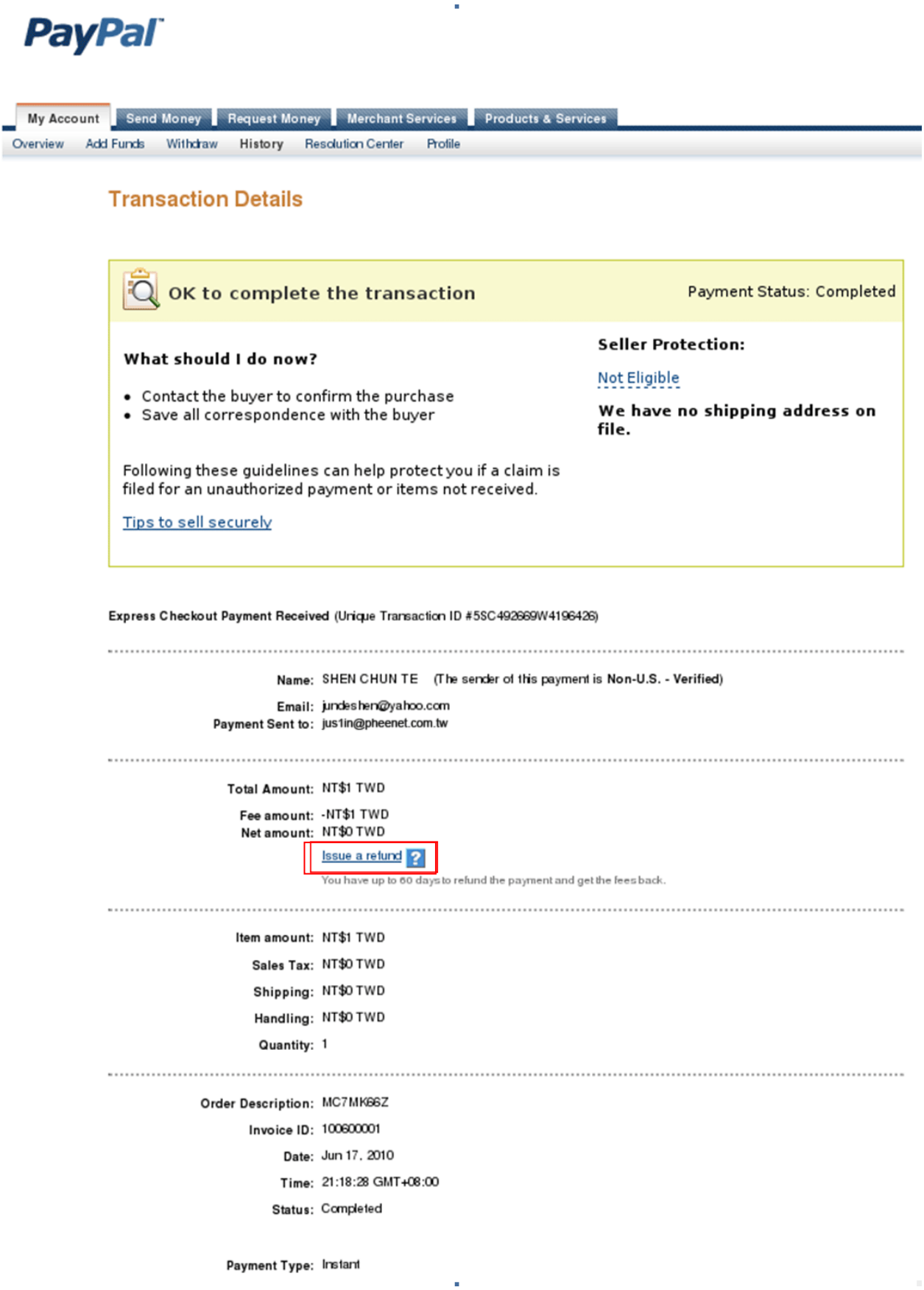
Step 1 : Click on **Service Domain -> Authentication -> On-Demand -> Payment Gateway Setup**, and then click ***Information*** button on the Billing Plan Setup List to enter **Payment Gateway Information** page. Click on selected passcode's hyperlinks for viewing this ticket's **Invoice Number**



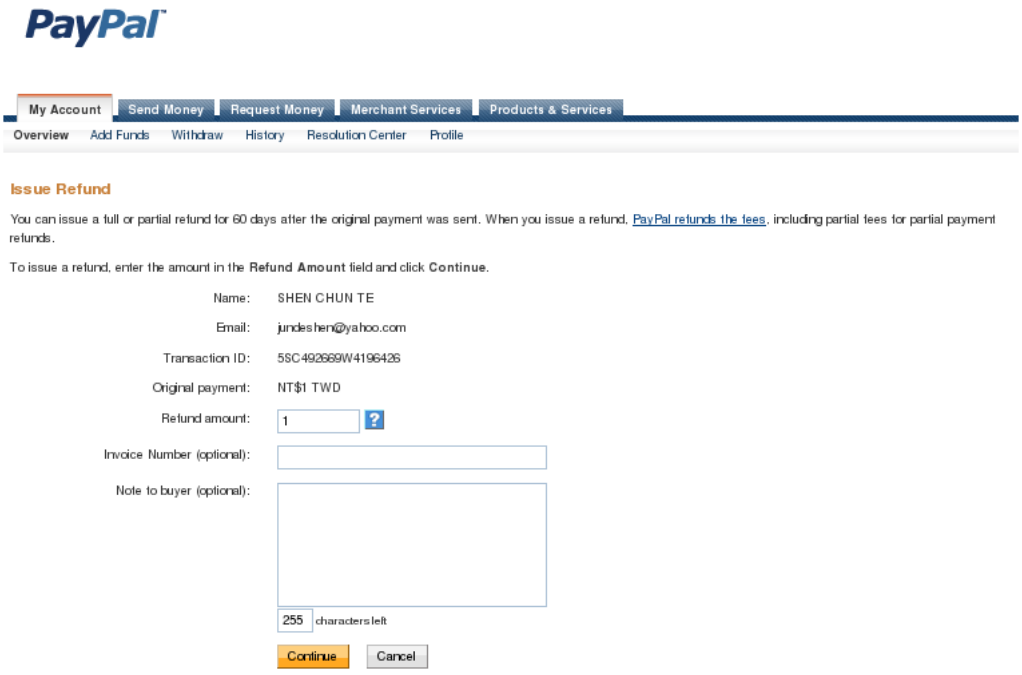


Step 2 : Please login in PayPal, and click on **History -> Find a transaction**. Then enter ***Invoice Number*** in "**Invoice ID**" and specify the time period for search. Click ***Search*** button to view the transaction details.

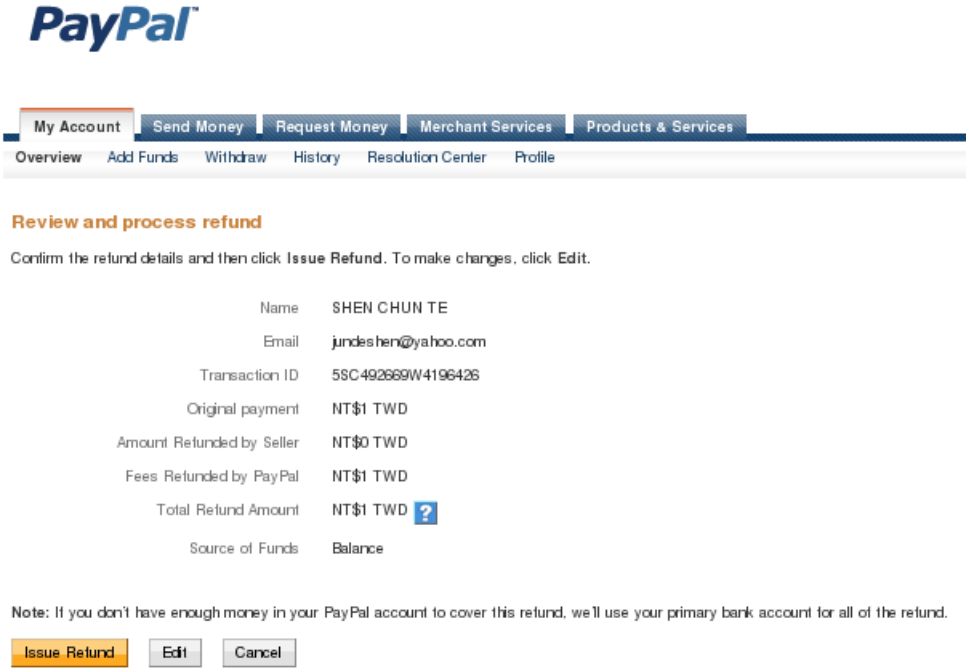
Step 3 : View the transaction detail and click "**Issue a refund**".



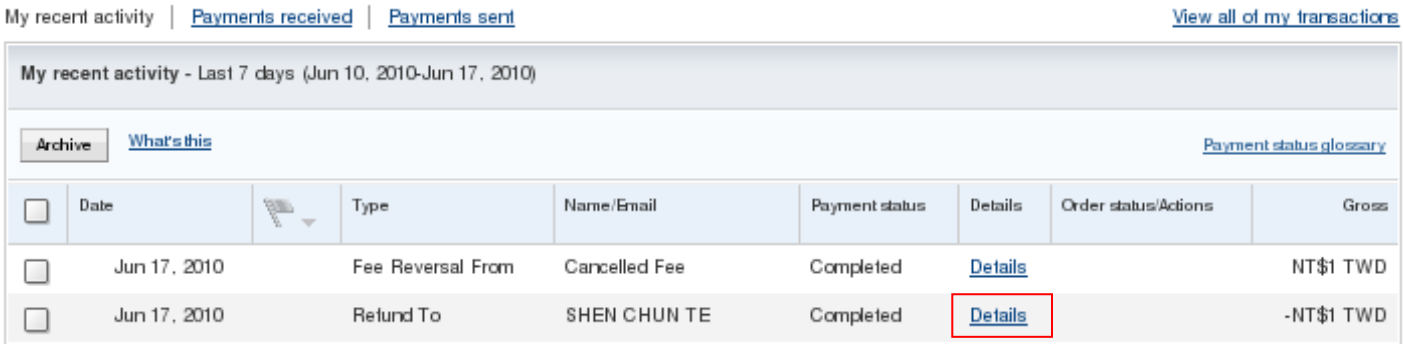
Step 4 : Click ***Continue*** button to next page.



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



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

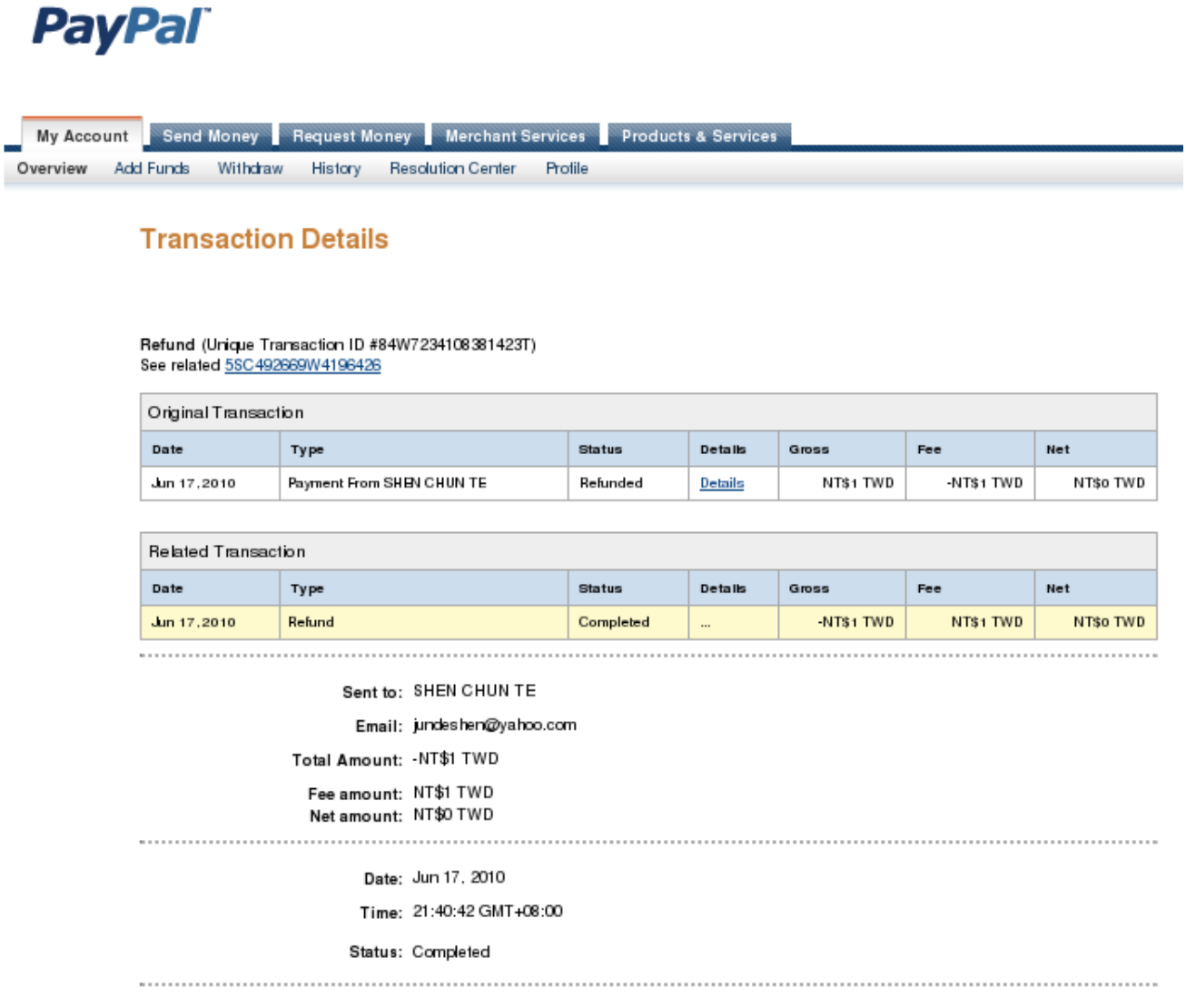


My recent activity | Payments received | Payments sent — View all of my transactions

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

Archive | What's this — Payment status glossary

	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



PayPal

My Account | Send Money | Request Money | Merchant Services | Products & Services

Overview | Add Funds | Withdraw | History | Resolution Center | Profile

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

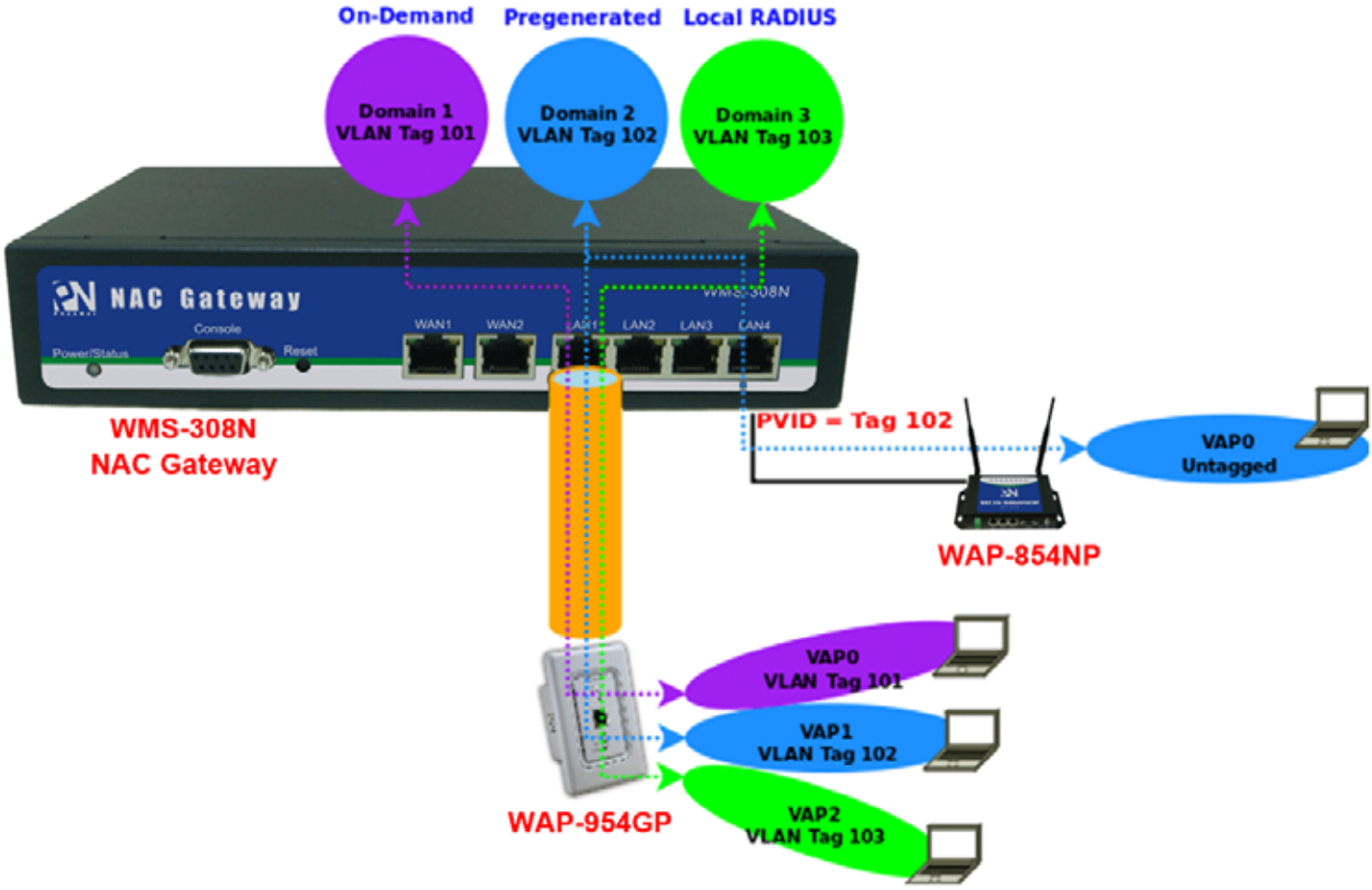
Sent to: SHEN CHUN TE
Email: jundeshen@yahoo.com
Total Amount: -NT$1 TWD
Fee amount: NT$1 TWD
Net amount: NT$0 TWD

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

Appendix F. Example of AP Device Connection With VLAN

This section is to show independent Hotspot owners how to setup different Service Domain for AP device with VLAN tagged or untagged.

The **Figure** shows an example for AP device with VLAN tagged and untagged connect to different Service Domain.



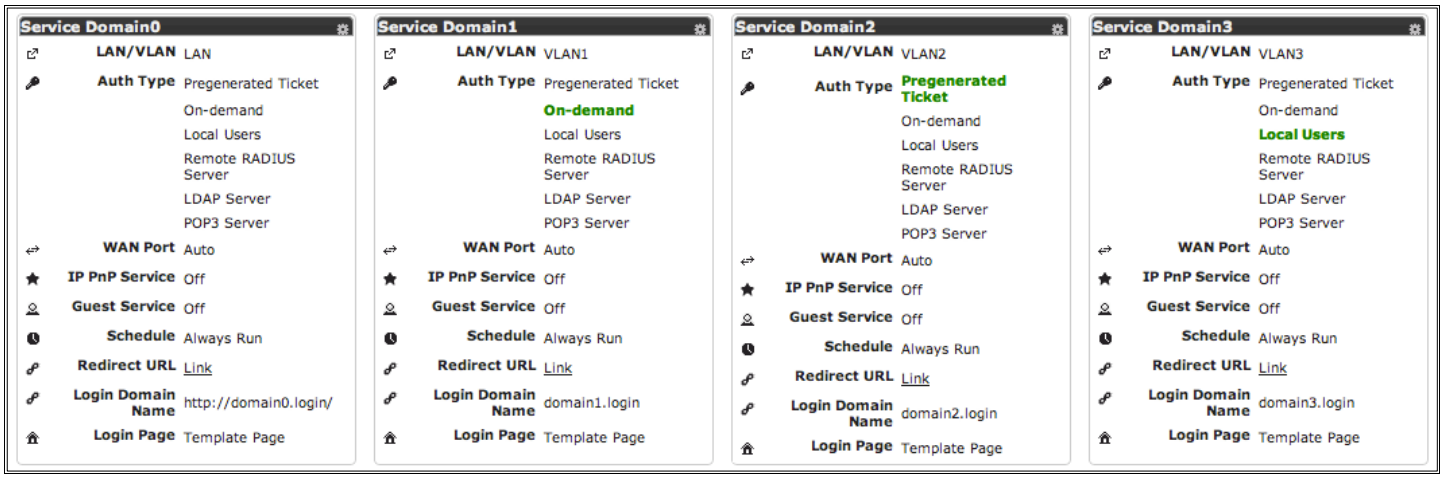
The **WMS-308N** create **three** Service Domains : Domain 1 use On-Demand authentication with VLAN tag 101, Domain 2 use Pregeneraged Tickets authentication with VLAN tag 102, Domain 3 use Local RADIUS accounts authentication with VLAN tag 103.

The **WAP-954GP** connect to WMS-308N's LAN1 port and create three VAPs with different VLAN tag(101, 102, and 103), and the wireless clients can connect Internet via WAP-954GP with different authentication.

The **WAP-854NP** connect to WMS-308N's LAN4 port and set VAP0 without VLAN tag, the wireless clients can connect Internet via WAP-854NP with Pregenereaged Tickets authentication.

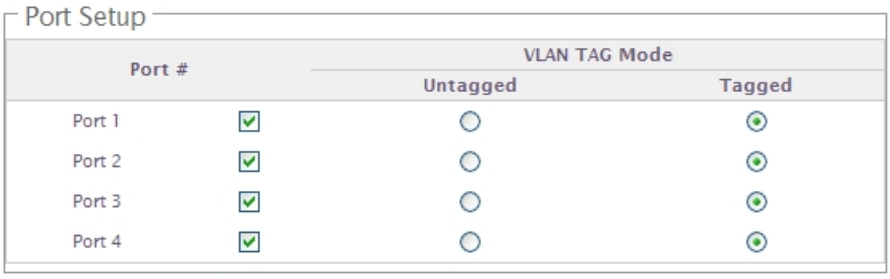
Step 1 : Verify **WAN** and System's Time.

Step 2 : Configure Service Domain, set **Domain 1** to **On-Demand** authentication, **Domain 2** to **Pregenerate Tickets** authentication, **Domain 3** to **Local Users** authentication.

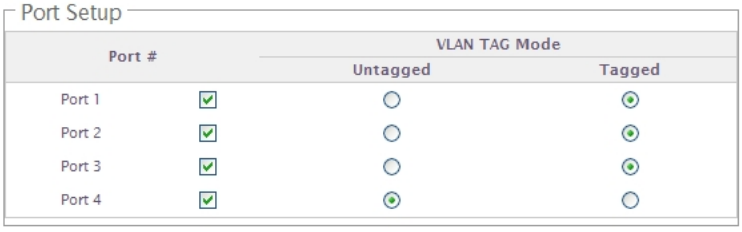


Step 3 : Configure **VLAN** on VLAN 1 ~ VLAN3 Setup page, set **VLAN1**'s tag to **101**, **VLAN2**'s tag to **102** and **VLAN3**'s tag to **103**.

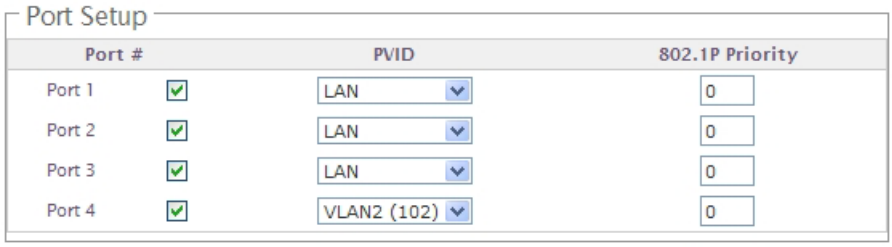
Step 3 : Configure **Port Setup** on **VLAN1 ~ VLAN3** Setup page, enable **Port 1** and set VLAN TAG Mode to **Tagged**.



Step 4 : Configure **Port Setup** on **VLAN2** Setup page, enable **Port 4** and set **Port 4** to **Untagged**.



Step 5 : Configure **Port Setup** on **LAN** Setup page, enable **Port 4** and set **Port 4**'s **PVID** to **VLAN2(102)**.



Step 6 : Reboot System

Step 7 : Verify Wireless clients can connect WAP-954GP and WAP-854NP with correct authentication type

Appendix G. Use Template to setup Managed APs

The system supports LAN setting, Time setting, Wireless Basic setting, Wireless Security setting and Firmware Upgrade, if administrator want to configure more managed APs with same settings, such as Time Server, HTTP Port, Wireless Advanced Setup … etc. The administrator can use template to configure. Below depicts an example for configuration managed APs with “Template”.

Environment Description:

1. Three WAP-854NP managed APs :
   - WAP-854NP-A – 00:1A:50:00:87:28
   - WAP-854NP-B – 00:1A:50:00:87:2E
   - WAP-854NP-C – 00:1A:50:00:87:2B
2. Set WAP-854NP-A's profile to template.

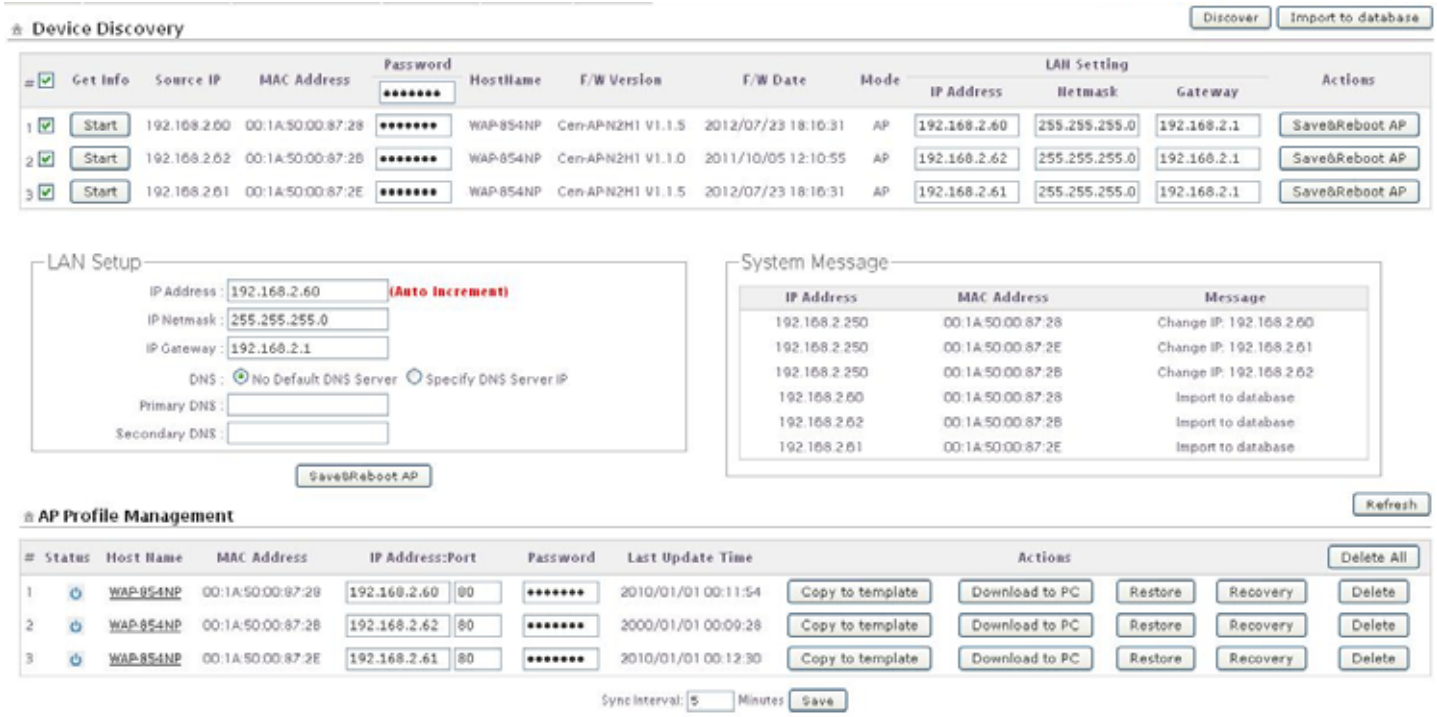
Step 1 : Click on **AP Management** → **Device Discovery**, and click ***Discover*** button to search managed AP.

Step 2 : Change the managed AP to specify IP address.

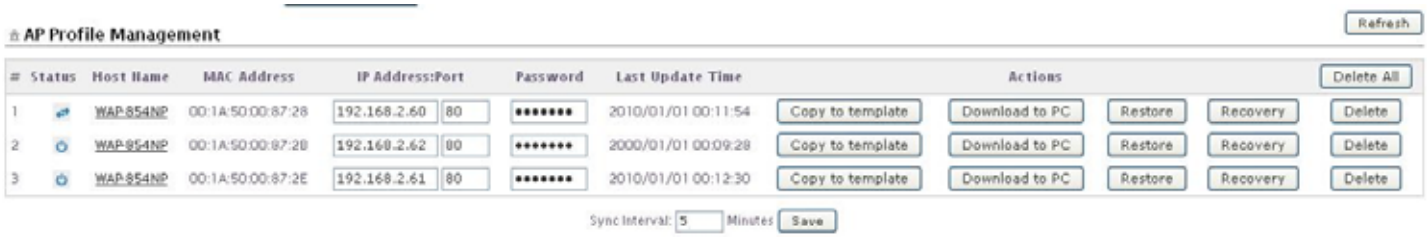
- Select all managed APs
- Enter specify IP address in LAN Setup setting field
- Click ***Save&RebootAP*** button to assign IP address to each managed AP

Step 3 : Import profile of the respective managed AP

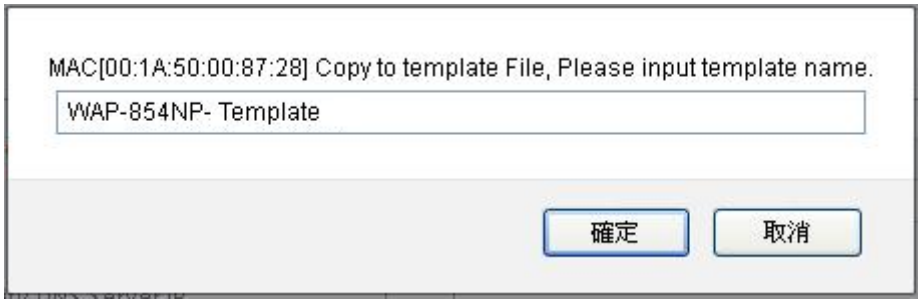
- Select all managed AP
- Click ***Import to database*** button to import the profile setting to database



Step 4 : Configure WAP-854NP-A managed AP, set VAP0's ESSID to "**WAP-854NP-A**". The Status of WAP-854NP--A should display "  " before system automatically download WAP-854NP's profile to database.



Setup 5 : Copy WAP-854NP-A's profile to template and set name to "**WAP-854NP-Template**"

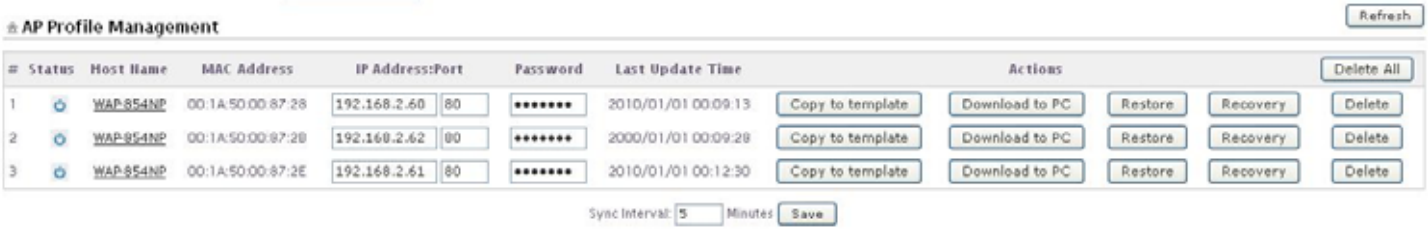


Step 6 : Configure WAP-854NP-B and WAP-854NP-C with WAP-854NP-A's template

- Click **Restore** button on the WAP-854NP-B and WAP-854NP-C, the AP Profile Restore page will appear.

- Select “**Load From Template Profile**” in **Restore Type** setting field
- Select “**WAP-854NP-Template**” in the Template Profile List, then click **Restore** button

Step 7 : Verify WAP-854NP-B and WAP-854NP-C settings. The VAP0's ESSID will be “**WAP-854NP-A**”. All settings will be the same with the WAP-854NP-A, in addition to IP address remains unchanged.



Appendix H. Use Auto Recovery To Setup Managed AP

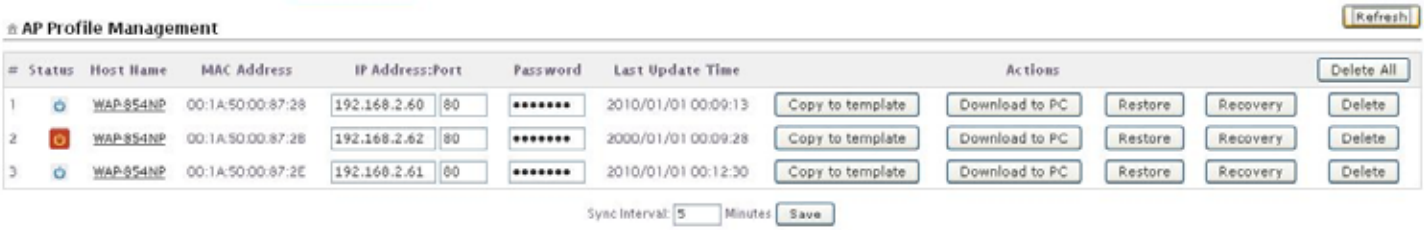
WMS-308N supports centralized management of each AP. When the system has failed AP, the administrator needs to replace the AP, and set the same as before. Using WMS-308N to quickly configure new AP, the new AP's setting will be the same as before. Below depicts an example for “Auto Recovery” function.

Environment Description:

In this case, the WMS-308N control three managed APs and one of managed AP is failed. We replace new AP, and use “Auto Recovery” to quickly setup.

1. Four WAP-854NP managed APs :
    - WAP-854NP-A – 00:1A:50:00:87:28
    - WAP-854NP-B – 00:1A:50:00:87:2E
    - WAP-854NP-C – 00:1A:50:00:87:2B
    - WAP-854NP-D – 00:1A:50:00:87:31
2. Replace WAP-854NP-D to WAP-854NP-C

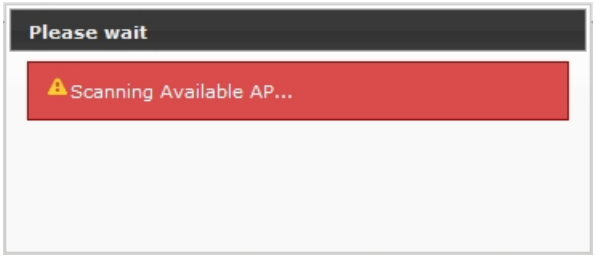
Step 1 : The WMS-308N can't detect WAP-854NP-C on AP Profile Management page.



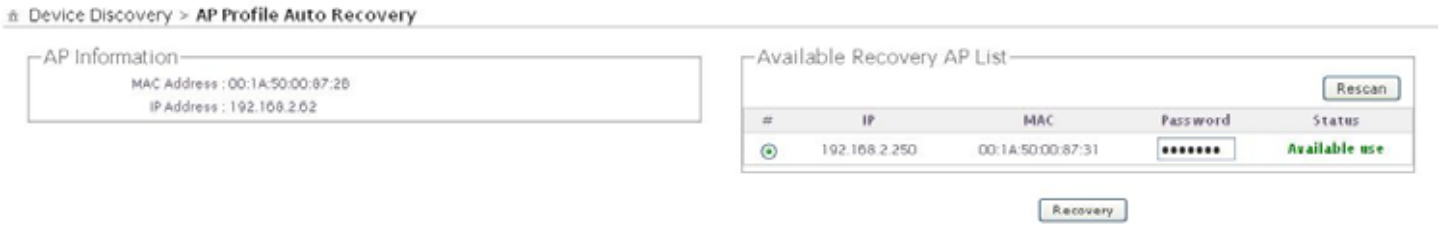
Step 2 : Replace WAP-854NP-D to WAP-854NP-C.

Step 3 : Click “**Recovery**” button on the WAP-854NP-C (**00:1A:50:00:87:2B**)

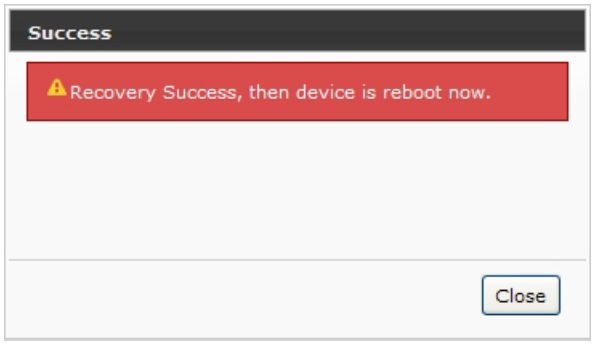
Step 4 : The “Scanning Available AP...” window will appear



Step 5 : The WAP-854NP-D(**00:1A:50:00:87:31**) will display on the Available Recovery AP List and the status show "**Available Use**".



Step 6 : Select WAP-854NP-D and click "**Recovery**" button, then the WAP-854NP-D will reboot.



Step 7 : The WAP-854NP-D(**00:1A:50:00:87:31**) will on the AP Profile Management List, and the configuration will be the same with the WAP-854NP-A