



Network Access Control Gateway / Controller

User's Manual Ver.0.0.3

WMS-308N



Table of Contents

Chapter 1. Before You Start	4
1.1 Preface	4
1.2 Package Contents	4
Chapter 2. System Overview	5
2.1 Introduction of WMS-308N	5
2.2 System Concept	5
2.3 Specification	6
Chapter 3. Base Installations	14
3.1 Installations	14
3.1.1 System Requirements	14
3.1.2 Panel Function Descriptions	14
3.1.3 Hardware Installation	16
3.2 Software Configuration	17
3.2.1 Getting Start	17
3.2.2 Quick Configuration	19
3.2.3 Access Internet	23
Chapter 4. Web Interface Configuration	24
4.1 Connect WMS-308N to the external Network	25
4.1.1 Network Requirement	25
4.1.2 Configure WAN Port	25
4.1.3 Configure WAN Traffic	28
4.1.4 Configure Dynamic DNS	30
4.1.5 Configure Local(LAN/VLAN) Network	31
4.1.6 Manage Switch QoS	37
4.2 Manage the System	38
4.2.1 Configure System Time	38
4.2.2 Configure Management	39
4.2.3 Configure SNMP	42
4.2.4 Backup / Restore and Reset to Factory	43
4.2.5 Firmware Upgrade	44
4.2.6 Network Utility	45
4.2.7 Format Database	46
4.2.8 Reboot	47
4.3 Access To External Network With Service Domain	48
4.3.1 Configure Service Domain	49
4.3.2 Configure Authentication	54
4.3.2.1 Authentication Management	54
4.3.2.2 Configure Pregenerated Tickets	55

4.3.2.3	Configure On-Demand.....	60
4.3.2.3.1	Create Billing Plans.....	61
4.3.2.3.2	Create On-Demand Users	62
4.3.2.3.3	Configure External Payment Gateway	66
4.3.2.3.4	Configure Thermal Printer.....	69
4.3.2.3.5	Billing Plan Report	74
4.3.2.3.6	Ticket Customization.....	75
4.3.2.4	Configure Local Radius Accounts	76
4.3.2.5	Configure Remote Radius Server	79
4.3.2.6	Configure LDAP Server	80
4.3.3	Configure Walled Garden	81
4.3.4	Configure Notification	82
4.3.5	Monitor Online Users.....	87
4.3.6	Log Information	88
4.4	Control your Managed AP	91
4.4.1	Discovery Managed AP	91
4.4.2	Managed AP's Profiles Management.....	93
4.4.3	Managed AP Batch Setup	96
4.4.4	Managed AP Group Management	99
4.4.5	AP Group Status.....	104
4.4.6	Third Party AP Monitor	106
4.5	Restrain the Users and Sharing Your Internal Service	107
4.5.1	Configure Time Policy.....	107
4.5.2	IP Filter	108
4.5.3	MAC Filter	109
4.5.4	Virtual Server (Port/ IP Forwarding).....	110
4.5.5	DMZ.....	111
4.5.6	IP Routing.....	112
4.6	Observer the Status.....	114
4.6.1	Overview	114
4.6.2	Extra Info	115
4.6.3	Event Log	117
Appendix A.	Web GUI valid Characters	118
Appendix B.	System Manager Privileges	124
Appendix D.	Examples of Making Payments for End Users	129
Appendix E.	Issue Refund for PayPal.....	132
Appendix F.	Example of AP Device Connection With VLAN	136
Appendix G.	Use Template to setup Managed APs.....	139
Appendix H.	Use Auto Recovery To Setup Managed AP.....	142

Chapter 1. Before You Start

1.1 Preface

The WMS-308N is a full-featured Network Access Control Gateway / Controller that aggregates up to 60 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 centralized 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

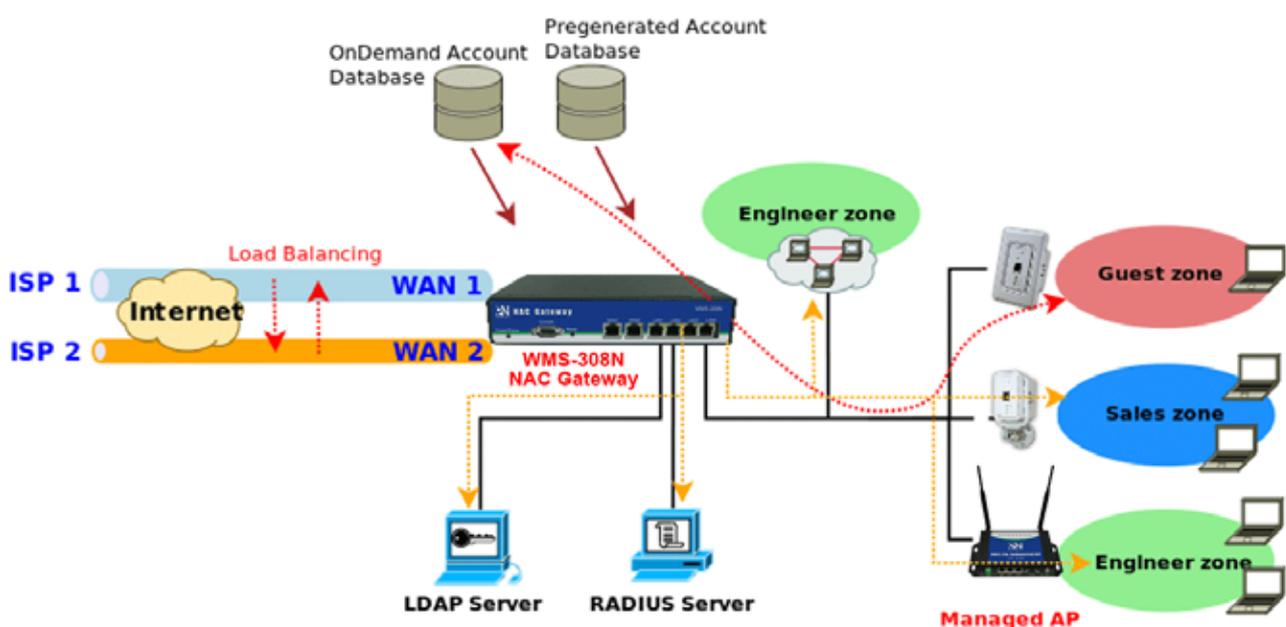
2.1 Introduction of WMS-308N

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: 60 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,CPE-2010G / CPE-2000GN-1, WLO-15814N / WLO-15802N)
- ✓ 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
- ✓ Support MIB's: 802.11, 802.1X, MIBII, RADIUS authentication, RADIUS Accounting
- ✓ SYSLOG support including remote servers
- ✓ Log-system log: operator action log

→ 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

→ Convergence

- 8 Hardware queues per port
- IEEE802.11p Class of Service/Quality of Service (CoS/QoS)
- IEEE802.11e Wi-Fi Multimedia (WMM)
- 8 BSSID per radio
- DiffServ Codpoint (DSCP)

→ 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 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
- SSL protected login portal page
- Session idle timer
- Login Session idle time out setting
- Session and account expiration control
- User Log and traffic statistic notification via automatically email service
- Login time frame control
- Session limit
- Real-Time Online Users Traffic Statistic Reporting
- Support local account roaming

- Seamless Mobility: User-centric networking manages wired and wireless users as they roam between ports or wireless APs

➤ Service Domain

- Integrating with WAP-854NP/ WAP-954GP and other future 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, 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, MAC authentication, and 802.1X
- Customizable Login and Logout Portal Pages
- Customizable Advertisement Links on Login Portal Page
- User authentication with UAM (Universal Access Method), 802.1X/EAPoLAN, MAC address
- Allow MAC address and 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

- Configurable user black list
- Export/Import local users list to/from a text file
- Web-based Captive Portal for SSL browser-based authentication
- Authentication Type
- IEEE802.1X (EAP, 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 on-demand and external RADIUS server
- Contain 10 configurable billing plans for on-demand accounts
- Support credit card billing system by PayPal
- Provide session expiration control for on-demand accounts
- 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

➤ QoS Enforcement

- ➔ Packet classification via DSCP (Differentiated Services code Point)
- ➔ Diff/ToS
- ➔ IEEE802.11p/CoS
- ➔ IEEE 802.1Q Tag VLAN priority control
- ➔ IEEE 802.11e WMM
- ➔ Automatic mapping of WMM priorities to 802.1p and IP DSCP
- ➔ IGMP Snooping for efficient multicast delivery
- ➔ Upload and Download Traffic Management

➤ Firewall

- ➔ Built-in DoS attack protection
- ➔ Inspection Full stateful packet filter
- ➔ Access Control List
- ➔ Layer 7 Protocol Blocking
- ➔ 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
- ➔ Binding VLAN with Ethernet interface
- ➔ Support MAC Filter

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

3.1.2 Panel Function Descriptions

Front Panel



1. **Power/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.

The screenshot displays the 'Overview' page of the WMS-308N Network Access Gateway / Controller. The interface is organized into several sections:

- System Info:** Host Name: WMS-308N, Location, Description: Network Access Control Gateway, Firmware Version: Cen-AC V0.0.3, Firmware Date: 2011/03/24 12:30:58, Device Time: 2011/03/28 03:55:59, System Up Time: 04:03, Primary DNS, Secondary DNS.
- Port Link Info:** WAN1, WAN2, LAN1, LAN2, LAN3, LAN4.
- WAN1 Monitor:** Mode: Dynamic IP Mode, Status: Renew, Release, MAC Address: 00:1A:50:00:74:94, IP Address, Netmask, Gateway.
- LAN Monitor:** Line graph showing Bps, MAC Address: 00:1A:50:00:74:93, IP Address: 192.168.2.254, Netmask: 255.255.255.0, RX(Bytes): 123682, TX(Bytes): 796909.
- Ticket Count:** Table with Auth Type and Tickets, Total: 0/15841, Used Space: 0.00%.
- Online Users:** Table with Domain, Auth, and Guest counts, Total: 0/0/0.

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 and retype in the **Check Root Password** field. (4-30 alphanumeric and specific characters; **not** support **Space**)
- Click Save button.

Root Password

New Root Password:

Check Root Password:



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

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

- Click **System** -> **WAN**, the WAN Setup page will appear.
- Select the appropriate Connection Type for WAN1 port, there are four types of WAN1 connections to be selected from: **Static IP**, **Dynamic IP**, **PPPoE Client** and **PPTP Client**.
- Enter the IP Address of a DNS Server provided by your ISP(Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.
- Click **Save** button.

WAN Setup

WAN1 Setup

Disable
 Static IP
 Dynamic IP
 PPPoE
 PPTP

Hostname:

Keep Default MAC Address
 Clone MAC Address: 00:1A:92:9F:A4:9B
 Manual MAC Address:

WAN2 Setup

Disable
 Static IP
 Dynamic IP
 PPPoE
 PPTP

DNS

DNS: No Default DNS Server Specify DNS Server IP

Primary:

Secondary:

Step 3 : Choose System's Time Zone

- Click **System** -> **Time Server**, the Time Server Setup page will appear.
- Select the appropriate NTP Server, Time Zone from drop-down list.
- Click **Save** button.

⊕ Setup Time Use NTP

Default NTP Server: (optional)

Time Zone:

Daylight Saving Time:



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

Step 4 : Select Authentication Type for Service Domain

- Click **Service Domain**, the Service Domain Setup page will appear

⚙ Service Domain Setup



Domain 0	Domain 1	Domain 2	Domain 3
LAN Port LAN Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service on Guest Service on Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN1 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN2 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN3 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page
Domain 4	Domain 5	Domain 6	Domain 7
LAN Port VLAN4 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN5 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN6 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN7 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page

✎ → Click **Tool Icon** on **Domain 0** window, the Service Domain0 Setup page will appear. For each Service Domain (by default, authentication type is **none**), authentication type can be selected in **Pregenerated Ticket**, **On-Demand**, **Local Radius**, **Remote Radius Server** and **LDAP Server**, and select one authentication type for Default Auth Type. Below depicts an example for **Local Radius**.

The screenshot shows the 'Service Domain0 Setup' window with the 'General Setup' tab selected. The 'Authentication Options' section has 'Local Radius' selected as the 'Auth Type' and 'Default Auth Type'. The 'Login Options' section shows 'Login Timeout' set to 10 minutes, 'Redirect URL' as 'http://www.phoenix.com', and 'Time Policy' as 'Always Run'. The 'Custom Pages' section shows 'Template Page' selected. The 'Template Page Setting' section shows 'Color Template' as 'Dark', 'Font Color' as '#4c4c4c', 'Background Color' as '#4c4c4c', 'Login Main Title' as 'NAC Gateway', 'Login Sub Title' as 'Access Controller', 'Login Help Content' as 'Please Input Passcode/Username and Password, then you can use our Internet service. Thanks!', and 'Login Footer Title' as 'Copyright by Phoenix Corp'. 'Save' and 'Preview' buttons are at the bottom.

- Select **Local Radius** for Domain0's Authentication Type.
- Enter the **Redirect URL** that users should be initially directed to when successfully authenticated to the network.
- 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**, the Reboot page will appear
- Click **Reboot** button to start the restarting process.

🏠 Reboot

⚠️ Press " Reboot " to Enable New Setting.

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

Reboot



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

椅

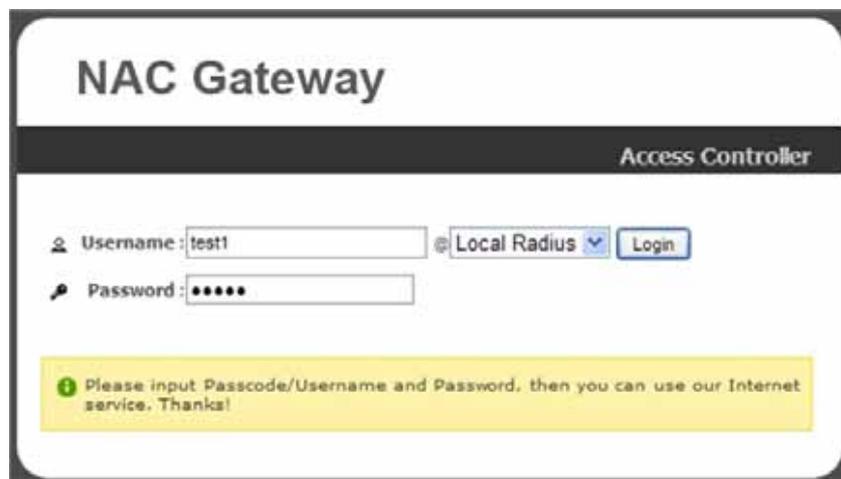
- When the "Home Page" appears, it means the restart process is now completed.

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 :

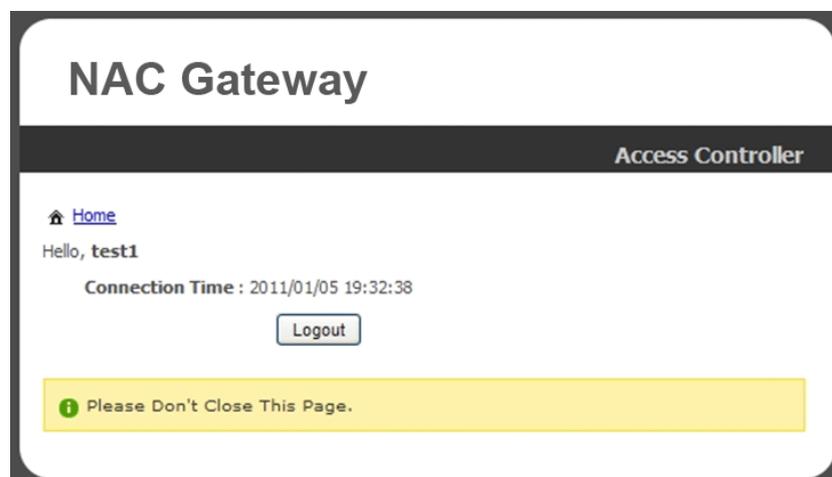
1. Connect a client device (e.g. Notebook) with wireless interface to scan the configured ESSID of WMS-308N (e.g. **AP00**) and get associated with this ESSID.
2. The client device will obtain an IP address automatically via DHCP from WMS-308N. Open a web browser on a client device, access any URL, and 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	AP Profile Management	IP Filter	Firmware Upgrade	Extra Info
	LAN	Walled Garden	AP Batch Setup Management	MAC Filter	Network Utility	Event Log
	Switch QoS	Notification	AP Group Setup Management	Virtual Server	Format Database	
	DDNS	Online Users	AP Group Status	IP Routing	Reboot	
	Management	Log Info	Website Monitor	Time Policy		
	Time Server					
	SNMP					



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

4.1 Connect 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.

WAN Setup

WAN1 Setup

Disable
 Static IP
 Dynamic IP
 PPPoE
 PPTP

Hostname:

Keep Default MAC Address
 Clone MAC Address: 00:1A:92:9F:A4:9B
 Manual MAC Address:

WAN2 Setup

Disable
 Static IP
 Dynamic IP
 PPPoE
 PPTP

DNS

DNS: No Default DNS Server
 Specify DNS Server IP

Primary:

Secondary:

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

WAN1 Setup

Disable
 Static IP
 Dynamic IP
 PPPoE
 PPTP

IP Address:

IP Netmask:

IP Gateway:

➔ **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.

The screenshot shows the 'WAN1 Setup' configuration page. At the top, there are five radio button options: 'Disable', 'Static IP', 'Dynamic IP', 'PPPoE', and 'PPTP'. The 'PPPoE' option is selected. Below the radio buttons, there are three input fields: 'Username', 'Password', and 'MTU'.

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

→ **Password** : Enter Password for PPPoE connection

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

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

The screenshot shows the 'WAN1 Setup' configuration page. At the top, there are five radio button options: 'Disable', 'Static IP', 'Dynamic IP', 'PPPoE', and 'PPTP'. The 'PPTP' option is selected. Below the radio buttons, there are six input fields: 'Username', 'Password', 'PPTP Server IP', 'My WAN IP', 'My WAN IP Netmask', and 'MTU'. At the bottom, there are two checkboxes for 'MPPE Encryption': 'MPPE-40' and 'MPPE-128'.

→ **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 through the WAN interface (WAN1 and WAN2 ports).

WAN Traffic Setup

■ 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.

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.

Dynamic DNS Setup

DDNS

Service : Enable Disable

Service Provider :

Hostname : .

Username :

Password :

- **Enabled:** Select Enable for DDNS function, each time your IP address for WAN is changed, the information will be updated to DDNS service provider automatically.
- **Service Provider:** Select the correct Service Provider from the drop-down list, here included are *dyndns*, *dhs*, *ods* and *tzo* embedded in the 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.

LAN Setup

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

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

Click "**Edit**" button on this page, the setup page should be appear. Below depicts an example for **LAN**.

LAN > LAN Setup (Domain0)

LAN IP

IP Address:

IP Netmask:

802.1s Multiple Spanning Tree

MSTP: Enable Disable

MSTI:

Bandwidth Control

Service: Enable Disable

Type: Even Distribution of Bandwidth Individual Bandwidth

Total Max. Upload: Kbit/s

Total Max. Download: Kbit/s

Guest Service: Enable Disable

Guest Upload: Kbit/s

Guest Download: Kbit/s

Session Limit per IP: sessions

DHCP Server

DHCP: Enable Disable

Start IP:

End IP:

DNS1 IP:

DNS2 IP:

WINS IP:

Domain:

Lease Time:

Port Setup

Port #		PVID	802.1P Priority
Port 1	<input checked="" type="checkbox"/>	LAN	<input type="text" value="0"/>
Port 2	<input checked="" type="checkbox"/>	LAN	<input type="text" value="0"/>
Port 3	<input checked="" type="checkbox"/>	LAN	<input type="text" value="0"/>
Port 4	<input checked="" type="checkbox"/>	LAN	<input type="text" value="0"/>

- 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.

VLAN

VLAN Tag(ID):



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.

Bandwidth Control

Service: Enable Disable

Type: Even Distribution of Bandwidth Individual Bandwidth

Total Max. Upload: Kbit/s

Total Max. Download: Kbit/s

Guest Service: Enable Disable

Guest Upload: Kbit/s

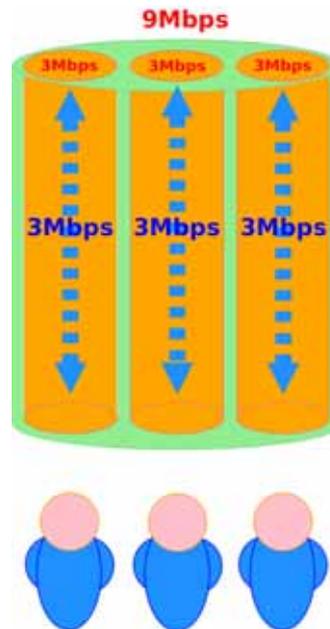
Guest Download: Kbit/s

Session Limit per IP: sessions

- Type** : Enable the desire option among "Even Distribution of Bandwidth" or "Individual Bandwidth".
- Even Distribution of Bandwidth** : Set users distribute Total Max. Upload/Download. Below depicts an

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

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



- **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.

Bandwidth Control

Service : Enable Disable

Type : Even Distribution of Bandwidth Individual Bandwidth

Individual Upload : Kbit/s

Individual Download : Kbit/s

Group Total Limit : Enable Disable

Group Upload : Kbit/s

Group Download : Kbit/s

Guest Service : Enable Disable

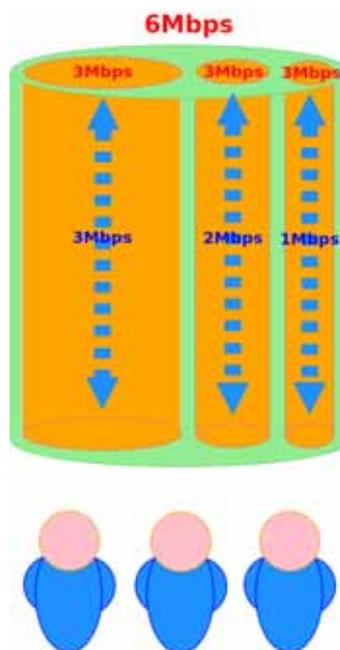
Guest Upload : Kbit/s

Guest Download : Kbit/s

Session Limit per IP : sessions

- ✓ **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 and 802.1p priority for the PVID. The specified priority will only be assigned to the **untagged** frame and then system can map the untagged frame to the proper output queue for 802.1Q-based QoS. Just specify the priority to **0** if you don't turn on the QoS or use other QoS mechanisms instead of 802.1Q-based. 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, when VLAN1's Port 1 enabled and set Port 1 to Untagged on VLAN Setup page. The Port 1 need set PVID to VLAN1 on LAN Setup page.

Port Setup			
Port #		PVID	802.1P Priority
Port 1	<input checked="" type="checkbox"/>	LAN	0
Port 2	<input checked="" type="checkbox"/>	LAN	0
Port 3	<input checked="" type="checkbox"/>	LAN	0
Port 4	<input checked="" type="checkbox"/>	LAN	0

Port Setup			
Port #		VLAN TAG Mode	
		Untagged	Tagged
Port 1	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Port 2	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Port 3	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
Port 4	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>

- ➔ **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.
- ➔ **802.1P Priority** : Priority value is in the range of **0~7**, the default is **0**. Specify desired priority value on the respective port.
- ➔ **VLAN TAG Mode** : Select **Tagged** or **Untagged** on the respective port.
- **MSTP** : By default, it's "**Disable**". To "**Enable**" to activate MSTP with up to **16** Spanning Tree instances.

The multiple spanning tree network protocol provides a loop free topology for any bridged LAN/VLAN. MSTP is defined in the IEEE Standard 802.1s.

- ➔ **MSTI** : Multiple Spanning Tree Instances, MSTI. MSTP enables the grouping and mapping of VLANs to different spanning tree instances. So, an MST Instance(MSTI) is a particular set of VLANs that are all using the same spanning tree. Each MSTI is identified by a number, the range can be numbered **0** through **15**.The Common Instance Spanning Tree (CIST) is always MSTI ID **0**.
- **DHCP** : Check "**Enable**" to activate DHCP Server on VLAN/LAN port.
 - ➔ **Start IP / End IP** : Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
 - ➔ **DNS1 / DNS2 IP** : The Domain Name System (DNS) is an Internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the 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.

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

4.1.6 Manage Switch QoS

The WMS-308N can recognize the QoS priority information of incoming packets to give a different egress service priority. The WMS-308N identifies the packets as high priority based on several types of QoS priority information : **Port-Base Priority**, **802.1p-Base Priority** and **DiffServ-Base Priority**. QoS function provides maximum **8** queues per port for packet scheduling with queue weight and priority assignment. With different queue number usage, threshold of flow control mechanism will be an important element in throughput improvement. Please click on **System -> Switch QoS Setup**, the Switch QoS Setup page should be appear.

Switch QoS Setup

#	Port Priority		#	Port Priority	
	Enable	Priority		Enable	Priority
Port 1	<input type="checkbox"/>	Priority 0	Port 3	<input type="checkbox"/>	Priority 0
Port 2	<input type="checkbox"/>	Priority 0	Port 4	<input type="checkbox"/>	Priority 0

802.1p	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
--------	------------------------------	--

DSCP	<input type="text"/>	Priority	0	<input type="button" value="Add"/>	
DSCP	Priority	Delete	DSCP	Priority	Delete
No DSCP QoS Priority in List					

Queue	Strict High	Weight	DSCP Remark		802.1p Remark	
			Enabled	Remark	Enabled	Remark
Priority 0	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 1	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 2	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 3	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 4	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 5	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 6	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Priority 7	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>

- **Port QoS Setup** : When port-based priority is enabled, packets received from the high-priority port are sent to the high priority queue of the destination port. The WMS-308N provides maximum **8** queue per port for packet scheduling with queue weight and priority assignment.
- **802.1p QoS Setup** : By default, it's "**Disable**". To **Enable** to set 802.1p priorities mapping to internal priority queue.
- **DSCP QoS Priority** : This function can be used to set the translation table for mapping DSCP value to internal priority queue. The range of DSCP is **0~63** and the range of priority queue is **0~7**.
- **Queue Weight Setup** : Set weight and type, Strict Priority(SP) or Weighted Fair Queue(WFQ) for dedicated port for using queues. There are priorities as queue value in strict queues. It means strict queue value 5 carrying higher priority than strict queue value 4.
 - ➔ **Queue** : Indicate 8 priority queue.
 - ➔ **Strict High** : By default, it's "**Enable**" for Strict Priority queue. To **Disable** to set WFQ weight value.
 - ➔ **Weight** : Set WFQ in weight ration from **1** to **128**
 - ➔ **DSCP Remark** : Select Enable to activate DSCP remark function of the respective priority queue and assign DSCP remark value from **0** to **63**.
 - ➔ **802.1p Remark** : Select Enable to activate 802.1p remark function of the respective priority queue and assign 802.1p remark value from **0** to **7**.

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.

Time Server Setup

System Time
Local Time : 2011/01/05 03:28:49

Setup Time Use NTP
 Default NTP Server : time.stdtime.gov.tw (optional)
 Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London
 Daylight Saving Time : Disable

User Setup
 Date : 2011 Jan 5
 Time : 11:28:59 (GMT+8:00)
 Set Time :

Time Display Format
 Display Format : %Y/%m/%d %H:%M:%S (YY/Km/%d %H:MM:SS)

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

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



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

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

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

4.2.2 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.

Management Setup

<p>System Information</p> <p>System Name: <input type="text" value="WMS-308N"/></p> <p>Description: <input type="text" value="Network Access Control Gateway"/></p> <p>Location: <input type="text"/></p>	<p>Login Methods</p> <p>Enable HTTP: <input checked="" type="checkbox"/> Port: <input type="text" value="80"/></p> <p>Enable HTTPS: <input type="checkbox"/> Port: <input type="text" value="443"/> <input type="button" value="UploadKey"/></p> <p>Enable Telnet: <input checked="" type="checkbox"/> Port: <input type="text" value="23"/></p> <p>Enable SSH: <input type="checkbox"/> Port: <input type="text" value="22"/> <input type="button" value="GenerateKey"/></p> <p>Host Key Footprint: <input type="text" value="None"/></p>
<p>Root Password</p> <p>New Root Password: <input type="text"/></p> <p>Check Root Password: <input type="text"/></p>	<p>E-mail SMTP Relay</p> <p>Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>IP Address/Domain: <input type="text"/></p>
<p>Admin Password</p> <p>New Admin Password: <input type="text"/></p> <p>Check New Password: <input type="text"/></p>	<p>Ping Watchdog</p> <p>Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>IP Address To Ping: <input type="text"/></p> <p>Ping Interval: <input type="text" value="300"/> Seconds</p> <p>Startup Delay: <input type="text" value="300"/> Seconds</p> <p>Failure Count To Reboot: <input type="text" value="3"/></p>
<p>Operator Password</p> <p>New Operator Password: <input type="text"/></p> <p>Check New Password: <input type="text"/></p>	<p><input type="button" value="Save"/></p>

■ 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.
- **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.

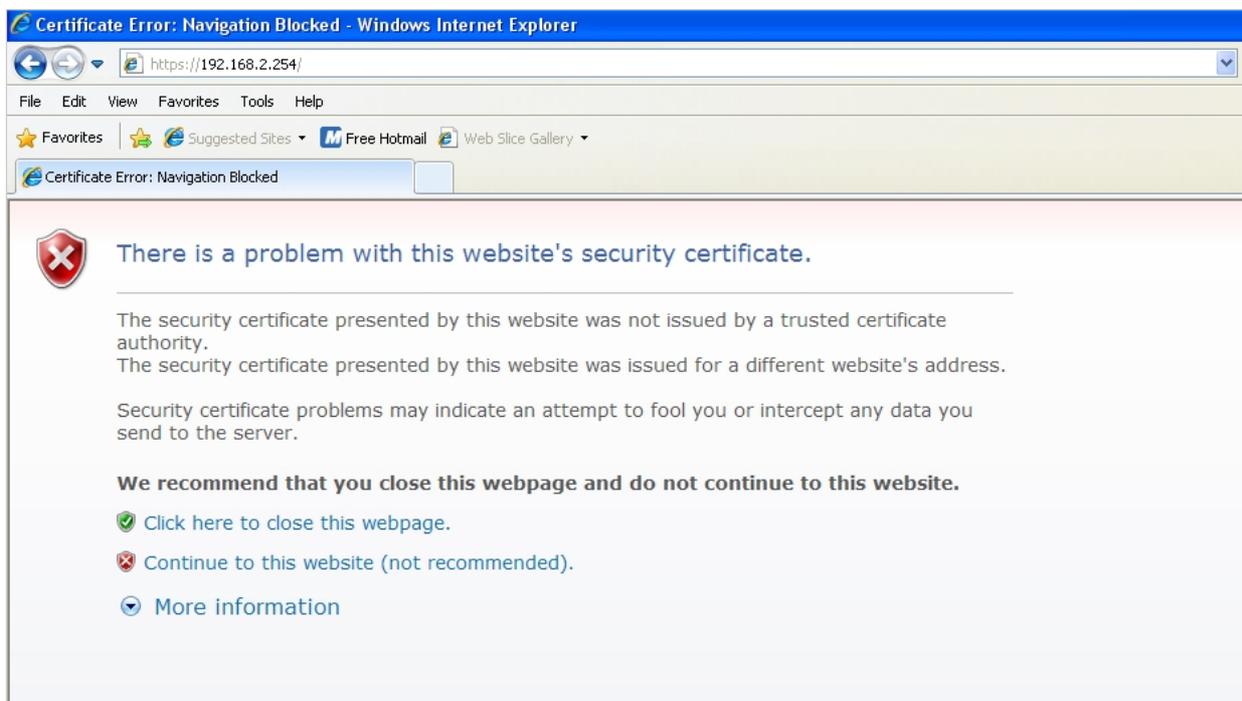
Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots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

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

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

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

Without a valid certificate, users may encounter the following problem in IE8 when they try to access 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.

Profile Save

Profile Save

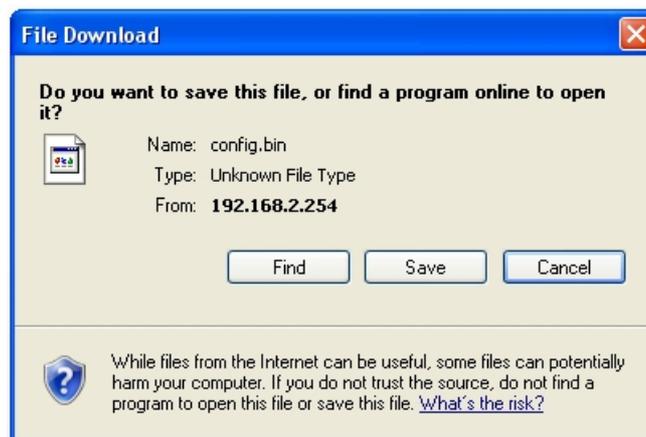
Save Settings To PC :

Load Settings From PC :

Reset To Factory Default :

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

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



- **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.

Firmware Upgrade

<p>Firmware Information</p> <p>Firmware Version : Cen-AC V0.0.3 Firmware Date : 2011/03/16 11:57:33</p> <p>! From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.</p>	<p>Upgrade Via Local PC</p> <p>Select File : <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upgrade"/></p>
	<p>Upgrade Via TFTP Server</p> <p>TFTP Server IP: <input type="text"/> File Name : <input type="text"/> <input type="button" value="Upgrade"/></p>
	<p>Upgrade Via HTTP URL</p> <p>URL : <input type="text"/> <input type="button" value="Upgrade"/></p>

- **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.

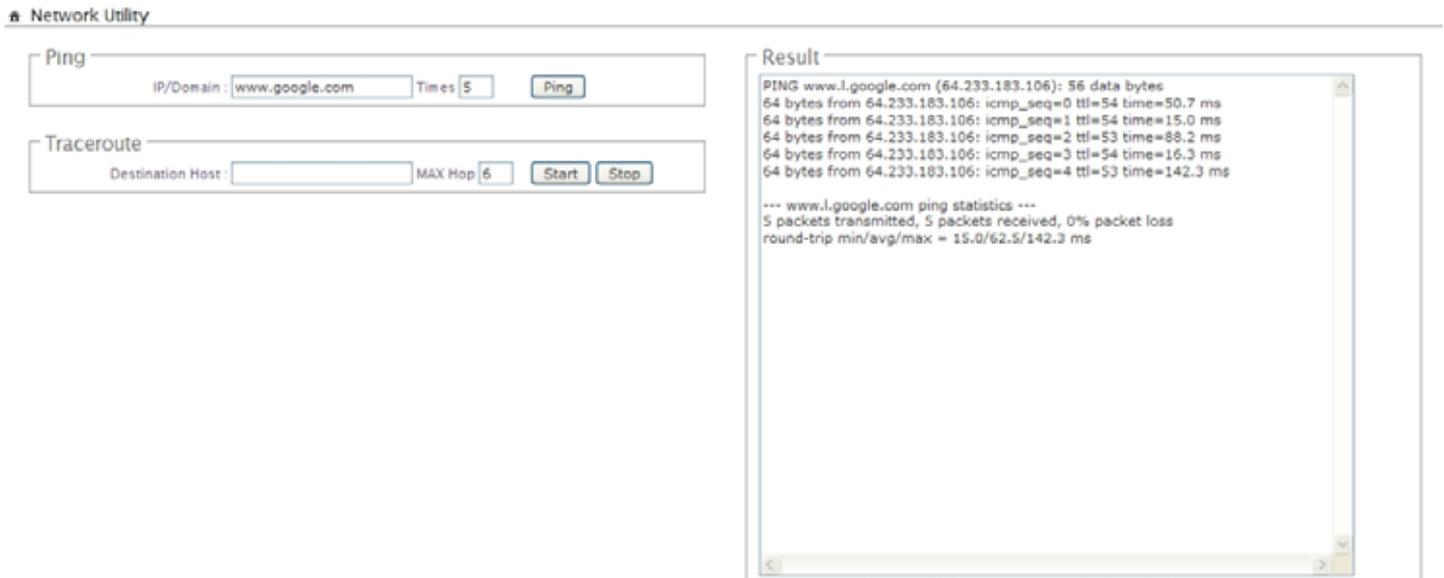


1. To prevent data loss during firmware upgrade, please backup current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

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.

4.2.7 Format Database

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

Format Database

Format Database

Clear Accounts/Tickets :



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

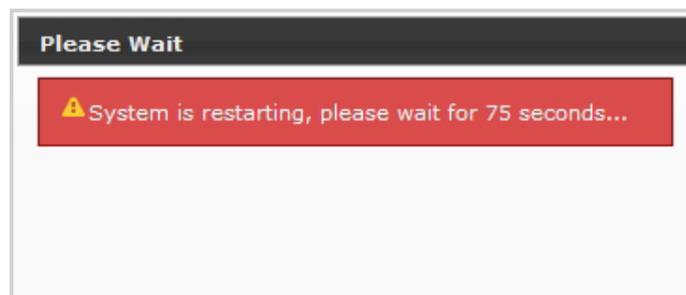
This function allows administrator to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

🏠 Reboot

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

Reboot

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.

Service Domain Setup

Domain 0	Domain 1	Domain 2	Domain 3
LAN Port LAN Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service on Guest Service on Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN1 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN2 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN3 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page
Domain 4	Domain 5	Domain 6	Domain 7
LAN Port VLAN4 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN5 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN6 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page	LAN Port VLAN7 Auth Type Pregenerated Ticket On-demand Local Users Remote Radius Server LDAP Server WAN Port Auto IPPNP Service off Guest Service off Time Policy Always Run Redirect URL Link Login Page Template Page

- **LAN Port** : The bonding interface for the respective Service Domain
- **Auth Type** : The authentication type for the respective Service Domain. There are **five** types : Pregenerated Ticket. On-demand, Local Users, Remote Radius Server and LDAP.
- **WAN Port** : Indicates the outgoing traffic for the respective Service Domain.
- **IPPNP Service** : Indicates status of IP PnP service for the respective Service Domain.
- **Guest Service** : Indicates status of Guest service for the respective Service Domain.
- **Time Policy** : Indicates scheduling of authentication service for the respective Service Domain.
- **Redirect URL** : The redirect URL for this Login page of Service Domain. Click Hyperlinks to enter redirect URL.
- **Login Page** : The custom page for this Service Domain. There are two types : Template page or Upload page
-  : Click tools icon 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.

Service Domain0 Setup

General Setup | IP Setup | DHCP Client

Authentication Options

Auth Type : Pre-generated Ticket
 On-Demand
 Local Radius
 Remote Radius Server
 LDAP Server

Default Auth Type : Local Radius

Specify WAN Port : Auto WAN traffic must be specified to Load Balance.

NAT Service : Enable Disable

Login Options

Login Timeout : 10 Minutes

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

Time Policy : Always Run

IP PnP Service : Enable Disable

Guest Service : Enable Disable

Guest Count Limit : 10

Guest Time : Minutes

Custom Pages

Login Page Setting : Template Page Upload Page

Template Page Setting

Color Template : Gray

Font Color : #4c4c4c

Background Color : #4c4c4c

Login Main Title : NAC Gateway Color : #4c4c4c

Login Sub Title : Access Controller Color : #cccccc

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

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

- **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**.

- ➔ **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 4.5.2.2**).
- **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.
 - ➔ **Login Redirect URL**: Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set, such as <http://www.yahoo.com.tw>. Regardless of the original webpage set in the users' computers, they will be redirect to this page after login.
 - ➔ **Time Policy** : Select desired scheduling of the respective Service Domain for authentication service. Scheduling setting is on **Time Policy** page.
 - ➔ **IP PnP** : IP Plug and Play, the 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.

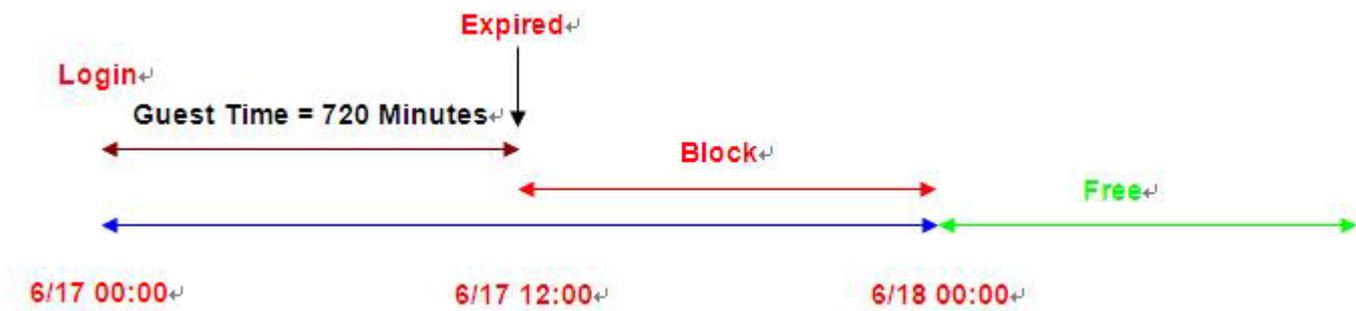


IP PnP only supports on **NAT** mode

- ➔ **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.

☞ **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.

```
<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.

```

```

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

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

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

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

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

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

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

4.3.2 Configure Authentication

WMS-308N support **5** types of authentication : **Pregenerated Tickets**, **On-Demand Users**, **Local RADIUS Accounts**, **Remote RADIUS Server** and **Remote LDAP Server**. This section depicts to configure the settings for pregenerated tickets, on-demand users and authentication server. If authentication 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.

🏠 Authentication Management

Multiple Login

Service : Enable Disable

Auth Type Alias

Auth Type	Service Name	Description
Pregenerated Ticket	<input type="text" value="Pregenerated Ticket"/>	<input type="text"/>
On-Demand	<input type="text" value="On-Demand"/>	<input type="text"/>
Local Radius	<input type="text" value="Local Radius"/>	<input type="text"/>
Remote Radius Server	<input type="text" value="Remote Radius Server"/>	<input type="text"/>
LDAP Server	<input type="text" value="LDAP Server"/>	<input type="text"/>

Save

- **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.

Service Domain > Pregenerated Tickets DB

Ticket Setting

File ID: (options)

Price: * Customize Currency

Quantity of Tickets: *

Passcode Type: All Digit All Letters Mix Letter Digit

No L/I/1 No O/0 No U/V

Passcode Length: 8 *

Description:

Pregenerated Tickets Database List

Import Tickets File:

#	File ID	Price	Quantity	Description	List	Delete
1	00001	2.00	100	One Time Package	Info	Delete
2	00002	5.00	100	Multiple Times Package	Info	Delete
3	00003	10.00	100	Unlimited Package	Info	Delete
4	00004	5.00	100	Volume - 3000MB Package	Info	Delete
5	00005	3.00	100	Volume - 2000MB Package	Info	Delete

Policy Setting

Type: One Time

Quota: Minutes

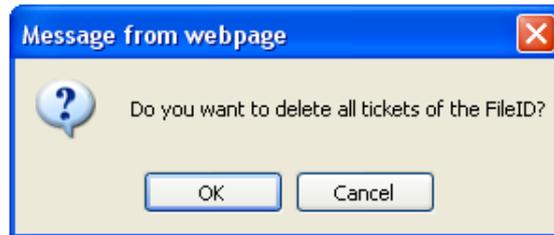
Effective Start Time: 2011 / 2 / 16 15 00 YYYY/MM/DD hh:mm

Effective End Time: 2012 / 2 / 16 15 00 YYYY/MM/DD hh:mm

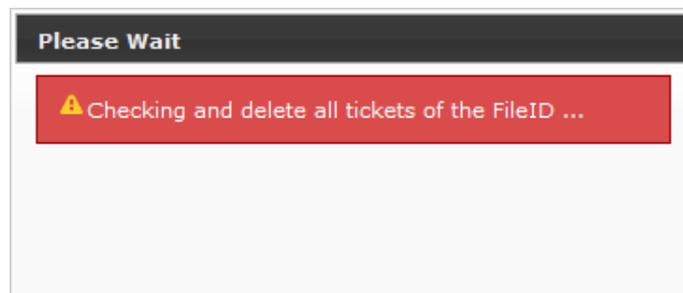
- **File ID** : Enter the **8 hex digit** number for identifying tickets databases
- **Price** : The price charged for this tickets databases
- **Currency** : Select currency from drop-down list or enter customize currency for this tickets databases
- **Quantity of Tickets** : Specify desired quantity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

Click **Save** button for generate ticket databases in the Pregenerated Tickets Database List.

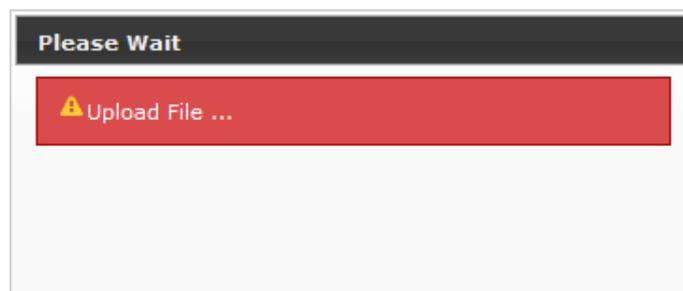
- **Delete** : Click **Delete** button to delete selected tickets databases. After clicking delete button, the alert message appears as below .



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



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



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

★ Service Domain > Pregenerated Tickets DB > Tickets Manager Refresh

Ticket Information

File ID : 00001
 Description : Unlimited Package
 Effective Start Time : 2011/01/06 17:00 GMT+08:00
 Effective End Time : 2011/02/06 17:00 GMT+08:00
 Type and Quota : Unlimited Until End Time
 Passcode Type : Mix Digit Letter
 Passcode Length : 8
 Quantity : 100
 Price : 10.00 USD

Statistics

Ticket Qty : 100
 Used Ticket Qty : 0
 Expired Ticket Qty : 0
 Total Price : 1000 USD

Export Tickets

Export Mode : Export BIN Export TXT Printable

[Export](#)

ID	Code	Type/Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
00001	FGKLVDTB	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	LZHS1Q14	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	LCNG2UZW	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	690MUO2P	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	K3QGQJ7H	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	YO90UAKF	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	NNC5IBH4	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	EX6BL9XM	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	CN23MPA1	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete
00001	DZHNA1ID	Unlimited Until End Time	Unused	2011/01/06 17:25:47		2011/01/06 17:00:00	2011/02/06 17:00:00		10.00	USD	Delete

Showing 1 to 10 of 100 entries

First Previous 1 2 3 4 5 Next Last

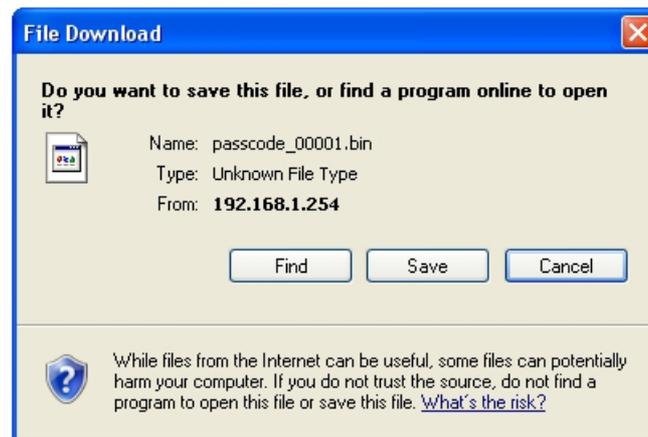
➔ **Ticket Information** : Show information for selected tickets database

- ✓ **File ID**: Identifying tickets databases
- ✓ **Description** : Denote information of the tickets databases
- ✓ **Effective Starting Time** : Denote effective starting time of the tickets databases
- ✓ **Effective Ending Time** : Denote effective ending time of the tickets databases
- ✓ **Type and Quota** : Denote tickets database time/volume policy and service quota.
- ✓ **Passcode Type** : Denote passcode type of the tickets databases
- ✓ **Passcode Length** : Denote ticket's passcode length
- ✓ **Quantity** : Denote ticket's quantity in this tickets databases
- ✓ **Price** : The price charged for this tickets database.

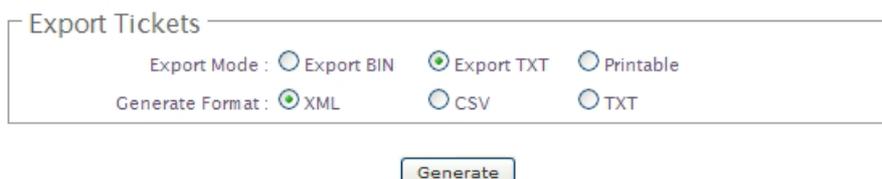
➔ **Statistic** : Show tickets database statistic information.

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

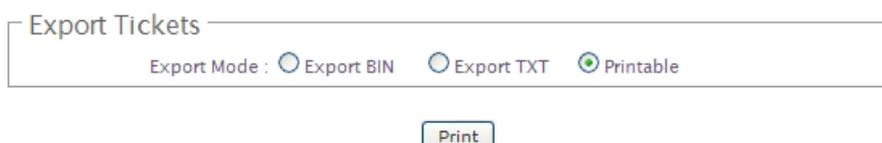
- ✓ **Used Ticket Qty** : Denote used ticket's quantity in this tickets databases
 - ✓ **Expired Ticket Qty** : Denote expired ticket's quantity in this tickets databases
 - ✓ **Total Price** : Denote total ticket's price and currency in this tickets database
- **Export Tickets** : There are **three** methods to backup your information of ticket databases
- ✓ **Export BIN** : The administrator can backup ticket database or copy to other 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	630M002P
Price	10.00 USD						
Start Time	2011-01-06 17:00:00						
End Time	2011-02-06 17:00:00						
Wireless ESSID		Wireless ESSID		Wireless ESSID		Wireless ESSID	
Passcode	K3QGGJ7H	Passcode	Y090UAKF	Passcode	NNCSIBH4	Passcode	EN68L9XM
Price	10.00 USD						
Start Time	2011-01-06 17:00:00						
End Time	2011-02-06 17:00:00						
Wireless ESSID		Wireless ESSID		Wireless ESSID		Wireless ESSID	

→ **Tickets List** : Show tickets information

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

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



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

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

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.

🏠 Service Domain > Billing Plans Setup

Billing Plans List							
#	Status	Plan Name	Type:Quota	Price	Edit	Info	
0	On	Package 0	Unlimited Until End Time	10.00 USD	Edit	Info	
1	On	Package 1	Multiple Times: 60 Minutes	5.00 USD	Edit	Info	
2	On	Package 2	One Time: 60 Minutes	3.00 USD	Edit	Info	
3	On	Package 3	Volume: 3000 MB	5.00 USD	Edit	Info	
4	Off	Package 4	Unlimited Until End Time	10.00 USD	Edit	Info	
5	Off	Package 5	Unlimited Until End Time	10.00 USD	Edit	Info	
6	Off	Package 6	Unlimited Until End Time	10.00 USD	Edit	Info	
7	Off	Package 7	Unlimited Until End Time	10.00 USD	Edit	Info	
8	Off	Package 8	Unlimited Until End Time	10.00 USD	Edit	Info	
9	Off	Package 9	Unlimited Until End Time	10.00 USD	Edit	Info	

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

4.3.2.3.1 Create Billing Plans

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

Service Domain > Billing Plans Setup > Billing Plan0 Setup

- **Status** : By default, it's "**Disable**". To "**Enable**" to activate this billing plan.
- **Plan Name** : Enter plan name for this billing plan.
- **Price** : The price charged and currency for this billing plan.



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

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

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

4.3.2.3.2 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.

Service Domain > Billing Plans Setup > On-Demand Information Refresh

Plan0 Information

Service : Enable
 Plan Name : Package 0
 Price : 10.00 USD
 Wireless ESSID : WAP-9546P
 Wireless Key : 1234567800
 Description : Unlimited Package
 Type and Quota : Unlimited Until End Time
 Effective Start Time : 0 Days 0 Hours 0 Mins
 Effective End Time : 5 Days 0 Hours 0 Mins

Statistics

Ticket Qty: 63
 Used Ticket Qty: 1
 Expired Ticket Qty: 17
 Total Price: 630 USD

Daily Tickets Chart

Plan	Code	Type Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
0	8R13XB7	Unlimited Until End Time	Unused	2011/01/22 14:03:52		2011/01/22 14:03:52	2011/01/27 14:03:52		10.00	USD	Delete
0	W45LCP8	Unlimited Until End Time	Unused	2011/01/22 14:03:47		2011/01/22 14:03:47	2011/01/27 14:03:47		10.00	USD	Delete
0	5MX7RXQ8	Unlimited Until End Time	Unused	2011/01/22 13:59:07		2011/01/22 13:59:07	2011/01/27 13:59:07		10.00	USD	Delete
0	Z129A135	Unlimited Until End Time	Unused	2011/01/22 13:59:04		2011/01/22 13:59:04	2011/01/27 13:59:04		10.00	USD	Delete
0	9PYGH83H	Unlimited Until End Time	Unused	2011/01/22 13:59:01		2011/01/22 13:59:01	2011/01/27 13:59:01		10.00	USD	Delete
0	WCQT7WB8	Unlimited Until End Time	Unused	2011/01/22 13:58:59		2011/01/22 13:58:59	2011/01/27 13:58:59		10.00	USD	Delete
0	GCTB12NC	Unlimited Until End Time	Unused	2011/01/22 13:58:56		2011/01/22 13:58:56	2011/01/27 13:58:56		10.00	USD	Delete
0	FCYDHY4Q	Unlimited Until End Time	Unused	2011/01/22 13:58:54		2011/01/22 13:58:54	2011/01/27 13:58:54		10.00	USD	Delete
0	45FH7B69	Unlimited Until End Time	Unused	2011/01/22 13:58:51		2011/01/22 13:58:51	2011/01/27 13:58:51		10.00	USD	Delete
0	9YZBY3DC	Unlimited Until End Time	Unused	2011/01/22 13:58:49		2011/01/22 13:58:49	2011/01/27 13:58:49		10.00	USD	Delete

Showing 1 to 10 of 63 entries First Previous 1 2 3 4 5 Next Last

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

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

Package 2

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

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

Package 2

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

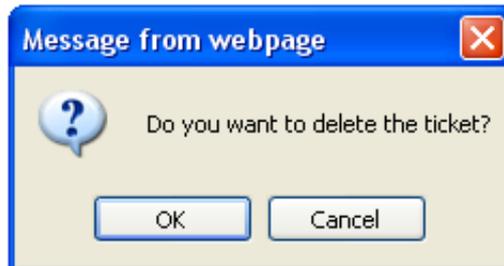
Click **Create** button to add new account for this billing plan. Below depicts an example for creating ticket.

Package 2

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

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

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



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



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

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.

Service Domain > Billing Plans Setup > Payment Gateway Setup

External Payment Gateway

Payment Mode: None PayPal

PayPal Payment Page Configuration

API Username:

API Password:

API Signature:

Client's Purchasing Record

Starting Invoice Number: -

Current NO: **110100001**

Billing Plan Setup List Information

#	Enable	Plan Name	Type:Quota	Price
0	<input type="checkbox"/>	Package 0	Unlimited Until End Time	10.00 USD
1	<input type="checkbox"/>	Package 1	Multiple Times: 60 Minutes	5.00 USD
2	<input type="checkbox"/>	Package 2	One Time: 60 Minutes	3.00 USD
3	<input type="checkbox"/>	Package 3	Volume: 3000 MB	5.00 USD
4	<input type="checkbox"/>	Package 4	Unlimited Until End Time	10.00 USD
5	<input type="checkbox"/>	Package 5	Unlimited Until End Time	10.00 USD
6	<input type="checkbox"/>	Package 6	Unlimited Until End Time	10.00 USD
7	<input type="checkbox"/>	Package 7	Unlimited Until End Time	10.00 USD
8	<input type="checkbox"/>	Package 8	Unlimited Until End Time	10.00 USD
9	<input type="checkbox"/>	Package 9	Unlimited Until End Time	10.00 USD

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

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

The **Paypal** payment gateway does not support “**Customize Currency**” 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.
- **Information** : Click this button to view accounts information for PayPal.

66

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

Payment Gateway Information

Payment Mode : Paypal
Current Invoice Number : **100600002**

[Edit](#)

Statistic

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

Daily Tickets Chart

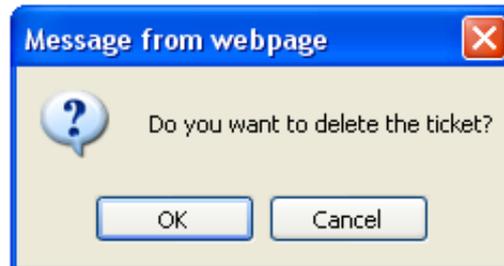
The chart displays a single data point for the date 6/17 with a value of 1. The y-axis ranges from 0 to 2, and the x-axis shows the date 6/17.

Plan	Code	Type/Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
2	MC7MK6EZ	One Time: 60 Minutes	Used	2010/06/17 21:18:24	2010/06/17 21:19:49	2010/06/17 21:18:24	2010/06/22 21:18:24	2010/06/17 21:19:49	1	TWD	Delete

Showing 1 to 1 of 1 entries

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

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



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



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



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.

🏠 [Service Domain](#) > [Billing Plans Setup](#) > [Thermal Printer Setup](#)

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



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

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

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

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

Thermal Printer0 Setup

Service: Disable Enabled

IP Address: *

Command Port: *

COM Port: COM1 COM2

New Lock Password: *

Confirm Lock Password: *

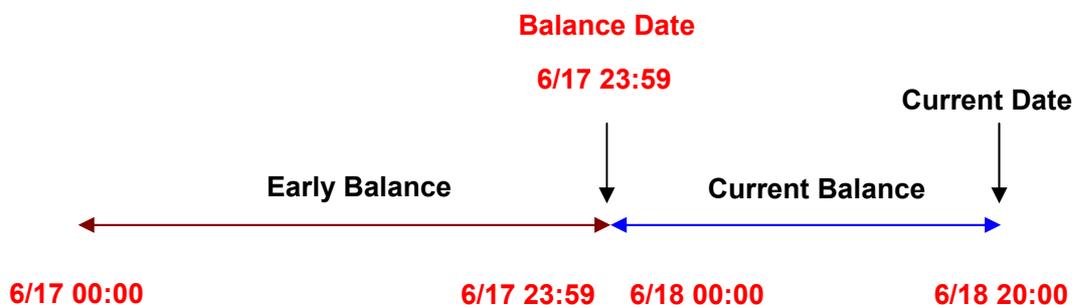
Balance Date: *hh:mm

Description:

Billing Plan Setup List

#	Enable	Plan Name	Type:Quota	Price
0	<input type="checkbox"/>	Package 0	Unlimited Until End Time	10.00 USD
1	<input type="checkbox"/>	Package 1	Multiple Times: 60 Minutes	5.00 USD
2	<input type="checkbox"/>	Package 2	One Time: 60 Minutes	3.00 USD
3	<input type="checkbox"/>	Package 3	Volume: 3000 MB	5.00 USD
4	<input type="checkbox"/>	Package 4	Unlimited Until End Time	10.00 USD
5	<input type="checkbox"/>	Package 5	Unlimited Until End Time	10.00 USD
6	<input type="checkbox"/>	Package 6	Unlimited Until End Time	10.00 USD
7	<input type="checkbox"/>	Package 7	Unlimited Until End Time	10.00 USD
8	<input type="checkbox"/>	Package 8	Unlimited Until End Time	10.00 USD
9	<input type="checkbox"/>	Package 9	Unlimited Until End Time	10.00 USD

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



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



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

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

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

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

Thermal Printer0 Information

Service : Enable
 IP Address : 192.168.2.253
 Command Port : 5000
 COM Port : COM1
 Balance Date : 12:00
 Description : Printer 1

[Edit](#)

Statistics

Ticket Qty : 33
 Used Ticket Qty : 0
 Expired Ticket Qty : 21
 Total Price : 162 USD

Daily Tickets Chart

Plan	Code	Type:Quota	Status	Create Time	Open Time	Start Time	End Time	Last Login	Price	Currency	Delete
0	P5WFCMR	Unlimited Until End Time	Unused	2011/01/20 10:28:30		2011/01/20 10:28:30	2011/01/25 10:28:30		10.00	USD	Delete
1	KYAZKFW	Multiple Times: 60 Minutes	Unused	2011/01/20 10:28:24		2011/01/20 10:28:24	2011/01/25 10:28:24		5.00	USD	Delete
2	ZNITWSIG	One Time: 60 Minutes	Unused	2011/01/20 10:28:18		2011/01/20 10:28:18	2011/01/25 10:28:18		3.00	USD	Delete
3	XQCI4ASW	Volume: 3000 MB	Unused	2011/01/20 10:28:03		2011/01/20 10:28:03	2011/01/25 10:28:03		5.00	USD	Delete
4	ZIBS378H	One Time: 30 Minutes	Unused	2011/01/20 10:27:58		2011/01/20 10:27:58	2011/01/25 10:27:58		1.00	USD	Delete
4	ZBYK2CJU	One Time: 30 Minutes	Unused	2011/01/19 11:13:52		2011/01/19 11:13:47	2011/01/24 11:13:47		1.00	USD	Delete
0	8CPRH2KD	Unlimited Until End Time	Unused	2011/01/19 11:13:37		2011/01/19 11:13:37	2011/01/24 11:13:37		10.00	USD	Delete
0	MBQNTM2G	Unlimited Until End Time	Unused	2011/01/18 11:28:12		2011/01/18 11:28:12	2011/01/23 11:28:12		10.00	USD	Delete
1	BK7HK24I	Multiple Times: 60 Minutes	Unused	2011/01/17 15:59:42		2011/01/17 15:59:42	2011/01/22 15:59:42		5.00	USD	Delete
2	56JR25E2	One Time: 60 Minutes	Unused	2011/01/17 15:59:37		2011/01/17 15:59:37	2011/01/22 15:59:37		3.00	USD	Delete

Showing 1 to 10 of 33 entries First Previous 1 2 3 4 Next Last

■ **Thermal Printer Information** : Show setting information in this Thermal Printer.

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

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

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

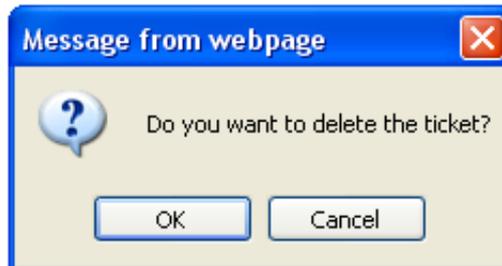
Package 2

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

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

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

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



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



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

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.

Service Domain > Billing Plans Setup > Billing Plan Report

Search Create Time Range

On-Demand Type:

Start Time: / / MM/DD/YYYY hh:mm

End Time: / / MM/DD/YYYY hh:mm

Search Result

Search Time: 2010/12/20 00:00:00 - 2011/01/20 23:59:59

#	Name	On Demand	Payment Gateway	Thermal Printer	Amount Qty	Unit Price	Subtotal
0	Package 0	43		6	49	10.00	490.00 USD
1	Package 1	30		5	35	5.00	175.00 USD
2	Package 2			8	8	3.00	24.00 USD
3	Package 3			5	5	5.00	25.00 USD
4	Package 4			4	4	1.00	4.00 USD
5	Package 5					10.00	USD
6	Package 6					10.00	USD
7	Package 7					10.00	USD
8	Package 8					10.00	USD
9	Package 9					10.00	USD
Total		73	0	28	101		718.00 USD

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

4.3.2.3.6 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.

🏠 Service Domain > Billing Plans Setup > Ticket Customization Setup

Ticket Customization Setup

Passcode:

Price:

Type:

Quota:

Create Time:

Start Time:

End Time:

Wireless ESSID:

Wireless Key:

Description:

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

Package 0

🔑	Passcode	*****
🛒	Price	10.00 USD
🕒	Type	Unlimited Until End Time
🕒	Create Time	2011/01/06 17:52:20
🕒	Start Time	2011/01/06 17:52:20
🕒	End Time	2011/01/11 17:52:20
📶	Wireless ESSID	AP981X
🔑	Wireless Key	1234567890
📄	Description	Unlimited Package

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.

Service Domain > Local Radius Accounts Management

Group

Group Name: *

Group List

#	Group Name	Delete	Edit
0	None		
1	Group1	Delete	Edit
2	Group2	Delete	Edit
3	Group3	Delete	Edit

Create Radius Accounts

Username: *

Password: *

MAC Address:

Description:

Group:

Local Radius Accounts List

Group:

Import Accounts File:
Export Accounts File:

#	Username	MAC Address	Description	Group	Delete	Edit
1	test1			Group1	Delete	Edit
2	test2			Group1	Delete	Edit
3	test3			Group2	Delete	Edit
4	test4			Group2	Delete	Edit
5	test5			Group3	Delete	Edit

Showing 1 to 5 of 5 entries

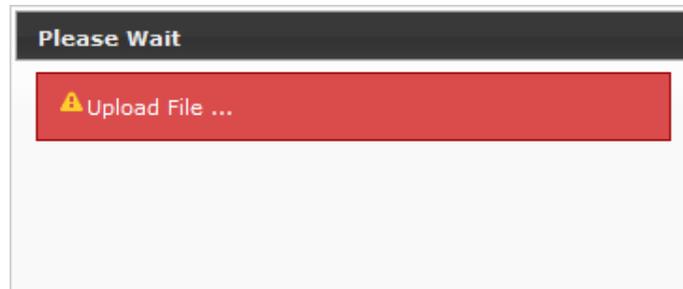
- **Group** : Enter specify name for group and click **Add** button to create. Up to **20** group can added.
- **Group List** : Display all of groups on the list, click **Delete** to remove Group Name and all of accounts in group, click **Edit** to change Group Name
- **Create Radius Accounts** :
 - ➔ **Username** : Enter the Username for local radius authentication. **4-16** alphanumeric and specify characters supported.
 - ➔ **Password** : Enter the Password for local radius authentication. **4-16** alphanumeric and specify characters supported.
 - ➔ **MAC Address** : Enter the MAC address for local radius authentication.(**optional**)
 - ➔ **Description** : Enter appropriate text to denote this account.
 - ➔ **Group** : Select specify group for 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**.

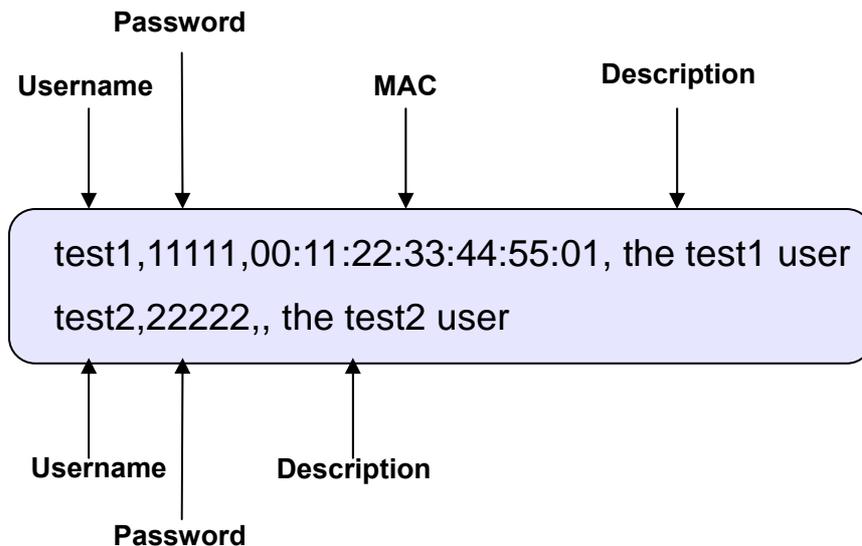
Local Radius Accounts List :

→ **Delete** : Select specify group and click Delete button to remove accounts of specified group.

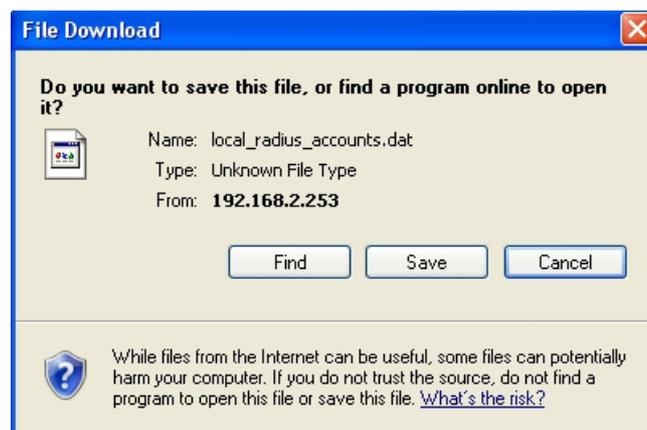
→ **Import Accounts File** : Select specify group on **Group** option and click **Select File** button to select the text file for uploading the accounts of specified group. The **“Upload File ...”** message will appear



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.



- **Export Accounts File** : Click **Export** button to save accounts file to PC. The 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.



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 Domain > Remote Radius Server Setup

Radius Server

Service : Enable Disable

Primary Server IP : *

Secondary Server IP :

Authentication Port : *

Accounting Port : *

Secret Key : *

Accounting Service : Enable Disable

Authentication Type : ▼

- **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. Please click on **Service Domain -> Authentication -> LDAP**, the page of **LDAP Server Setup** will appear

🏠 Service Domain > LDAP Server Setup

LDAP Server

Service : Enable Disable

Server IP : *

Port : *

Identity : *(ex. manager)

Password : *

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

Account Attribute : *(ex. cn)

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

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

4.3.3 Configure Walled Garden

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

Walled Garden Setup

Walled Garden

Walled Name:

IP Address/Domain:

Homepage:

Description:

Walled Garden List

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

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

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

NAC Gateway

Access Controller

Username: @ Local Radius

Password:

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

Copyright by PhoeNet Corporation

4.3.4 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.

Notification Setup

The screenshot shows the 'Notification Setup' interface. It is divided into three main sections:

- SMTP Server Setup:** Contains two columns for SMTP 1 and SMTP 2. Each column has an 'Enable' checkbox, 'Sender From', 'SMTP Server', 'Port (Default: 25)', 'Encryption' (None, TLS, SSL), 'SMTP Auth' checkbox, 'Username', and 'Password' fields.
- Syslog Setup:** Contains three rows for 'System Log', 'On-Demand User Log', and 'Session Log'. Each row has a checkbox, an 'IP' field, and a 'Port' field (Default: 514).
- Notification E-mail Setup:** Contains a table with columns: Receiver Email, Traffic Log, On-Demand Log, Session Log, Monitor IP Report, and AP Status. Below the table are 'Sending Interval (Minutes)', 'SMTP 1 Sending Test', and 'SMTP 2 Sending Test' buttons.

A 'Save' button is located at the bottom right of the configuration area.

- **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)
 - ➔ **Encryption :** Some SMTP server need encryption linking for sending E-mail. The system provides encryption for sender's SMTP server
 - ➔ **SMTP Auth :** Some SMTP server need authentication username and password for sending E-mail. The system provides authentication for sender's SMTP server
 - ➔ **Username :** The sender's authentication username for STMP server
 - ➔ **Password:** The sender's authentication password for STMP server

■ Notification E-mail Setup :

- **Receiver E-mail Address (es)** : Up to 3 E-mail address can be set up to receive the notification. These are the receiver's E-mail address.
- **Sending Interval** : The time interval (in minute) to send the E-mail report. (Default is **1440** minutes; the range is between **10** to **4200** minutes)
- **SMTP Sending Test** : Click **Send** button to verify Notification E-mail settings. Below depicts an example for success sending test.



- **Syslog Setup** : There are 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** : Indicate that current event's date and time

#Date	AuthType	Status	Passcode/Username	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out
2011-02-16 16:36:24	On-Demand	LOGIN	3CC28M93	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 16:36:54	On-Demand	KICK	3CC28M93	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	Pre-generated	LOGIN	GBORORDL	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 17:30:14	Pre-generated	TIME OUT OF RANGE	GBORORDL	192.168.1.10	00:1A:92:9F:A4:9B	393	255.2KB	344	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	248.9KB	395	69.3KB
2011-02-16 17:50:52	On-Demand	LOGIN	XKEQHPAY	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	XKEQHPAY	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	213.5KB
2011-02-16 18:34:06	On-Demand	LOGIN	2WSHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 18:52:57	On-Demand	IDLE TIMEOUT	2WSHX7BE	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	2WSHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B
2011-02-16 19:05:03	On-Demand	USE UP	2WSHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	1095	747.4KB	978	204.9KB
2011-02-16 19:07:28	Pre-generated	LOGIN	UJTD79G4	192.168.1.10	00:1A:92:9F:A4:9B	0	0B	0	0B

- ➔ **Auth Type** : There will show 6 types of authentication : **Pre-generated, On-Demand, Local Users**(Local Radius Users), **Remote Radius, LDAP** and **Guest**.
- ➔ **Status** : There will show 10 types of status as below :
 - ✓ **LOGIN** : Indicate that the user login system.
 - ✓ **LOGOUT** : Indicate that the user logout system.
 - ✓ **IDLE TIMEOUT** : Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
 - ✓ **USE UP** : Indicate that the user's service time is done.
 - ✓ **SESSION TIMEOUT** : Indicate that the user session timeout for **Remote Radius**.
 - ✓ **VOLUME USE UP** : Indicate that the user's bandwidth is done.
 - ✓ **KICK** : Indicate that the system kick out the user.
 - ✓ **TIME OUT OF RANGE** : Indicate that the service time of Service Domain is not on schedule.
- ➔ **Passcode/Username** : Indicate that the user's passcode or username.
- ➔ **IP** : Indicate that the user's IP address
- ➔ **MAC** : Indicate that the user's MAC address
- ➔ **Packets In** : Indicate that the current user's packets in.
- ➔ **Bytes In** : Indicate that the current user's bytes in.
- ➔ **Packet Out** : Indicate that the current user's packets out.
- ➔ **Bytes Out** : Indicate that the current user's bytes out.

■ On-Demand Log :

As shown in the following figure, each line is traffic history record consisting of 12 fields : **Date**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out**, **Start Time**, **End Time** and **Plan**

IDate	Status	Passcode/Username	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Start Time	End Time	Plan
2011-02-16 14:17:00	ADD OD ACCOUNT	7HQATY2	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:00	2011-02-21 14:17:00	Plan 0
2011-02-16 14:17:01	ADD OD ACCOUNT	KKEQHPAY	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:01	2011-02-21 14:17:01	Plan 0
2011-02-16 14:17:40	ADD OD ACCOUNT	8G4SDS8F	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:40	2011-02-21 14:17:40	Plan 0
2011-02-16 14:17:54	ADD OD ACCOUNT	SCF8MS9	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 14:18:17	DELETE OD ACCOUNT	KCF8MS9	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-01-17 15:40:11	2011-01-22 15:40:11	Plan 1
2011-02-16 14:18:26	DELETE OD ACCOUNT	EMSGV8G	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-01-17 15:40:27	2011-01-22 15:40:27	Plan 1
2011-02-16 14:18:31	LOGIN	SCC28MS9	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 14:18:31	LOGOUT	SCC28MS9	192.168.1.10	00:1A:92:9F:A4:98	0	8	8	812B	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 14:18:24	LOGIN	SCC28MS9	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 14:18:54	KICK	SCC28MS9	192.168.1.10	00:1A:92:9F:A4:98	0	9	9	872B	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 14:18:54	DELETE OD ACCOUNT	SCC28MS9	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:54	2011-02-21 14:17:54	Plan 0
2011-02-16 17:16:27	LOGIN	8G4SDS8F	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 14:17:48	2011-02-21 14:17:48	Plan 0
2011-02-16 17:16:27	LOGOUT	8G4SDS8F	192.168.1.10	00:1A:92:9F:A4:98	1094	1.187KB	827	98.7KB	2011-02-16 14:17:48	2011-02-21 14:17:48	Plan 0
2011-02-16 17:31:48	ADD OD ACCOUNT	24Q288K	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 17:31:48	2011-02-21 17:31:48	Plan 0
2011-02-16 17:31:56	ADD OD ACCOUNT	MFT8KED5	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 17:31:56	2011-02-21 17:31:56	Plan 0
2011-02-16 17:32:24	DELETE OD ACCOUNT	9GT88ED	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-11 10:10:03	2011-02-16 10:10:03	Plan 2
2011-02-16 17:33:49	DELETE OD ACCOUNT	8MFP8AM	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2011-02-16 14:17:41	2011-02-21 14:17:41	Plan 0
2011-02-16 17:33:52	LOGIN	KKEQHPAY	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 14:17:41	2011-02-21 14:17:41	Plan 0
2011-02-16 18:00:32	TIME OUT OF RANGE	KKEQHPAY	192.168.1.10	00:1A:92:9F:A4:98	1269	1.051KB	861	147.7KB	2011-02-16 14:17:41	2011-02-21 14:17:41	Plan 0
2011-02-16 18:04:06	LOGIN	2W8K7BE	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 12:32:17	2011-02-20 12:32:17	Plan 4
2011-02-16 18:02:57	IDLE TIMEOUT	2W8K7BE	192.168.1.10	00:1A:92:9F:A4:98	27	9.1KB	40	9.4KB	2011-02-16 12:32:17	2011-02-20 12:32:17	Plan 4
2011-02-16 18:04:06	LOGIN	2W8K7BE	192.168.1.10	00:1A:92:9F:A4:98	0	0	0	0	2011-02-16 12:32:17	2011-02-20 12:32:17	Plan 4
2011-02-16 19:08:00	USE UP	2W8K7BE	192.168.1.10	00:1A:92:9F:A4:98	1098	767.4KB	978	204.9KB	2011-02-16 12:32:17	2011-02-20 12:32:17	Plan 4

➔ **Date** : Indicate that current event's date and time

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

- ✓ **LOGIN** : Indicate that the user login system.
- ✓ **LOGOUT** : Indicate that the user logout system.
- ✓ **IDLE TIMEOUT** : Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
- ✓ **USE UP** : Indicate that the user's service time is done.
- ✓ **VOLUME USE UP** : Indicate that the user's bandwidth is done.
- ✓ **KICK** : Indicate that the system kick out the user.
- ✓ **TIME OUT OF RANGE** : Indicate that the service time of Service Domain is not on schedule.
- ✓ **ADD OD ACCOUNT** : Indicate that the system add On-Demand user account.
- ✓ **DELETE OD ACCOUNT** : Indicate that the system delete On-Demand user account.

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

➔ **IP** : Indicate that the user's IP address

➔ **MAC** : Indicate that the user's MAC address

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

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

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

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

➔ **Start Time** : Indicate that the start time of current service users

➔ **End Time** : Indicate that the end time of current service users

→ **Plan** : Indicate that the current user's billing plan.

- **Session Log** : The system can record connection details of each user accessing the Internet and sent out to a specified Syslog Server or E-Mail based on defined interval time. As shown in the following figure, each line is traffic history record consisting of 10 fields, **Date, Time, Session Type, Username, Service Domain, Source IP, Source Port, Destination IP, Destination Port, MAC.**

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

- **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.**

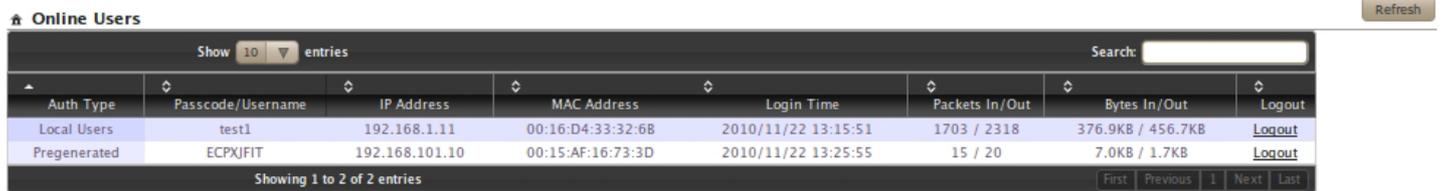
```
2011/02/15 12:16:17 http://192.168.2.64 offline
2011/02/15 12:16:29 http://192.168.2.68 offline
```

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

```
2011/02/15 13:49:47 WAP-954GP (64) 192.168.1.64 0011A31B3ED9 offline
```

4.3.5 Monitor Online Users

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



Online Users Refresh

Show 10 entries Search:

Auth Type	Passcode/Username	IP Address	MAC Address	Login Time	Packets In/Out	Bytes In/Out	Logout
Local Users	test1	192.168.1.11	00:16:D4:33:32:68	2010/11/22 13:15:51	1703 / 2318	376.9KB / 456.7KB	Logout
Pregenerated	ECPXJFIT	192.168.101.10	00:15:AF:16:73:3D	2010/11/22 13:25:55	15 / 20	7.0KB / 1.7KB	Logout

Showing 1 to 2 of 2 entries First Previous 1 Next Last

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

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

4.3.6 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 Passcode/Username, IP Address, MAC Address, Packets In/Out and Bytes In/Out. Please click on **Service Domain -> Log Info**, the page of **Log Info** will appear.

🏠 Log

Traffic Log

Date

2011/02/15

On-Demand Log

Date

2011/02/15



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

■ Traffic Log :

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

🏠 Traffic Log

Show 25 entries Search:

Date	Auth Type	Status	Passcode/Username	IP Address	MAC Address	Packets In/Out	Bytes In/Out
2011/02/16 17:16:27	On Demand	LOGIN	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:29:14	On-Demand	LOGOUT	BG4SD5HJ	192.168.1.10	00:1A:92:9F:A4:9B	1094 / 827	1.157MB / 95.7KB
2011/02/16 17:29:18	Pregenerated	LOGIN	GB0R0RDL	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:30:14	Pregenerated	TIME OUT OF RANGE	GB0R0RDL	192.168.1.10	00:1A:92:9F:A4:9B	395 / 344	283.2KB / 57.0KB
2011/02/16 17:47:37	Local Users	LOGIN	test1	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 17:50:28	Local Users	LOGOUT	test1	192.168.1.10	00:1A:92:9F:A4:9B	467 / 395	348.9KB / 63.3KB
2011/02/16 17:50:52	On Demand	LOGIN	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:00:32	On-Demand	TIME OUT OF RANGE	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	1265 / 861	1.051MB / 147.7KB
2011/02/16 18:22:00	Guest	LOGIN		192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:32:48	Guest	USE UP		192.168.1.10	00:1A:92:9F:A4:9B	1183 / 1088	702.8KB / 273.5KB
2011/02/16 18:34:06	On-Demand	LOGIN	2WBHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 18:52:57	On-Demand	IDLE TIMEOUT	2WBHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	27 / 40	9.1KB / 9.4KB
2011/02/16 18:54:06	On-Demand	LOGIN	2WBHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B
2011/02/16 19:05:03	On-Demand	USE UP	2WBHX7BE	192.168.1.10	00:1A:92:9F:A4:9B	1095 / 978	767.4KB / 204.9KB
2011/02/16 19:07:28	Pregenerated	LOGIN	UJTD79C4	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B

Showing 1 to 15 of 15 entries First Previous 1 Next Last

- ➔ **Date** : Indicate that current event's date and time
- ➔ **Auth Type** : There will shows 6 types of authentication : **Pregenerated**, **On-Demand**, **Local Users**(Local Radius Users), **Remote Radius**, **LDAP** and **Guest**.

- **Status** : There will show **10** types of status as below :
 - ✓ **LOGIN** : Indicate that the user login system.
 - ✓ **LOGOUT** : Indicate that the user logout system.
 - ✓ **IDLE TIMEOUT** : Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
 - ✓ **USE UP** : Indicate that the user's service time is done.
 - ✓ **SESSION TIMEOUT** : Indicate that the user session timeout for **Remote Radius**.
 - ✓ **VOLUME USE UP** : Indicate that the user's bandwidth is done.
 - ✓ **KICK** : Indicate that the system kick out the user.
 - ✓ **TIME OUT OF RANGE** : Indicate that the service time of Service Domain is not on schedule.
- **Passcode/Username** : Indicate that the user's passcode or username.
- **IP** : Indicate that the user's IP address
- **MAC** : Indicate that the user's MAC address
- **Packets In** : Indicate that the current user's packets in.
- **Bytes In** : Indicate that the current user's bytes in.
- **Packet Out** : Indicate that the current user's packets out.
- **Bytes Out** : Indicate that the current user's bytes out.

■ On-Demand Log :

As shown in the following figure, each line is traffic history record consisting of 12 fields : **Date**, **Status**, **Passcode/Username**, **IP**, **MAC**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out**, **Start Time**, **End Time** and **Plan**

- **Date** : Indicate that current event's date and time
- **Status** : There will show **10** types of status as below :
 - ✓ **LOGIN** : Indicate that the user login system.
 - ✓ **LOGOUT** : Indicate that the user logout system.
 - ✓ **IDLE TIMEOUT** : Indicate that the user idle time is over timeout setting of **Service Domain**, the system will logout user automatically
 - ✓ **USE UP** : Indicate that the user's service time is done.
 - ✓ **VOLUME USE UP** : Indicate that the user's bandwidth is done.
 - ✓ **KICK** : Indicate that the system kick out the user.
 - ✓ **TIME OUT OF RANGE** : Indicate that the service time of Service Domain is not on schedule.
 - ✓ **ADD OD ACCOUNT** : Indicate that the system add On-Demand user account.

- ✓ **DELETE OD ACCOUNT** : Indicate that the system delete On-Demand user account.

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
2011/02/16 17:16:27	LOGIN	8G45D5HJ	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B	2011/02/16 14:17:48	2011/02/21 14:17:48	0
2011/02/16 17:29:14	LOGOUT	8G45D5HJ	192.168.1.10	00:1A:92:9F:A4:9B	1094 / 827	1.157MB / 95.7KB	2011/02/16 14:17:48	2011/02/21 14:17:48	0
2011/02/16 17:31:45	ADD OD ACCOUNT	34Q238KX	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2011/02/16 17:31:45	2011/02/21 17:31:45	0
2011/02/16 17:31:56	ADD OD ACCOUNT	M8TG8KD5	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2011/02/16 17:31:56	2011/02/21 17:31:56	3
2011/02/16 17:32:24	DELETE OD ACCOUNT	9GT9E8DE	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2011/02/11 10:18:03	2011/02/16 10:18:03	2
2011/02/16 17:33:49	DELETE OD ACCOUNT	9NMF8AGW	0.0.0.0	00:00:00:00:00:00	0 / 0	0B / 0B	2011/02/11 10:18:36	2011/02/16 10:18:36	2
2011/02/16 17:50:52	LOGIN	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B	2011/02/16 14:17:41	2011/02/21 14:17:41	0
2011/02/16 18:00:32	TIME OUT OF RANGE	XKEQHPAY	192.168.1.10	00:1A:92:9F:A4:9B	1265 / 861	1.051MB / 147.7KB	2011/02/16 14:17:41	2011/02/21 14:17:41	0
2011/02/16 18:34:06	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B	2011/02/15 12:32:17	2011/02/20 12:32:17	4
2011/02/16 18:52:57	IDLE TIMEOUT	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	27 / 40	9.1KB / 9.4KB	2011/02/15 12:32:17	2011/02/20 12:32:17	4
2011/02/16 18:54:06	LOGIN	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	0 / 0	0B / 0B	2011/02/15 12:32:17	2011/02/20 12:32:17	4
2011/02/16 19:05:03	USE UP	2W8HX7BE	192.168.1.10	00:1A:92:9F:A4:9B	1095 / 978	767.4KB / 204.9KB	2011/02/15 12:32:17	2011/02/20 12:32:17	4

Showing 1 to 12 of 12 entries First Previous 1 Next Last

- ➔ **Passcode/Username** : Indicate that the user's passcode or username.
- ➔ **IP** : Indicate that the user's IP address
- ➔ **MAC** : Indicate that the user's MAC address
- ➔ **Packets In** : Indicate that the current user's packets in.
- ➔ **Bytes In** : Indicate that the current user's bytes in.
- ➔ **Packet Out** : Indicate that the current user's packets out.
- ➔ **Bytes Out** : Indicate that the current user's bytes out.
- ➔ **Start Time** : Indicate that the start time of current service users
- ➔ **End Time** : Indicate that the end time of current service users
- ➔ **Plan** : Indicate that the current user's billing plan.

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

4.4 Control your Managed AP

WMS-308N supports to manage up to **60** 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, AP Profile Management, AP Batch Setup Management, AP Group Setup Management, AP Group Status, 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.

The screenshot displays the 'Device Discovery' page. At the top right, there are 'Refresh' and 'Import' buttons. Below them is a table with the following columns: Import, Source IP, MAC Address, Password, HostName, F/W Version, F/W Date, Mode, LAN Setting (sub-columns: IP Address, Netmask, Gateway), and Edit. The table contains four rows of discovered APs, each with a 'Get Info' button and a 'Save&Reboot AP' button. Below the table, there are two panels: 'LAN Setup' and 'System Message'. The 'LAN Setup' panel includes fields for IP Address (192.168.2.60), IP Netmask (255.255.255.0), IP Gateway (192.168.2.1), and DNS settings. The 'System Message' panel has a table with columns for IP Address, MAC Address, and Message.

- **Import** : Click “**Get Info**” button to get current information of the selected managed AP or Click “**Refresh**” button to get information of the detected managed APs . Select desired managed AP and click “**Import**” 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 **60** 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** : Indicate the current IP address of the respective managed AP.
- **MAC Address** : Indicate the current MAC address of the respective managed AP.
- **Password** : Enter the current password of the respective 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. The correct password must be entered on this field and click “**Get Info**” button to get information of the respective managed AP, or click “**Save&Reboot AP**” button to change password of the respective managed AP.

- **HostName** : Indicate the current hostname of the respective managed AP.
- **F/W Version** : Indicate the current firmware version of the respective managed AP.
- **F/W Date** : Indicate the current firmware date of the respective managed AP.
- **Mode** : Indicate the current operating mode of the respective managed AP.
- **LAN Setting** : Indicate 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**", "**Get Info**", "**Import**" or "**Refresh**" button
 - ➔ **IP Address** : Indicate the current IP address of the respective managed AP.
 - ➔ **MAC Address** : Indicate 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 "**Get Info**" or "**Refresh**" 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 **Refresh** button, the switch will rescan managed AP.



To support switch discovery, the WAP-954GP need use firmware version 2.0.10 or higher; the WAP-854NP need use firmware version 1.0.4 or higher; the CPE-2010G / CPE-2000GN-1 need use firmware version 2.1.2 or higher; the WLO-15814N / WLO-15802N need use firmware version V1.1.4 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 **60** 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** → **AP Profile Management**, the **AP Profile Management** page will appear.

▲ AP Profile Management Refresh

Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
	WAP-854NP	00:1A:50:2F:0C:AB	192.168.2.60 80	*****	2000/01/01 00:04:19	Copy	Download	Restore	Recovery	Delete
	1200-Serial	00:1A:50:04:91:07	192.168.2.62 80	*****	2000/01/01 00:11:04	Copy	Download	Restore	Recovery	Delete
	1200-Serial	00:1A:50:01:C6:97	192.168.2.61 80	*****	2000/01/01 00:11:10	Copy	Download	Restore	Recovery	Delete
	CPE-2010G	00:1A:50:1B:74:9B	192.168.2.65 80	*****	2009/01/01 00:07:46	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:05:08:29	192.168.2.68 80	*****	2009/01/01 00:04:02	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:1B:3E:D9	192.168.2.67 80	*****	2009/01/01 00:04:00	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:07:01:11	192.168.2.66 80	*****	2009/01/01 00:07:22	Copy	Download	Restore	Recovery	Delete
	CPE-2010G	00:1A:50:07:06:C1	192.168.2.63 80	*****	2009/01/01 00:02:07	Copy	Download	Restore	Recovery	Delete

Auto Download Profile Interval: Minutes

■ **Status** : Indicate the current status of the respective managed AP. The following three status :

- **On Line** : Indicate the current managed AP able detected
- **Off Line** : Indicate the current managed AP unable detected.
- **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.



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

■ **Host Name** : Indicate the current system name of the respective managed AP.

■ **AP MAC Address** : Indicate the current MAC address of the respective managed AP.

■ **IP Address/Port** : Indicate the current LAN IP address and port of the respective managed AP.

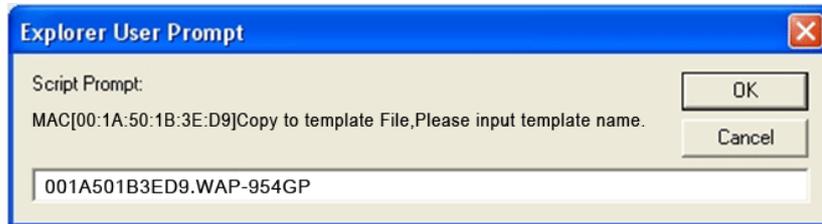


If the managed AP's *IP Address* and *Port* changed after importing profile. Administrator need change IP address and port, then click **Save** button to activated. Otherwise the switch **unable** access managed AP.

■ **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** : Indicate the last update time of the respective managed AP.

- 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 Profile Management > AP Profile Restore

AP Information

MAC Address : 00:1A:50:07:01:11
IP Address : 192.168.2.62

AP Profile List

AP Profile List :

- 001A502F0CAB.bin
- 001A501B3ED9.bin
- 001A50050809.bin
- 001A50070111.bin

Restore Type

Select Type :

- Load From AP Profile
- Load From Template Profile
- Load From Upload file

- ➔ **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.

Template Profile List

Template Profile List :

- 001A501B3ED9-WAP-954GP.bin
- 001A502F0CAB-WAP-854NP.bin

Delete Template File :

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

Upload File From PC

Load Profile From PC:

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

AP Profile Management > AP Profile Auto Recovery

AP Information		Available Recovery AP List				
MAC Address : 00:1A:50:2F:0C:AB IP Address : 192.168.2.60		<input type="button" value="Rescan"/> <input type="button" value="Test"/>				
#	IP	MAC	Password	Status		
1	192.168.2.254	00:1A:50:2F:0C:AB	*****	Available Use		
<input type="button" value="Recovery"/>						

- ➔ **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** : Indicate the current IP address of the respective available managed AP.
 - ✓ **MAC** : Indicate 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** : Display 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.
- **Auto Download Profile 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 on 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.

AP Batch Setup Management

The screenshot displays the 'AP Batch Setup Management' interface. On the left, the 'Available AP Profile List' table shows a list of managed APs with their respective host names, MAC addresses, and IP addresses. The table includes columns for 'Select', 'Host Name', 'AP MAC Address', 'IP Address-Port', and 'Status'. Below the table are 'Apply AP' and 'Reboot AP' buttons. On the right, the 'Batch Setup' section is visible, featuring a 'Select Setup' dropdown menu set to 'LAN Setup'. Below this, the 'LAN Setup' form contains fields for 'IP Address' (192.168.2.60), 'IP Netmask' (255.255.255.0), and 'IP Gateway' (192.168.2.1). There are also radio buttons for 'DNS' configuration: 'No Default DNS Server' (selected) and 'Specify DNS Server IP'. Fields for 'Primary DNS' and 'Secondary DNS' are also present.

- **Available AP Profile List** : All managed AP's profiles will be display on the list.
 - ➔ **Group** : Select a specific group of managed APs for batch configuration.
 - ➔ **Select** : Select desired managed AP for batch configuration.
 - ➔ **Host Name** : Indicate the current system name of the respective managed AP.
 - ➔ **AP MAC Address** : Indicate the current MAC address of the respective managed AP.
 - ➔ **IP Address** : Indicate the current IP address of the respective managed AP.
 - ➔ **Status** : Indicate 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.

System Information

System Name: (Auto Increment)

Description:

Location:

Root Password

New Root Password:

Check Root Password:

Login Methods

HTTP Port:

Enable Telnet: 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.

Setup Time Use NTP

NTP: Enable Disable

NTP Server:

Default NTP Server: (optional)

Time Zone:

Daylight Saving Time:

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

Wireless Basic Setup

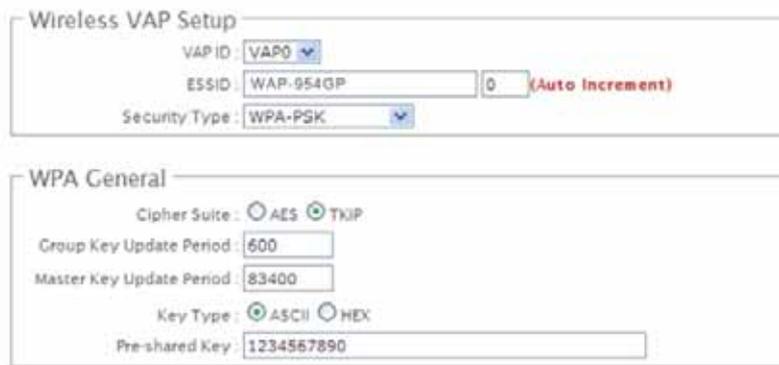
Band Mode:

Country:

Channel: Auto Assign One Channel

Tx Power:

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



The image shows two configuration panels. The top panel, titled "Wireless VAP Setup", contains the following fields: "VAP ID" with a dropdown menu showing "VAP0", "ESSID" with a text box containing "WAP-954GP" and a numeric box containing "0" with the text "(Auto Increment)" to its right, and "Security Type" with a dropdown menu showing "WPA-PSK". The bottom panel, titled "WPA General", contains the following fields: "Cipher Suite" with radio buttons for "AES" and "TKIP" (where "TKIP" is selected), "Group Key Update Period" with a text box containing "600", "Master Key Update Period" with a text box containing "83400", "Key Type" with radio buttons for "ASCII" and "HEX" (where "ASCII" is selected), and "Pre-shared Key" with a text box containing "1234567890".

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



The image shows a configuration panel titled "Firmware Upgrade Via TFTP Server". It contains two text input fields: "TFTP Server IP:" and "File Name:".

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



The image shows a configuration panel titled "Firmware Upgrade Via HTTP URL". It contains one text input field: "URL:".

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.

AP Group Setup Management

Create AP Group Setup

Group Name:

Group Description:

Group Map Background:

Dynamic Channel Allocation

Service: Enable Disable

Maximum Clients Control

Service: Enable Disable

MAC Filter Control

Service: Enable Disable

AP Group List

Group Name	Description	Background	MAC Filter Setup	Map	Edit	Delete
WAP-054GP Group	WAP-054GP Group 1	example-2.jpg	Disable	Map	Edit	Delete
WAP-054NP Group	WAP-054NP Group 1	example.jpg	Disable	Map	Edit	Delete

Upload Map Setup

Upload Map:

File Name	File Size	Preview	Delete
example-2.jpg	272.21 KB	Preview	Delete
example.jpg	98.40 KB	Preview	Delete
Total Use Space	370.61 KB		

- **Create AP Group Setup** : Create group managed APs
 - ➔ **Group Name** : Specify desired name for group.
 - ➔ **Group Description** : Enter appropriate text to denote this group.
 - ➔ **Group Map Background** : Select desired map for group background. The Map must upload from Upload MAP Setup field first.
- **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 switch will automatically assign suitable channel and tx power for group managed APs after the **Auto Download Profile Interval (Please see section 4.3.2)**. **Figure 4-3** depict flow chart for dynamic channel allocation.

Dynamic Channel Allocation

Service: Enable Disable

Country:

Band Mode:

Channel:

Free Channel	Move	Select Channel
2 (2.417 Ghz)		1 (2.412 Ghz)
3 (2.422 Ghz)		6 (2.437 Ghz)
4 (2.427 Ghz)	<input type="button" value=">>"/>	11 (2.462 Ghz)
5 (2.432 Ghz)	<input type="button" value=">"/>	
7 (2.442 Ghz)		
8 (2.447 Ghz)	<input type="button" value="<"/>	
9 (2.452 Ghz)		
10 (2.457 Ghz)	<input type="button" value="<<"/>	

RSSI Threshold:

High Power Level:

Low Power Level:



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

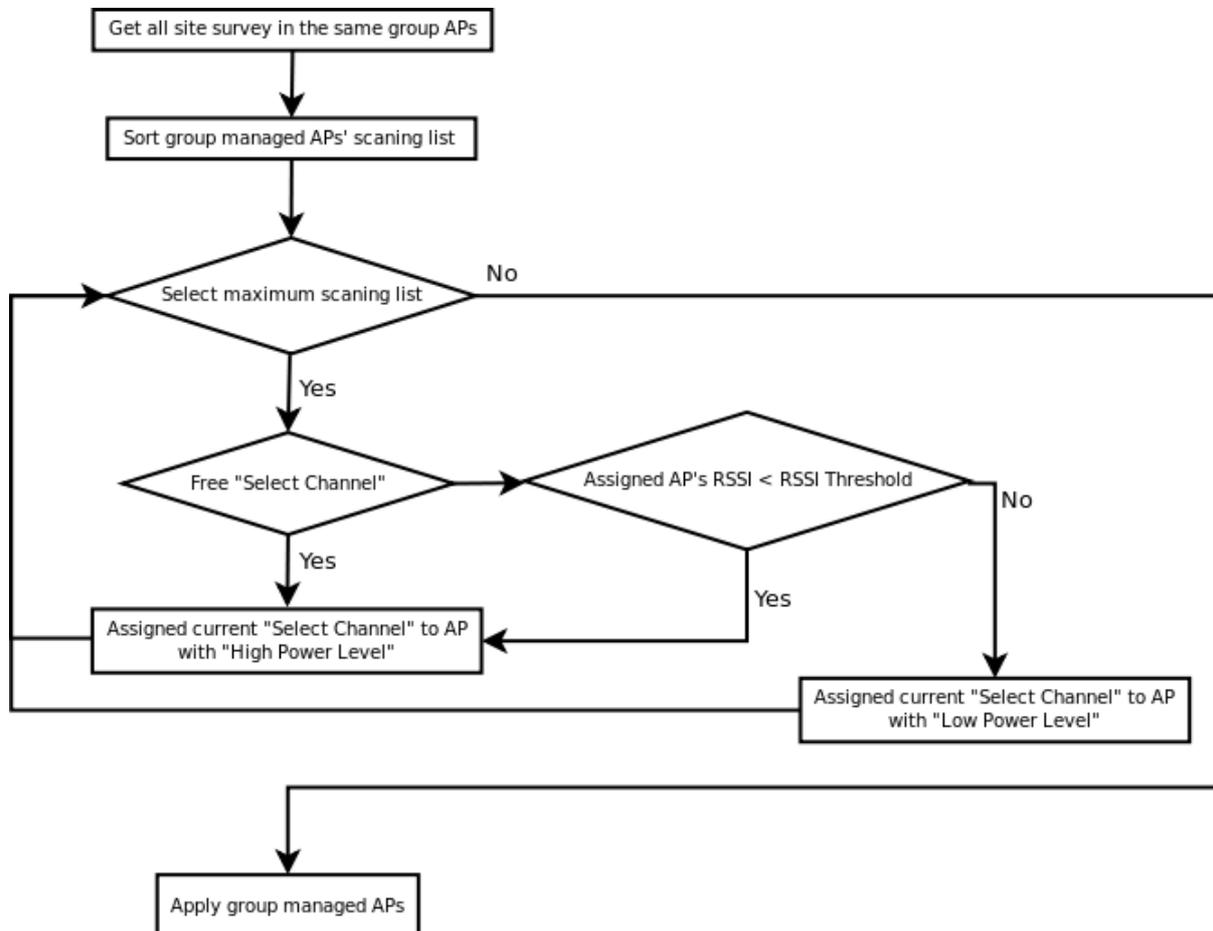


Figure 4-3 Dynamic Channel and Tx Power Allocation Flow Chart

- Maximum Clients Control** : By default, it's **"Disable"**. To **Enable** to activated maximum clients limitation in the same group APs, the switch will automatically assign maximum clients limitation for group managed APs after the **Auto Download Profile Interval** (Please see **section 4.3.2**)

Maximum Clients Control

Service : Enable Disable

RX Threshold : KBps

TX Threshold : KBps

Group MAX Service Clients :

→ **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 each managed AP in the same group.
- **MAC Filter Control** : By default, it's "**Disable**". To **Enable** to activate MAC filter control in the same group APs, the switch will automatically assign block MAC address of the wireless clients for group managed APs after the **Auto Download Profile Interval** (Please see **section 4.3.2**)
- **AP Group List** : Display created group in the list.
 - **Group Name** : Display name of the respective group.
 - **Description** : Display description of the respective group.
 - **Background** : Indicate an used photo of the respective group.
 - **MAC Filter** : Indicate an used MAC filter of the respective group. Click link to configure MAC Filter of the respective group, the the respective Group MAC Filter Setup page will appear. The each group managed APs use the same MAC filter setting.

▲ AP Group Setup Management > Group1 MAC Filter Setup

MAC Rules

Action: Only Deny List MAC Save

MAC Address: Add

MAC Filter List

#	MAC Address	Delete	#	MAC Address	Delete
1	00:1A:50:00:11:aa	Delete			

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

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

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

- ✓ **MAC Address** : Enter MAC address in this field. There are maximum **20** clients 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**" buttons.

→ **Map** : Click **Map** to configure location setting, the respective Group Location Setup page will appear, and the administrator specify flag mark as location on the Map from the Device List.



The MAP function ONLY supports monitor with width resolution for **1280** or **above**

AP Group Setup Management > Group[WAP-954GP Group] Location Setup

The screenshot displays the 'AP Group Setup Management' interface for the 'Group[WAP-954GP Group] Location Setup'. On the left, a 'Device List' table shows two columns of device types: '1200-Serial' and 'CPE-2010G'. The main area contains four floor plan maps. The top-left map is labeled 'WAP-954GP-Site0', the top-right 'WAP-954GP-Site1', the bottom-left 'WAP-954GP-Site2', and the bottom-right 'WAP-854NP'. Each map shows a grid of rooms and corridors with various icons representing network equipment and user locations.

Double click flag on MAP, 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 AP

The screenshot shows the 'WAP-954GP-Management Setup' dialog box. It is divided into two sections: 'System Information' and 'Login Methos'. In the 'System Information' section, the 'System Name' is set to 'WAP-954GP', the 'Description' is 'InWall, WiFi,G , 500mW', and the 'Location' field is empty. In the 'Login Methos' section, the 'HTTP Port' is set to '80', and the 'Enable Telnet' checkbox is checked with the 'Port' set to '23'. At the bottom right, there are 'Cancel' and 'Save & Reboot' buttons.

- **Edit** : Click **Edit** to configure settings of the respective group in the list.
- **Delete** : Click **Delete** to remove the respective group in the list.

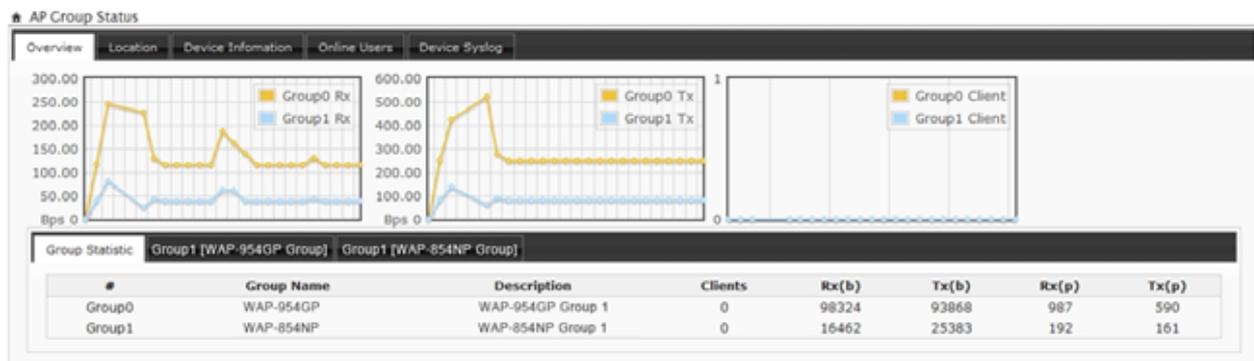
- **Upload Map Setup** : Select desired Map to upload. Click **Preview** to view the respective Map, click **Delete** to remove the respective Map. The system supports JPG, JPEG, PNG and GIF format.



1. If you enable “**Dynamic Channel Allocation**”, “**Maximum Clients Control**” or “**MAC Filter Control**” service, you also need manually enable managed AP's settings to activated these services(on **Wireless Advanced** Page).
2. When these services enabled, the switch will automatically control channel, txpower, maximum clients and MAC filter during every “**Auto Download Profile Interval**” (Please see **section 4.3.2**).

4.4.5 AP Group Status

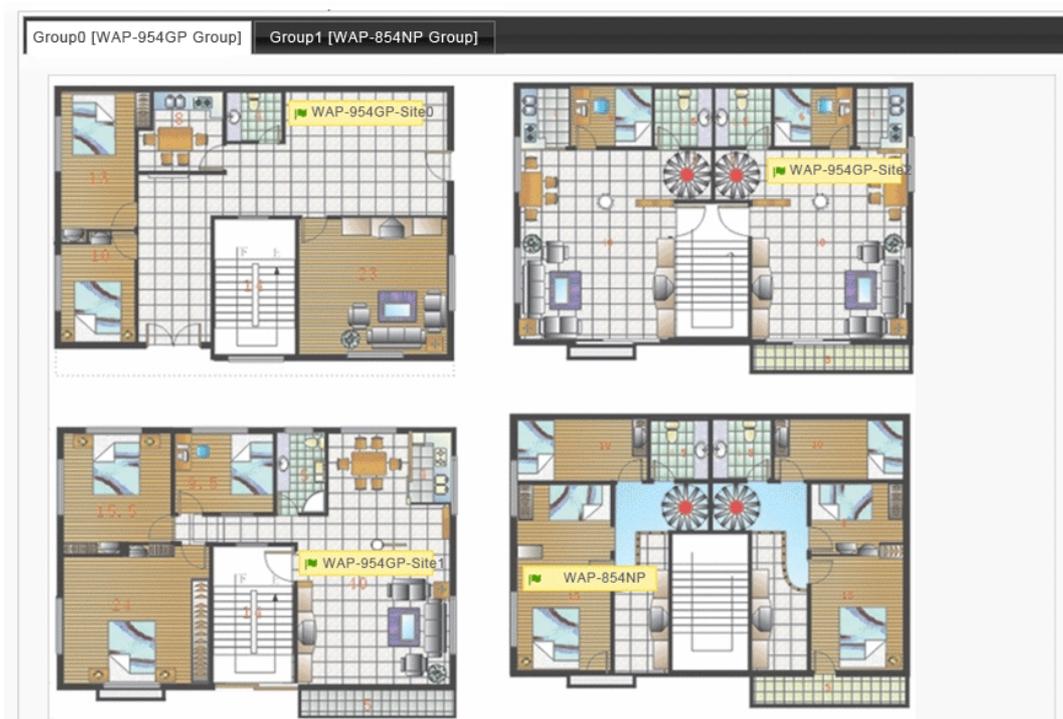
This section provide detailed information of group on **Overview**, **Location**, **Device Information**, **Online Users** and **Device Syslog** can be reviewed via this page.



- Overview** : Show graphs which continuously represent the current data traffic and on-line clients on the respective group.

IP Address	Firmware Version	Clients	Rx(b)	Tx(b)	Rx(p)	Tx(p)
192.168.2.62	Cen-AP-G2H5 V2.0.6 Release Version	0	16686	30878	201	190
192.168.2.63	Cen-AP-G2H5 V2.0.6 Release Version	0	68444	39593	630	255
192.168.2.61	Cen-AP-G2H5 V2.0.6 Release Version	0	16686	30876	201	190

- Location** : Show current managed AP's location on the respective group. The green flag mark indicate the AP can be accessed and double click to view the respective **"System Information"**, the question mark indicate the AP can not be accessed.



- **Device Information** : Display the device information of the respective group.



- **Online Users** : Display all associated clients status of the respective group.

IP Address	VAP	ESSID	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ
192.168.2.61	VAP0	WAP-954GP-0	00:1A:50:16:73:3d	52	36M/36M	2/247

- **Devices Syslog** : Display all system events of the respective group.

Time	Facility	Severity	Message
2009-01-01 00:04:59	System	Info	Authentication successful for root from 192.168.2.50
2009-01-01 05:09:54	Wireless	Info	ath0: STA 00:1A:50:16:73:3d IEEE 802.11: associated
2009-01-01 05:09:54	Wireless	Info	ath0: STA 00:1A:50:16:73:3d RADIUS: starting accounting session 495C0783-00000000
2009-01-01 05:09:54	Wireless	Info	ath0: STA 00:1A:50:16:73:3d WPA: pairwise key handshake completed (WPA)
2009-01-01 05:09:55	Wireless	Info	ath0: STA 00:1A:50:16:73:3d WPA: group key handshake completed (WPA)
2009-01-01 05:10:04	Wireless	Info	ath0: STA 00:1A:50:16:73:3d WPA: group key handshake completed (WPA)
2009-01-01 05:10:04	Wireless	Info	ath0: STA 00:1A:50:16:73:3d WPA: received EAPOL-Key 2/2 Group with unexpected replay counter

4.4.6 Third Party AP 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.

Website Monitor

Website URL

Website URL:

Website Monitor List

#	Status	Website URL	Delete
1		http://192.168.2.151	Delete
2		http://192.168.2.161	Delete
3		https://192.168.2.103	Delete

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

Time Policy Setup

Policy 1

Policy: Policy 1

Schedule Rule: On Schedule Out of Schedule

Save Action

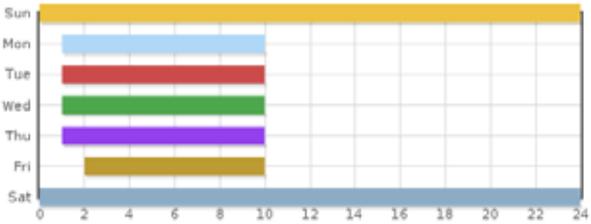
Time Schedule

Day of Week: Sun Mon Tue Wed Thu Fri Sat

Start From: 00 : 00

End To: 23 : 59

Save Clear

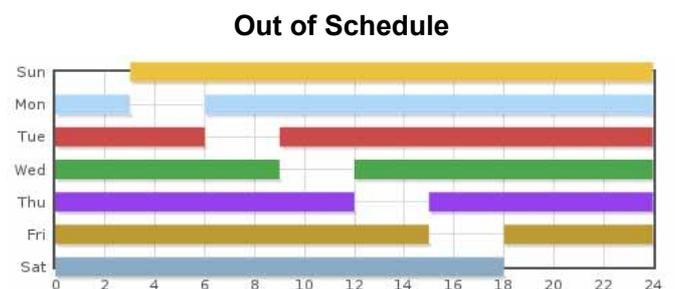
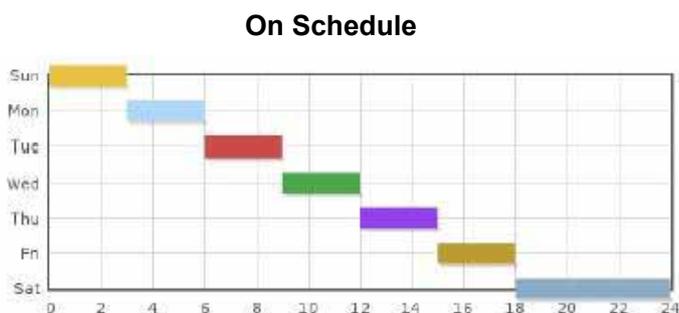


Time Schedule List

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

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

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



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.

IP Filter Setup

IP Rules

Source Address/Mask:

Source Port:

Destination Address/Mask:

Destination Port:

In/Out: In Out

Protocol: TCP UDP ICMP

Listen: Yes No

Action: Deny Pass

Interface:

Time Policy:

IP Filter List

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

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

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

4.5.3 MAC Filter

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

MAC Filter Setup

MAC Rules

Action: Disabled Save

MAC Address: Add

Time Policy: Always Run

MAC Filter List

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

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

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

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

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

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

4.5.4 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.

Virtual Server Setup

Virtual Server

Virtual Server: Enable Disable

Description:

Private IP:

Protocol Type: TCP UDP

Private Port:

WAN Interface: WAN1 WAN2

Public Port:

Time Policy:

Virtual Server List

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

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



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

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

4.5.5 DMZ

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

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

DMZ Setup

WAN1 DMZ	WAN2 DMZ
Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable	Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address: <input type="text"/>	IP Address: <input type="text"/>
Time Policy: <input type="text" value="Always Run"/>	Time Policy: <input type="text" value="Always Run"/>

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

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

4.5.6 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.

IP Routing Setup

OSPF Settings

OSPF Service: Enable Disable

RouterID: 192.168.1.254 (LAN)

Distribute RIP over OSPF:

Routing Rules

Service: Enable Disable

Destination Net/Mask:

Via: Gateway Interface

Gateway:

Protocol: OSPF RIP

OSPF Area:

RIP Settings

RIP Service: Enable Disable

Side(Devices):

- WAN1
- WAN2
- LAN
- VLAN1
- VLAN2
- VLAN3
- VLAN4
- VLAN5
- VLAN6
- VLAN7

Distribute OSPF over RIP:

Routing Rules List

#	Service	Destination Net/Mask	Via	OSPF	RIP	Delete	Edit
1	On	192.168.9.0/24	192.168.9.1	On (0)	Off	Delete	Edit
2	On	192.168.8.0/24	192.168.8.1	Off (0)	On	Delete	Edit
3	On	192.168.76.0/24	192.168.76.254	On (1)	On	Delete	Edit

■ OSPF Settings :

- **OSPF 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.
- **Distribute RIP over OSPF** : Allow RIP routes will redistributed into OSPF.

■ RIP Settings :

- **RIP 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 :

- **Mode** : 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
- ✓ **OSPF Area** : Default is **0**, the range is from **0** to **4294967295**.

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.

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.

The screenshot displays the 'Status' page of the WMS-308N Network Access Gateway / Controller. The page is organized into several panels:

- System Info:** Host Name: WMS-308N, Location, Description: Network Access Control Gateway, Firmware Version: Cen-AC V0.0.3, Firmware Date: 2011/03/24 12:30:58, Device Time: 2011/03/28 03:55:59, System Up Time: 04:03, Primary DNS, Secondary DNS.
- Port Link Info:** A diagram showing WAN1 and WAN2 ports (red) and LAN1, LAN2, LAN3, and LAN4 ports (LAN1 is green, others are red).
- WAN1 Monitor:** A line graph showing bandwidth usage (Bps) over time. Below the graph, it displays Mode: Dynamic IP Mode, Status: Renew/Release, MAC Address: 00:1A:50:00:74:94, IP Address, Netmask, and Gateway.
- LAN Monitor:** A line graph showing bandwidth usage (Bps) over time. Below the graph, it displays MAC Address: 00:1A:50:00:74:93, IP Address: 192.168.2.254, Netmask: 255.255.255.0, RX(Bytes): 123682, and TX(Bytes): 796909.
- Ticket Count:** A table showing authentication types and their ticket counts.

Auth Type	Tickets
Pregenerated	0
On-Demand	0
Payment Gateway	0
Thermal Printer	0
Local Radius	0
Total	0/15841
- Online Users:** A table showing domains and their authentication and guest counts.

Domain	Auth	Guest
Domain 0	0	0
Domain 1	0	0
Domain 2	0	0
Domain 3	0	0
Domain 4	0	0
Domain 5	0	0
Domain 6	0	0
Domain 7	0	0
Total	0	0

- **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.

Extra Information Refresh

Extra Information
Information: Netstat Information

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

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

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.

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.

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.

System Log

Result			
Time	Facility	Severity	Message
2011-01-05 20:28:52	System	Info	dnsmasq: started, version 2.22 cachesize 150
2011-01-05 20:28:52	System	Info	dnsmasq: cleared cache
2011-01-05 20:28:52	System	Info	dnsmasq: reading /etc/resolv.conf
2011-01-05 20:29:00	System	Info	Authentication successful for root from 192.168.1.44
2011-01-05 20:29:08	System	Info	dnsmasq: reading /etc/resolv.conf
2011-01-05 20:29:08	System	Info	dnsmasq: using nameserver 192.168.2.254#53

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

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

Appendix A. Web GUI valid Characters

Table A Web GUI Valid Characters

Block	Field	Valid Characters
LAN/VLAN 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
	Hostname	Length : Up to 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . =
	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
	802.1P Priority	0~7
	MSTI	0~15
	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	
Switch QoS	DSCP	0~63
	Weight	1~128
	DSCP Remark	0~63
	802.1p Remark	0~7
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

Password	0-9, A-Z, a-z
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
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
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	32 characters
	Private IP	A.B.C.D IP Format
	Private/Public Port	1 ~ 65535
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
	Guest Count Limit	1~100; default is 5
	Guest Time	1~720; default is 10
Pregenerated Tickets	File ID	1 ~ 32767
	Price	1-7 digit number : xxxxx.xx
	Currency	1~3 letters characters
	Quantity of Tickets	1 ~ 3069
	Passcode Length	8 ~ 31, default is 8
	Description	Up to 32 characters Space
	Time Quota	1 ~ 366x24x60 , default is 60
	Volume Quota	Default 10; Max is 102400
	Effective Start/ End Time	Date / Time Format : MM/DD/YYYY HH:MM Start Time < End Time
Billing Plan	Plan Name	Up to 32 characters
	Price	1-7 digit number : xxxxx.xx
	Currency	1~3 letters characters
	Passcode Length	8 ~ 31, default is 8
	Wireless ESSID	Up to 100 characters Space
	Wireless Key	Up to 100 characters Space
	Description	Up to 100 characters Space
	Time Quota	1 ~ 366x24x60 , default is 60
	Volume Quota	Default 10; Max is 102400

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
Thermal Printer	IP Address	A.B.C.D IP Format
	Command Port	1 ~ 65535, default is 5000
	New Lock Password	4-8 digit number
	Confirm Lock Password	4-8 digit number
	Balance Date	Time format : HH:MM
	Description	Up to 32 characters Space
Local Radius	Username	Length : 4-16 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` . =
	Password	Length : 4-16 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` . =
	MAC Address	MAC Format; 12 HEX characters
	Description	Up to 32 characters Space
Remote Radius	Primary/Secondary Server IP	A.B.C.D IP Format
	Authentication/Account Port	1 ~ 65535
	Secret Key	1-64 characters
LDAP	Server IP	A.B.C.D IP Format
	Port	1 ~ 65535
	Identity	Length : 1-16 0-9, A-Z, a-z @-_.
	Password	1-16 characters
	Base DN	1-64 characters
	Account Attribute	1-64 characters
Walled Garden	Walled Name	4-32 characters Space
	IP Address/ Domain	A.B.C.D IP Format or Domain
	Homepage	URL Format
	Description	32 characters Space

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
	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	Operator Privilege	
System	WAN		None	None	
	WAN Traffic		None	None	
	LAN/VLAN		Read & Write	None	
	Switch QoS Setup		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
Time Server		None	None		
SNMP		None	None		
Service Domain	Service Domain		Read & Write	None	
	Authentication – Management		Read & Write	None	
	Authentication – Pregenerated		Read & Write	None	
	Authentication – OnDemand	Billing Plan Setup		Read & Write	None
		Create Accounts		Read & Write	Read & Write
		Payment Gateway		Read & Write	Read & Write
		Thermal Printer Setup		Read & Write	Read & Write
		Billing Plan Report		Read & Write	Read & Write
	Authentication – Local Radius		Read & Write	None	
	Authentication – Remote Radius		Read & Write	None	
	Authentication – LDAP		Read & Write	None	
	Walled Garden		Read & Write	None	
	Notification		Read & Write	None	
Online Users		Read & Write	Read & Write		
Log Info		Read & Write	Read & Write		
AP Management	Device Discovery		Read & Write	None	
	AP Profile Management		Read & Write	None	
	AP Batch Setup Management		Read & Write	None	
	AP Group Setup Management		Read & Write	None	
	AP Group Status		Read & Write	Read & Write	
	Website Monitor		Read & Write	None	
Advance	DMZ		Read & Write	None	
	IP Filter		Read & Write	None	
	MAC Filter		Read & Write	None	
	Virtual Server		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

PayPal

Create your PayPal account Secure

Your country or region
Taiwan

Your language
English

Already have a PayPal account? [Upgrade now.](#)

<h3>Personal</h3> <p>For individuals who shop online</p> <p>Get Started</p>	<h3>Premier</h3> <p>For individuals who buy and sell online</p> <p>Get Started</p>	<h3>Business</h3> <p>For merchants who use a company or group name</p> <p>Get Started</p>
---	--	---

Learn about [low PayPal fees.](#)

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



Choose Account Type → Enter Information → Confirm → Done

Account Sign Up Business Account

[Secure Transaction](#)

Business Name:

Category:

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

Address Line 2:
(optional)

City:

State / Province / Region:

Postal Code:

Country Of Registration: Taiwan

Date of Registration: / /

Business Type:

Primary Currency:

Customer Service Email:

Customer Service Phone: (+886) ext.

Business URL:
(optional)

Your Business Information

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

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

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

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

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

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

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



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

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

Profile Summary

Merchant Name: Justin Shen
Secure Merchant Account ID: SK6K6AHMBTV7Y

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

Account Information

[Email](#)
[Street Address](#)
[Phone](#)
[Password](#)
[Notifications](#)
[Language Preference](#)
[Time Zone](#)
[Manage User](#)
[API Access](#)
[Business Information](#)
[Additional Owners](#)
[Close Account](#)
[Identification Preference](#)
[Merchant Fees](#)

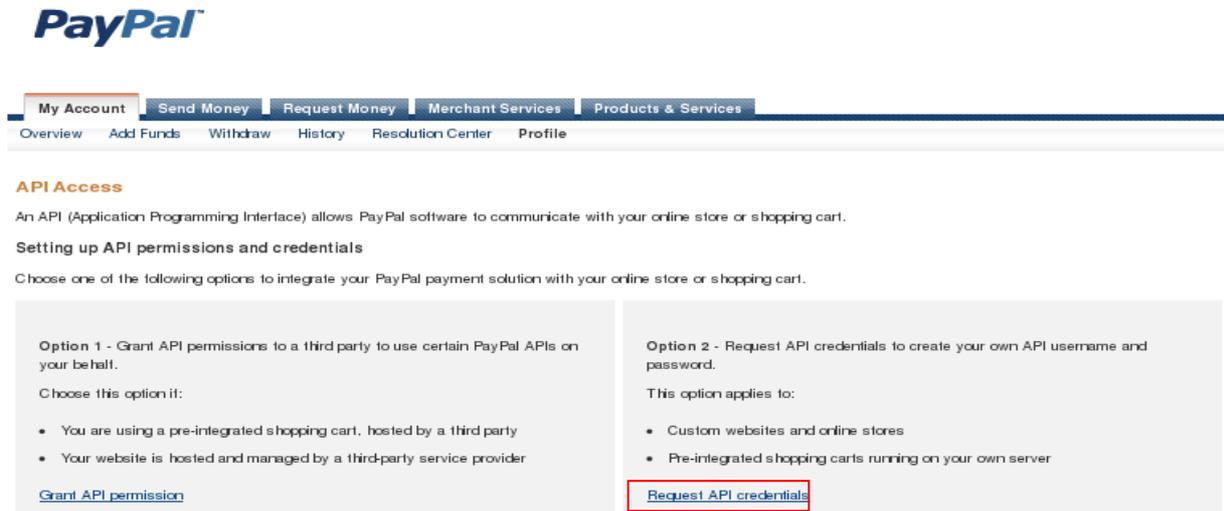
Financial Information

[Credit/Debit Cards](#)
[Bank Accounts](#)
[Currency Balances](#)
[Gifts and Discounts](#)
[Monthly Account Statements](#)
[Recurring payments dashboard](#)
[My preapproved payments](#)

Selling Preferences

[Auctions](#)
[Regional Tax](#)
[Shipping Calculations](#)
[My Saved Buttons](#)
[Payment Receiving Preferences](#)
[Instant Payment Notification Preferences](#)
[Reputation](#)
[Customer Service Message](#)
[Website Payment Preferences](#)
[Encrypted Payment Settings](#)
[Custom Payment Pages](#)
[Invoice Templates](#)
[Language Encoding](#)

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



PayPal

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

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

API Access

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

Setting up API permissions and credentials

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

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

Choose this option if:

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

[Grant API permission](#)

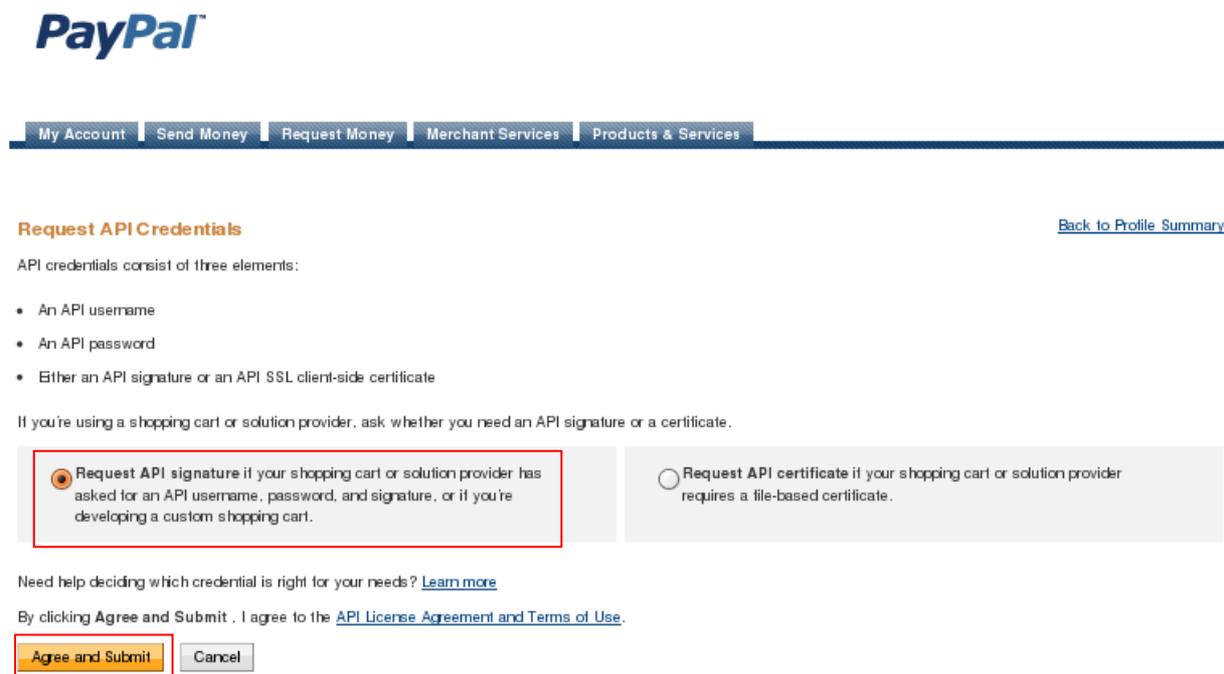
Option 2 - Request API credentials to create your own API username and password.

This option applies to:

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

[Request API credentials](#)

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



PayPal

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

Request API Credentials [Back to Profile Summary](#)

API credentials consist of three elements:

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

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

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

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

Need help deciding which credential is right for your needs? [Learn more](#)

By clicking Agree and Submit, I agree to the [API License Agreement and Terms of Use](#).

[Agree and Submit](#)

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

View or Remove API Signature

[Back to Profile Summary](#)

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

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

Credential	API Signature
API Username	justin_api1.phenet.com.tw
API Password	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Signature	AyMwAW0yzbHCvFaSaqblUnuIP-LaATbvgrOPgTWwks0RQ1WyigEQ7Wum
Request Date	Jun 7, 2010 17:55:47 GMT+08:00

Appendix D. Examples of Making Payments for End Users

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

WAS-105R Hotspot Gateway
802.11B/G/N MIMO Hotspot Gateway

Passcode:

[Click here to purchase by PayPal or Credit Card Online.](#)

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

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

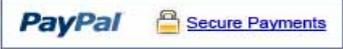
WAS-105R Hotspot Gateway
802.11B/G/N MIMO Hotspot Gateway

Price	Type	Effective Time Range
<input type="radio"/> USD 10.00	Unlimited	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins
<input type="radio"/> USD 5.00	Multiple Times: 60 mins	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins
<input type="radio"/> USD 3	One Time: 60 mins	0 days 0 hrs 0 mins to 5 days 0 hrs 0 mins

WAS-105R Hotspot Gateway
802.11B/G/N MIMO Hotspot Gateway

Connecting to PayPal.....

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

PayPal is the safer, easier way to pay 

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

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

Don't have a **PayPal account**?
No problem, [continue checkout](#)

Cancel and return to [Cenwell Hotspot](#).

Log in to PayPal

Email

Password

Forgot [email address](#) or [password](#)?

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

Review your payment 

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

[Learn more](#) about how PayPal withdraws funds.

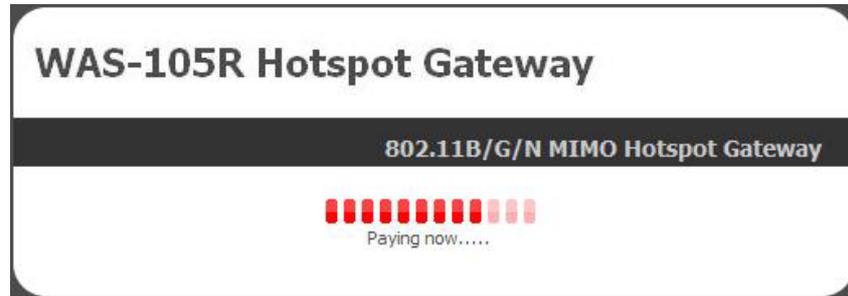
Description	Amount
Item total	NT\$1
Add special instructions to merchant	Item total: NT\$1
	Total: NT\$1 TWD
	Enter gift certificate, reward, or discount

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

Contact Information jundeshen@yahoo.com

Cancel and return to [Cenwell Hotspot](#).

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

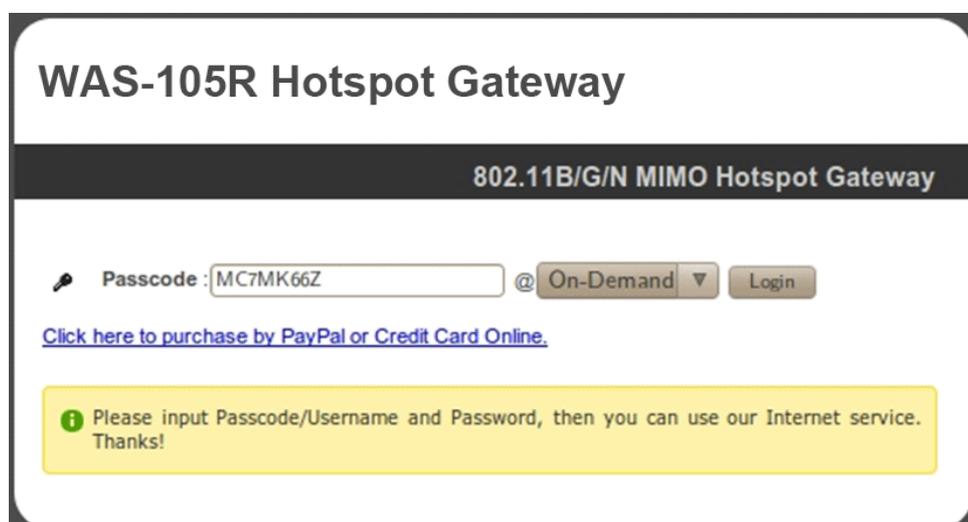


Step 6 : After paying confirm, the system will create **Passcode** for end users login. Click **Login** button to enter Login page. (Write down your “**Login Passcode**” before you click **Login** button)

Create Success

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

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



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**

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

Showing 1 to 1 of 1 entries

Package 2

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

Print Close

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.

PayPal

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

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

History

Balance: NT\$61 TWD

Recent Activity | All activity | Find a transaction

100600001 In Invoice ID

TWD USD ALL

5/18/2010 to 6/17/2010 Search

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



[My Account](#) | [Send Money](#) | [Request Money](#) | [Merchant Services](#) | [Products & Services](#)
[Overview](#) | [Add Funds](#) | [Withdraw](#) | [History](#) | [Resolution Center](#) | [Profile](#)

Transaction Details

OK to complete the transaction

Payment Status: Completed

What should I do now?

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

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

[Tips to sell securely](#)

Seller Protection:

[Not Eligible](#)

We have no shipping address on file.

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

Name: SHEN CHUN TE (The sender of this payment is Non-U.S. - Verified)
 Email: jundeshen@yahoo.com
 Payment Sent to: justin@pheenet.com.tw

Total Amount: NT\$1 TWD
 Fee amount: -NT\$1 TWD
 Net amount: NT\$0 TWD

[Issue a refund ?](#)

You have up to 60 days to refund the payment and get the fees back.

Item amount: NT\$1 TWD
 Sales Tax: NT\$0 TWD
 Shipping: NT\$0 TWD
 Handling: NT\$0 TWD
 Quantity: 1

Order Description: MC7MK66Z
 Invoice ID: 100600001
 Date: Jun 17, 2010
 Time: 21:18:28 GMT+08:00
 Status: Completed

Payment Type: Instant

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

Issue Refund

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

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

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

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

Review and process refund

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

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

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

Issue Refund Edit Cancel

Step 6 : Go **My Account**, and verify **Transaction Details**.My recent activity | [Payments received](#) | [Payments sent](#)[View all of my transactions](#)

My recent activity - Last 7 days (Jun 10, 2010-Jun 17, 2010)									
<input type="button" value="Archive"/>		What's this							Payment status glossary
<input type="checkbox"/>	Date		Type	Name/Email	Payment status	Details	Order status/Actions	Gross	
<input type="checkbox"/>	Jun 17, 2010		Fee Reversal From	Cancelled Fee	Completed	Details		NT\$1 TWD	
<input type="checkbox"/>	Jun 17, 2010		Refund To	SHEN CHUN TE	Completed	Details		-NT\$1 TWD	



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 [55C492669W4196426](#)

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

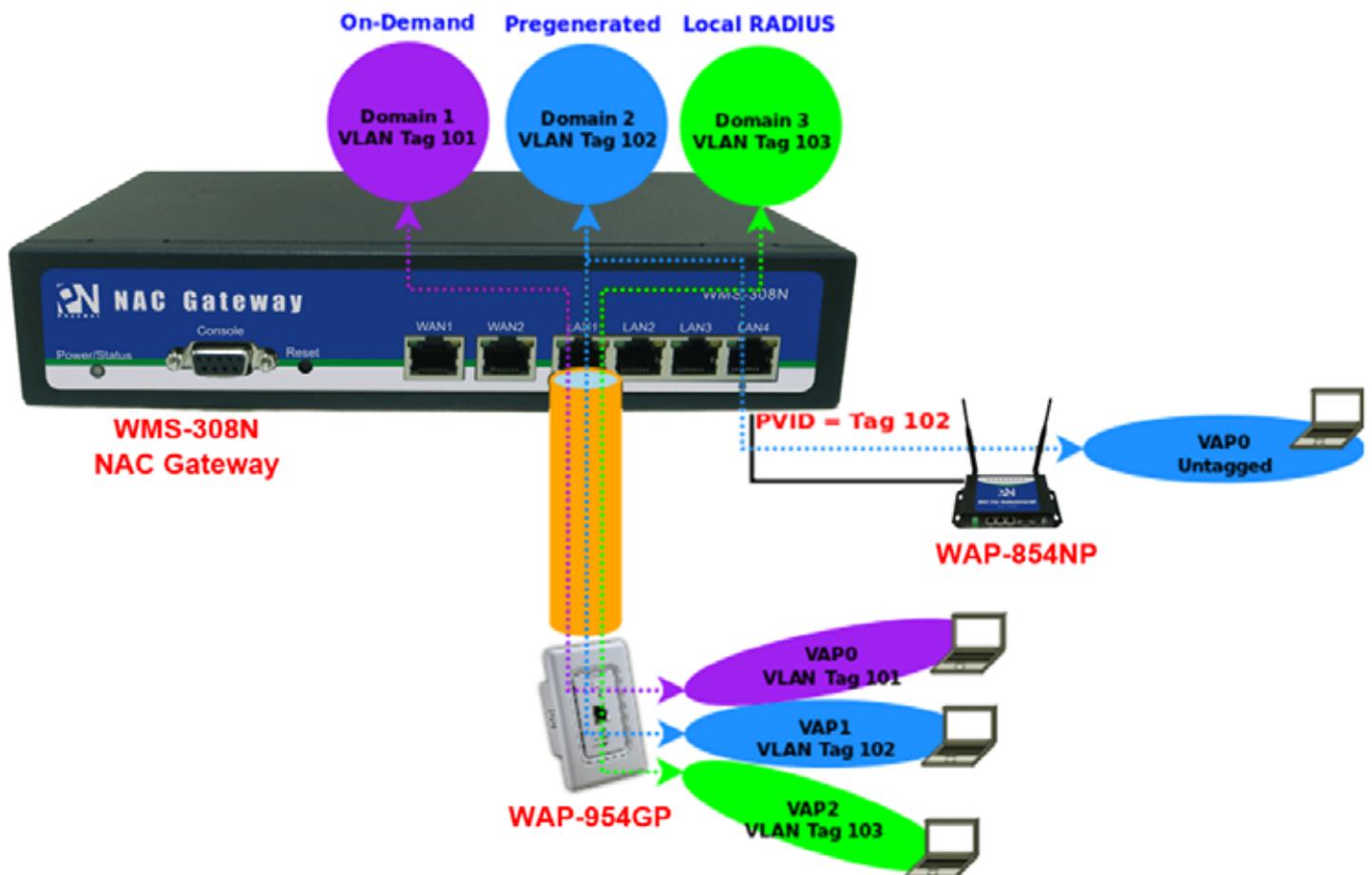
Time: 21:40:42 GMT+08:00

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 Pregenerated 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 Pregenerated 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.

Service Domain Setup

The screenshot shows four configuration panels for Service Domains:

- Domain 0:** LAN Port: LAN; Auth Type: Pregenerated Ticket; WAN Port: Auto; IPPnP Service: off; Guest Service: off; Time Policy: Always Run; Redirect URL: Link; Login Page: Template Page.
- Domain 1:** LAN Port: VLAN1; Auth Type: On-demand; WAN Port: Auto; IPPnP Service: off; Guest Service: off; Time Policy: Always Run; Redirect URL: Link; Login Page: Template Page.
- Domain 2:** LAN Port: VLAN2; Auth Type: Pregenerated Ticket; WAN Port: Auto; IPPnP Service: off; Guest Service: off; Time Policy: Always Run; Redirect URL: Link; Login Page: Template Page.
- Domain 3:** LAN Port: VLAN3; Auth Type: Local Users; WAN Port: Auto; IPPnP Service: off; Guest Service: off; Time Policy: Always Run; Redirect URL: Link; Login Page: Template Page.

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**.

VLAN

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

Port Setup

Port #	VLAN TAG Mode	
	Untagged	Tagged
Port 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Port Setup

Port #	VLAN TAG Mode	
	Untagged	Tagged
Port 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

Port #		PVID	802.1P Priority
Port 1	<input checked="" type="checkbox"/>	LAN	0
Port 2	<input checked="" type="checkbox"/>	LAN	0
Port 3	<input checked="" type="checkbox"/>	LAN	0
Port 4	<input checked="" type="checkbox"/>	VLAN2 (102)	0

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 :

- Three WAP-954GP managed APs :
 - WAP-954GP-A – 00:1A:50:05:08:29
 - WAP-954GP-B – 00:1A:50:1B:3E:D9
 - WAP-954GP-C – 00:1A:50:07:01:11
- Set WAP-954GP-A's profile to template.

Step 1 : Device Discovery

Device Discovery Refresh Import

Import	Source IP	MAC Address	Password	HostName	F/W Version	F/W Date	Mode	LAN Setting			Edit
								IP Address	Netmask	Gateway	
<input type="checkbox"/> Get Info	192.168.2.254	00:11:A3:05:08:29	*****	WAP-954GP	Cen-AP-G2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.254	255.255.255.0	192.168.2.1	Save&Reboot AP
<input type="checkbox"/> Get Info	192.168.2.254	00:11:A3:07:01:11	*****	WAP-954GP	Cen-AP-G2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.254	255.255.255.0	192.168.2.1	Save&Reboot AP
<input type="checkbox"/> Get Info	192.168.2.254	00:11:A3:1B:3E:D9	*****	WAP-954GP	Cen-AP-G2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.254	255.255.255.0	192.168.2.1	Save&Reboot AP

Step 2 : Change IP address of the respective managed AP

Device Discovery Refresh Import

Import	Source IP	MAC Address	Password	HostName	F/W Version	F/W Date	Mode	LAN Setting			Edit												
								IP Address	Netmask	Gateway													
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>LAN Setup</p> <p>IP Address: <input type="text" value="192.168.2.60"/> (Auto Increment)</p> <p>IP Netmask: <input type="text" value="255.255.255.0"/></p> <p>IP Gateway: <input type="text" value="192.168.2.1"/></p> <p>DNS: <input checked="" type="radio"/> No Default DNS Server <input type="radio"/> Specify DNS Server IP</p> <p>Primary DNS: <input type="text"/></p> <p>Secondary DNS: <input type="text"/></p> <p style="text-align: center;">Save&Reboot AP</p> </div> <div style="width: 45%;"> <p>System Message</p> <table border="1"> <thead> <tr> <th>IP Address</th> <th>MAC Address</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>192.168.2.254</td> <td>00:1A:50:05:08:29</td> <td>Change IP: 192.168.2.60</td> </tr> <tr> <td>192.168.2.254</td> <td>00:1A:50:07:01:11</td> <td>Change IP: 192.168.2.61</td> </tr> <tr> <td>192.168.2.254</td> <td>00:1A:50:1B:3E:D9</td> <td>Change IP: 192.168.2.62</td> </tr> </tbody> </table> </div> </div>												IP Address	MAC Address	Message	192.168.2.254	00:1A:50:05:08:29	Change IP: 192.168.2.60	192.168.2.254	00:1A:50:07:01:11	Change IP: 192.168.2.61	192.168.2.254	00:1A:50:1B:3E:D9	Change IP: 192.168.2.62
IP Address	MAC Address	Message																					
192.168.2.254	00:1A:50:05:08:29	Change IP: 192.168.2.60																					
192.168.2.254	00:1A:50:07:01:11	Change IP: 192.168.2.61																					
192.168.2.254	00:1A:50:1B:3E:D9	Change IP: 192.168.2.62																					

Step 3 : Import profile of the respective managed AP

Device Discovery Refresh Import

Import	Source IP	MAC Address	Password	HostName	F/W Version	F/W Date	Mode	LAN Setting			Edit
								IP Address	Netmask	Gateway	
<input checked="" type="checkbox"/> Get Info	192.168.2.61	00:1A:50:07:01:11	*****	WAP-954GP	Cen-APG2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.61	255.255.255.0	192.168.2.1	Save&Reboot AP
<input checked="" type="checkbox"/> Get Info	192.168.2.60	00:1A:50:05:08:29	*****	WAP-954GP	Cen-APG2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.60	255.255.255.0	192.168.2.1	Save&Reboot AP
<input checked="" type="checkbox"/> Get Info	192.168.2.62	00:1A:50:1B:3E:D9	*****	WAP-954GP	Cen-APG2H5 V2.0.10	2011-02-08 17:12:38	AP	192.168.2.62	255.255.255.0	192.168.2.1	Save&Reboot AP

LAN Setup

IP Address: (Auto Increment)

IP Netmask:

IP Gateway:

DNS: No Default DNS Server Specify DNS Server IP

Primary DNS:

Secondary DNS:

[Save&Reboot AP](#)

System Message

IP Address	MAC Address	Message
192.168.2.254	00:1A:50:07:01:11	Change IP: 192.168.2.60
192.168.2.254	00:1A:50:05:08:29	Change IP: 192.168.2.61
192.168.2.254	00:1A:50:1B:3E:D9	Change IP: 192.168.2.62
192.168.2.61	00:1A:50:07:01:11	Import to Database
192.168.2.60	00:1A:50:05:08:29	Import to Database
192.168.2.62	00:1A:50:1B:3E:D9	Import to Database

Step 4 : Check the respective managed AP's profile in the Profile List, and change "Auto Download Profile Interval" to 1 minute, then click **Save** button.

AP Profile Management Refresh

Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
	WAP-954GP	00:1A:50:07:01:11	192.168.2.61 80	*****	2009/01/01 00:36:24	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:05:08:29	192.168.2.60 80	*****	2009/01/01 00:34:59	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:1B:3E:D9	192.168.2.62 80	*****	2009/01/01 00:35:03	Copy	Download	Restore	Recovery	Delete

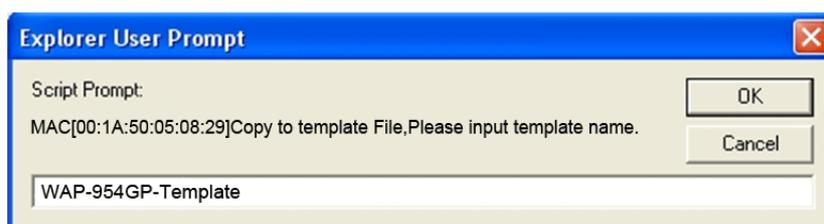
Auto Download Profile Interval: Minutes [Save](#)

Setup 5 : Configure WAP-954GP-A managed AP, set VAP0's ESSID to "WAP-954GP-A". The Status of WAP-954GP-A should display "" before system automatically download WAP-954GP's profile to database.

AP Profile Management Refresh

Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
	WAP-954GP	00:1A:50:07:01:11	192.168.2.61 80	*****	2009/01/01 00:01:17	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:05:08:29	192.168.2.60 80	*****	2009/01/01 00:14:59	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:1B:3E:D9	192.168.2.62 80	*****	2009/01/01 00:12:48	Copy	Download	Restore	Recovery	Delete

Auto Download Profile Interval: Minutes [Save](#)

Step 6 : Copy WAP-954GP-A's profile to Template and set name to "WAP-954GP-Template"

Step 7 : Configure WAP-954GP-B and WAP-954GP-C with WAP-954GP-A's Template

- Click **Restore** button on the WAP-954GP-B and WAP-954GP-C, the AP Profile Restore page will appear.
- Select **“Load From Template Profile”** in **Restore Type**.
- Select **“WAP-954GP-Template”** in the Template Profile List, then click **Restore** button

AP Profile Management > AP Profile Restore

AP Information

MAC Address : 00:1A:50:07:01:11
IP Address : 192.168.2.61

Template Profile List

Template Profile List : ● WAP-954GP-Template.bin
Delete Template File :

Restore Type

Select Type : Load From AP Profile
 Load From Template Profile
 Load From Upload File

Step 8 : Verify WAP-954GP-B and WAP-954GP-C settings. The VAP0's ESSID will be **“WAP-954GP-A”**. All settings will be the same with the WAP-954GP-A, in addition to IP address remains unchanged.

Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
●	WAP-954GP	00:1A:50:07:01:11	192.168.2.61 80	*****	2009/01/01 00:07:25	<input type="button" value="Copy"/>	<input type="button" value="Download"/>	<input type="button" value="Restore"/>	<input type="button" value="Recovery"/>	<input type="button" value="Delete"/>
●	WAP-954GP	00:1A:50:05:08:29	192.168.2.60 80	*****	2009/01/01 00:10:20	<input type="button" value="Copy"/>	<input type="button" value="Download"/>	<input type="button" value="Restore"/>	<input type="button" value="Recovery"/>	<input type="button" value="Delete"/>
●	WAP-954GP	00:1A:50:1B:3E:D9	192.168.2.62 80	*****	2009/01/01 00:09:41	<input type="button" value="Copy"/>	<input type="button" value="Download"/>	<input type="button" value="Restore"/>	<input type="button" value="Recovery"/>	<input type="button" value="Delete"/>

Auto Download Profile Interval: Minutes

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-954GP managed APs :
 - WAP-954GP-A – 00:1A:50:05:08:29
 - WAP-954GP-B – 00:1A:50:07:01:11
 - WAP-954GP-C – 00:1A:50:1B:3E:D9
 - WAP-954GP-D – 00:1A:50:05:08:19

2. Replace WAP-954GP-D to WAP-954GP-A

Step 1 : The WMS-308N can't detect WAP-954GP-A on AP Profile Management page.

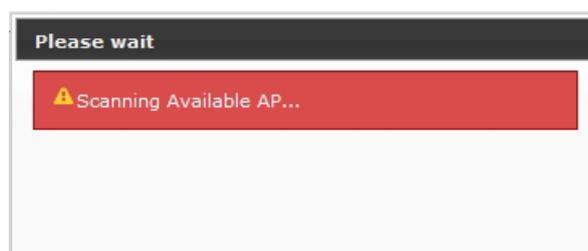
AP Profile Management										Refresh
Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
	WAP-954GP	00:1A:50:07:01:11	192.168.2.61 80	*****	2009/01/01 00:07:25	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:05:08:29	192.168.2.60 80	*****	2009/01/01 00:10:20	Copy	Download	Restore	Recovery	Delete
	WAP-954GP	00:1A:50:1B:3E:D9	192.168.2.62 80	*****	2009/01/01 00:09:41	Copy	Download	Restore	Recovery	Delete

Auto Download Profile Interval: Minutes

Step 2 : Replace WAP-954GP-D to WAP-954GP-A.

Step 3 : Click “**Recovery**” button on the WAP-954GP-A (00:1A:50:05:08:29)

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



Step 5 : The WAP-954GP-D(00:1A:50:05:08:19) will display on the Available Recovery AP List and the status show “Available Use”.

AP Profile Management > AP Profile Auto Recovery

AP Information
 MAC Address : 00:1A:50:05:08:29
 IP Address : 192.168.2.60

Available Recovery AP List Rescan Test

#	IP	MAC	Password	Status
<input type="radio"/>	192.168.2.65	00:1A:50:1B:74:9B	*****	Model is Different.
<input type="radio"/>	192.168.2.63	00:1A:50:07:02:40	*****	Model is Different.
<input checked="" type="radio"/>	192.168.2.254	00:1A:50:05:08:19	*****	Available Use

Recovery

Success

⚠ Recovery Success, then device is reboot now.

Close

Step 6 : Select WAP-954GP-D and click “Recovery” button, then the WAP-954GP-D will reboot.

Step 7 : The WAP-954GP-D(00:1A:50:05:08:19) will on the AP Profile Management List, and the configuration will be the same with the WAP-954GP-A

AP Profile Management Refresh

Status	Host Name	AP MAC Address	IP Address:Port	Password	Last Update Time	Copy To Template	Download To PC	Restore	Auto Recovery	Delete
<input checked="" type="checkbox"/>	WAP-954GP	00:1A:50:07:01:11	192.168.2.61 80	*****	2009/01/01 00:54:00	Copy	Download	Restore	Recovery	Delete
<input checked="" type="checkbox"/>	WAP-954GP	00:1A:50:05:08:29	192.168.2.60 80	*****	2009/01/01 00:01:19	Copy	Download	Restore	Recovery	Delete
<input checked="" type="checkbox"/>	WAP-954GP	00:1A:50:1B:3E:09	192.168.2.62 80	*****	2009/01/01 00:55:42	Copy	Download	Restore	Recovery	Delete

Auto Download Profile Interval: 1 Minutes Save