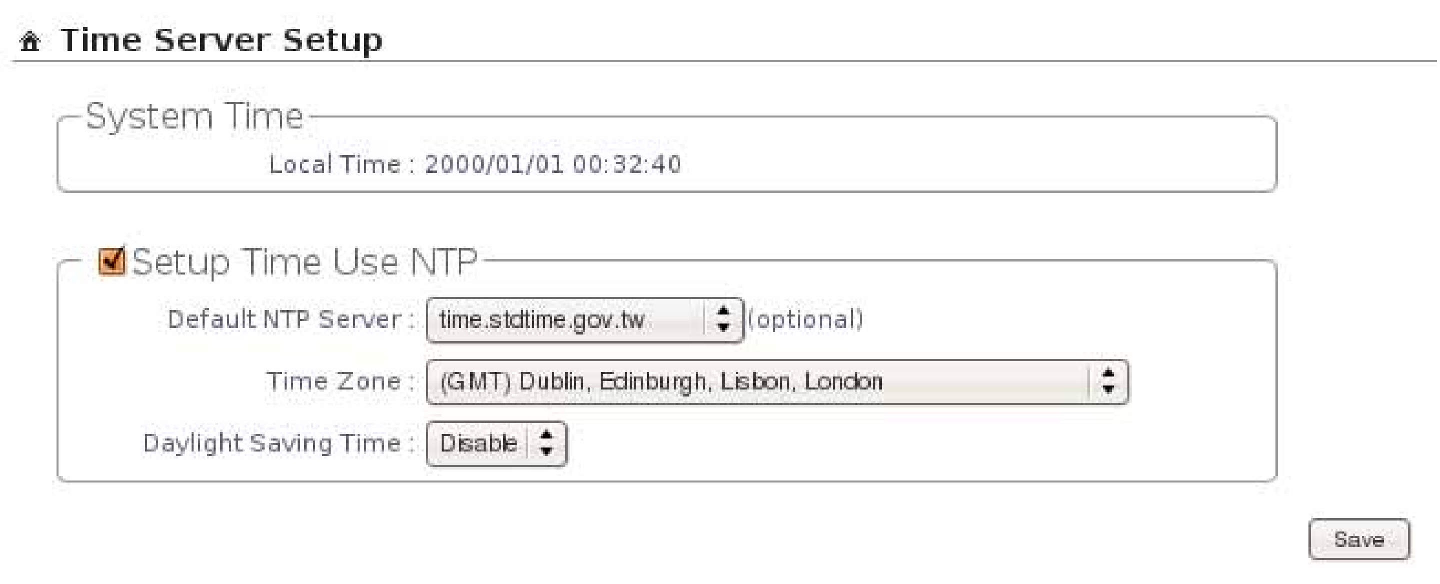
4.4 Manage the System

4.4.1 Configure System Time

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



Time Server Setup

System Time

Local Time : 2000/01/01 00:32:40

☑ Setup Time Use NTP

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

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

Daylight Saving Time : Disable

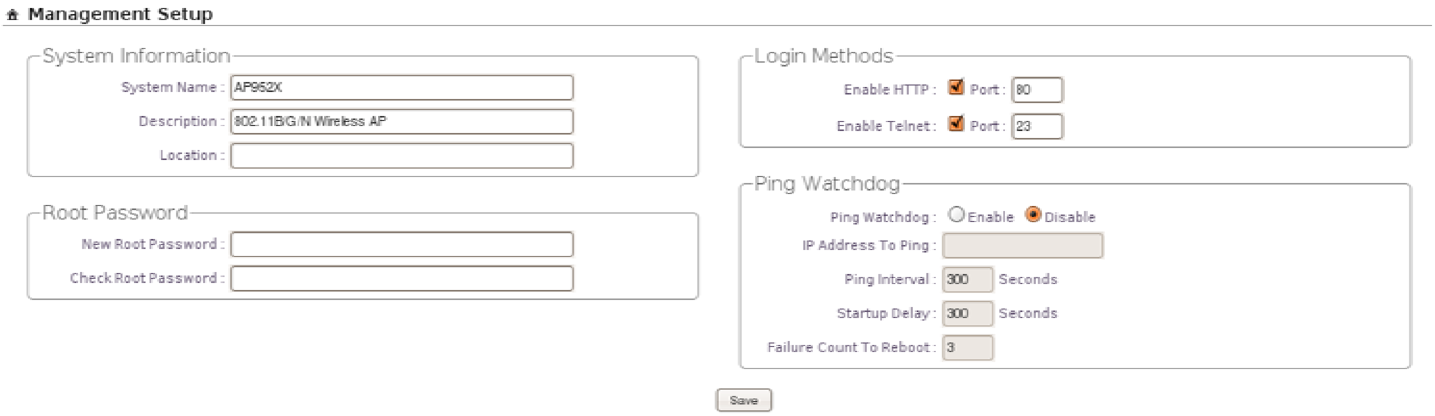
- **Local Time :** Display the current time of the system.
- **Setup Time Use NTP :** Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Please set a time zone from where 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 DNS and Default Gateway setting first.

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

4.4.2 Configure Management

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



Management Setup

System Information

System Name : AP952X

Description : 802.11B/G/N Wireless AP

Location :

Root Password

New Root Password :

Check Root Password :

Login Methods

Enable HTTP : ☑ Port : 80

Enable Telnet : ☑ Port : 23

Ping Watchdog

Ping Watchdog : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 300 Seconds

Startup Delay : 300 Seconds

Failure Count To Reboot : 3

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default provided.
  - ➔ **Description :** Denote further information of the system.
  - ➔ **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Root Password :** Log in as a root user and is allowed to change its own. Root user also can change **admin** user's and **operator** user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.

- **Admin 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 Telnet :** Select Enable HTTP to activate HTTP Service
  - ➔ **Telnet Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **23**

- **Ping Watchdog :** The ping watchdog sets the AP-952X 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 AP-952X 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.

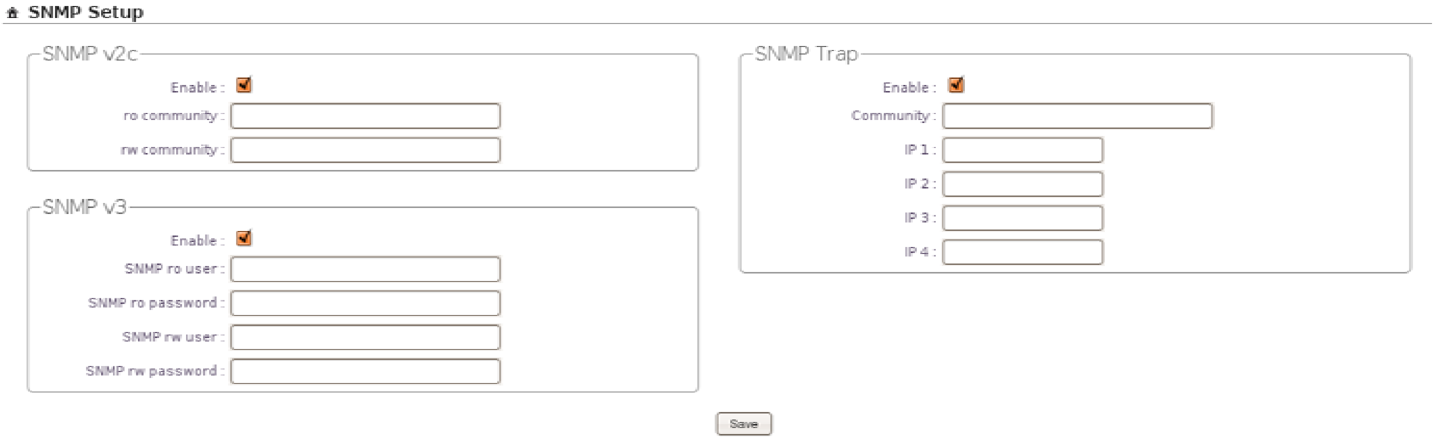
➔ **Failure Count To Reboot :** specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

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

Click “***Continue to this website***” to access the AP-952X's GUI. The AP-952X's Home page will be appear.

4.4.3 Configure SNMP

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



SNMP Setup

SNMP v2c
Enable : ☑
ro community :
rw community :

SNMP v3
Enable : ☑
SNMP ro user :
SNMP ro password :
SNMP rw user :
SNMP rw password :

SNMP Trap
Enable : ☑
Community :
IP 1 :
IP 2 :
IP 3 :
IP 4 :

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

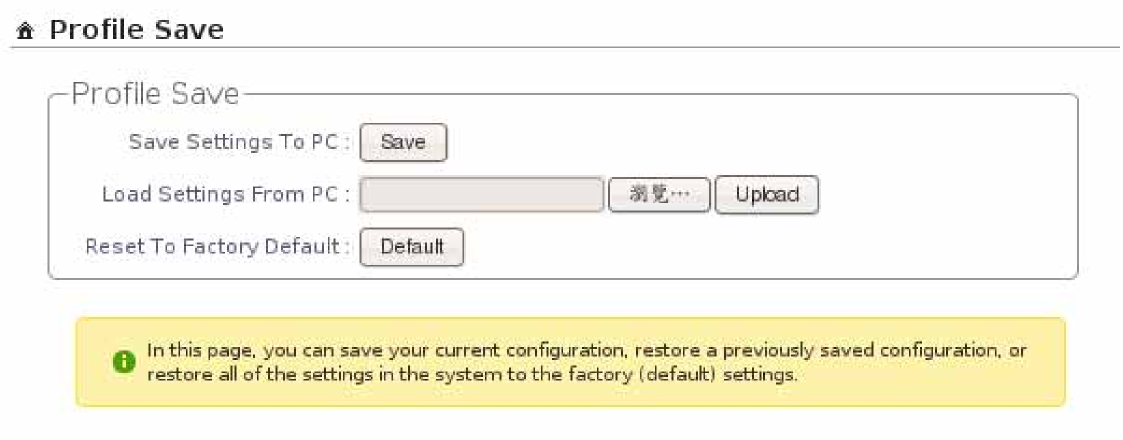
SNMPv3 supports the highest level SNMP security.

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

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

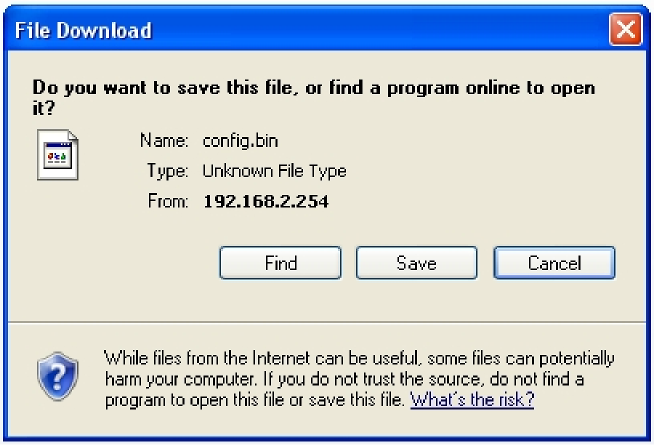
4.4.4 Bacup / Restore and Reset to Factory

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.



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.



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

Name: config.bin
Type: Unknown File Type
From: 192.168.2.254

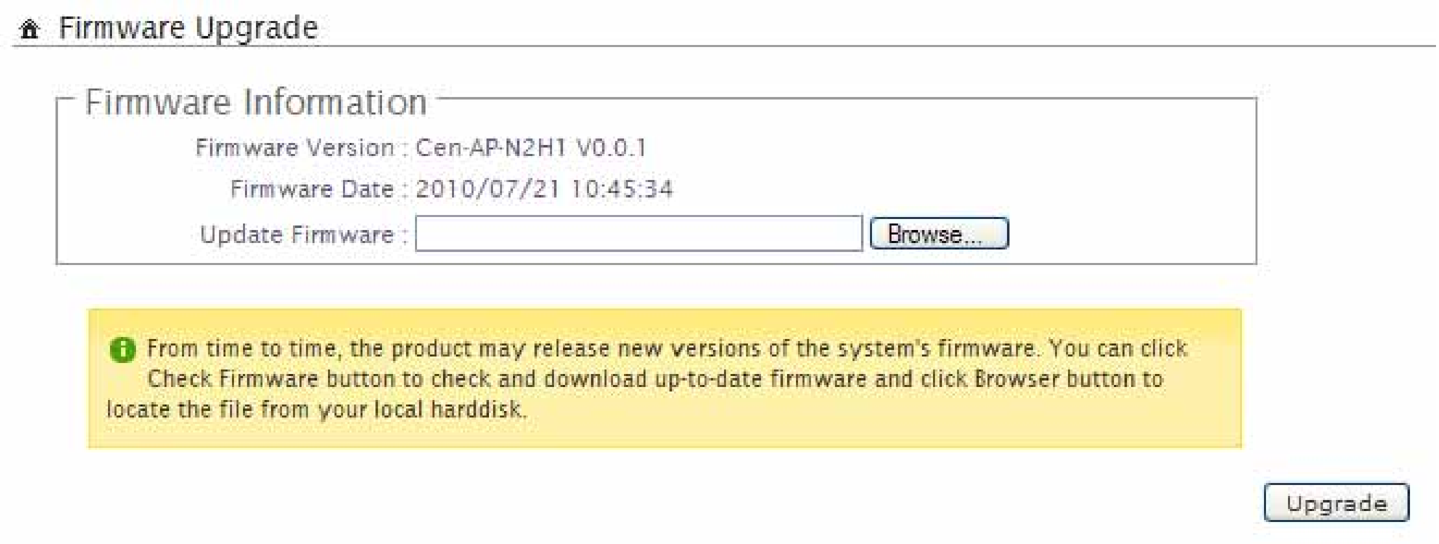
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

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

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

4.4.5 Firmware Upgrade

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


Firmware Upgrade

Firmware Information

Firmware Version : Cen-AP-N2H1 V0.0.1

Firmware Date : 2010/07/21 10:45:34

Update Firmware :

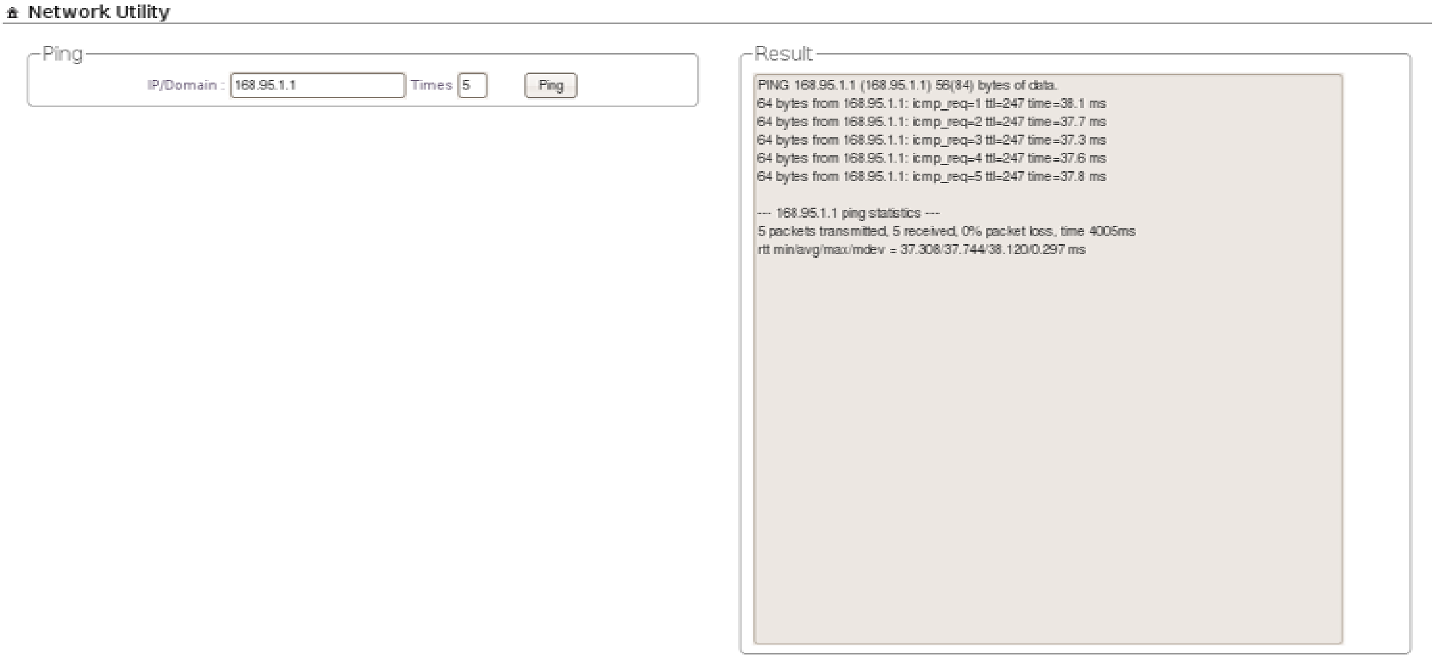
From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

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

4.4.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

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



IP/Domain : 168.95.1.1 Times 5

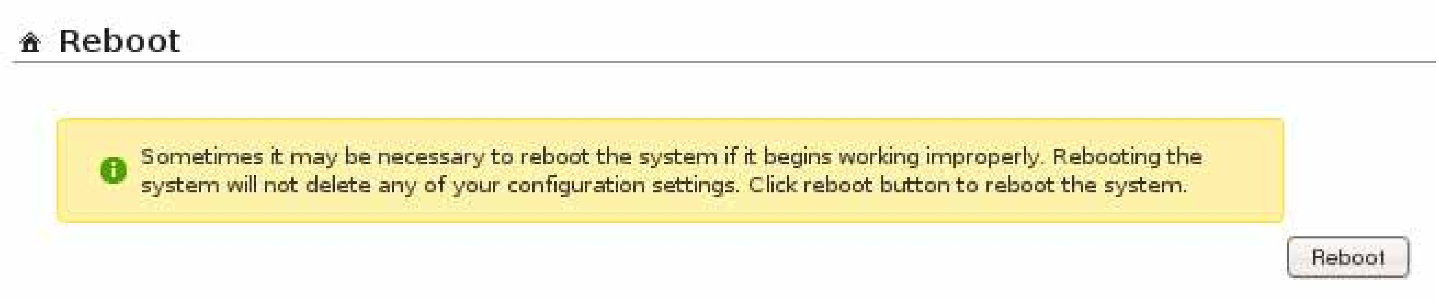
```
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_req=1 ttl=247 time=38.1 ms
64 bytes from 168.95.1.1: icmp_req=2 ttl=247 time=37.7 ms
64 bytes from 168.95.1.1: icmp_req=3 ttl=247 time=37.3 ms
64 bytes from 168.95.1.1: icmp_req=4 ttl=247 time=37.6 ms
64 bytes from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

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

- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - **Times :** By default, it’s 5 and the range is from 1 to 60. It indicates number of connectivity test.

4.4.7 Reboot

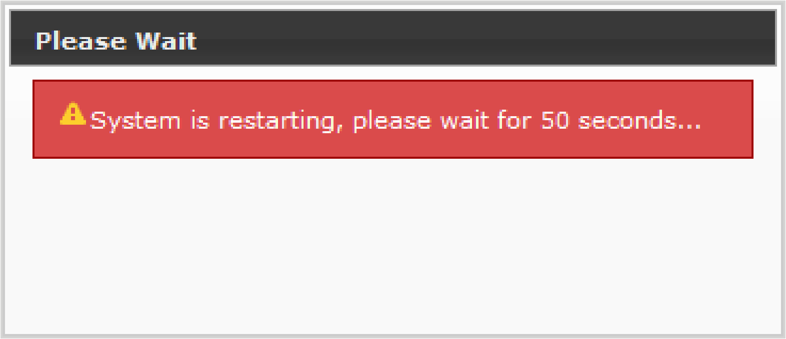
This function allows administrator to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

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

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



Please Wait

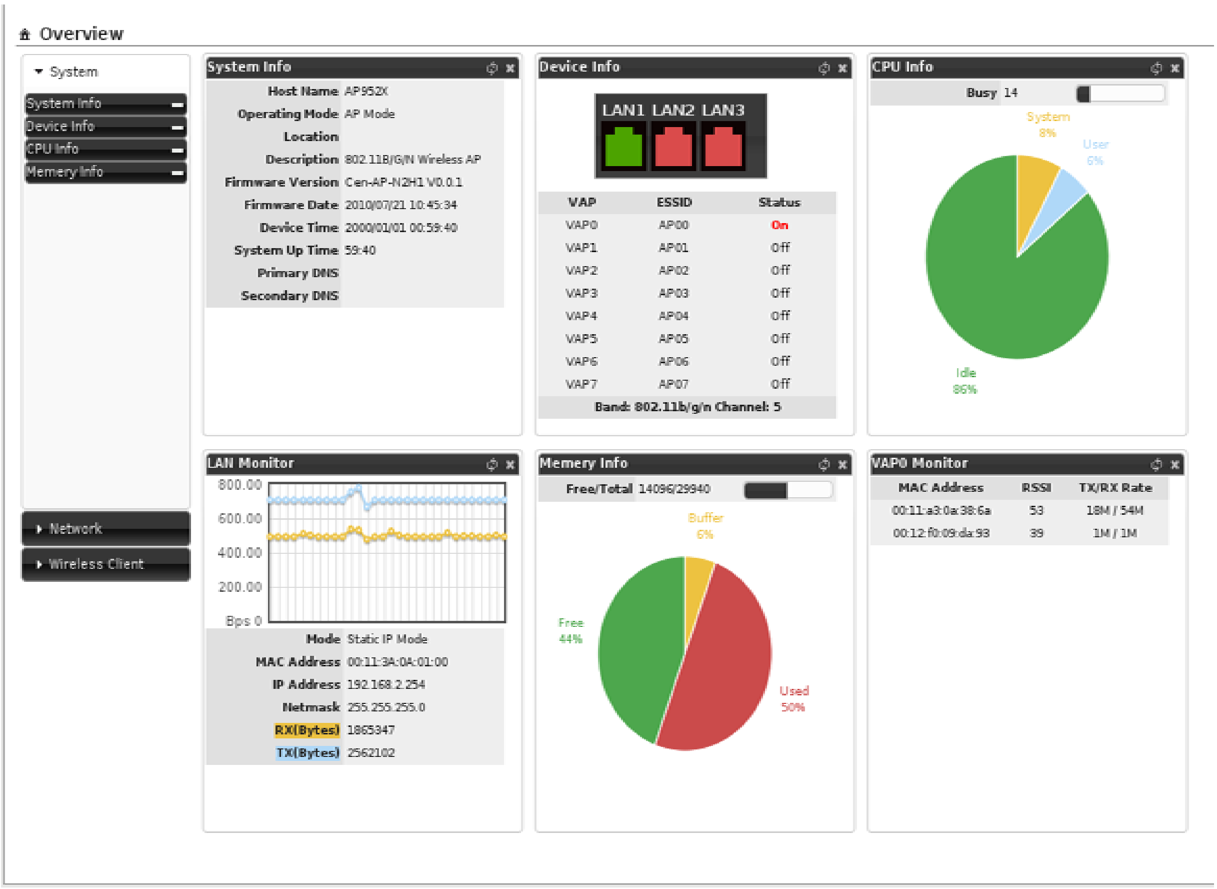
System is restarting, please wait for 50 seconds...

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

4.5 Observer the Status

4.5.1 Overview

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



System Info

Host Name	AP952X
Operating Mode	AP Mode
Location	
Description	802.11B/G/N Wireless AP
Firmware Version	Cen-AP-N2H1 V0.0.1
Firmware Date	2010/07/21 10:45:34
Device Time	2000/01/01 00:59:40
System Up Time	59:40
Primary DNS	
Secondary DNS	

Device Info

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

Band: 802.11b/g/n Channel: 5

CPU Info

LAN Monitor

Mode	Static IP Mode
MAC Address	00:11:3A:0A:01:00
IP Address	192.168.2.254
Netmask	255.255.255.0
RX(Bytes)	1865347
TX(Bytes)	2562102

Memery Info

Free/Total 14096/29940

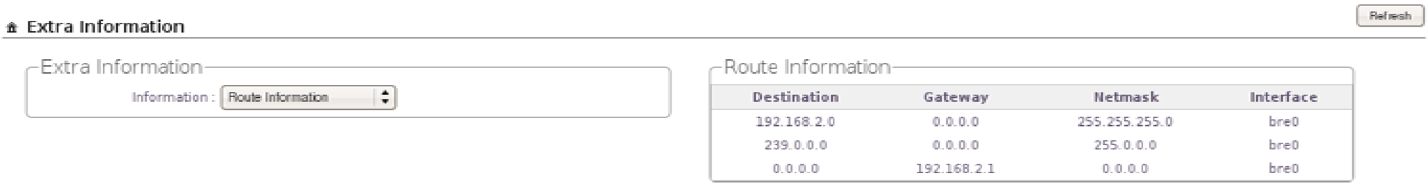
VAP0 Monitor

MAC Address	RSSI	TX/RX Rate
00:11:a3:0a:38:6a	53	18M / 54M
00:12:f0:09:da:93	39	1M / 1M

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

4.5.2 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.



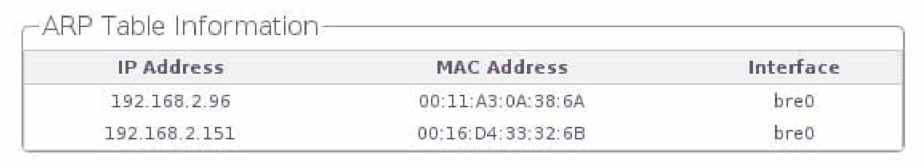
Destination	Gateway	Netmask	Interface
192.168.2.0	0.0.0.0	255.255.255.0	bre0
239.0.0.0	0.0.0.0	255.0.0.0	bre0
0.0.0.0	192.168.2.1	0.0.0.0	bre0

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

AP-952X 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.

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

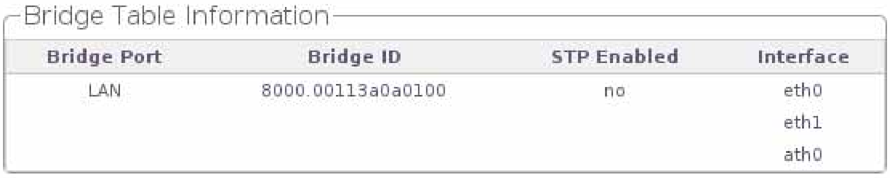
ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.



IP Address	MAC Address	Interface
192.168.2.96	00:11:A3:0A:38:6A	bre0
192.168.2.151	00:16:D4:33:32:6B	bre0

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

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, eth1, ath0~ath7).

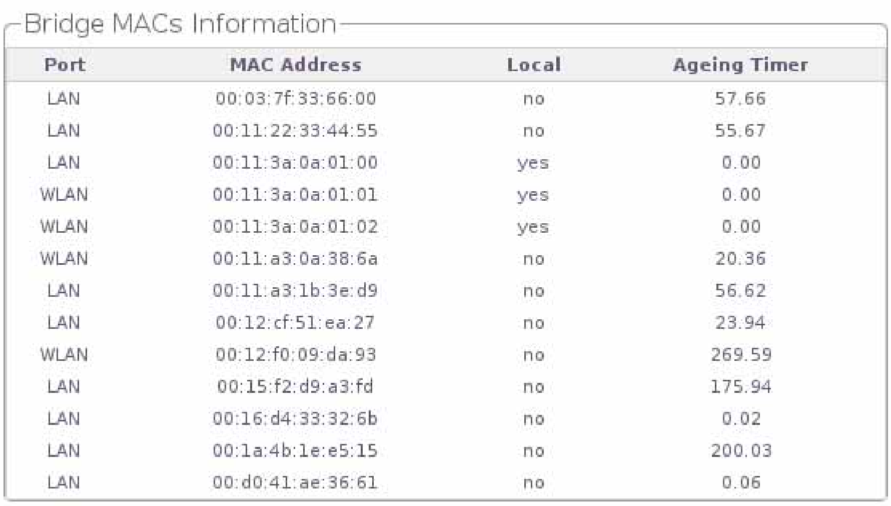


Bridge Port	Bridge ID	STP Enabled	Interface
LAN	8000.00113a0a0100	no	eth0 eth1 ath0

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

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

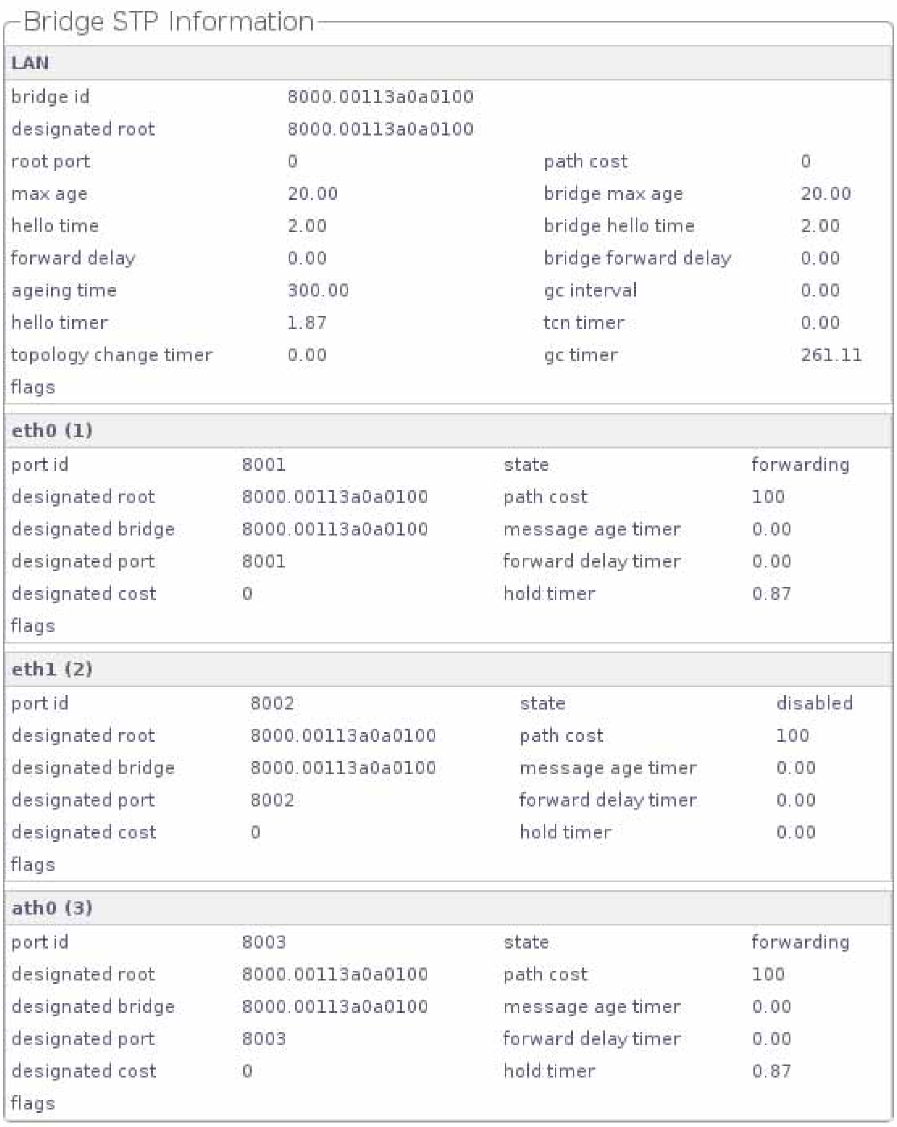
Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC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



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:03:7f:33:66:00	no	57.66
LAN	00:11:22:33:44:55	no	55.67
LAN	00:11:3a:0a:01:00	yes	0.00
WLAN	00:11:3a:0a:01:01	yes	0.00
WLAN	00:11:3a:0a:01:02	yes	0.00
WLAN	00:11:a3:0a:38:6a	no	20.36
LAN	00:11:a3:1b:3e:d9	no	56.62
LAN	00:12:cf:51:ea:27	no	23.94
WLAN	00:12:f0:09:da:93	no	269.59
LAN	00:15:f2:d9:a3:fd	no	175.94
LAN	00:16:d4:33:32:6b	no	0.02
LAN	00:1a:4b:1e:e5:15	no	200.03
LAN	00:d0:41:ae:36:61	no	0.06

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



Bridge STP Information

LAN			
bridge id	8000.00113a0a0100		
designated root	8000.00113a0a0100		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	0.00	bridge forward delay	0.00
ageing time	300.00	gc interval	0.00
hello timer	1.87	tcn timer	0.00
topology change timer	0.00	gc timer	261.11
flags			

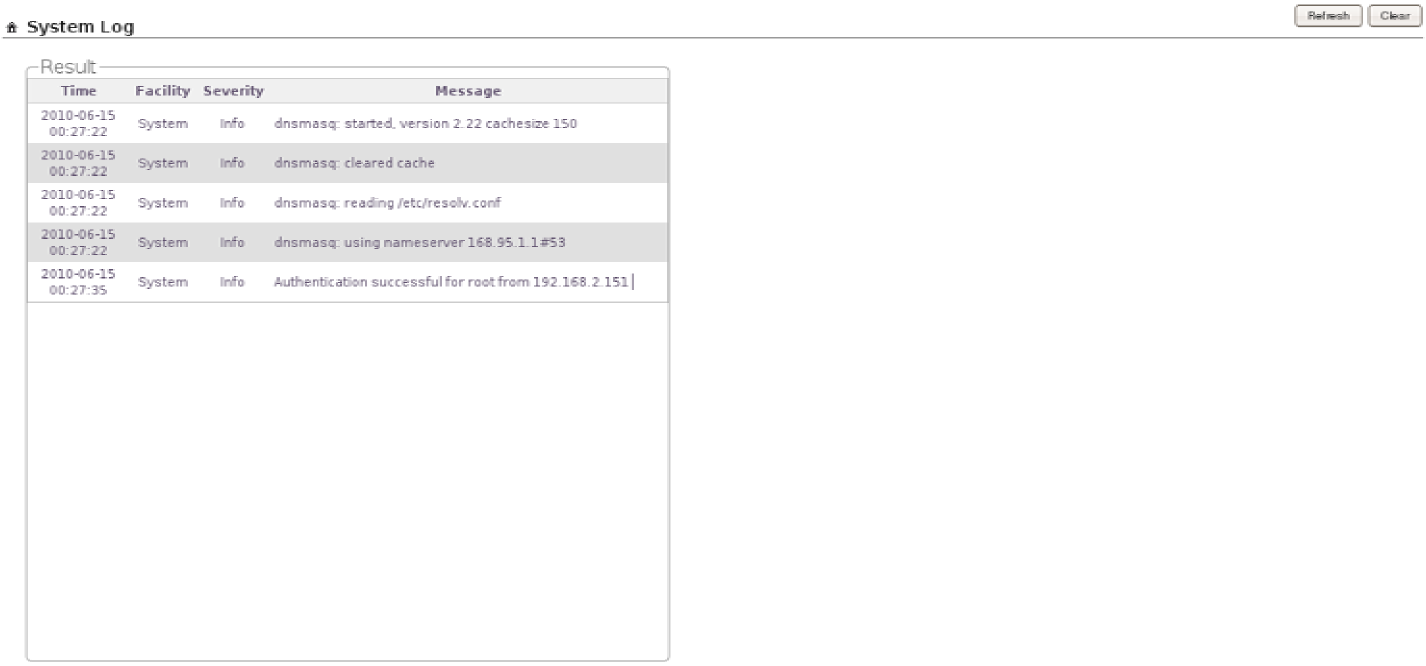
eth0 (1)			
port id	8001	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

eth1 (2)			
port id	8002	state	disabled
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ath0 (3)			
port id	8003	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

4.5.3 Event Log

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



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

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

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

Chapter 5. WDS Mode Configuration

This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Setup	Profiles Settings	System Overview
	LAN	Advanced Setup	Firmware Upgrade	Extra Info
	Management	WDS Setup	Network Utility	Event Log
	Time Server	WDS Status	Reboot	
	SNMP			

Table 5-1: WDS Mode Functions

5.1 Connect AP-952X to the Wired Local Network

5.1.1 Network Requirement

You could expand your Ethernet network via WDS link. In this mode, the AP-952X connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in Figure 5-1. In the mode, it can't associate with any wireless clients.

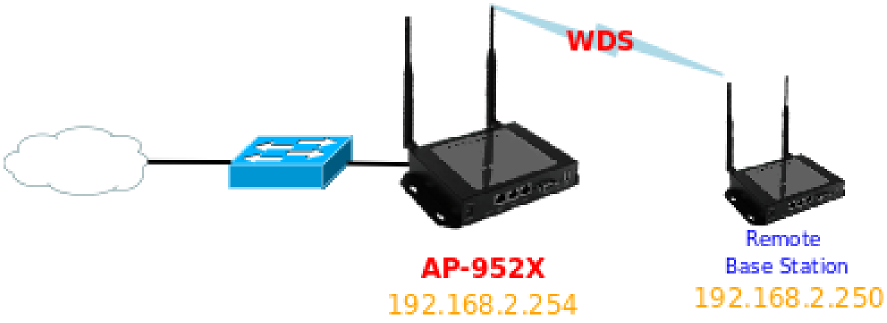
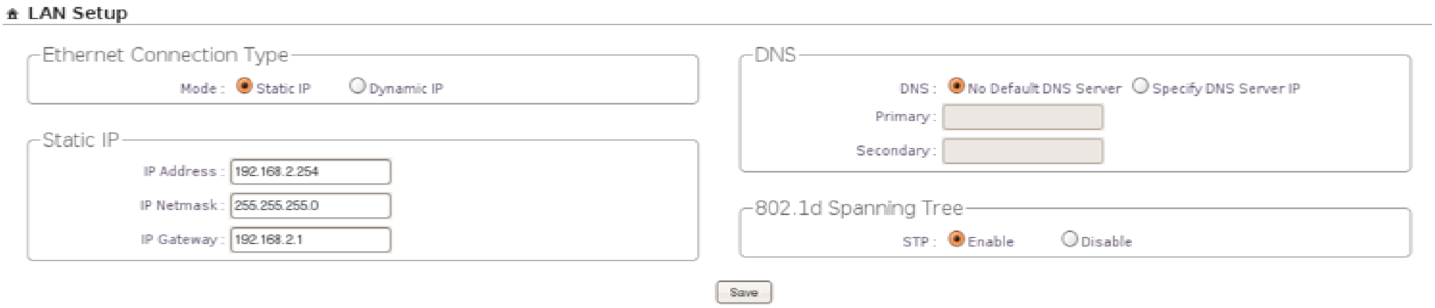


Figure 5-1 Point to Point network Configuration

5.1.2 Configure LAN Port

Here is instruction for how to setup the LAN. The connection types for LAN port : **Static IP** and **Dynamic IP**, Please click on **System -> LAN** and follow the below setting.



LAN Setup

Ethernet Connection Type

Mode : ● Static IP ○ Dynamic IP

Static IP

IP Address : 192.168.2.254

IP Netmask : 255.255.255.0

IP Gateway : 192.168.2.1

DNS

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

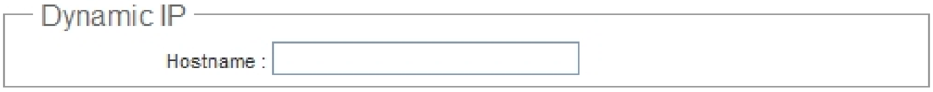
Primary :

Secondary :

802.1d Spanning Tree

STP : ● Enable ○ Disable

- **Mode :** Check either "Static IP" or "Dynamic IP" button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.2.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the WCB1200H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.



Dynamic IP

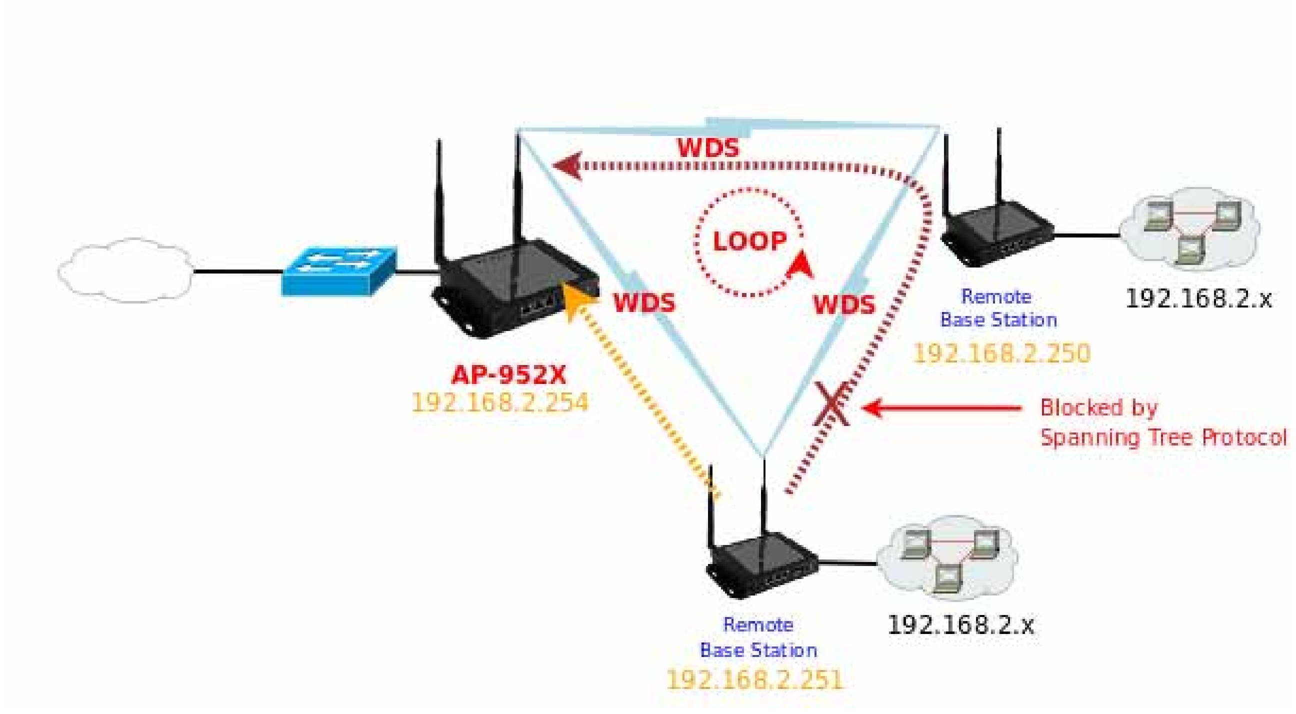
Hostname :

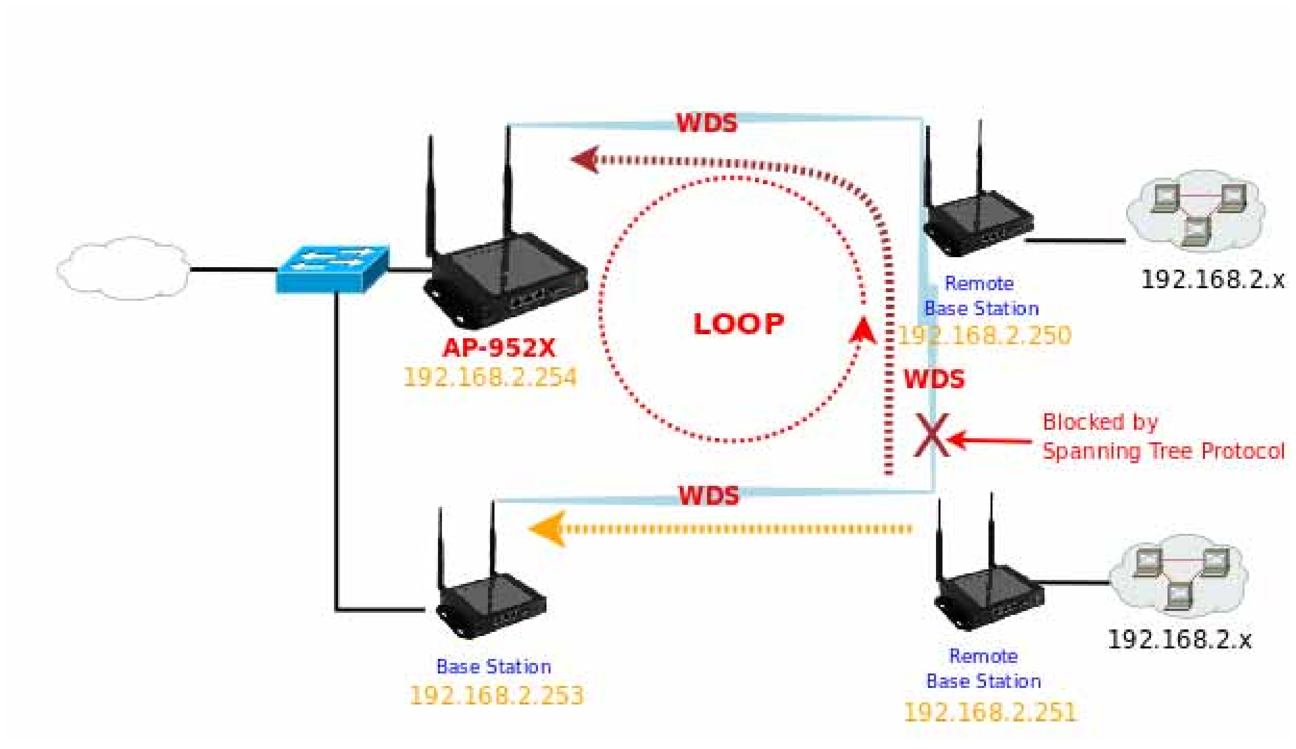
- ✓ **Hostname :** The Hostname of the LAN port

- **DNS :** Check either "No Default DNS Server" or "Specify DNS Server IP" button as desired to set up the system DNS.
  - **Primary :** The IP address of the primary DNS server.
  - **Secondary :** The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from WDS0 to WDS7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. The Spanning tree always enabled on AP-952X. Below Figures depict a loop for a bridged LAN between LAN and WDS link





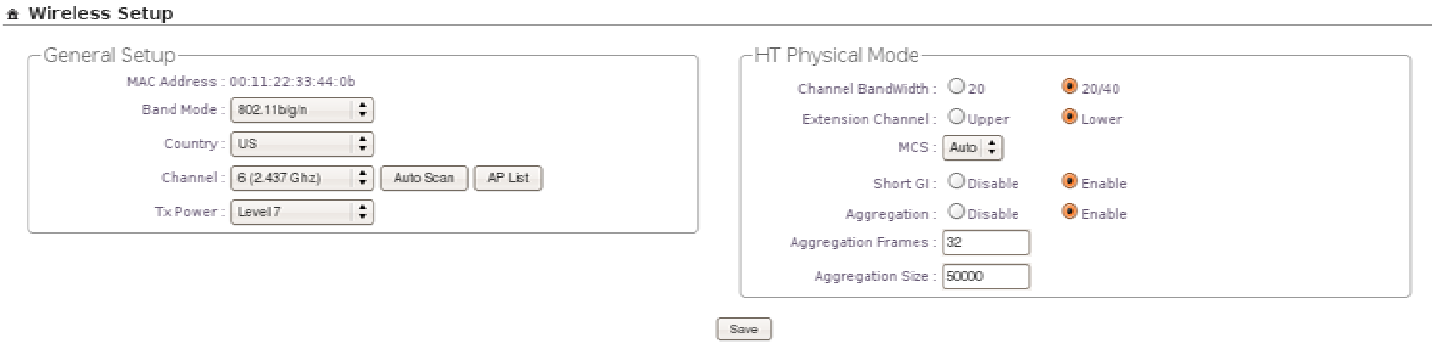
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.2 Expand Your Wireless Network

The system manager can configure related wireless settings, **General Settings, Advanced Settings, WDS Setup** and **WDS Status**.

5.2.1 Configure Wireless General Setup

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



Wireless Setup

General Setup

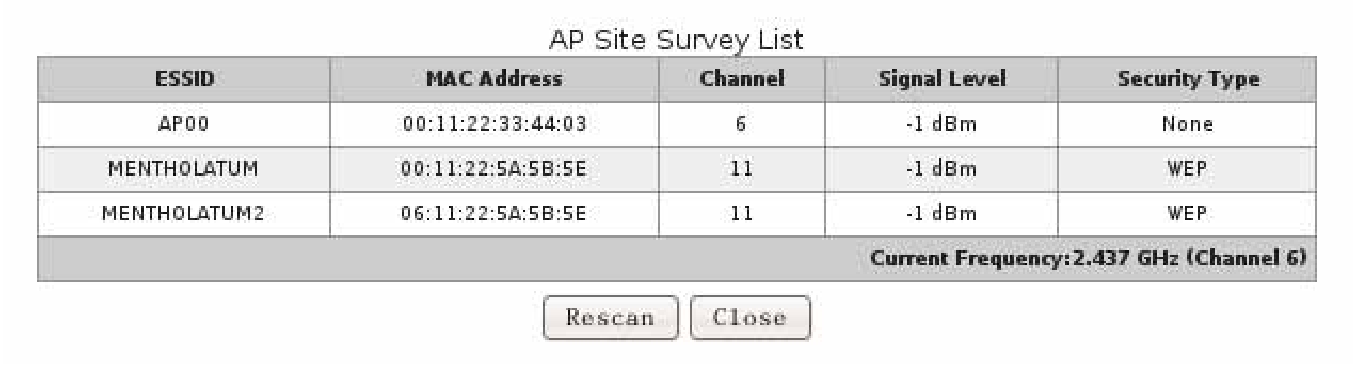
MAC Address : 00:11:22:33:44:0b
Band Mode : 802.11b/g/n
Country : US
Channel : 6 (2.437 Ghz)
Tx Power : Level 7

HT Physical Mode

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

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

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



AP Site Survey List

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

Current Frequency:2.437 GHz (Channel 6)

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

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

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

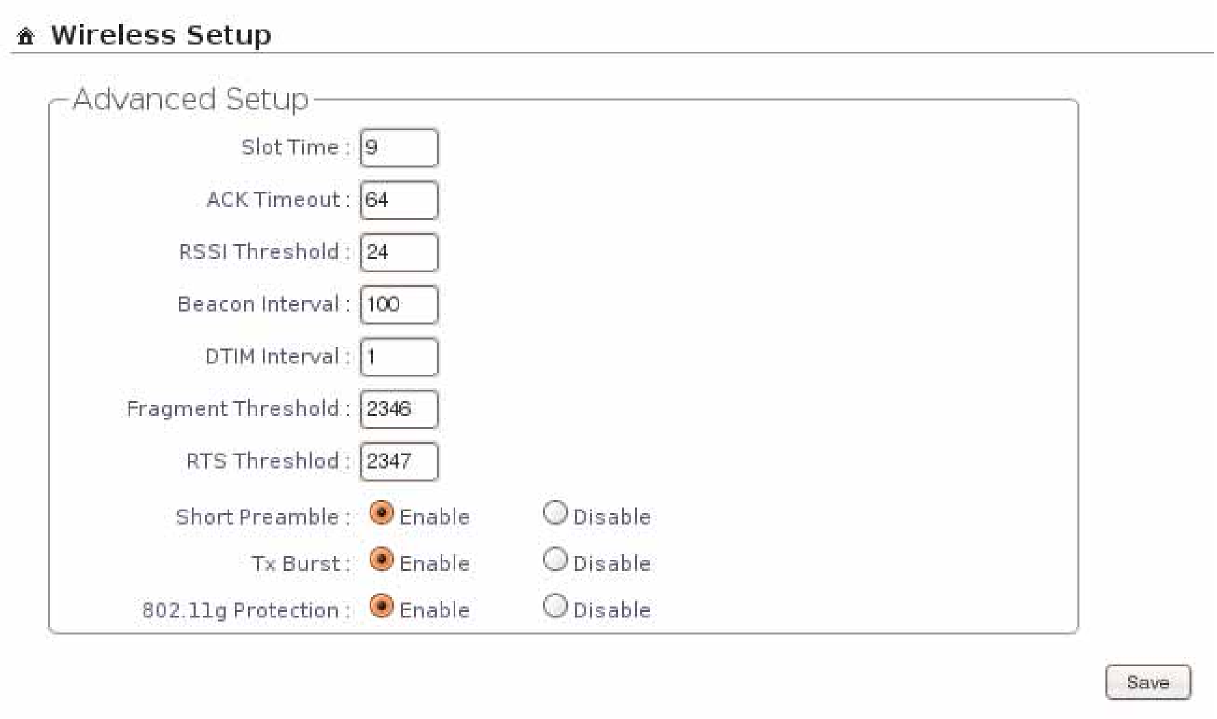
A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class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

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

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

5.2.2 Configure Wireless Advanced Setup

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



Wireless Setup

Advanced Setup

Slot Time : 9

ACK Timeout : 64

RSSI Threshold : 24

Beacon Interval : 100

DTIM Interval : 1

Fragment Threshold : 2346

RTS Threshlod : 2347

Short Preamble : ● Enable ○ Disable

Tx Burst : ● Enable ○ Disable

802.11g Protection : ● Enable ○ Disable

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

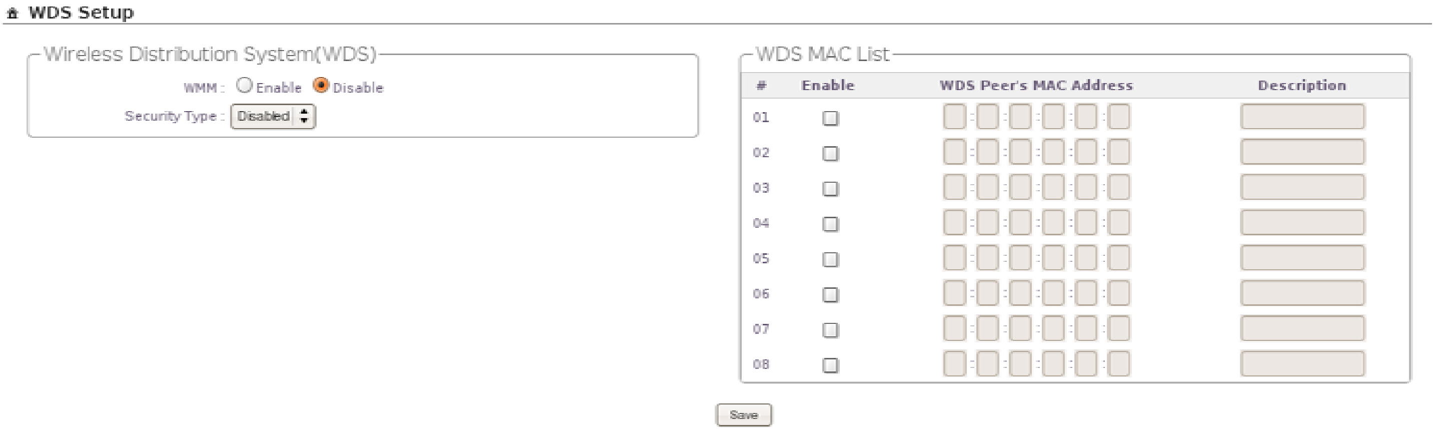
- **802.11g Protection :** Click ***Enable*** button to activate 802.11g Protection Mode, and Disable to inactivate 802.11g Protection Mode.

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

5.2.3 Create WDS Link

The administrator could create WDS Links for expanding wireless network via this page. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. ***A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.***

Please click on **Wireless -> WDS Setup** and follow the below setting.



WDS Setup

Wireless Distribution System(WDS)

WMM : ○ Enable ● Disable

Security Type : Disabled

WDS MAC List

#	Enable	WDS Peer's MAC Address	Description
01	□		
02	□		
03	□		
04	□		
05	□		
06	□		
07	□		
08	□		

43. **WMM : Select Enable, the packets with QoS WMM has higher priority.**

44. **Security Type :** Option is "**Disable**", "**WEP**" or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.

➔ **WEP Key :** Enter **5 / 13 / 16 ASCII** or **10 / 26 /32 HEX** format WEP key.

➔ **AES Key :** Enter **32 HEX** format AES key.

AES Encryption only support between AP-952X and AP-952X

45. **WDS MAC List**

➔ **Enable :** Click ***Enable*** to create WDS link.

➔ **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.

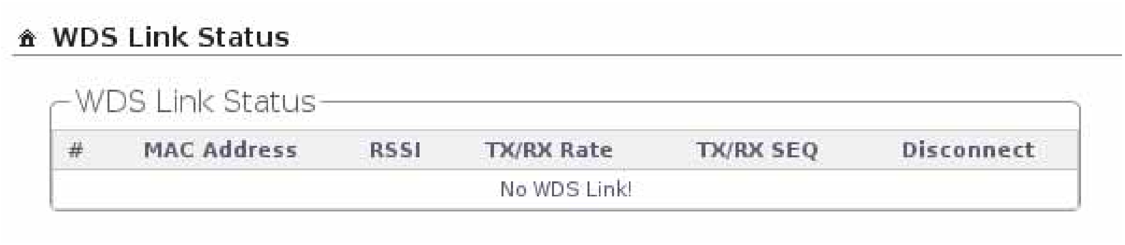
➔ **Description :** Description of WDS link.

The WDS link needs to be set at same **Channel** and **Security Type** between WDS link.

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

5.2.4 View WDS Link Status

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



WDS Link Status

WDS Link Status

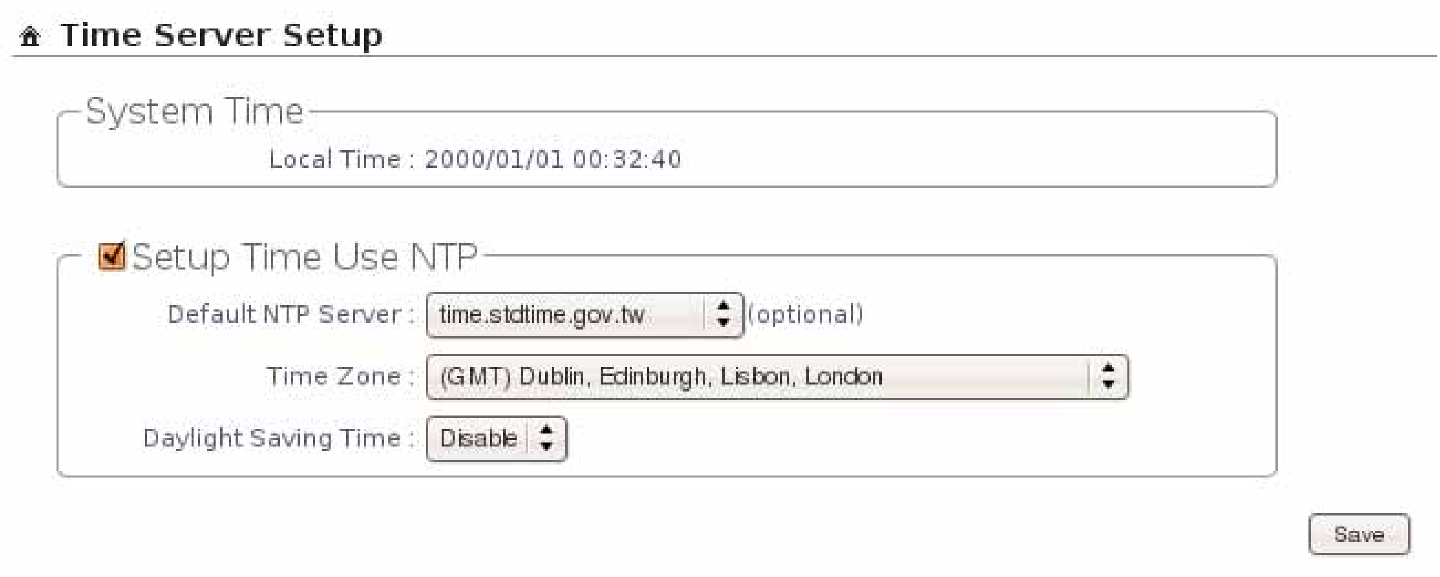
#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	Disconnect
No WDS Link!					

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

5.3 Manage the System

5.3.1 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 : 2000/01/01 00:32:40

☑ Setup Time Use NTP

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

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

Daylight Saving Time : Disable

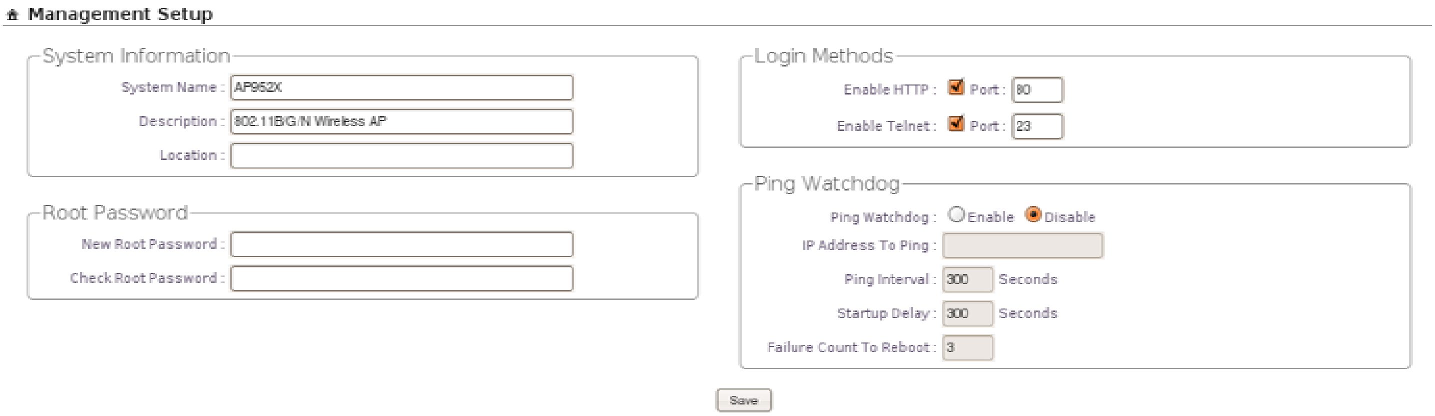
- **Local Time :** Display the current time of the system.
- **Setup Time Use NTP :** Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Please set a time zone from where 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 DNS and Default Gateway setting first.

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

5.3.2 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

System Information

System Name : AP952X

Description : 802.11B/G/N Wireless AP

Location :

Root Password

New Root Password :

Check Root Password :

Login Methods

Enable HTTP : ☑ Port : 80

Enable Telnet : ☑ Port : 23

Ping Watchdog

Ping Watchdog : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 300 Seconds

Startup Delay : 300 Seconds

Failure Count To Reboot : 3

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default provided.
  - ➔ **Description :** Denote further information of the system.
  - ➔ **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Root Password :** Log in as a root user and is allowed to change its own. Root user also can change **admin** user's and **operator** user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.

- **Admin 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 Telnet :** Select Enable HTTP to activate HTTP Service
  - ➔ **Telnet Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **23**

- **Ping Watchdog :** The ping watchdog sets the AP-952X 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 AP-952X 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.

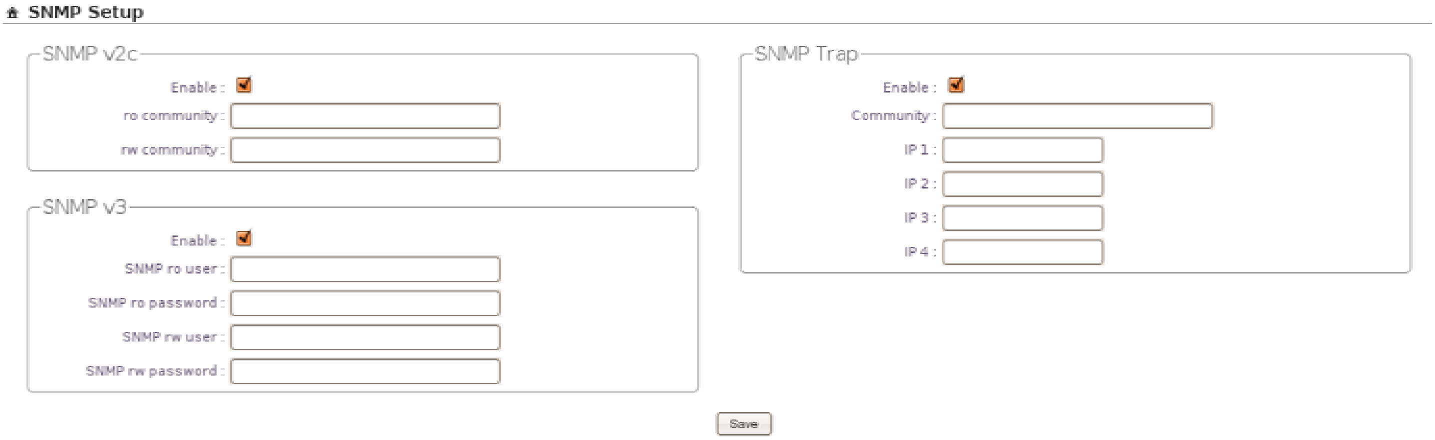
- ➔ **Enable Ping Watchdog :** control will enable Ping Watchdog Tool.
- ➔ **IP Address To Ping :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping 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

Click “***Continue to this website***” to access the AP-952X's GUI. The AP-952X's Home page will be appear.

5.3.3 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.

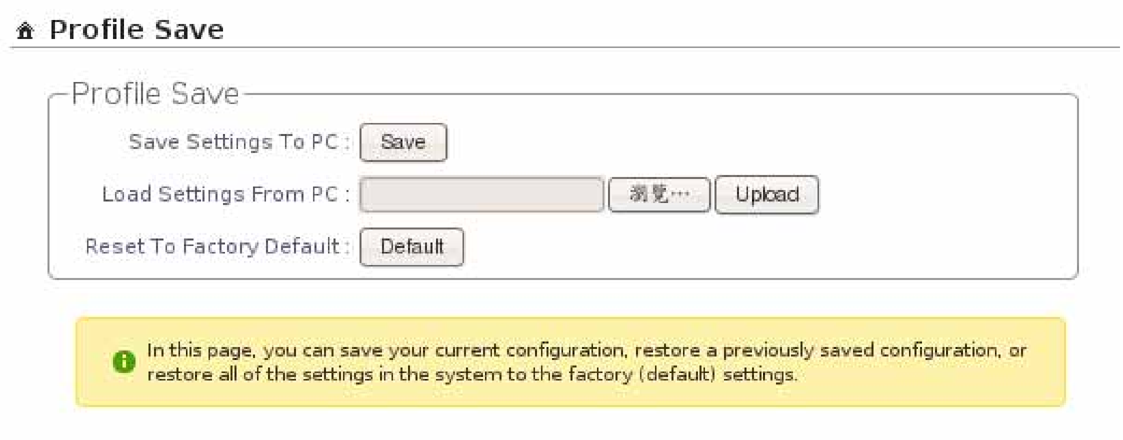
- ➔ **SNMP ro user :** Set a community string to authorize read-only access.
- ➔ **SNMP ro password :** Set a password to authorize read-only access.
- ➔ **SNMP rw user :** Set a community string to authorize read/write access.
- ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **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

5.3.4 Bacup / 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

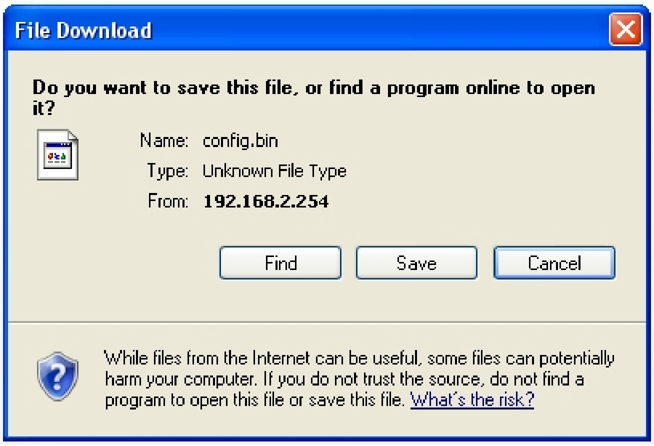
Save Settings To PC : Save

Load Settings From PC : 浏览… Upload

Reset To Factory Default : Default

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

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



File Download

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

Name: config.bin
Type: Unknown File Type
From: 192.168.2.254

Find Save Cancel

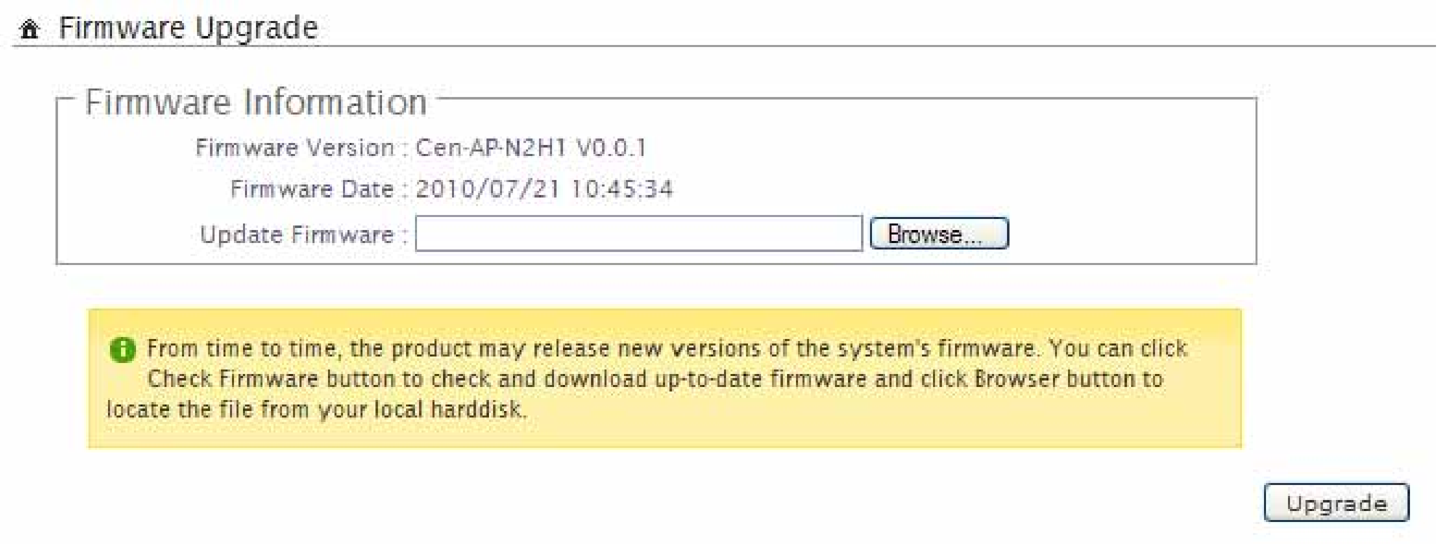
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

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

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

5.3.5 Firmware Upgrade

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



Firmware Upgrade

Firmware Information

Firmware Version : Cen-AP-N2H1 V0.0.1

Firmware Date : 2010/07/21 10:45:34

Update Firmware :

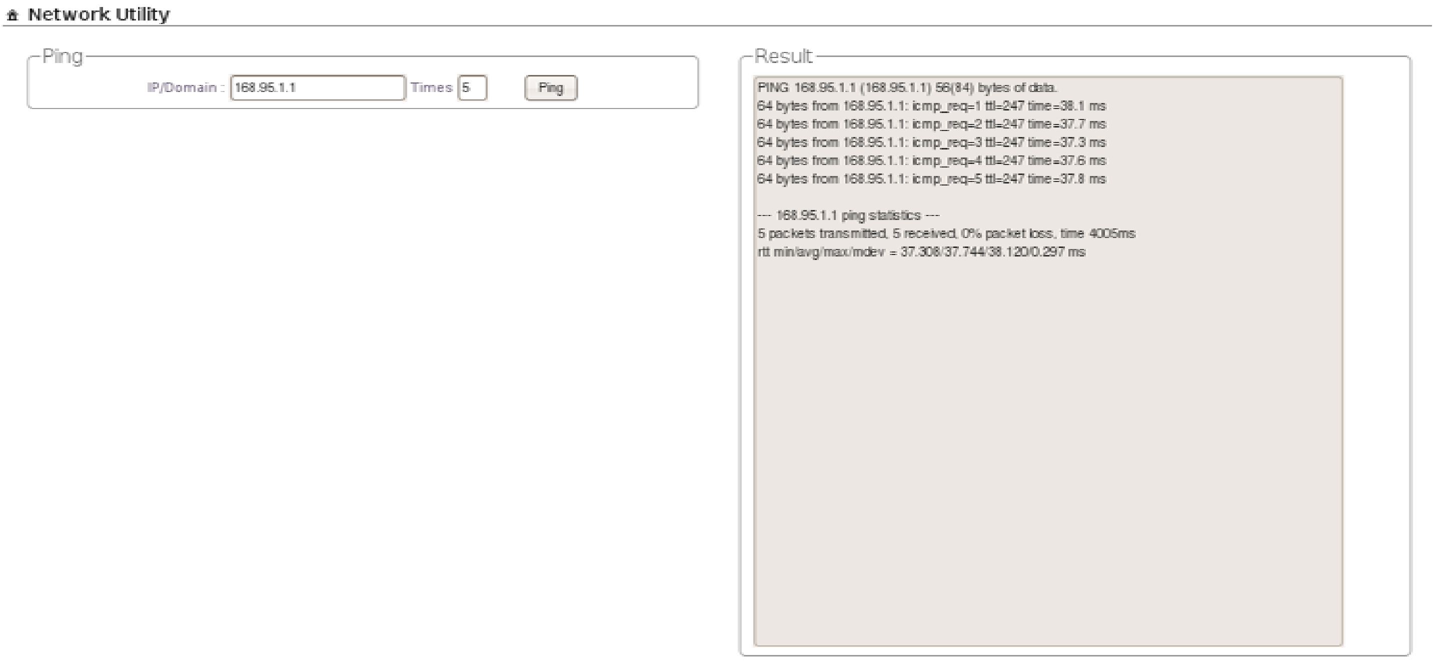
From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

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

5.3.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

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



IP/Domain : 168.95.1.1 Times 5

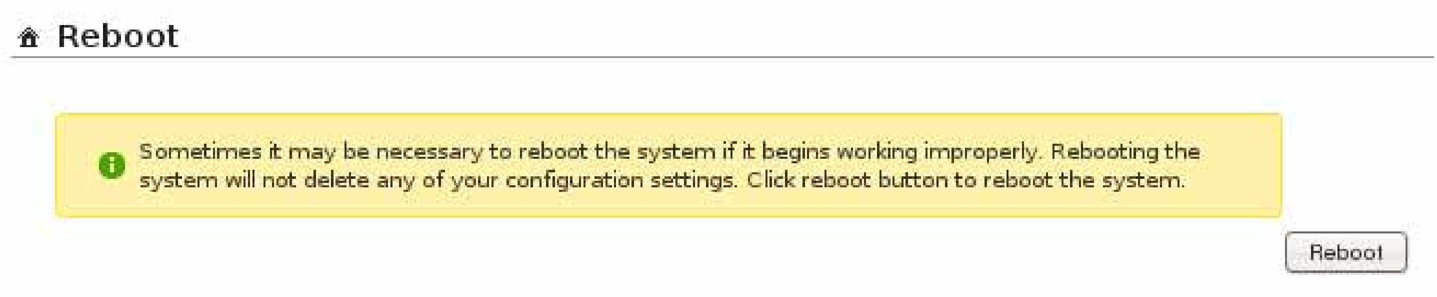
```
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_req=1 ttl=247 time=38.1 ms
64 bytes from 168.95.1.1: icmp_req=2 ttl=247 time=37.7 ms
64 bytes from 168.95.1.1: icmp_req=3 ttl=247 time=37.3 ms
64 bytes from 168.95.1.1: icmp_req=4 ttl=247 time=37.6 ms
64 bytes from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

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

- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - **Times :** By default, it’s 5 and the range is from 1 to 60. It indicates number of connectivity test.

5.3.7 Reboot

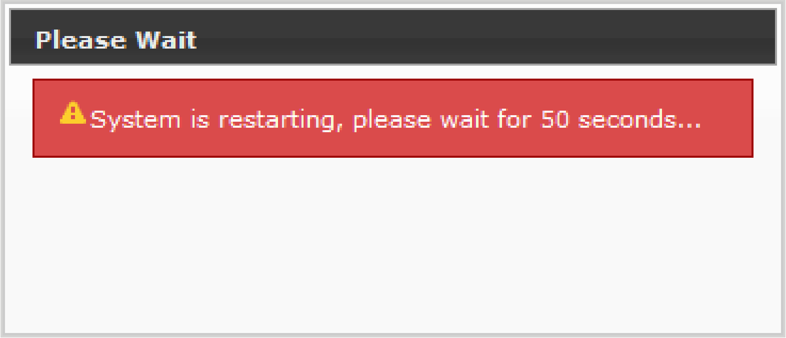
This function allows administrator to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

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

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



Please Wait

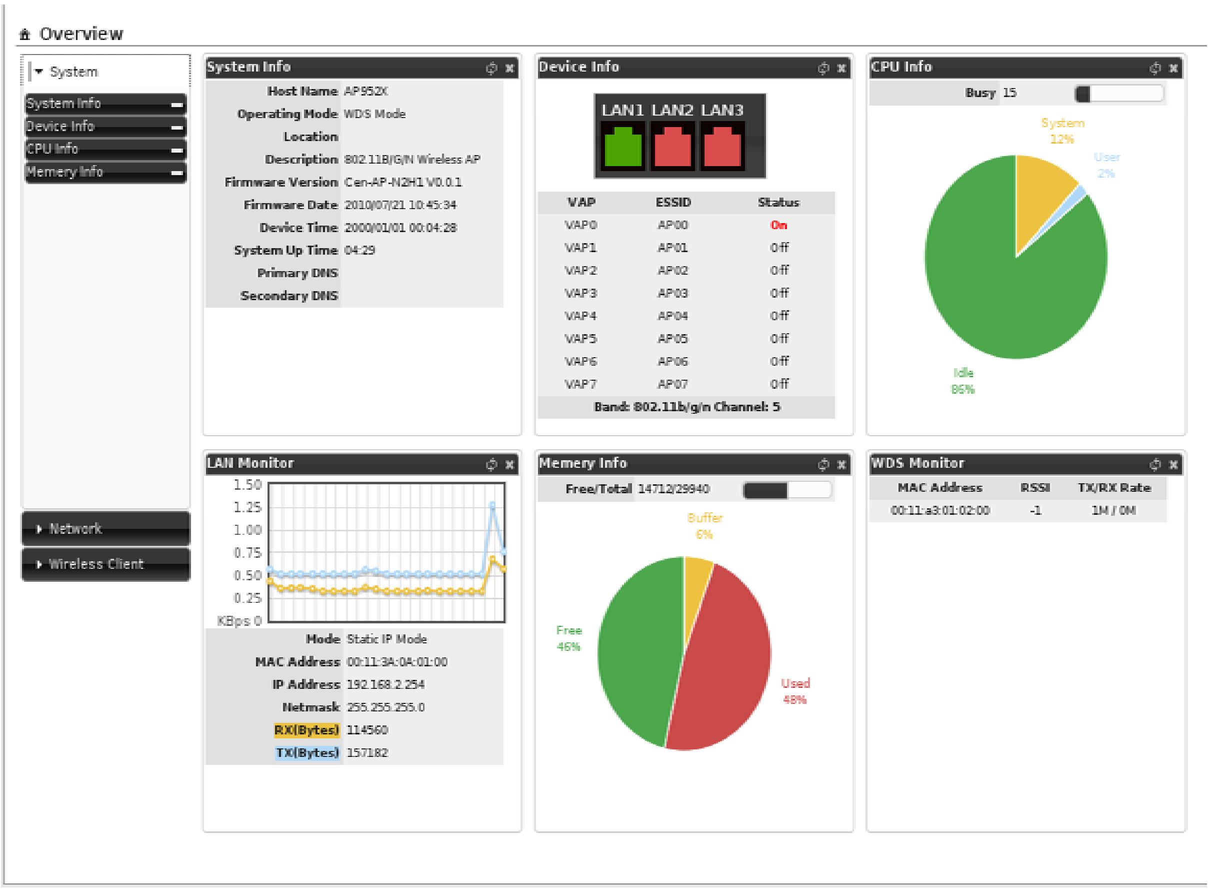
⚠System is restarting, please wait for 50 seconds...

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

5.4 Observer the Status

5.4.1 Overview

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



System Info

Host Name	AP952X
Operating Mode	WDS Mode
Location	
Description	802.11B/G/N Wireless AP
Firmware Version	Cen-AP-N2H1 V0.0.1
Firmware Date	2010/07/21 10:45:34
Device Time	2000/01/01 00:04:28
System Up Time	04:29
Primary DNS	
Secondary DNS	

Device Info

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

Band: 802.11b/g/n Channel: 5

CPU Info

Busy 15

LAN Monitor

Mode	Static IP Mode
MAC Address	00:11:3A:0A:01:00
IP Address	192.168.2.254
Netmask	255.255.255.0
RX(Bytes)	114560
TX(Bytes)	157182

Memery Info

Free/Total 14712/29940

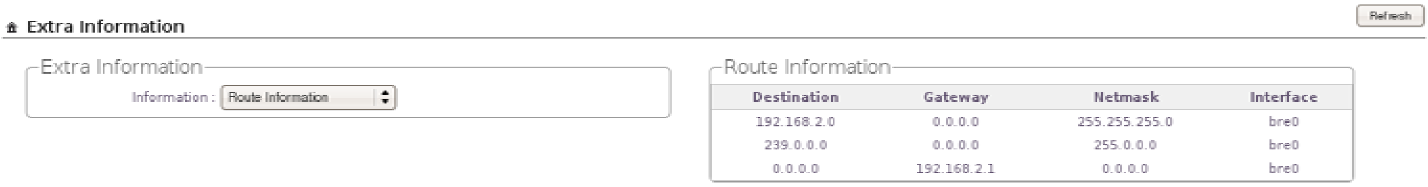
WDS Monitor

MAC Address	RSSI	TX/RX Rate
00:11:a3:01:02:00	-1	1M / 0M

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

5.4.2 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

Information : Route Information

Route Information

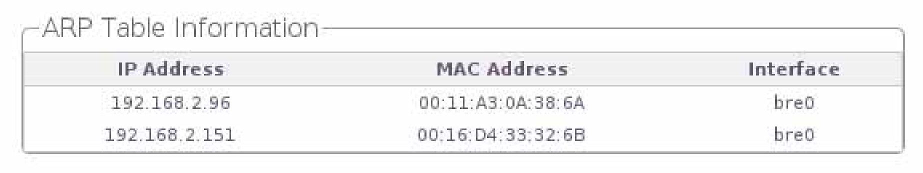
Destination	Gateway	Netmask	Interface
192.168.2.0	0.0.0.0	255.255.255.0	bre0
239.0.0.0	0.0.0.0	255.0.0.0	bre0
0.0.0.0	192.168.2.1	0.0.0.0	bre0

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

AP-952X 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.

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

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

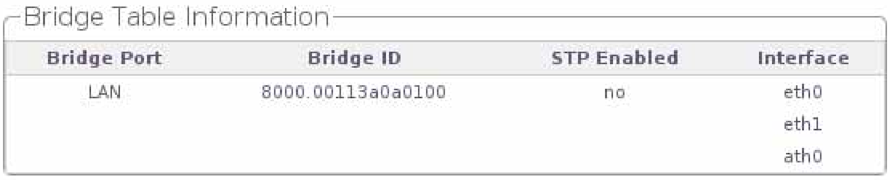


ARP Table Information

IP Address	MAC Address	Interface
192.168.2.96	00:11:A3:0A:38:6A	bre0
192.168.2.151	00:16:D4:33:32:6B	bre0

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

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, eth1, ath0).



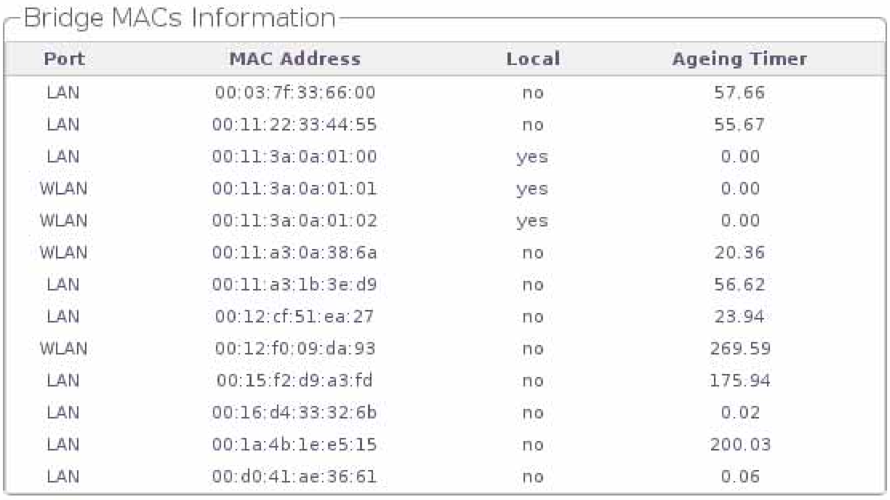
Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
LAN	8000.00113a0a0100	no	eth0 eth1 ath0

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

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

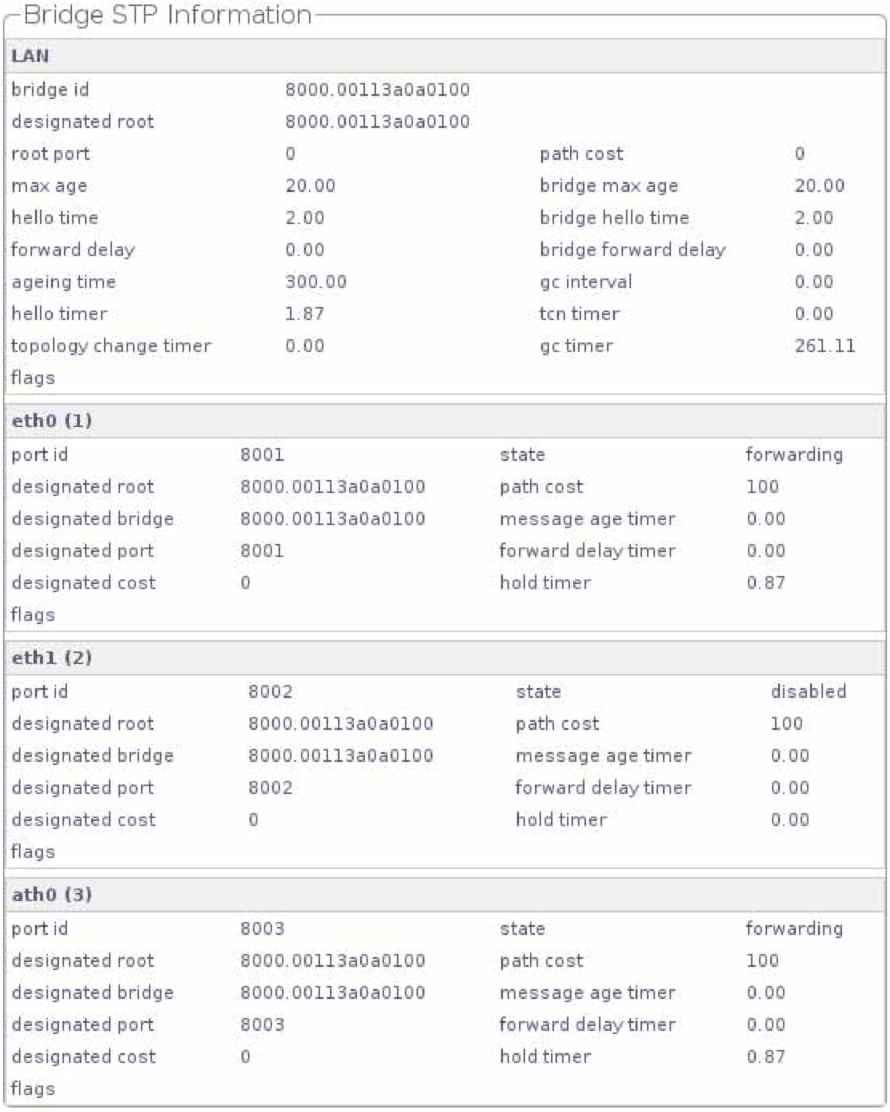
Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC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



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:03:7f:33:66:00	no	57.66
LAN	00:11:22:33:44:55	no	55.67
LAN	00:11:3a:0a:01:00	yes	0.00
WLAN	00:11:3a:0a:01:01	yes	0.00
WLAN	00:11:3a:0a:01:02	yes	0.00
WLAN	00:11:a3:0a:38:6a	no	20.36
LAN	00:11:a3:1b:3e:d9	no	56.62
LAN	00:12:cf:51:ea:27	no	23.94
WLAN	00:12:f0:09:da:93	no	269.59
LAN	00:15:f2:d9:a3:fd	no	175.94
LAN	00:16:d4:33:32:6b	no	0.02
LAN	00:1a:4b:1e:e5:15	no	200.03
LAN	00:d0:41:ae:36:61	no	0.06

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



Bridge STP Information

LAN

bridge id	8000.00113a0a0100		
designated root	8000.00113a0a0100		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	0.00	bridge forward delay	0.00
ageing time	300.00	gc interval	0.00
hello timer	1.87	tcn timer	0.00
topology change timer	0.00	gc timer	261.11
flags			

eth0 (1)

port id	8001	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

eth1 (2)

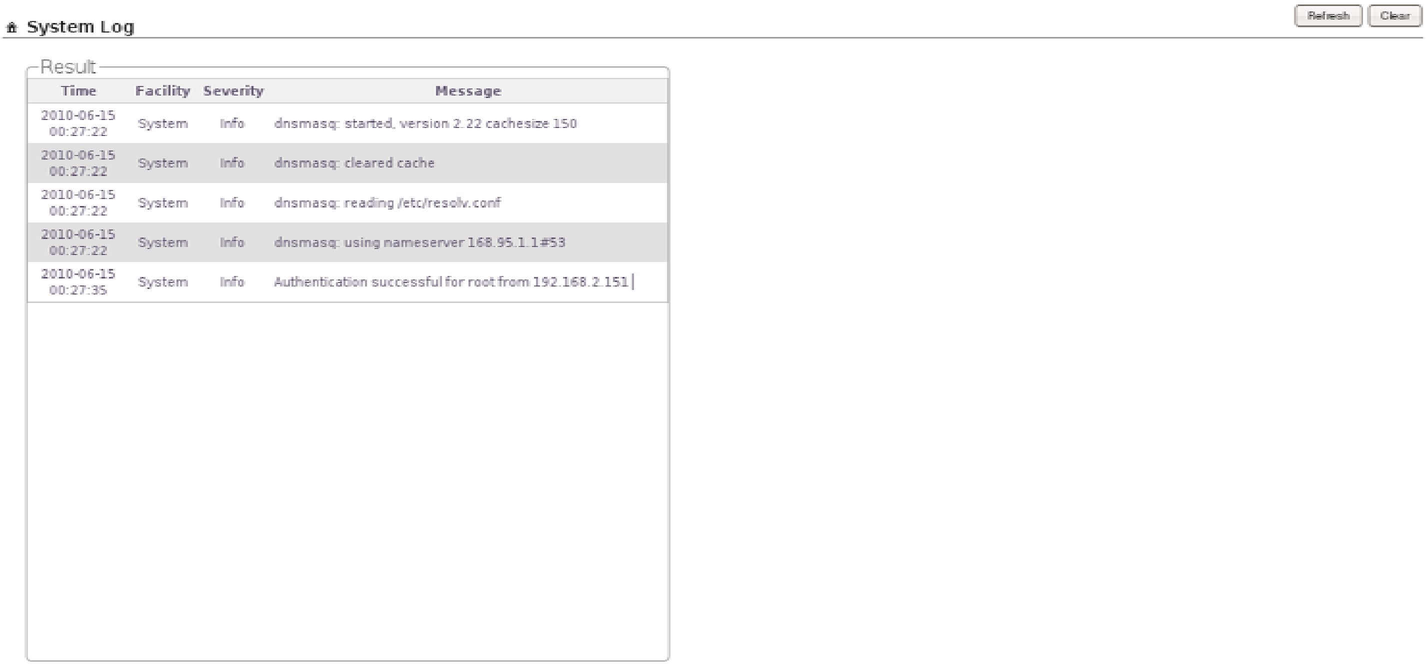
port id	8002	state	disabled
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ath0 (3)

port id	8003	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

5.4.3 Event Log

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



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

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

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

Appendix A. Web GUI valid Characters

Table A Web GUI Valid Characters

Block	**Field**	**Valid Characters**
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254

Block	**Field**	**Valid Characters**
	Hostname	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	DNS	IP Format; 1-254
Management	System Name	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	Length : 45 chars Space
	Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Port	1 ~ 65535
	IP Address To Ping	IP Format; 1-254
	Ping Interval	60 ~ 3600, default is 300
	Startup Delay	60 ~ 3600, default is 300
	Failure Count To Reboot	1 ~ 99 , default is 3
SNMP	RO/ RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	IP Format; 1-254

Table A Web GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
General Setup	Aggregation Frames	2-64, default is 32
	Aggregation Size	1024-65535, default is 50000
Advanced Setup	Beacon Interval	40 ~ 3500
	DTIM Interval	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347
Virtual AP Setup	ESSID	Length : 1-31 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII chars
	Group Key Update Period	>=10 seconds, default is 600
	Master Key Update Period	>= 10 seconds, default is 86400
	WEP Key Update Period	>=0 seconds, default is 300, 0 is disable
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	1 ~ 64 characters
	EAP Reauth Period	>= 0 seconds; 0 is disable, default is 3600
WDS Setup	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII chars
	AES Key	32 Hex chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars Space

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

SAR compliance has been established in typical laptop computer(s) with USB slot, and product could be used in typical laptop computer with USB slot. Other application like handheld PC or similar device has not been verified and may not compliance with

related RF exposure rule and such use shall be prohibited.

CE CAUTION

European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835 GHz; In France, the equipment must be restricted to the 2.4465-2.4835 GHz frequency range and must be restricted to indoor use.

For the following equipment: Wireless AP

EAP200, EAP206

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC), Low-voltage Directive (2006/95/EEC) and the Amendment Directive (93/68/EEC), the procedures given in European Council Directive 99/5/EC and 89/3360EEC.

The equipment was passed. The test was performed according to the following European standards:

EN 300 328 V1.6.1

EN 301 489-17/-1 V.1.2.1/V1.4.1

EN 50385

EN 60950-1: 2001 + A11

E=6.05603 V/m is the maximum E-Field strength when safety distance between the EUT and human body is maintained at least 20cm, which is below 61V/m