



WAB-3003
108M 11g Outdoor PoE AP

User's Manual v1.1



Regulatory Information



Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive) for

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Model: WAB-3003

For 2.4 GHz radios, the devices have been tested and passed the requirements of the following standards, and hence fulfills the EMC and safety requirements of R&TTE Directive within the CE marking requirement.

- Radio: EN 300.328:2006
- Radio: EN 50392:2004
- EMC: EN 301.489-1:2005, EN 301.489-17:2002,
- EMC: EN 55022:2006 Class B, EN 55024:1998 + A1:2001 + A2:2003 including the followings:
 - EN 61000-3-2, EN 61000-3-3.
 - EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,
 - EN 61000-4-5, EN 61000-4-6, EN 61000-4-11
- Safety: EN 60950-1:2001 + A11:2004,

Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 Functionalities	4
1.3 Document Conventions	5
2. System Overview	6
2.1 Package Contents	6
2.2 Panel Function Description	7
3. Installation	8
3.1 Hardware Installation	8
3.2 Basic Configuration	9
3.2.1 Introduction to Web Management Interface	9
3.2.2 Quick Configuration	11
4. AP Mode Configuration	16
4.1 System	18
4.1.1 System Information	19
4.1.2 Network Settings	21
4.1.3 Management Services	22
4.1.5 QoS Classification	24
4.2 Wireless	25
4.2.1 Virtual AP Overview	26
4.2.2 General Settings	27
4.2.3 VAP Configuration	29
4.2.4 Security Settings	30
4.2.5 Advanced Wireless Settings	34
4.2.6 Access Control Settings	36
4.3 Firewall	40
4.3.1 Layer 2 Firewall Settings	40
4.3.2 Firewall Service	45
4.3.3 Advanced Firewall Settings	46
4.4 Utilities	47
4.4.1 Change Password	48
4.4.2 Network Utilities	49
4.4.3 Configuration Save & Restore	50
4.4.4 System Upgrade	51
4.4.5 Reboot	52
4.5 Status	53
4.5.1 System Overview	54
4.5.2 Associated Client Status	56
4.5.3 Event Log	57
4.6 Online Help	58

1. Introduction

1.1 Overview

This manual is designed for **system integrators**, **field engineers** and **network administrators** to set up **WAB-3003 108M 11g Outdoor PoE AP** in their network environments. It contains step-by-step procedures and graphic examples to guide users with networking knowledge to complete the installation.

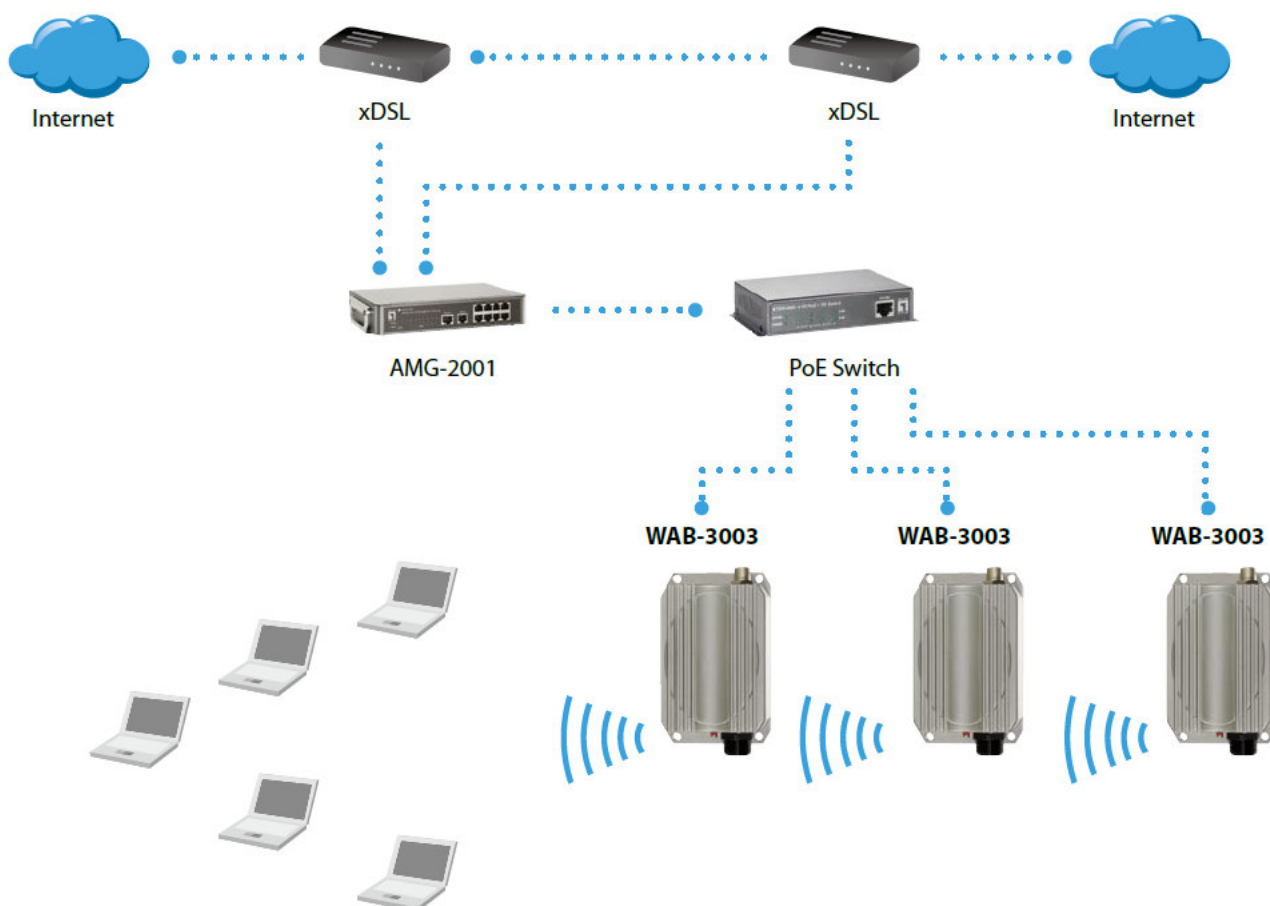


WAB-3003 (with N type antenna)

The 802.11 b/g compliant **WAB-3003** is a Last-Mile Broadband solution for Wireless Internet Service Provider (WISP). It can be deployed as a traditional fixed wireless Access Point (AP mode), either indoors or outdoors.

The **WAB-3003** is compact in size and weatherproof. Coming with a mounting kit, it can be mounted on a pole or wall. Specifically developed for outdoor usage, the fully-hardened, IP68-rated **WAB-3003** can withstand wind, rain, lightning, power surges, and extreme temperatures.

The following is a network diagram for a typical WISP application.



WAB-3003 Long range wireless transmission

The **WAB-3003** can be deployed in various environments, for example:



- Hot zones such as business districts, office complexes, airports, hotels, conference centers, recreation areas, and shopping malls.
- Outdoor access point for school campuses, enterprise campuses, or manufacture plants.
- Indoor access point for hotels, factories, or warehouses where metal industrial grade devices are preferred.
- Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
- Wireless coverage for indoor and outdoor ground for private resorts, acre estate/home's yards, or gulf course communities.



1.2 Functionalities

- Acts as a "**Wireless Modem**" to bring wireless bandwidth to home and office buildings.
- **Wireless Bandwidth Allocation** (uplink/downlink) delivered to each building depending on different subscription plans.
- Full range of **wireless security** mechanisms such as WEP, WPA and WPA2 (802.11i) that are important for enterprise wireless deployments.
- Acts as a **Home Router** for **IP Sharing** and firewall, all-in-one installation solution - no need for extra router.
- Purposely built rugged access point for harsh **outdoor / industrial** conditions.
- **Weatherproof** and watertight from its rugged aluminum housing (IP68 Approved).
- **Power over Ethernet (PoE)** built-in for single cable installation.
- On board **Ethernet surge protection**.

1.3 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

2. System Overview

2.1 Package Contents

The standard package of **WAB-3003** includes:

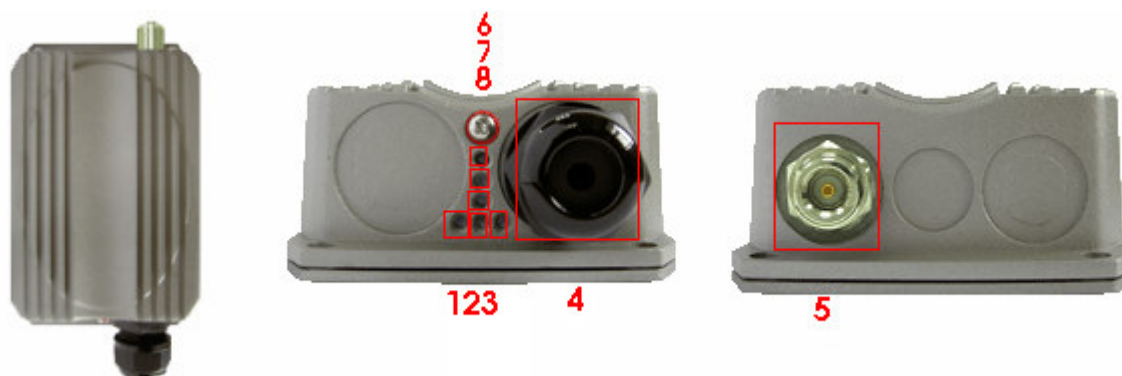
- **WAB-3003** x 1
- Quick Installation Guide (QIG) x 1
- CD-ROM (with User's Manual and QIG) x 1
- PSE with AC cable x 1
- Mounting Kit x 1
- Water Proof Connector (installed) x 1

Caution:

It is highly recommended to use all the components supplied to ensure best performance of the system.

2.2 Panel Function Description

WAB-3003

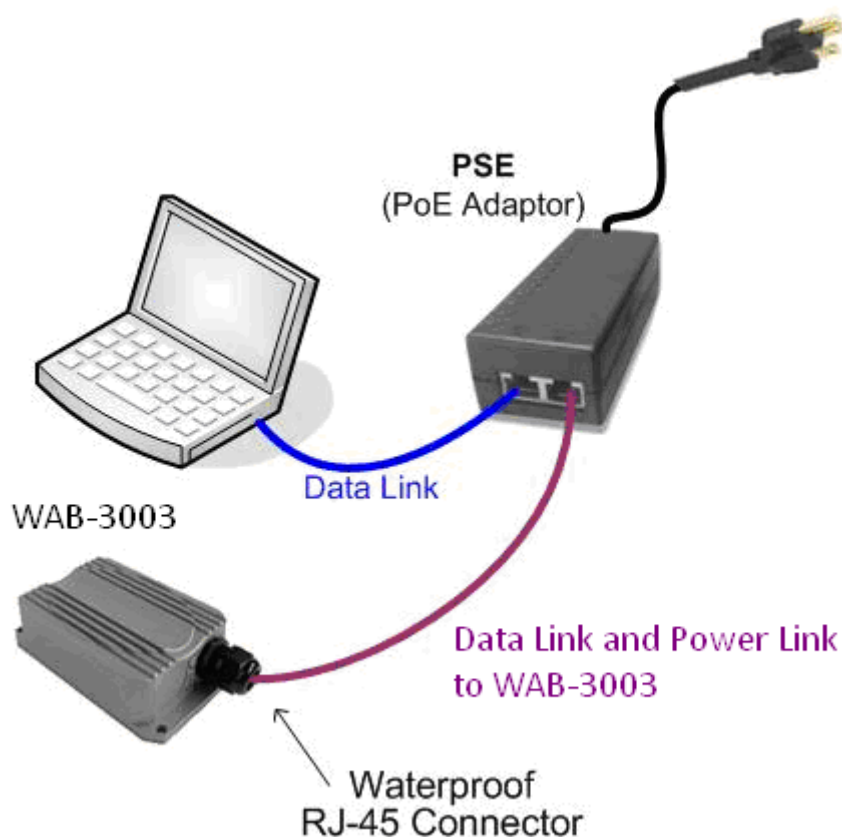


1	WLAN	Green LED ON indicates system ready
2	Wireless Signal Strength	For showing the signal strength situation
3	Ethernet	Green LED ON indicates connection, OFF indicates no connection, and BLINKING indicates transmitting data.
4	PoE Connector	For connecting to the Power Sourcing Equipment (PSE)
5	N-type Connector	For connecting to an antenna
6	Power	Red LED ON indicates power on, and OFF indicates power off
7~8	Wireless Signal Strength	For showing the signal strength situation (7: Yellow; 8: Green)

3. Installation

3.1 Hardware Installation

The following diagram is a **basic network topology** which can be used for testing and configuring the **WAB-3003**.



Installation Steps:

- Step 1.** Connect an antenna to the connector.
- Step 2.** Connect the PSE (POWER & DATA OUT) to the PSE 1 connector on the lower panel.
- Step 3.** Connect one end of an Ethernet cable to the PSE 2 connector on the lower panel and connect the other end to a computer.
- Step 4.** Connect the power cord to the PSE.
- Step 5.** Power on the PSE in order to supply power to the **WAB-3003**.

3.2 Basic Configuration

3.2.1 Introduction to Web Management Interface

WAB-3003 provides a user friendly web management interface for configuration. It is required to follow the respective installation procedures provided to properly set up the desired mode for this system.

- **Default IP Address of Web Management Interface:**

The default IP address and Subnet Mask are as follows:

Mode	AP Mode
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

- **Default User Name and Password:**

The default **User name** and **Password** for the **root** and **admin** accounts are as follows:

Mode	AP Mode
Management Account	Root Account
User Name	root
Password	admin

Step 1: IP Segment Set-up for Administrator PC

Set a static IP address on the same subnet mask as **WAB-3003** in TCP/IP of the administrator PC, such as the following example. Do not duplicate the IP address used here with the IP address of **WAB-3003** or any other devices within the same network.

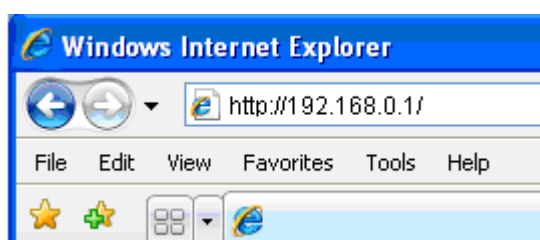
>> Example of IP Segment:

The valid range of IP address is 1 ~ 254. However, **1** must be avoided as it is already used by **WAB-3003**. Below depicts an example of using **100** (the underlined value can be changed as desired).

- IP Address: 192.168.0.100
- Subnet Mask: 255.255.255.0

Step 2: Launch Web Browser

Launch a web browser to access the web management interface of AP mode by entering the default IP address, **http://192.168.0.1/**, in the URL field, and then press **Enter**.



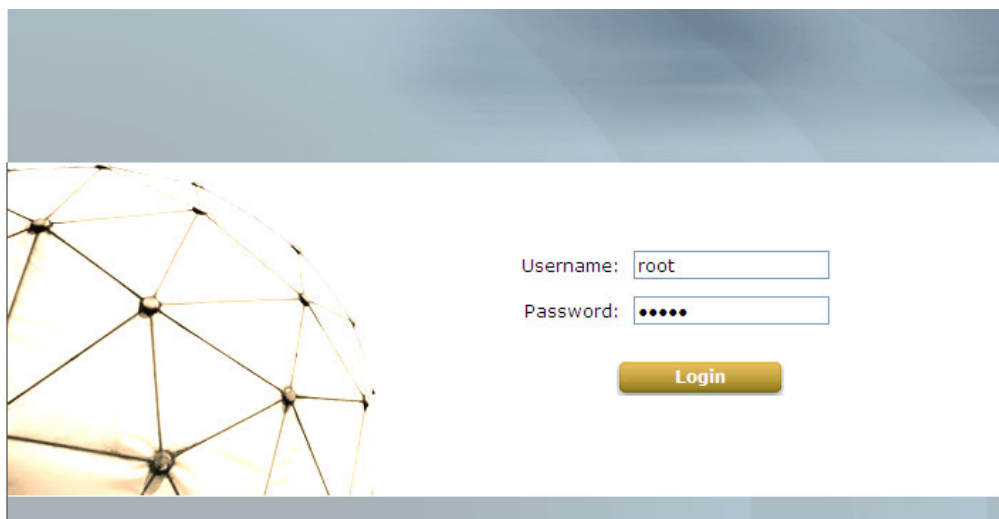
Caution:

Using an incorrect default IP address will result in no Login page shown on the web browser. Please make sure a correct IP address is used for the desired mode; refer to **Section 3.2.1 Instruction to Web Management Interface** for detailed default IP addresses.

Step 3: System Login


The system manager Login Page will then appear.


Enter **"root"** in the *User name* field and **"admin"** in the *Password* field, and then click **OK** to log in.


**Step 4: Login Success**


The **System Overview** page will appear after a successful login.


To logout, simply click on the Logout button on the top right hand corner of the management interface.


System


Wireless


Firewall


Utilities


Status

Overview

Clients

Repeater

Event Log

Home > Status > System Overview

System Overview

System

System Name	
Firmware Version	4.10.00
Build Number	1.5-1.2393
Location	
Site	EN-A
Device Time	1999/12/31 16:20:23
System Up Time	0 days, 0:20:23
Operating Mode	AP

Radio Status

MAC Address	00:1F:D4:00:21:25
Band	802.11b+g
Channel	1
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:00:21:24
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:21:25	VAP-1	None	0

Note:

By default, AP mode is enabled. Therefore, the administrator must login to the system via the AP mode login page at the first time. The administrator is then able to switch between modes afterwards. For information on switching between modes, please refer to **Section 4.1.2 Operating Mode**.

3.2.2 Quick Configuration

This section provides a step-by-step configuration procedure for installing WAB-3003.

Step 1: Mode Confirmation

Home > Status > System Overview

System Overview

System

System Name	
Firmware Version	4.10.00
Build Number	1.5-1.2393
Location	
Site	EN-A
Device Time	1999/12/31 17:23:26
System Up Time	0 days, 1:23:26
Operating Mode	AP

Radio Status

MAC Address	00:1F:D4:00:21:25
Band	802.11b+g
Channel	1
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:00:21:24
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:21:25	VAP-1	None	0

- Ensure that the *Operating Mode* is currently at **AP** mode.
- Click on the **Status** button and then select the **System Overview** tab. The *Operating Mode* is at the **System** section on the **System Overview** page.

Note:

For more information on switching to AP mode, if it is not currently active, please refer to **AP Mode Section 4.1.2 Operating Mode**.

Step 2: Change Password

System Wireless Firewall **Utilities** Status

Change Password Network Utilities Config Save & Restore System Upgrade Reboot

Home > Utilities > Change Password

Change Password

Name : root

Old Password : ●●●●

New Password : ●●●● *up to 32 characters

Re-enter New Password : ●●●●

SAVE CLEAR

- Click on the **Utilities** button and then select the **Password** tab.
- Enter a new password in the *New Password* field and retype it in the *Re-enter New Password* field.
- Click **SAVE** to save the changes.

Step 3: Network Settings

System Wireless Firewall Utilities Status

System Information Operating Mode **Network** Management QoS Classification

Home > System > Network Interface

Network Settings

Mode : Static DHCP

IP Address : 192.168.0.1 *

Netmask : 255.255.255.0 *

Default Gateway : 192.168.0.254 *

Primary DNS Server : 168.95.1.1 *

Alternate DNS Server :

Layer2 STP : Disable Enable

SAVE CLEAR

【Settings here are for example only. 】

- Click on the **System** button and then select the **Network** tab.

- Enable *Static*, and then enter the related information in the fields marked with red asterisks.
- Click **SAVE** to save the settings.

Step 4: SSID Settings

The screenshot shows a web interface for configuring a wireless network. At the top, there are five main menu buttons: System, Wireless, Firewall, Utilities, and Status. The 'Wireless' button is highlighted with a red box. Below these are sub-menu tabs: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The 'General' tab is selected and highlighted with a red box. The breadcrumb path is 'Home > Wireless > General'. The main content area is titled 'General Settings' and contains the following configuration options:

- Band :** 802.11b+802.11g (dropdown menu)
- Super G :** Bursting Fast Frames Dynamic Turbo
- Short Preamble :** Disable Enable
- Channel :** 1 (dropdown menu)
- Max Transmit Rate :** Auto (dropdown menu)
- Transmit Power :** Auto (dropdown menu)

At the bottom of the settings area, there are two yellow buttons: **SAVE** and **CLEAR**.

- Click on the **Wireless** button and then select the **General** tab.
- **Band:** Select an appropriate band from the drop-down list box.
- Click **SAVE** to save the settings.

Step 5: Security Settings

Home > Wireless > Security

Security Settings

Profile Name :

Security Type :

Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.

802.11 Authentication: Open System Shared Key Auto

WEP Key Length : 64 bits 128 bits 152 bits

WEP Key Format : ASCII Hex

WEP Key Index :

WEP Keys :

1

2

3

4

- Click on the **Wireless** button and then select the **Security** tab.
- Select the desired *VAP Profile and Security Type* from the drop-down list boxes. The above figure depicts an example of selecting VAP-1 and **WEP**.
- Enter the information required in the blank fields.

Caution:

*You must use the same information provided here to configure the network devices that are to be associated with **WAB-3003**.*

- Click **SAVE** to save all settings configured so far; all updated settings will take effect upon reboot.

Congratulations!


WAB-3003 is now successfully configured.


4.AP Mode Configuration


When AP mode is activated, the system can be configured as an Access Point. This chapter will guide you through setting up the AP mode with graphical illustrations. The following table shows all the functions of WAB-3003 in its AP mode.


OPTION	System	Wireless	Firewall	Utilities	Status
FUNCTION	System Information	VAP Overview	Firewall List	Change Password	System Overview
	Operating Mode	General Settings	Service	Network Utilities	Associate Client Status
	Network Settings	VAP Configuration	Advanced	Configuration Save & Restore	Repeater Information
	Management Services	Security Settings		System Upgrade	Event Log
	QoS Classification	Repeater Settings		Reboot	
		Advanced Wireless Settings			
		Access Control Settings			
		Site Survey			


Table 4-1: AP Mode Functions


System


Wireless


Firewall


Utilities


Status

Overview

Clients

Repeater

Event Log

Home > Status > System Overview

System Overview

System

System Name	
Firmware Version	4.10.00
Build Number	1.5-1.2393
Location	
Site	EN-A
Device Time	1999/12/31 17:31:51
System Up Time	0 days, 1:31:51
Operating Mode	AP

Radio Status

MAC Address	00:1F:D4:00:21:25
Band	802.11b+g
Channel	1
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:00:21:24
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:21:25	VAP-1	None	0

Figure 4-1: AP Mode Main Page

4.1 System

This section provides information for configuring the following functions: **System Information**, **Operating Mode**, **Network Settings**, **Management Services**, and **QoS Classification**.

The screenshot shows a web interface for configuring a system. At the top, there are five main menu buttons: System (highlighted with a red border), Wireless, Firewall, Utilities, and Status. Below these are sub-menu tabs: System Information, Operating Mode, Network, Management, and QoS Classification. The breadcrumb trail reads "Home > System > General".

System Information

Name : *

Description :

Location :

Time

Device Time : 1999/12/31 17:32:24

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

Note:

A system restart is required when a reminding message appears after clicking the **SAVE** button; all settings entered and saved will take effect only after the system restart.

4.1.1 System Information

For maintenance purpose, it is required to specify the system name, its location and corresponding basic parameters. Fields such as *Name*, *Description* and *Location* are used for mnemonic purpose. It is recommended to have different values in each AP.

System Information

Home > System > General

System Information

Name : *

Description :

Location :

Time

Device Time : 1999/12/31 17:32:24

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

SAVE **CLEAR**

- **System Information**

For maintenance purpose, it is recommended to have the following information stated as clearly as possible. Fields Name, Description, and Location are used for mnemonic purpose. It is recommended to have different values in each wireless device.

- *Name*: The system name used to identify this system
- *Description*: Further information of the system.
- *Location*: The information on geographical location of the system for the administrator to locate the system easily.

- **Time**

Time settings allow the system time synchronized with NTP server or manually set.

- *Device Time*: Display the current time of the system.
- *Time Zone*: Select an appropriate time zone from the drop-down list box.
- *Synchronization*: Synchronize the system time either by NTP server or manual setup.

(1) Enable NTP:

By selecting **Enable NTP**, WAB-3003 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided. If FQDN (full qualified domain name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **4.1.3 Network Settings**).

Time

Device Time : 1999/12/31 17:32:24

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time : Enable NTP Manually set up

NTP Server 1 : tock.stdtime.gov.tw *

NTP Server 2 :

(2) Manually set up:

By selecting *Manually set up*, the administrator can manually set the system date and time.

Time

Device Time : 1999/12/31 17:32:24

Time Zone : (GMT-08:00)Pacific Time(US&Canada),Tijuana

Time : Enable NTP Manually set up

Set Date : ---- Year -- Month -- Day

Set Time : -- Hour -- Min -- Sec

- *Set Date*: Select the appropriate *Year*, *Month*, and *Day* from the drop-down list box.
- *Set Time*: Select the appropriate *Hour*, *Min*, and *Sec* from the drop-down list box.

4.1.2 Network Settings

LAN settings can be configured on this page.

System Information Operating Mode **Network** Management QoS Classification

Home > System > Network Interface

Network Settings

Mode : Static DHCP

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Layer2 STP : Disable Enable

SAVE **CLEAR**

- **Mode:** Determine the way to obtain the IP address, by *DHCP* or *Static* manually set.
 - **Static:** Static setting is set these parameters manually. The basic parameters need to provide such as IP address, subnet mask and Gateway.
 - **IP Address:** The IP address of the LAN port.
 - **Netmask:** The Subnet mask of the LAN port.
 - **Gateway:** The Gateway IP address of the LAN port.
 - **Primary/Secondary DNS Server:** Please provide at least on DNS server's IP address.
 - **DHCP:** The option is provided when a DHCP server is provided in the network. The following IP address/Netmask/Gateway setting will be disabled.
- **Layer 2 STP:** Depends on the configuration of the system including wired and wireless settings, when it is configured to bring several networks, we need enable STP.

4.1.3 Management Services

The system supports **VLAN**, **SNMP**, **Remote Syslog**, and **Auto Reboot** functions for easy management. These functions can be configured on this page.

- **VLAN for Management:** The Ethernet traffic from the system can be tagged with VLAN tag with specific ID.
- **SNMP Configuration:** By enabling SNMP service, the remote SNMP manager could obtain the system status.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
 - **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
 - **Read:** Enter the community string to access the MIB with Read privilege.
 - **Write:** Enter the community string to access the MIB with Write privilege.
 - **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to an assigned server.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
 - **Server IP Address:** Enter the IP address of the assigned server for receiving the trap

report.

- **Syslog Configuration:** By enabling this function, specify a remote syslog server which could accept system log messages from the system remotely. Therefore, by reading the syslog message in the remote server, review activities of all installed the system in the network.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
 - **Server IP:** The IP address of the Syslog server for receiving the reported events.
 - **Server Port:** The port number of the Syslog server.
 - **Log Level:** Select the desired level of received events from the drop-down list box.

- **Auto Reboot:** The option can be enabled to reboot system automatically with preferred Reboot Time from drop-down list.
 - **Enable/ Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
 - **Reboot Time:** Select an appropriate time from the drop-down list box. Since all users on the network will be disconnected during reboot, it is suggested to set the reboot time during an off-peak period to reduce impacts on online users.

4.1.5 QoS Classification

The system supports function of QoS classification where specified **VLAN ID** can be assigned to a specific **QoS access category** for priority handling of traffics.

System Information
Operating Mode
Network
Management
QoS Classification

Home > System > QoS Classification

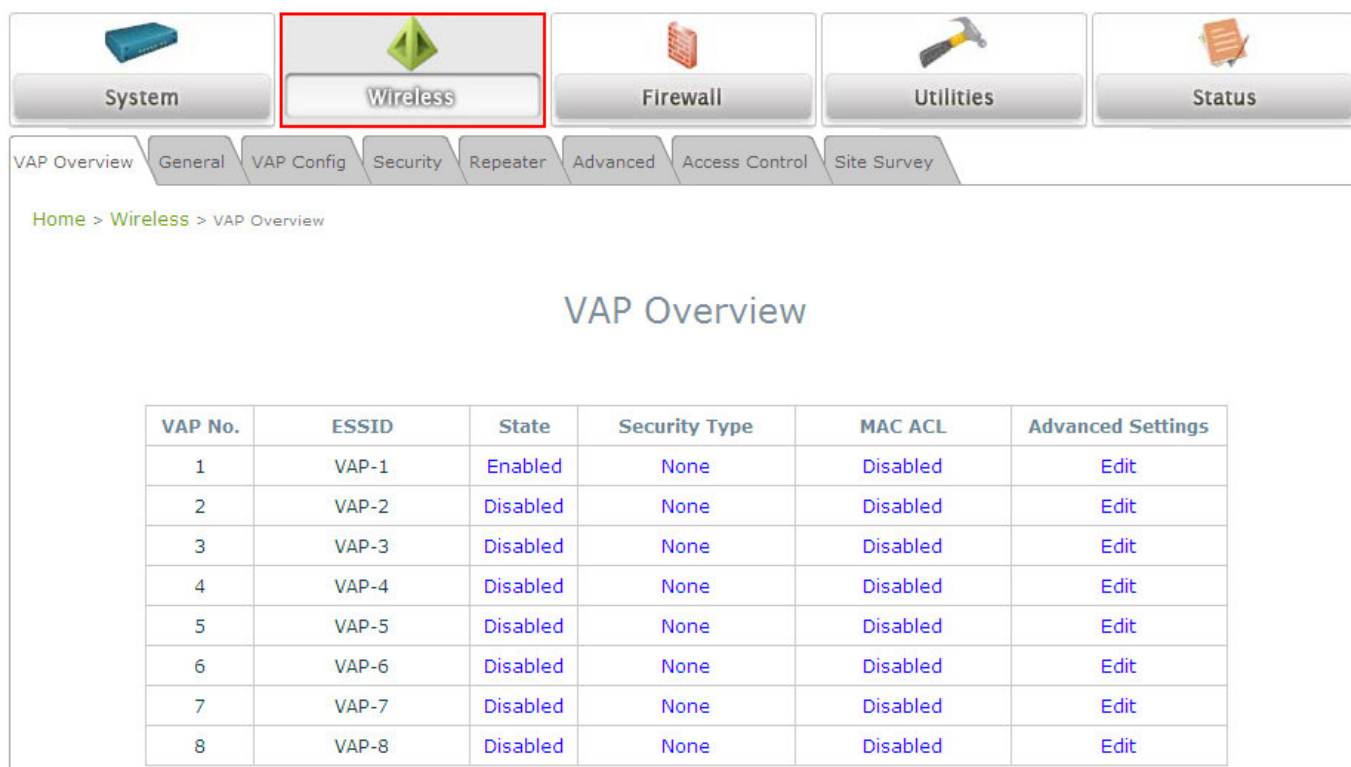
QoS Classification

No.	VLAN ID	QoS Access Category	Remark
1	<input type="text" value="0"/>	Best Effort ▼	<input type="text"/>
2	<input type="text"/>	Best Effort ▼	<input type="text"/>
3	<input type="text"/>	Best Effort ▼	<input type="text"/>
4	<input type="text"/>	Best Effort ▼	<input type="text"/>
5	<input type="text"/>	Best Effort ▼	<input type="text"/>
6	<input type="text"/>	Best Effort ▼	<input type="text"/>
7	<input type="text"/>	Best Effort ▼	<input type="text"/>
8	<input type="text"/>	Best Effort ▼	<input type="text"/>
9	<input type="text"/>	Best Effort ▼	<input type="text"/>

SAVE
CLEAR

4.2 Wireless

The administrator can configure the following wireless settings on this page: **VAP Overview**, **General Settings**, **VAP Configuration**, **Security Settings**, **Advanced Wireless Settings**, **Access Control Settings**, and **Site Survey**. The system supports up to eight Virtual Access Points (VAPs). Each VAP can have its own settings including ESSID, VLAN ID, security settings, etc. Such VAP capability enables different levels of service to meet actual requirements.



The screenshot displays the configuration interface for the Wireless section. At the top, there are five main menu buttons: System, Wireless (highlighted with a red border), Firewall, Utilities, and Status. Below these are sub-menu tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail shows 'Home > Wireless > VAP Overview'. The main heading is 'VAP Overview', and below it is a table listing eight VAPs.

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	VAP-1	Enabled	None	Disabled	Edit
2	VAP-2	Disabled	None	Disabled	Edit
3	VAP-3	Disabled	None	Disabled	Edit
4	VAP-4	Disabled	None	Disabled	Edit
5	VAP-5	Disabled	None	Disabled	Edit
6	VAP-6	Disabled	None	Disabled	Edit
7	VAP-7	Disabled	None	Disabled	Edit
8	VAP-8	Disabled	None	Disabled	Edit

4.2.1 Virtual AP Overview

An overall status is collected in this page, including *Enable/Disable State*, *Security Type*, *MAC ACL* state, and *Advanced Settings*. The system has 8 VAPs; each has its own settings. In this table, please click on the hyperlink for further configuration of each VAP respectively.

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	VAP-1	Enabled	None	Disabled	Edit
2	VAP-2	Disabled	None	Disabled	Edit
3	VAP-3	Disabled	None	Disabled	Edit
4	VAP-4	Disabled	None	Disabled	Edit
5	VAP-5	Disabled	None	Disabled	Edit
6	VAP-6	Disabled	None	Disabled	Edit
7	VAP-7	Disabled	None	Disabled	Edit
8	VAP-8	Disabled	None	Disabled	Edit

- **State:** The hyperlink showing *Enable* or *Disable* connects to the screen of **VAP Configuration**.
- **Security Type:** The hyperlink showing security type connects to the screen of **Security Settings**.
- **MAC ACL:** The hyperlink showing *Allow* or *Disable* connects to the screen of **Access Control Settings**.
- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

4.2.2 General Settings

This section is for configuring the system RF settings.

Home > Wireless > General

General Settings

Band : 802.11b+802.11g

Super G : Bursting Fast Frames Dynamic Turbo

Short Preamble : Disable Enable

Channel : 1

Max Transmit Rate : Auto

Transmit Power : Auto

SAVE **CLEAR**

- **Band:** Select an appropriate wireless frequency band of this system. Select one frequency band from *Disable*, *802.11b*, *802.11g* or mixed mode *802.11b+802.11g*.
- **Super G:** Options of Bursting, Fast Frames, and Atheros' featured Dynamic Turbo can be selected to boost wireless throughput.
- **Short Preamble:** The option can be turned on the enable Short-Preamble frames.
- **Channel:** Select the appropriate channel from the drop-down list box to correspond with your network settings, for example, Channel 1-11 is available in North America and Channel 1-13 in Europe, or choose the default *Auto*.
- **Max Transmit Rate:** Select transmit rate from *1M* to *54M* or *Auto*.
- **Transmit Power:** Select from the lowest to highest power level or choose *Auto*.

The RF settings in this page will be applied to all VAPs.

Under normal circumstances, the available RF configurations are illustrated as below:

Band	Super G	Short Preamble	Channel	Max Transmit Rate	Transmit Power
Disable	N/A	N/A	N/A	N/A	N/A
802.11b	N/A	Disable/Enable	Auto, 1~11, 13, or 14	1M, 2M, 5.5M, 11M	Auto, Lowest, Low, Medium, High, Highest
802.11g	Bursting, Compression, Fast Frames, Dynamic Turbo	Disable/Enable	Auto, 1~11 or 13	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11b+802.11g	Bursting, Compression, Fast Frames, Dynamic Turbo	Disable/Enable	Auto, 1~11, 13, or 14	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M	

4.2.3 VAP Configuration

Home > Wireless > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : VAP-1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

SAVE CLEAR

To enable each VAP, the administrator must configure each VAP manually. The settings of each VAP are collected as its profile.

- **Enable VAP:** Enable or disable VAP function.
- **Profile Name:** The profile name of each VAP for identity/management purpose.
- **ESSID:** ESSID (Extended Service Set ID) indicates a unique SSID used by a client device to associate with a specified VAP. ESSID determines the service level assigned to a client.
- **VLAN ID:** The system supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP must have a unique VLAN ID; valid values are ranged from 1 to 4094.

4.2.4 Security Settings

The system supports various user authentication and data encryption methods in each VAP profile. Thus the administrator can depend on the need to provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** No authentication is required.

The screenshot shows the 'Security Settings' page for profile 'VAP-1'. The 'Security Type' is set to 'None'. There are 'SAVE' and 'CLEAR' buttons at the bottom.

- **WEP:** WEP (Wired Equivalent Privacy) supports key length of 64/128/152 bits.

The screenshot shows the 'Security Settings' page for profile 'VAP-1' with 'Security Type' set to 'WEP'. It includes a note: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' Below the note are radio button options for '802.11 Authentication' (Open System, Shared Key, Auto), 'WEP Key Length' (64 bits, 128 bits, 152 bits), and 'WEP Key Format' (ASCII, Hex). There is a 'WEP Key Index' dropdown set to '1' and four input fields for 'WEP Keys' numbered 1 through 4. 'SAVE' and 'CLEAR' buttons are at the bottom.

- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select from *64-bit*, *128-bit*, or *152-bit* key length.
- **WEP Key Format:** Select from *ASCII* or *Hex* format for the WEP key.
- **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames during data

transmission.

- **WEP Keys:** Provide WEP key value; the system supports up to 4 sets of WEP keys.

- **802.1X:** Provide RADIUS authentication and enhanced WEP.

The screenshot displays the 'Security Settings' configuration page. At the top, there are navigation tabs: VAP Overview, General, VAP Config, Security (selected), Repeater, Advanced, Access Control, and Site Survey. Below the tabs, a breadcrumb trail reads 'Home > Wireless > Security'. The main heading is 'Security Settings'. The configuration is organized into sections:

- Profile Name:** A dropdown menu set to 'VAP-1'.
- Security Type:** A dropdown menu set to '802.1X'.
- Dynamic WEP:** Radio buttons for 'Disable' and 'Enable', with 'Enable' selected.
- WEP Key Length:** Radio buttons for '64 bits' and '128 bits', with '64 bits' selected.
- Rekeying Period:** A text input field containing '300' followed by 'second(s)'.
- Primary RADIUS Server:**
 - Host:** A text input field with a red asterisk and the text '(Domain Name / IP Address)'.
 - Authentication Port:** A text input field containing '1812' with a red asterisk.
 - Secret Key:** A text input field.
 - Accounting Service:** Radio buttons for 'Disable' and 'Enable', with 'Disable' selected.
 - Accounting Port:** A text input field containing '1813' with a red asterisk.
 - Accounting Interim Update Interval:** A text input field containing '60' followed by 'second(s)*'.
- Secondary RADIUS Server:**
 - Host:** A text input field with a red asterisk and the text '(Domain Name / IP Address)'.
 - Authentication Port:** A text input field containing '1812'.
 - Secret Key:** A text input field.
 - Accounting Service:** Radio buttons for 'Disable' and 'Enable', with 'Disable' selected.
 - Accounting Port:** A text input field containing '1813'.
 - Accounting Interim Update Interval:** A text input field containing '60' followed by 'second(s)'.

At the bottom of the form, there are two yellow buttons: 'SAVE' and 'CLEAR'.

➤ **Dynamic WEP Settings:**

- **Dynamic WEP:** By enabling this function, the system will automatically generate WEP keys for encryption.
- **WEP Key Length:** Select from 64-bit or 128-bit key length.
- **Rekeying Period:** The time interval for the WEP key to be updated; the time unit is in second.

➤ **Primary RADIUS Server Settings:**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enable or disable the accounting service.
- **Accountin Port:** The port number used by the RADIUS server. Specify a port number

or use the default, 1813.

- **Accounting Interim Update Interval:** The time interval for the accounting to be updated; the time unit is in second.
- **WPA-PSK:** Provide shared key authentication in WPA data encryption.

The screenshot shows the 'Security Settings' page for a VAP profile named 'VAP-1'. The page has a breadcrumb trail: Home > Wireless > Security. The settings are as follows:

- Profile Name:** VAP-1 (dropdown menu)
- Security Type:** WPA-PSK (dropdown menu)
- Cipher Suite:** TKIP (WPA) (dropdown menu)
- Pre-shared Key Type:** PSK(Hex)*(64 chars) Passphrase*(8 - 63 chars)
- Pre-shared Key:** [Empty text input field]
- Group Key Update Period:** 600 [text input field] second(s)

At the bottom of the form, there are two buttons: 'SAVE' and 'CLEAR'.

- **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
- **Pre-shared Key Type:** Select a pre-shared key type: *PSK (Hex)* or *Passphrase*.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in second.

- **WPA-RADIUS:** Authenticate users by RADIUS and provide WPA data encryption.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : WPA-RADIUS

Cipher Suite : TKIP (WPA)

Group Key Update Period: 600 second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key :

Accounting Service : Disable Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s) *

Secondary RADIUS Server :

Host: (Domain Name / IP Address)

Authentication Port: 1812

Secret Key:

Accounting Service: Disable Enable

Accounting Port: 1813

Accounting Interim Update Interval: 60 second(s)

➤ **WPA Settings:**

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

➤ **Primary RADIUS Server Settings:**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enable or disable the accounting service.
- **Accountin Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The time interval for the accounting to be updated; the time unit is in second.

4.2.5 Advanced Wireless Settings

The advanced wireless settings for the system's VAP profiles allow customization of data transmission settings. The administrator can tune the following parameters to improve network communication performance if a poor connection occurs.

Home > Wireless > Advanced

Advanced Wireless Settings

Profile Name : VAP-1

Beacon Interval : 100 *(100 - 500ms)

RTS Threshold : 2346 *(1 - 2346)

Fragment Threshold : 2346 *(256 - 2346)

Broadcast SSID : Disable Enable

Wireless Station Isolation : Disable Enable

WMM : Disable Enable

IAPP : Disable Enable

802.11g Protection : Disable Enable

SAVE CLEAR

- **Beacon Interval:** Enter a value between 100 and 500 ms. The default is 100 milliseconds. The specified value represents the amount of time between beacon signal transmissions.
- **RTS Threshold:** To control station access to the medium and to alleviate this effect of the hidden terminal problem, the administrator can tune this RTS threshold value. A lower RTS Threshold setting can be useful in areas where many client devices are associating with WAB-3003 or in areas where the clients are far apart and can detect only WAB-3003 and not each other.
- **Fragmentation Threshold:** A unicast frame larger than this threshold will be fragmented before transmission. If a significant number of collisions are occurring, the administrator can try to set a smaller value of the threshold to see whether it helps. A smaller value results in smaller packets but allows a larger number of packets in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
- **Broadcast SSID:** Disabling this function will prevent the system from broadcasting its SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect to the system.
- **Station Isolation:** By enabling this function, all stations associated with the system can only communicate with the system.
- **WMM:** The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that

prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than voice and video. In short, WMM decides which data streams are the most important and assign them a higher traffic priority.

< To receive the benefits of WMM QoS >

- The application must support WMM.
 - You must enable WMM in this system.
 - You must enable WMM in the wireless adapter in your computer.
- **IAPP:** IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations that are connected to them. By enabling this function, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.
 - **802.11g Protection:** When enabled, the associated 802.11g stations will benefit from this function since their transmission speed will not be affected by the surrounding 802.11b stations.

4.2.6 Access Control Settings

The administrator can restrict the wireless access of client devices based on their MAC addresses.

The screenshot shows the 'Access Control Settings' page in a web browser. At the top, there is a navigation menu with tabs: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control (selected), and Site Survey. Below the menu, the breadcrumb path is 'Home > Wireless > Access Control'. The main heading is 'Access Control Settings'. There are three configuration fields: 'Profile Name' is a dropdown menu set to 'VAP-1'; 'Maximum Number of Clients' is a text input field containing '32' with a red asterisk and the text '(Range: 1 ~ 32)' next to it; 'Access Control Type' is a dropdown menu set to 'Disable Access Control'. At the bottom, there are two yellow buttons: 'SAVE' and 'CLEAR'.

- **Maximum Number of Clients**

The system supports various methods of authenticating clients for using wireless LAN. The default policy is unlimited access without any authentication required. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, while the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

The selected **Access Control Type** will be the activated policy while the rest will be omitted. The following is a list of the supported methods for MAC ACL control:

- (1) **Disable Access Control**

No MAC address check required.

(2) MAC ACL Allow List

Deny all except those MAC addresses in the Allow List. When selecting *MAC ACL Allow List*, all wireless connections to the specified VAP will be denied except the MAC addresses listed in the Allow List ("allowed MAC addresses"). The administrator can disable any allowed MAC address to connect to the VAP temporarily by checking *Disable*. For example, 11:22:33:44:55:66 is in the Allow List; to temporarily deny its access, check *Disable* in the **State** section.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 32)

Access Control Type : MAC ACL Allow List

No.	MAC Address	State
1	11:22:33:44:55:66	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
2		<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3		<input checked="" type="radio"/> Disable <input type="radio"/> Enable

(3) MAC ACL Deny List

Allow all except those in the Deny List. When selecting *MAC ACL Deny List*, all wireless connections to the specified VAP will be allowed except the MAC addresses listed in the Deny List ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the VAP temporarily by checking *Enable*.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 *(Range: 1 ~ 32)

Access Control Type : MAC ACL Deny List

No.	MAC Address	State
1	1a:2b:3c:4d:5e:6f	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
2		<input checked="" type="radio"/> Disable <input type="radio"/> Enable
3		<input checked="" type="radio"/> Disable <input type="radio"/> Enable

(4) RADIUS ACL

Authenticate incoming MAC addresses by RADIUS. When selecting *RADIUS ACL*, all incoming MAC addresses will be authenticated by RADIUS. Please note that each VAP's MAC ACL and its security type (showing on the **Security Settings** page) share the same RADIUS configuration.

System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : *(Range: 1 ~ 32)

Access Control Type : RADIUS ACL

Primary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host: *(Domain Name / IP Address)

Authentication Port: *(1 - 65535)

Secret Key: *

Secondary RADIUS Server :

Host:

Authentication Port:

Secret Key:

SAVE CLEAR

4.3 Firewall

The system provides an added security feature, L2 firewall, in addition to typical AP security. Layer-2 firewall offers a firewall function that is tailored specifically for layer 2 traffics, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach.

4.3.1 Layer 2 Firewall Settings

It provides an overview of firewall rules in the system; 6 default rules with up to total 20 firewall rules are available for configuration.

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall Disable Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv
4	<input type="checkbox"/>	DROP	RIP	IPv4		Del Ed In Mv
5	<input type="checkbox"/>	DROP	HSRP	IPv4		Del Ed In Mv
6	<input type="checkbox"/>	DROP	OSPF	IPv4		Del Ed In Mv
7	<input type="checkbox"/>					Del Ed In Mv
8	<input type="checkbox"/>					Del Ed In Mv
9	<input type="checkbox"/>					Del Ed In Mv
10	<input type="checkbox"/>					Del Ed In Mv

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

From the overview table, each rule is designated with the following fields:

- ◆ **No.:** The numbering will decide the priority to let system carry out the available firewall rules in the table.
- ◆ **State:** The check marks will enable the respective rules.
- ◆ **Action:** "DROP" denotes a block rule; "ACCEPT" denotes a pass rule.
- ◆ **Name:** It shows the name of rule.

- ◆ **EtherType:** It denotes the type of traffics subject to this rule.
- ◆ **Remark:** It shows the note of this rule.
- ◆ **Setting:** 4 actions are available; "Del" denotes to delete the rule, "Ed" denotes to edit the rule, "In" denotes to insert a rule, and "Mv" denotes to move the rule.

>>To delete a specific rule,

"Del" in "Setting" column of firewall list will lead to the following page for removal confirmation. After "SAVE" button is clicked and system reboot, the rule will be removed.

The screenshot shows the 'Layer 2 Firewall Settings' page. At the top, there are tabs for 'Firewall List', 'Service', and 'Advanced'. Below the tabs, a breadcrumb trail reads 'Home > Firewall > Firewall List'. The main heading is 'Layer 2 Firewall Settings'. Below this, there is a section labeled 'Remove rule | 1'. At the bottom of the page, there are two yellow buttons: 'SAVE' and 'CLEAR'.

>>To edit a specific rule,

"Ed" in "Setting" column of firewall list will lead to the following page for detail configuration. From this page, the rule can be edited form scratch or from an existing rule for revision.

The screenshot shows the 'Layer 2 Firewall Configuration' page. At the top, there are tabs for 'Firewall List', 'Service', and 'Advanced'. Below the tabs, a breadcrumb trail reads 'Home > Firewall List > Rule Config'. The main heading is 'Layer 2 Firewall Configuration'. The configuration fields are as follows:

- Rule ID: 1
- Rule name: CDP and VTP *
- EtherType: IEEE802.3
- Interface: From (selected), To
- Interface: VAP1
- DSAP/SSAP: aa
- Type: 2000 (ie IPv4: 0800)
- Source: MAC Address: [] Mask: []
- Destination: MAC Address: 01:00:0C:CC:CC:CC Mask: []
- Action: Block (selected), Pass
- Remark: []

At the bottom of the page, there are two yellow buttons: 'SAVE' and 'CLEAR'.

- ◆ **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- ◆ **Rule name:** The rule name can be specified here.
- ◆ **EtherType:** The drop-down list will provide the available types of traffics (ALL, IPv4, IEEE802.3, 802.1Q, ARP, and RARP) subject to this rule.
- ◆ **Interface:** It can indicate inbound/outbound direction with desired interfaces (VAP1~VAP8)
- ◆ **Service (when EtherType is IPv4):** Select the available upper layer protocols/services from the drop-down list.
- ◆ **DSAP/SSAP (when EtherType is IEEE802.3):** The value can be further specified for the fields in 802.2 LLC frame header.
- ◆ **Type (when EtherType is IEEE802.3):** The field can be used to indicate the type of encapsulated traffics.
- ◆ **Vlan ID (when EtherType is 802.1Q):** The Vlan ID is provided to associate with certain VLAN-tagging traffics.
- ◆ **Priority (when EtherType is 802.1Q):** It denotes the priority level with associated VLAN traffics.
- ◆ **Encapsulated Type (when EtherType is 802.1Q):** It can be used to indicate the type of encapsulated traffics.
- ◆ **Opcode (when EtherType is ARP/RARP):** This list can be used to specify the ARP Opcode in ARP header.
- ◆ **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- ◆ **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- ◆ **Action:** The rule can be chosen to be "Block" or "Pass".
- ◆ **Remark:** The note of this rule can be specified here.

When the configuration for firewall rules is provided, please click "**SAVE**" and reboot system to let the firewall rules take effect.

>>To insert a specific rule,

"In" in "Setting" column of firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

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

Firewall List Service Advanced

Home > Firewall List > Rule Config

Layer 2 Firewall Configuration

Rule ID : 1

Rule name : CDP and VTP *

EtherType : IEEE802.3

Interface : From To

VAP1

DSAP/SSAP : aa

Type : 2000 (ie IPv4: 0800)

Source : MAC Address: Mask:

Destination : MAC Address: 01:00:0C:CC:CC:CC Mask:

Action : Block Pass

Remark :

SAVE CLEAR

>>To move a specific rule,

"Mv" in "Setting" column of firewall list will lead to the following page for re-ordering confirmation. After "SAVE" button is clicked and system reboot, the order of rules will be updated.

Firewall List Service Advanced

Home > Firewall > Move rule

Move Rule

ID : 1

Move to : Before After ID : *(1 - 20)

SAVE CLEAR

Please make sure all desired rules (state of rule) are **checked** and **saved** in overview page; the rule will be enforced upon system reboot.

Firewall List Service Advanced

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall
 Disable
 Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input checked="" type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv
4	<input type="checkbox"/>	DROP	RIP	IPv4		Del Ed In Mv
5	<input type="checkbox"/>	DROP	HSRP	IPv4		Del Ed In Mv
6	<input type="checkbox"/>	DROP	OSPF	IPv4		Del Ed In Mv
7	<input type="checkbox"/>					Del Ed In Mv
8	<input type="checkbox"/>					Del Ed In Mv
9	<input type="checkbox"/>					Del Ed In Mv
10	<input type="checkbox"/>					Del Ed In Mv

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

SAVE
CLEAR

Layer 2 Firewall Settings (Check State)

4.3.2 Firewall Service

The administrator can add or delete firewall services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

Firewall List
Service
Advanced

[Home](#) > [Firewall](#) > Service Config

Firewall Service

No.	Name	Description	Delete
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP	<input type="checkbox"/>
5	FTP	TCP/UDP, Destination Port: 20~21	<input type="checkbox"/>
6	HTTP	TCP/UDP, Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP, Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP, Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP, Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP, Destination Port: 67~68	<input type="checkbox"/>

[First](#) [Prev](#) [Next](#) [Last](#) (total: 28)

Overview of Firewall Services

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click SAVE to save the settings before leaving this page.

4.3.3 Advanced Firewall Settings

Advanced firewall settings are used to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of system.

Home > Firewall > Advanced

Advanced Firewall Settings

Trust Interface :

VAP1 VAP2 VAP3 VAP4 VAP5 VAP6 VAP7 VAP8

WDS1 WDS2 WDS3 WDS4

LAN

DHCP Snooping : Disable Enable

ARP Inspection : Disable Enable

Trust List Broadcast : Disable Enable

Static Trust List : Disable Enable

SAVE **CLEAR**

- ◆ **Trust Interface:** Each interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.
- ◆ **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rogue DHCP server.
- ◆ **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing. **Trust List Broadcast** can be enabled to let other WAB-3003 (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests. **Static Trust List** can be used to add MAC or MAC/IP pairs to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears in the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

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

4.4 Utilities

The administrator can maintain the system on this page: **Change Password, Network Utilities, Configuration Save & Restore, System Upgrade, and Reboot.**

The screenshot displays the web interface for the WAB-3003 108M 11g Outdoor PoE AP. At the top, there is a navigation bar with five main menu items: System, Wireless, Firewall, Utilities, and Status. The Utilities menu item is highlighted with a red border. Below this bar, there are sub-menu tabs for Change Password, Network Utilities, Config Save & Restore, System Upgrade, and Reboot. The main content area shows the breadcrumb path: Home > Utilities > Change Password. The title of the page is "Change Password". The form contains the following fields:

- Name : root
- Old Password : [password field]
- New Password : [password field] *up to 32 characters
- Re-enter New Password : [password field]

At the bottom of the form, there are two buttons: SAVE and CLEAR.

4.4.1 Change Password

The administrator can update or change password. The system provides one management account for AP mode, **root** account. The administrator can change password on this page.

The screenshot shows a web interface for changing a password. At the top, there are navigation tabs: "Change Password" (selected), "Network Utilities", "Config Save & Restore", "System Upgrade", and "Reboot". Below the tabs is a breadcrumb trail: "Home > Utilities > Change Password". The main heading is "Change Password". The form contains the following fields:

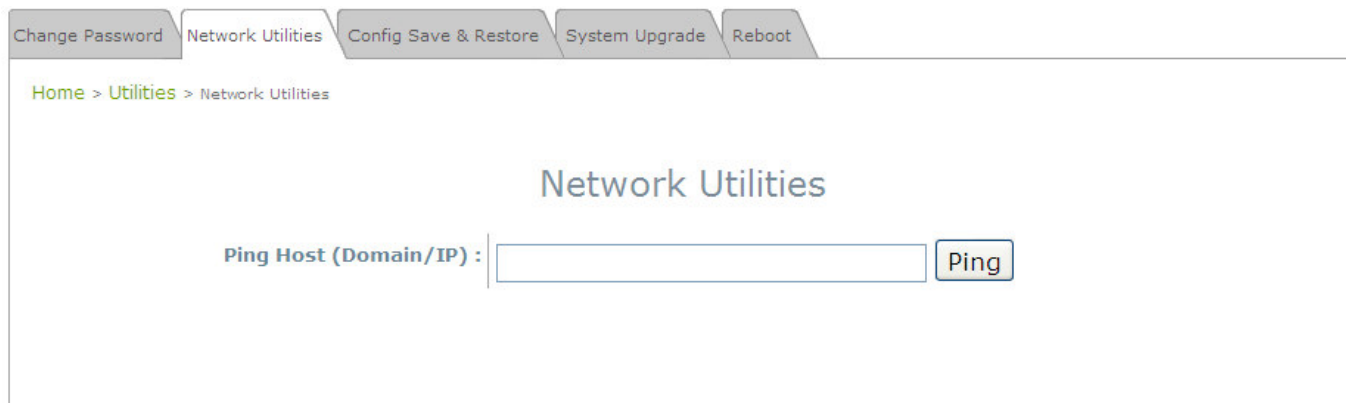
- Name :** root
- Old Password :** [password field with 5 dots]
- New Password :** [password field with 5 dots] *up to 32 characters
- Re-enter New Password :** [password field with 5 dots]

At the bottom of the form are two buttons: "SAVE" and "CLEAR".

- **"root" account:** Enter the original password ("**admin**") and a new password, and then re-enter the new password in the *Re-enter New Password* field. Click **SAVE** to save the new password.

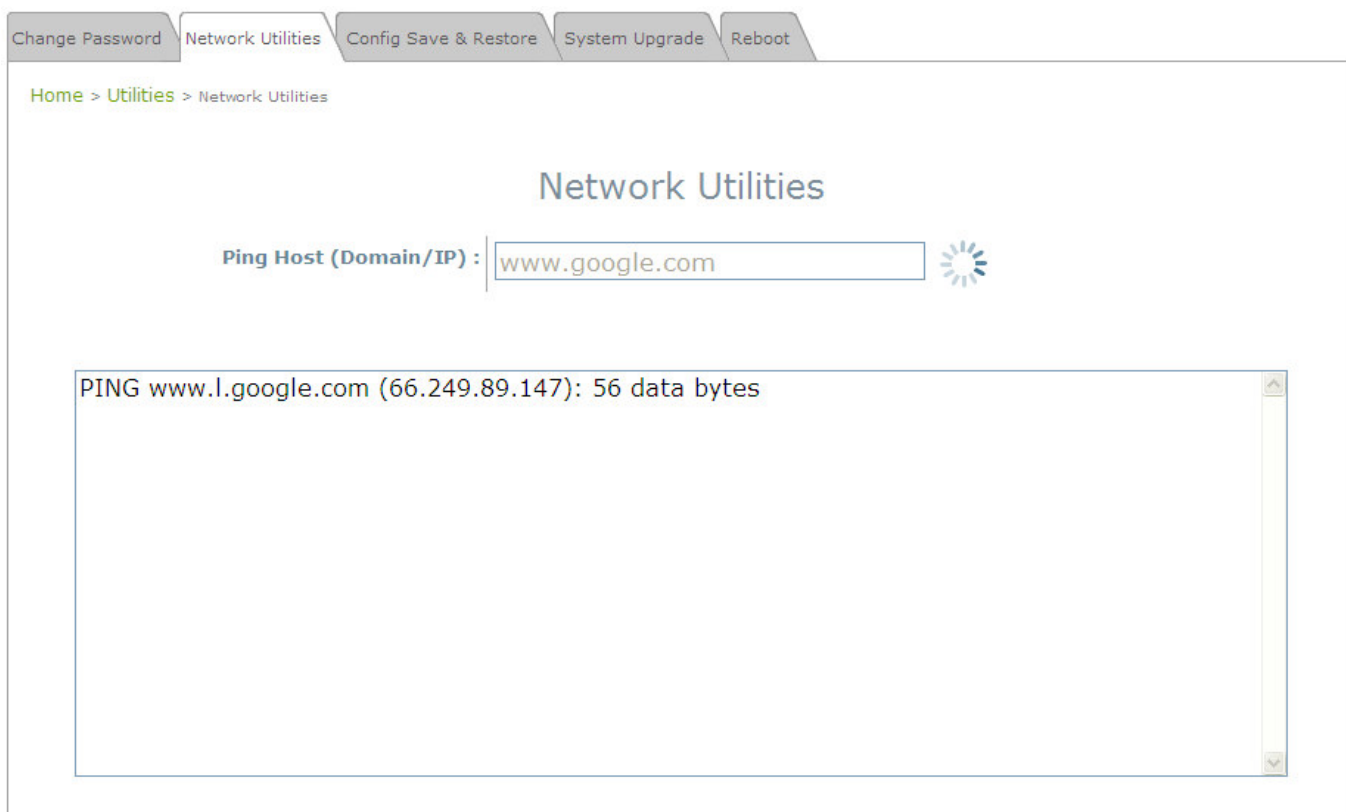
4.4.2 Network Utilities

The administrator can check the network connectivity via this function. The current provided network utility is Ping and the target host FQDN-compliant name or IP address can be provided to test network connection.



The screenshot shows the 'Network Utilities' page in a web interface. At the top, there are navigation tabs: 'Change Password', 'Network Utilities' (selected), 'Config Save & Restore', 'System Upgrade', and 'Reboot'. Below the tabs, a breadcrumb trail reads 'Home > Utilities > Network Utilities'. The main heading is 'Network Utilities'. Below this, there is a label 'Ping Host (Domain/IP) :' followed by an empty text input field and a 'Ping' button.

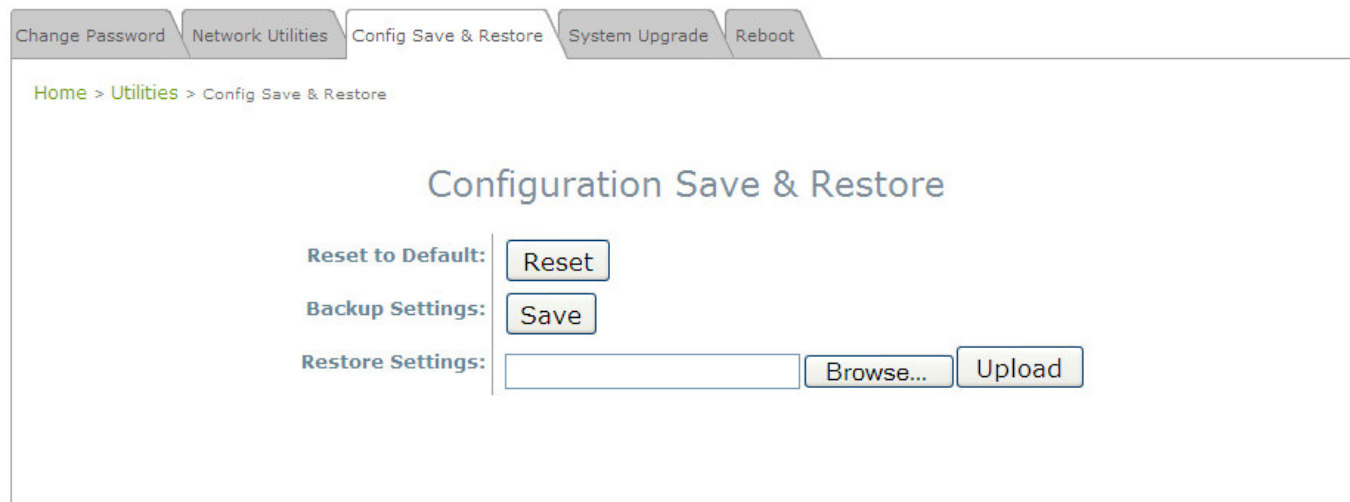
- **Ping Host (Domain/ IP):** Enter the domain name or IP address of a target device for diagnosis purpose, for example, www.google.com.tw, and click **Ping** to proceed. The ping result will be shown in the **Result** field.



The screenshot shows the 'Network Utilities' page after a ping test. The 'Ping Host (Domain/IP) :' label is followed by an input field containing 'www.google.com' and a loading spinner icon. Below this, a scrollable text area displays the result: 'PING www.l.google.com (66.249.89.147): 56 data bytes'. The rest of the page layout is identical to the previous screenshot.

4.4.3 Configuration Save & Restore

This function is used to backup or restore the current settings. The system can be restored to the default setting by clicking on Reset. The setting of the device can be backup to a file. It can be used to duplicate setting to the other WAB-3003 device.



- **Reset to Default:**

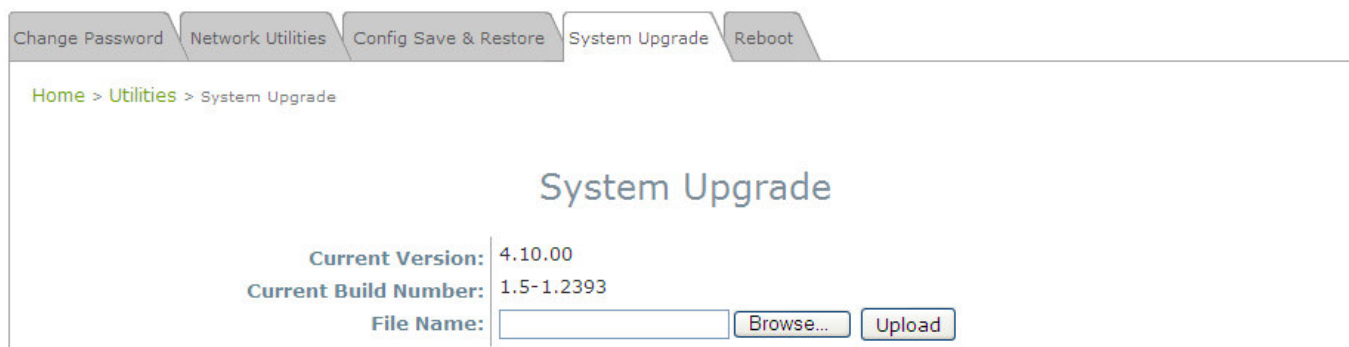
- Click **Reset** to load the factory default settings of WAB-3003. A pop-up screen will appear to reconfirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.



- A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.
 - The **System Overview** page will appear upon the completion of reboot.
- **Backup Settings:** Click **Save** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).
 - **Restore Settings:** Click **Browse** to search for a previously saved backup file, and then click **Upload** to restore the settings. The backup file will replace the active configuration file currently running on the system.

4.4.4 System Upgrade

To upgrade the system firmware, click **Browse** to search for the new firmware file, and then click **Apply** to execute the upgrade process. The first step is to acquire the correct firmware file and supply it in the User Interface field. During firmware update, please don't turn off the power to prevent from damaging the device permanently.



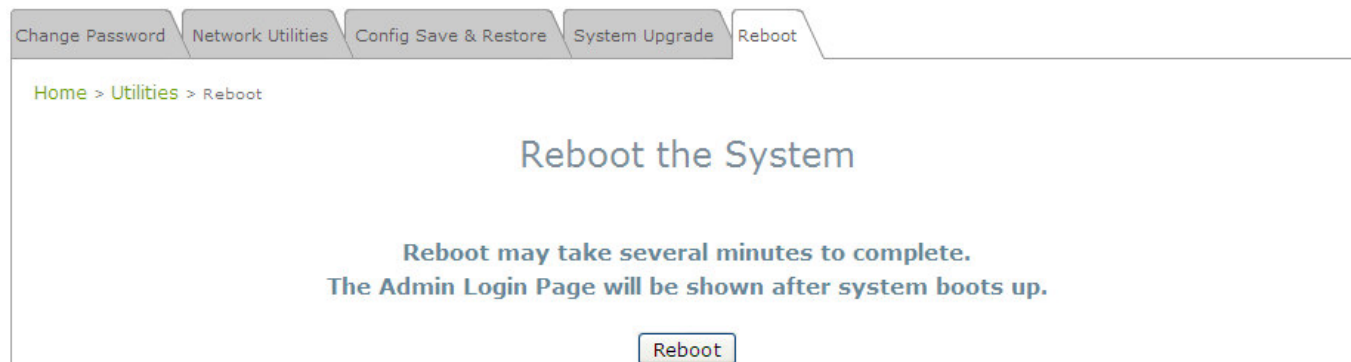
The screenshot shows a web interface for system upgrade. At the top, there are navigation tabs: Change Password, Network Utilities, Config Save & Restore, System Upgrade (selected), and Reboot. Below the tabs, a breadcrumb trail reads "Home > Utilities > System Upgrade". The main heading is "System Upgrade". Below this, the current system information is displayed: "Current Version: 4.10.00" and "Current Build Number: 1.5-1.2393". At the bottom, there is a "File Name:" label followed by an empty text input field, a "Browse..." button, and an "Upload" button.

Note:

- To prevent data loss during firmware upgrade, please back up the current settings before proceeding further.
- Please restart the system after the upgrade. Do not interrupt the system, i.e. power on/off, during the upgrade or restart process since it may cause damage to the system.

4.4.5 Reboot

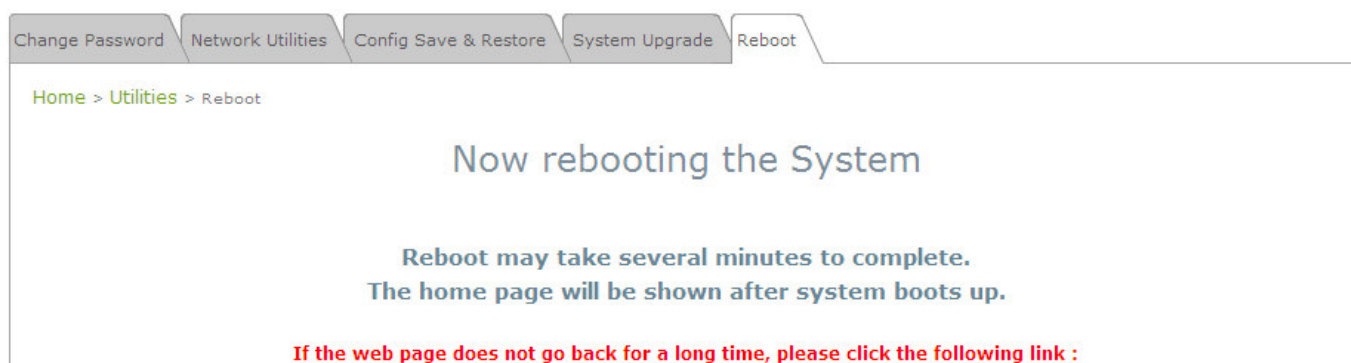
The administrator can reboot the device remotely. Click **Reboot** to restart the system immediately.



A pop-up screen will appear to confirm the request to restart the system. Click **OK** to proceed, or click **Cancel** to cancel the restart request.




A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.





The **System Overview** page will appear upon the completion of reboot.


4.5 Status


This section displays the status of **System Overview**, **Clients**, and **Event Log**.


System


Wireless


Firewall


Utilities


Status

Overview

Clients

Repeater

Event Log

Home > Status > System Overview

System Overview

System

System Name	
Firmware Version	4.10.00
Build Number	1.5-1.2393
Location	
Site	EN-A
Device Time	1999/12/31 16:01:26
System Up Time	0 days, 0:01:26
Operating Mode	AP

Radio Status

MAC Address	00:1F:D4:00:21:25
Band	802.11b+g
Channel	1
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:00:21:24
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:21:25	VAP-1	None	0

4.5.1. System Overview

The **System Overview** page provides an overview of the system status for the administrator.

Overview
Clients
Repeater
Event Log

[Home](#) > [Status](#) > System Overview

System Overview

System

System Name	
Firmware Version	4.10.00
Build Number	1.5-1.2393
Location	
Site	EN-A
Device Time	1999/12/31 16:01:26
System Up Time	0 days, 0:01:26
Operating Mode	AP

Radio Status

MAC Address	00:1F:D4:00:21:25
Band	802.11b+g
Channel	1
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:00:21:24
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.254

AP Status

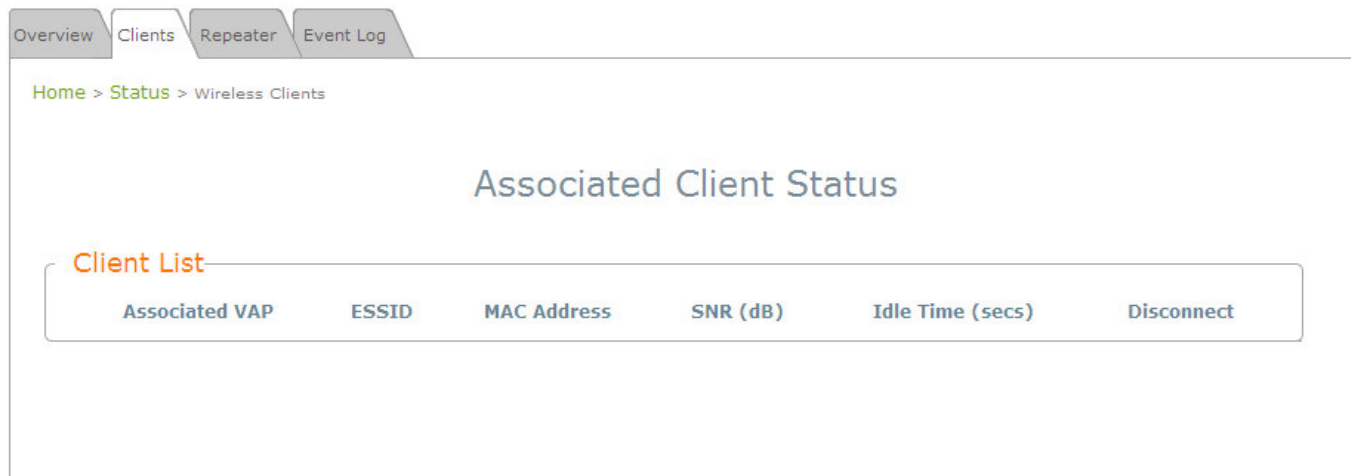
Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:1F:D4:00:21:25	VAP-1	None	0

The description of the table is shown below:

ITEM	DESCRIPTION	
System	System Name	The name provided in System Information.
	Firmware Version	The present firmware version of the system.
	Build Number	The Build Number of the firmware.
	Location	The location provided in System Information.
	Site	The firmware version for specific region.
	Device Time	The current time on the device.
	System Up Time	The system elapsing time since last reboot.
	Operating Mode	Either CPE or AP.
LAN Interface	MAC Address	The MAC address of LAN Interface.
	IP Address	The IP address of the LAN Interface.
	Subnet Mask	The Subnet Mask of the LAN Interface.
	Gateway	The gateway of LAN interface.
Radio Status	MAC Address	The MAC address of RF interface.
	Band	The operating band.
	Channel	The operating channel.
	Tx Power	The level of transmitted power.
AP Status	BSSID	The BSSID (MAC) of AP.
	ESSID	The assigned ESSID of AP.
	Security Type	The security type of AP.
	Online Client	The number of online clients associated with AP.

4.5.2. Associated Client Status

The administrator can remotely oversee the status of all associated clients on this page. Associated client's MAC, SNR and Idle Time are listed in the table.

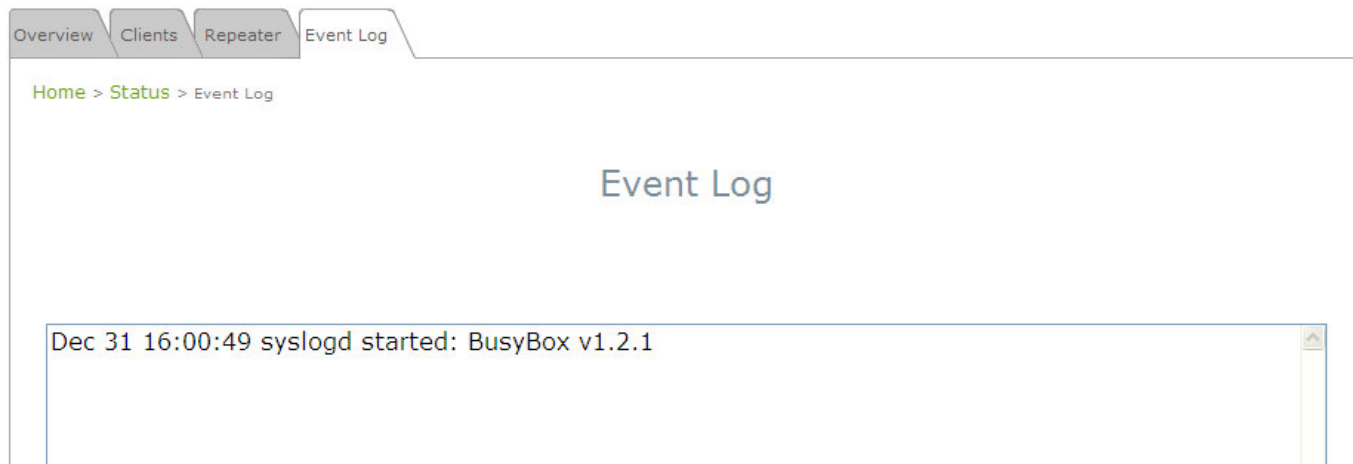


The screenshot shows a web interface with a navigation menu at the top containing 'Overview', 'Clients', 'Repeater', and 'Event Log'. Below the menu is a breadcrumb trail: 'Home > Status > Wireless Clients'. The main heading is 'Associated Client Status'. Underneath, there is a section titled 'Client List' which contains a table with the following columns: 'Associated VAP', 'ESSID', 'MAC Address', 'SNR (dB)', 'Idle Time (secs)', and 'Disconnect'.

- **ESSID:** The Extended Service Set ID which the client is associated with.
- **MAC Address:** The MAC address of associated clients.
- **SNR:** The Signal to Noise Ratio of respective client's association.
- **Idle Time:** Time period that the associated client is inactive; the time unit is in second.

4.5.3. Event Log

Event log provides the records of the system activities. All the system events are shown here.

**Note:**

As the Event Log is stored in RAM, it will be refreshed after the system is restarted. The system also supports a Syslog reporting function of reporting the events to an external Syslog server.

- **Date/ Time:** The date and time when the event happened.
- **Hostname:** Indicate which Host records this event. Note that all events in this page are local events and this field of all events is the same. However, in remote Syslog service, this field will help the network administrator identify which event is from this system. For more information, please refer to **Section 4.1.4 Management Services**.
- **Process name (with square brackets):** Indicate which process with the specific event is associated.
- **Description:** Description of the event.

4.6 Online Help

The **Help** button is at the upper right hand corner of the display screen.

Click **Help** for the **Online Help** window, and then click the hyperlink of the desired topic for further information.

Online Help (AP Mode)

Organization of the Configuration Web:

<u>System</u>	<u>Wireless</u>	<u>Utilities</u>	<u>Status</u>
System Information	VAP Overview	Password	System Overview
Operating Mode	General	Network Utilities	Clients
Network	VAP Config	Config Save Restore	Repeater
Management Services	Security	System Upgrade	Event Log
	Repeater	Reboot	
	Advanced		
	Access Control		
	Site Survey		

