Air Live®

www.airlive.com

WH-9100MESH

Dual-Band MESH AP/Bridge

User's Manual

OvisLink Corp. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of OvisLink Corp. to provide notification of such revision or change.

OvisLink Corp. provides this documentation without warranty, term or condition of any kind, implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. OvisLink Corp. may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software or removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the printed documentation, or on the removable media in a readable file such as license.txt or the like. If you are unable to locate a copy of the license, contact OvisLink Corp. and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States Government agency, then this documentation and the product described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in OvisLink Corp.’s standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

OvisLink Corp. and the OvisLink Corp. logo are registered trademarks.

Windows is a registered trademark of Microsoft Corporation. Any other company and product name mentioned herein is a trademark of the respective company with which they are associated.

EXPORT RESTRICTIONS

This product contains components, software, and/or firmware exported from the United States in accordance with

U. S. export administration regulations. Diversion contrary to U.S. law is prohibited.

This product requires professional installation. Please do not attempt to install the device without the necessary knowledge to your country's wireless regulations.

Content

Chapter 1: Introduce

1.1 Introduce

The AirLive WH-9100MESH product is ruggedized and wall-mountable IEEE 802.11 Wireless Access Point (AP) and Bridge device. The AP and Bridge mode can work simultaneously by dual radio interfaces. The WH-9100MESH serial products are designed for use in industrial and outdoor environments. They are powered by the Power over Ethernet (PoE) to simple cabling installations. So, they are suitable to set up at outdoor environment and using AP function to provide wireless network service and Bridge function to link to another location where is within infrastructure network.

The WH-9100MESH product is designed as a high security wireless network device. They are with the following cryptographic modules: WEP (64,128or 152 bits), WPA (TKIP / AES-CCMP) or WPA2 in AP mode, and AES-CCMP (128 bits) for the bridging mode; and HTTPS/TLS for secure web communication. Moreover, the WH-9100MESH serial products also provide the wireless client MAC address filtering, Rogue AP detection to protect your wireless network.

There are serial of products for you choose. The 9100MESH is the basic line product works at 2.4GHz band (802.11b/g) and 5GHz (802.11a) with AP and bridge function. The 9100MESH also provides **Super G / Turbo A** function to enhance transmit data rate up to 108Mbps. (Turbo A mode doesn't support at ETSI domain region.) The 9100MESH adopts newest **802.11i WPA2** standard to enhance the wireless security. The major feature of 9100MESH is **Wireless Mesh Network** function and introduce at section 1.1.3. The 9100MESH works at 2.4GHz and 5GHz band too. The 9100MESH also provides **Gateway mode, Layer 2 (Client) isolation**, **Multiple SSID/VLAN** and **Gateway Mode** features. When 9100MESH set up at Gateway mode, it provides firewall function to enhance network security.

1.1.1 802.11g Super and 802.11a Turbo:

802.11g Super and 802.11a Turbo technologies provide speed and throughput of more than double standard wireless LAN technologies in networking products. The Maximum link speed available is 108Mbps and the typical maximum end-user throughput ranges from approximately 40Mbps to 60+Mbps, depending on application demand and network environment.

1.1.2 Wireless Mesh Network:

The mesh network function let you set up the point-to-multipoint bridge function easily. You don't need to key in each remote bridge's BSSID (WLAN MAC address) to form bridge topology. It calls as auto-forming function. Beside the auto-forming function, it also detects network topology status. If some of bridge devices are log out, the other devices will find out it and re-forming network topology again. This is also call as auto-hearing function.

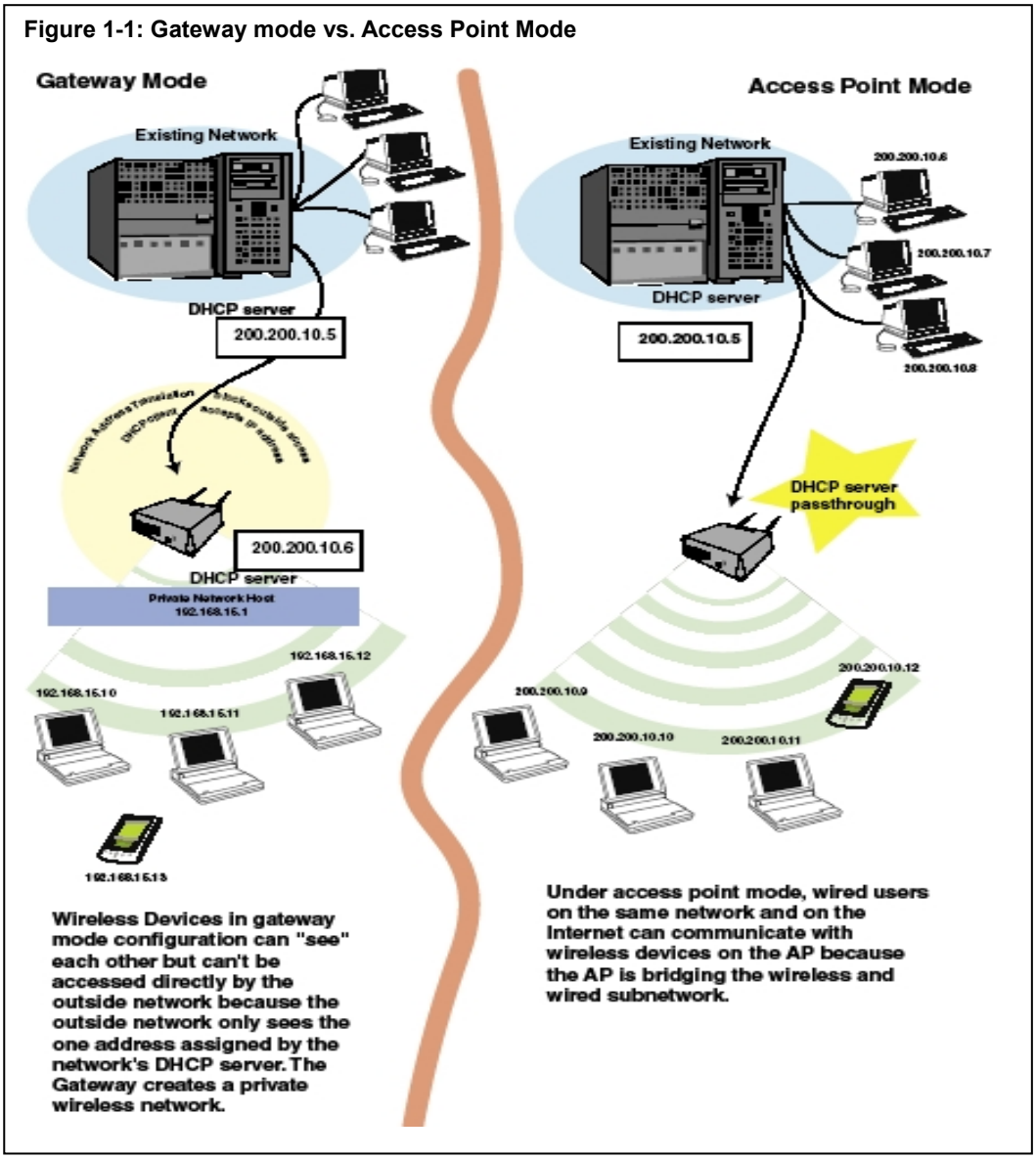
1.1.4 AP Mode vs. Gateway Mode

At AP mode, IP address for wireless devices are typically assigned by the wired network's DHCP server. The AP virtually connects wireless users to the host wired network. All wireless devices connected to the AP are configured on the same sub network as the wired network interface and can be accessed by

devices on the wired network.

Unlike the AP mode that the wireless clients get IP address from upstream network equipment and is at the same sub-network with wired network interface. Gateway mode provides private IP address for the wireless clients and is different sub-network from wired network interface. Gateway mode takes advantage of some built-in “router” function, such as the Network Address Translation (NAT) and Firewall. The NAT provides private IP address for the wireless clients and the Firewall enhance the security of wireless network.

Figure 1-1: Gateway mode vs. Access Point Mode



1.1.5 Multiple SSID/VLAN:

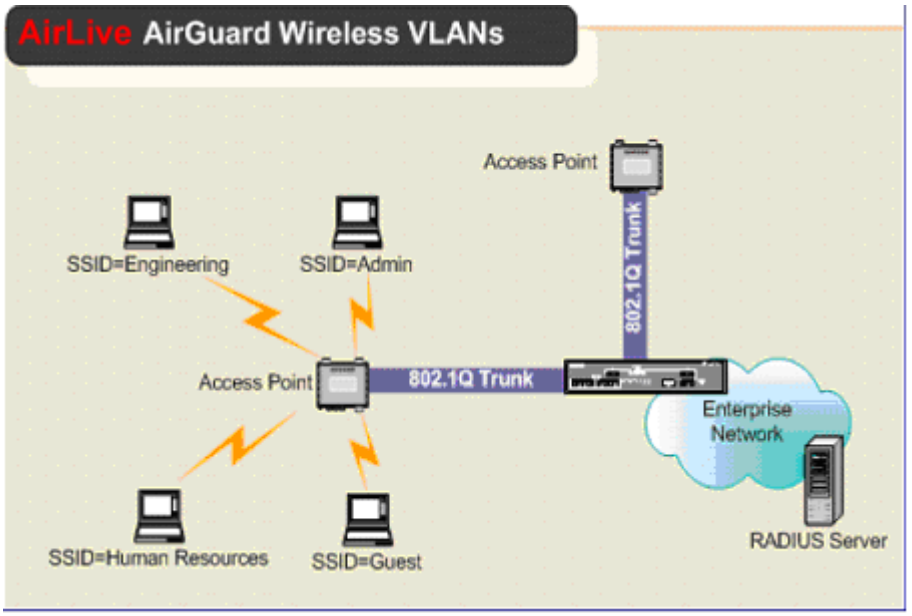
The Multiple SSID function working with VLAN switch provides the feature that different level clients link to one AP with different privilege.

Traditional AP only provides one SSID. All clients link to this SSID are in same network domain with same privilege. If you want different level clients link to different network domain with different privilege,

you need use another AP with different SSID name. And those APs link to different wire network domains to provide different privilege.

The Multiple SSID AP can provide couples SSID in one device. A VLAN Switch provides a switched network that is logically segmented by function, project team, or application in the same physical LAN. Within Multiple SSID AP and VLAN Switch, each SSID is associated with a VLAN to provide different privilege to distinguish different level client. Different level

Figure 1-2: Multi-SSID with VLAN Topology



clients can link to same AP by different SSID with different privilege.

1.1.6 Layer 2 (Client) Isolation

The Layer 2 (Client) Isolation function can protect your computer to prevent other users in the same network domain log in your computer to access data.

1.2 Function Navigation

WH-9100MESH Navigation Options`	
Access Point Mode	**Gateway Mode**
System Configuration	**System Configuration**
General	General
WAN — IP Setting	WAN — IP Setting, IP Aliasing
LAN	LAN
Wireless Access Point	**Wireless Access Point**
General	General
Security — None, Static WEP, 802.11i and WPA	Security — None, Static WEP, 802.11i and WPA
Wireless VLAN	Wireless VLAN

MAC Address Filtering Rogue AP Detection Advance	Load Balance Client Isolation	MAC Address Filtering Rogue AP Detection Advance	Load Balance Client Isolation
Wireless Bridge		**Wireless Bridge**	
General	Manual Bridge Auto Bridge	General	Manual Bridge Auto Bridge
Radio Encryption MAC Address Filtering	AES-CCM (Auto Bridge Mode Only)	Radio Encryption MAC Address Filtering	AES-CCM (Auto Bridge Mode Only)
Service Setting		**Service Setting**	
SNMP Agent		SNMP Agent	
Firewall		**Firewall**	
		Content Filtering IP Filtering Port filtering Virtual Server DMZ Advance	
Admin User Management		**Admin User Management**	
List All Users Add New User		List All Users Add New User	
Monitoring Reports		**Monitoring Reports**	
System Status Bridging Status Bridging Site Map Wireless Clients Adjacent AP List DHCP Client List		System Status Bridging Status Bridging Site Map Wireless Clients Adjacent AP List DHCP Client List	
Logs		**Logs**	
System Log Web Access Log		System Log Web Access Log	
System Administration		**System Administration**	
System Upgrade Factory Remote Logging Reboot Utilities	Firmware Upgrade Local Configuration Upgrade Remote Configuration Upgrade	System Upgrade Factory Remote Logging Reboot Utilities	Firmware Upgrade Local Configuration Upgrade Remote Configuration Upgrade

1.3 Appearance

1. **AP Antenna (TX+RX)**
2. **AP Antenna (RX)**
3. **Bridge Antenna (TX+RX)**
4. **Reset Button**
5. **Console Port**
6. **WAN / LAN Port**
7. **Ground Pin**

1.4 Product Features

1.4.1 Basic Features

- Access Point and Bridging Mode work simultaneously
- Point to Point and Point to Multi-Point manual bridge function support
- Wireless Mesh Network – Auto Bridge, support
- Bridge site map support
- Gateway Mode support.
- Ethernet uplink WAN port, can be as DHCP client or static IP
- Local Ethernet LAN port, can be as DHCP server or static IP
  - 9100MESH is as LAN function when set up as Gateway mode
- Dual Wireless (802.11a/b/g) interface, separate for AP and Bridge function
- Two antenna connectors for AP with diversity function and one Bridge
- Power over Ethernet (PoE)
- LED indicator: Power, WAN, WLAN1 (AP), WLAN2 (Bridge) and Received Radio Strength

(Bridge)

1.4.2 Wireless Features

- AP
  - Disable SSID broadcast
  - MAC address filtering (MAC address Authentication)
  - Wireless client information (MAC address, Signal Strength, Transmit rate) list
  - Adjacent AP list
  - Rogue AP detection
  - Load Balancing
  - Support SNMP V1/ V2/ V3
  - Layer 2 Isolation
  - Multi SSID
- Bridge
  - Manual Bridge (Point-to-Point and Point-to-Multi Point)
  - Auto Bridge
  - MAC layer optimize for long distance transmit
  - Bridge site map
  - Adjustable ACK timing
- Radio
  - Support IEEE 802.11a/b/g
  - Adjustable Radio Power
  - Automatically optimal channel selection

1.4.3 Security Features

- Configuration through HTTPS/TLS secure web
- AP
  - WEP: (64-bit, 128-bit and 152-bit)
  - WPA
    - Pre-shared key
    - TKIP/AES-CCMP
  - WPA2 (802.11i)
  - MAC based authentication (MAC address filtering)
  - In band Rouge AP detection
- Bridge
  - AES-CCMP for wireless (128 bits)

1.4.4 Firewall

- Content Filtering
- IP Filtering

- Port Filtering
- Virtual Server
- DMZ

1.4.5 Enclosure Features

- Waterproof and dustproof enclosure (IP67)
- Waterproof RJ45 connector
- External waterproof reset button for reset system or back to factory default setting
- Mounting kits

1.4.6 Operation Temperature

- Standard model: 0 degree ~ 50 degree C
- Industrial model (with TEC): -40 degree ~ 70 degree C

1.5 Radio Characteristic

- **802.11b**
  - Frequency band:
    - American (FCC): 2.412 ~ 2.462GHz (11 channels)
    - Europe (ETSI): 2.412 ~ 2.472GHz (13 channels)
  - Data Rate:
    - 1, 2, 5.5, 11Mbps
  - Modulation:
    - Direct Sequence Spread Spectrum (DSSS)
      - Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps
      - Differential Quadrature Phase Shift Keying (DQPSK) at 2Mbps
      - Complementary Code Keying (CCK) at 5.5 and 11 Mbps
  - Transmit Output Power (Typical):
    - 19 dBm +/-3dBm for all rates

    Note: Maximum power setting will vary according to individual country regulations.
  - Receive Sensitivity (Typical):
    - -93dBm at 1Mbps
    - -88dBm at 11Mbps
- **802.11g**
  - Frequency band:
    - American (FCC): 2.412 ~ 2.462GHz (11 channels)
    - Europe (ETSI): 2.412 ~ 2.462GHz (13 channels)
  - Data rate:
    - 6, 9, 12, 18, 24, 36,48, 54 Mbps

- 72, 96, 108 Mbps (Super G mode)

- Modulation:
  - Orthogonal Frequency Divisional Multiplexing (OFDM)
    - BPSK at 6 and 9 Mbps
    - QPSK at 12 and 18 Mbps
    - 16-quadrature amplitude modulation (QAM) at 24 and 36Mbps
    - 64-QAM at 48 and 54Mbps
- Transmit Output Power (Typical):
  - 19 dBm +/- 3dBm at 6 ~ 24Mbps
  - 18 dBm +/- 3dBm at 36Mbps
  - 17 dBm +/- 3dBm at 48Mbps
  - 16 dBm +/- 3dBm at 54Mbps

  Note: Maximum power setting will vary according to individual country regulations.
- Receive Sensitivity (Typical):
  - -89dBm at 6Mbps
  - -73dBm at 48Mbps
  - -70dBm at 54Mbps

- **802.11a**
  - Frequency band
    - 5.15 ~ 5.25GHz / 5.25 ~ 5.35GHz/5.725 ~ 5.825GHz

    Note: Frequency band setting will vary according to individual country regulations.
  - Data rate:
    - 6, 9, 12, 18, 24, 36,48, 54 Mbps
    - 72, 96, 108 Mbps (Super A mode)
  - Modulation:
    - Orthogonal Frequency Divisional Multiplexing (OFDM)
      - BPSK at 6 and 9 Mbps
      - QPSK at 12 and 18 Mbps
      - 16-quadrature amplitude modulation (QAM) at 24 and 36Mbps
      - 64-QAM at 48 and 54Mbps
  - Transmit Output Power (Typical):
    - 18 dBm +/- 2dBm at 6 ~ 24Mbps
    - 16 dBm +/- 2dBm at 36Mbps
    - 15 dBm +/- 2dBm at 48Mbps
    - 14 dBm +/- 2dBm at 54Mbps

    Note: Maximum power setting will vary according to individual country regulations.
  - Receive Sensitivity (Typical):
    - -84dBm at 6Mbps
    - -70dBm at 48Mbps
    - -68dBm at 54Mbps

1.6 Package list

- Access Point
- 2 attachable 5dBi omni-directional antennas
- 1 Power injector with power cord
- 15m CAT5 cable with waterproof RJ45 connector
- 1 Ground cable
- Documentation as PDF files on CD-ROM
- 1 Mounting kit set
- 1.5m low loss antenna cable

1.7 Optional accessory

You can contact OvisLink to buy below accessory

- High gain directional antenna for bridge
- Lightning Arrestor

Chapter 2: System Installation

The manual deals only and specifically with the single device as a unit. The purpose of this chapter is the description of the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit.
Preliminary setup information provided below is intended for information and instruction of the wireless LAN system administration personnel.

It is intended, and is the philosophy of the manufacturer, that the user not be required to open the individual unit. Any maintenance required is limited to the external enclosure surface, cable connections and to the management software only. A failed unit should be returned to the manufacturer for maintenance.

2.1 Prepare for use

The WH-9100MESH is designed to be attached to the wall at appropriate locations. To complete the configuration, you should have at least the following components:

- PCs with one of the following operation systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A compatible IEEE 802.11a/b/g PC card or device for each computer that you wish to wirelessly connect to your wireless network;
- Access to one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit;
- A Web browser program, such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later, installed on the PC or laptop you will be using to configure the Access Point
- TCP/IP Protocol (usually comes installed on any Windows PC)

The WH-9100MESH operates with Power over Ethernet (PoE) which requires the installation of a separate power injector which “injects” DC current into the CAT5 cable (including in package).

2.2 Site Survey

The WH-9100MESH requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation.

2.2.1 Estimate Bridge Transmit Distance

Normally, the bridge need transmit RF signal to another bridge device at long distance. You may be able to use below equation to calculate the RF link Budget.

Fade Margin = received signal – receiver threshold

Where

Received signal = Transmitter power – Transmitter cable loss + Transmitter antenna gain – free space path loss + Receiver antenna gain – Receiver cable loss

Received threshold = Received sensitivity

- **Free Space Path Loss**

Using below Free Space Loss Formula to calculate free space path loss

$$L_P = 96.6 + 20\log_{10} F + 20\log_{10} D$$

Where

L_P = free space path loss between antennas

F = frequency in GHz

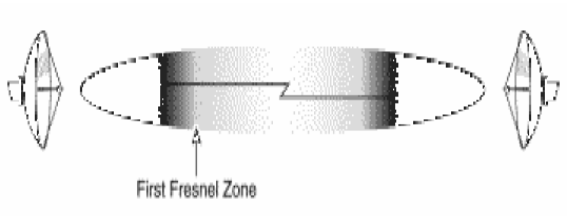
D = path length in miles

2.2.2 Estimation Bridge's antenna Location

When as bridge device, the WH-9100MESH may need to be mounted outdoors on a high place to achieve the best bridge result. The Fresnel zone and Earth bulge dominate to decide how high that the unit's Antenna need be put. The total antenna height equals the width of Fresnel zone plus the height of earth bulge.

- **Fresnel zone:**

The Fresnel zone is the area around the visual line-of-sight that radio waves spread out into after they leave the antenna. This area must be clear or else signal strength will weaken. The rule of thumb is that 60% of the Fresnel zone must be clear of obstacles. Typically, 20% Fresnel Zone blockage introduces little signal loss to the link. Beyond 40% blockage, signal loss will become significant. The equation of the width of Fresnel Zone is



$$W = 43.3 \times \sqrt{\frac{D}{4F}}$$

Where

W = Width of the Fresnel Zone (in feet)

D = Distance between the antennas (in miles)

F = Frequency in GHz

- **Earth Bulge**

When the transmit distance of RF signal is longer than seven miles, the curvature of the earth may be a factor and require the antenna put at higher location. The additional antenna height can be calculated by below formula:

$$H = \frac{D^2}{8}$$

Where

H = Height of earth bulge (in feet)

D = Distance between antennas (in miles)

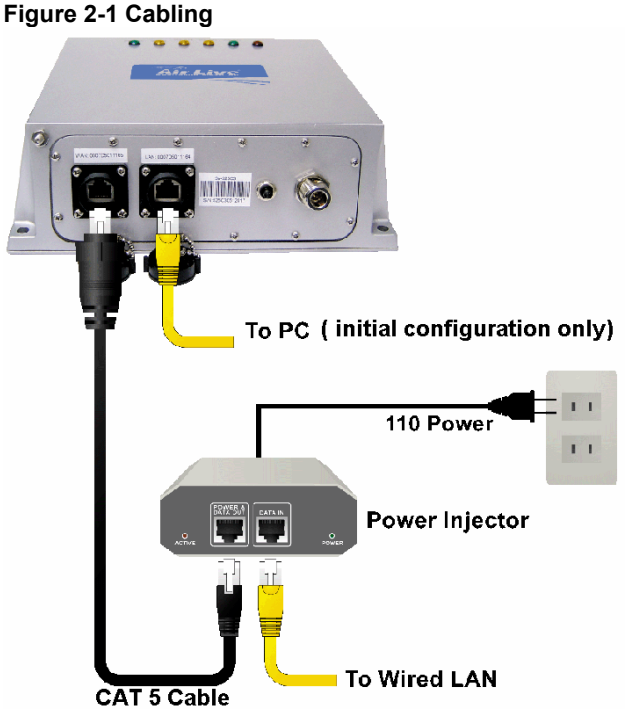
2.3 Cabling

The following figure illustration shows the external cable connectors on the WH-9100MESH. The WAN

port is used to connect the WH-9100MESH to the organization's LAN. The Ethernet cable is run from the WH-9100MESH WAN port to the Power Injector which is then connected to a power source and wired LAN. A second (LAN port) Ethernet RJ45 connector is designed for use during initial configuration and as LAN function when set up as Gateway mode

This uses an RJ45 cable to connect the WH-9100MESH to a laptop. The following diagram demonstrates the setup.

Figure 2-1 Cabling



2.4 Antenna Installation

2.4.1 Antenna for AP

The package includes two 5dBi omni-directional antennas and two antenna connectors at WH-9100MESH's real panel are used for AP to support diversity function. Thus, for getting best performance, those two antenna connectors need plug with antennas. Don't let antenna connectors are open when unit is working, or you need to enter configuration screen to set the Tx Pwr Mode as Off at Wireless Access Point –General. Some experience show us and we want to suggest that the equipment may need to up side down while the it is put at high location. For the case where the AP is placed high on a tower, the part of the antenna pattern is pointed towards the sky instead of the ground where the clients are. Hence if you are standing underneath the antenna, you may not get much of a signal.

2.4.2 Antenna for Bridge

The antenna connector at front panel is used for bridge. To get the best performance, the bridge's antenna should far away AP's antenna. Using 1.5m low loss antenna cable connects to this connector then connects a directional antenna at the other end of cable. Since the Bridge's antenna is directional antenna normally; it should be toward to another WH-9100MESH Bridge unit's antenna directly. Anything in the line of sight between on antenna at the other can cause major issue for RF link. You can exploit the SS LED or enter configuration screen Wireless Bridge –General to understand received radio signal strength and make sure the Bridge antennas are installing well.

⚠ To comply with FCC RF exposure compliance requirements, the antennas used with the WH-9100MESH must be installs with a minimum separation distance of 20 cm from all people and must

not to be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized antenna and/or cable provided with the device or available form the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by manufacture or party responsible for this FCC compliance could void the user's authority to operate the equipment.

2.4.3 Sealing Antenna Connections

Once all antennas have been installed, the connection should be sealed to protect them in an exterior harsh environment using a self amalgamating polyisobutylene tape which, over a period of hours, adheres to itself and forms a single amalgamated rubber molding conforming to the shape of the item it is covering. Once the tape is in place for several hours, it forms a shaped rubber molding that is resistant to water and most solvents. It remains stable over a wide temperature range and degrades very slowly in sunlight. Be sure that it is completely dry when applied. If you need to uninstall it after it has sealed for 30 minutes or more, cut it away with a sharp knife.

2.4.4 Lightning Arrestor Installation

The potential for lightning damage should always be considered when setup this machine at outdoor environment. A variety of lightning protections are available. Make sure the equipment is properly grounded to provide low-impedance paths for lightning currents and using the lightning arrestor to protect antennas. You can contact OvisLink to buy Lightning Arrestor and follow Appendix B to install lightning arrestor.

2.5 Mounting Kit Setup

Step1: Choosing a suitable post for mounting kits

Step2: Mounting the mounting kits to post by U-Ring, screw and nut.

Step3: Mounting the unit to mounting kits by screw.

Chapter 3: LED Indicator

The top panel of the WH-9100MESH contains a set of indicator lights that help describe the state of various networking and connection operations. Figure 3-1 illustrate LED location and Table 3-1 describe the detail LED definition

Figure 3-1 LED Location

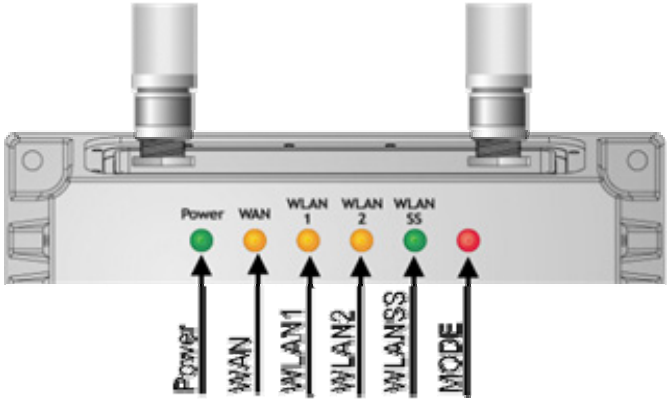


Table 3-1: LED definition

LED	Description
Power	If this light is on, the unit is on; If it is not on, the unit is off
WAN	If this light is on, the unit is connected to network If it is off, the unit does not have an active connection to network
WLAN1 (AP)	The light is ling for indicate the WLAN 1 is active. The light is blinking to indicates data transmission
WLAN2 (Bridge)	The light is ling for indicate the WLAN 2 is active. The light is blinking to indicates data transmission
WLAN2 SS (Signal Strength)	This indicates the WLAN2 received signal strength 1. LED off: no connection on the bride side, or the signal is very week 2. LED blink slowly (every 1 second): there is a connection and signal quality is poor 3. LED blink fast: there is a connection, and the signal quality is good 4. LED steady: there is connection, and the signal quality is excellent
Mode	No using

Chapter 4 Enter Configuration Screen

The WH-9100MESH comes with the capability to be configured as an AP and bridge. However, you need to know how to enter system configuration environment. This chapter describes how to enter WH-9100MESH system setup screen.

4.1 Configuration Steps

4.1.1 Before Configuration

To complete the configuration, you should have at least the following components:

- PCs with one of the following operation systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- Access to one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit;
- A Web browser program, such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later, installed on the PC or laptop you will be using to configure the Access Point
- TCP/IP Protocol (usually comes installed on any Windows PC)

4.1.2 Computer setting

Plug one end of a CAT5 Ethernet cable to the LAN port of the WH-9100MESH (See Figure 1-x) and the other end to an Ethernet port on your computer. This LAN port in the WH-9100MESH connects you to the device's internal DHCP server which will dynamically assign an IP address to your computer so you can access the device for reconfiguration. In order to connect properly to the WH-9100MESH on the LAN port, the TCP/IP parameters on your laptop/PC must be set to "obtain IP address automatically"

If you are unfamiliar with above procedure, the following instructions can be as a reference
In Windows 2000/XP, follow the part Start → Settings →Network and Dialup Connections → Local Area Connection and select the Properties button. In the Properties window, highlight the TCP/IP protocol and click properties. Make sure that the radio button for "Obtain an IP address automatically" is checked

Once the DHCP server has recognized your laptop and has assigned a dynamic IP address, you will need to find that IP address.

In Windows 2000/XP, click start, then Run and type **cmd** in the run instruction box. Then click OK. This will bring up a window. In this window, type **ipconfig /all | more**. This will list information assigned to your laptop/PC, including the IP address assigned. Verify that the IP address is 192.168.15.X

4.1.3 Enter WH-9100MESH configure screen

The default IP of LAN port is 192.168.15.1. This IP can be change after you enter the configure screen. Please refer to section 5.5 to understand how to change IP. After you change IP, the IP of LAN will change as the first one that your new DHCP IP range.

On your computer, pull up a browser window and put the default URL (https://192.168.15.1), or new IP for the WH-9100MESH Local LAN in the address line.

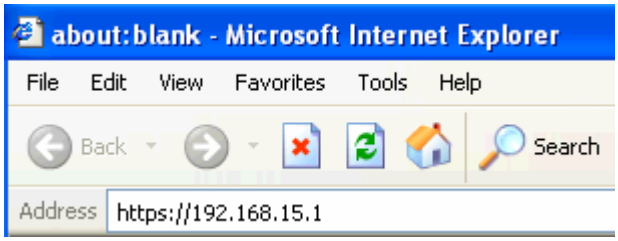
Note: be sure that you use the **https** prefix, not **http**

Note: For WH-9100MESH, be sure that the operation mode you choose. The URL is https://192.168.15.1 for AP mode and is https://192.168.16.1 as Gateway mode.

4.1.4 Enter WH-9100MESH Gateway mode configure screen

If the unit is 9100MESH and set up its operation mode as Gateway mode, the URL change as https://192.168.16.1

Figure 4-1 Log in IP screen



Key in https://192.168.15.1, or https://192.168.16.1 for 9100MESH set up as Gateway mode

4.1.5 Username and Password

Figure 4-2 Login in username and password screen

You will be asked for your user name and password. The default is "**airlive**" with the password "**airlive**" to give full access for setup configuration. (This password is case-sensitive)

After you key in the username and password, please read the terms and conditions and check the checkbox "I agree to the terms and conditions below" then click the "Sign In" button" to continue configuration. You can change the username and password as you want after you enter configuration screen.

4.2 Forget username, password and IP

How can you do if you had changed username, password and IP but you forget it? You can find there is

a Reset button at front plane. Press this button over 8 seconds, the unit will go back as factory default setting. The username and password will back to “**airlive**” and “**airlive**”, and the IP will be back to 192.168.15.1 or 192.168.16.1 when 9100MESH as Gateway mode.

Chapter 5: System Configuration

The chapter describes how to do System Configuration. If you don't know how to enter configuration screen, chapter 4 describes how to do it.

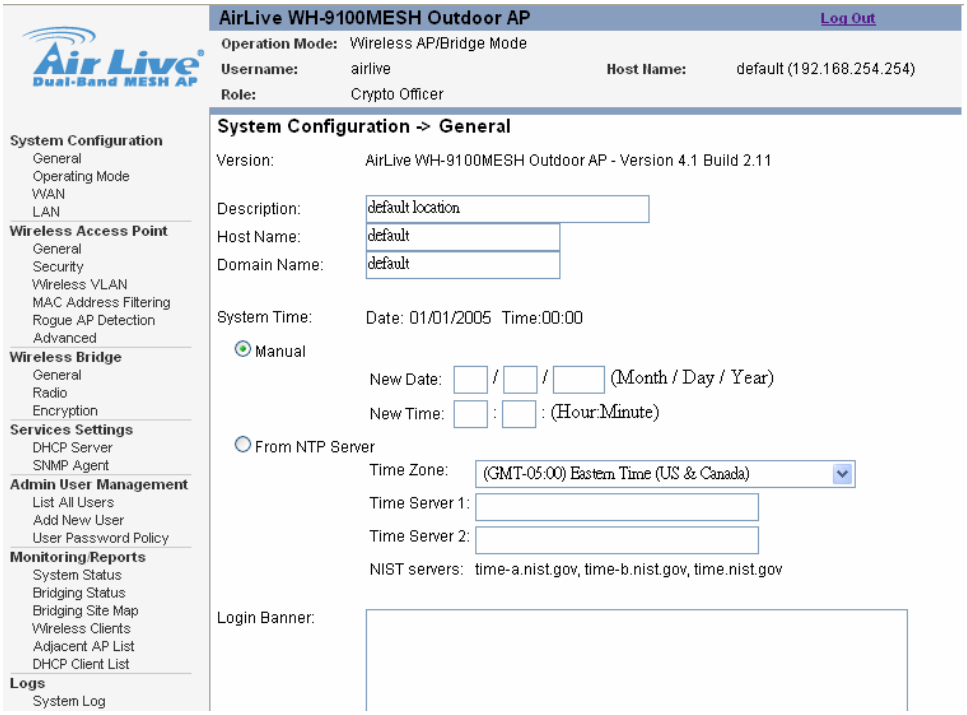
5.1 Prepare for using static IP

If your network environment is without DHCP function, then you need to use static IP for WAN port. Then, the 9100MESH network administrator may need the following information:

- IP address -a list of IP addresses available on the organization's LAN there are available to be used for assignment to the AP(s)
- Subnet mask
- DNS IP address

5.2 System Configuration – General

Click the entry on the left hand navigation panel for enter System Configuration -General. This directs you to the System Configuration – General page.



This screen lists the software version number for your WH-9100MESH and allows you to set the Host Name and Domain Name as well as establish system date and time.

- Description: You can enter a description of the physical location of the unit in it. This is useful when deploying units to remote locations to understand where the unit is.
- Host and Domain Name: Both set at the factory for "default" but can optionally be assigned a unique name for each.

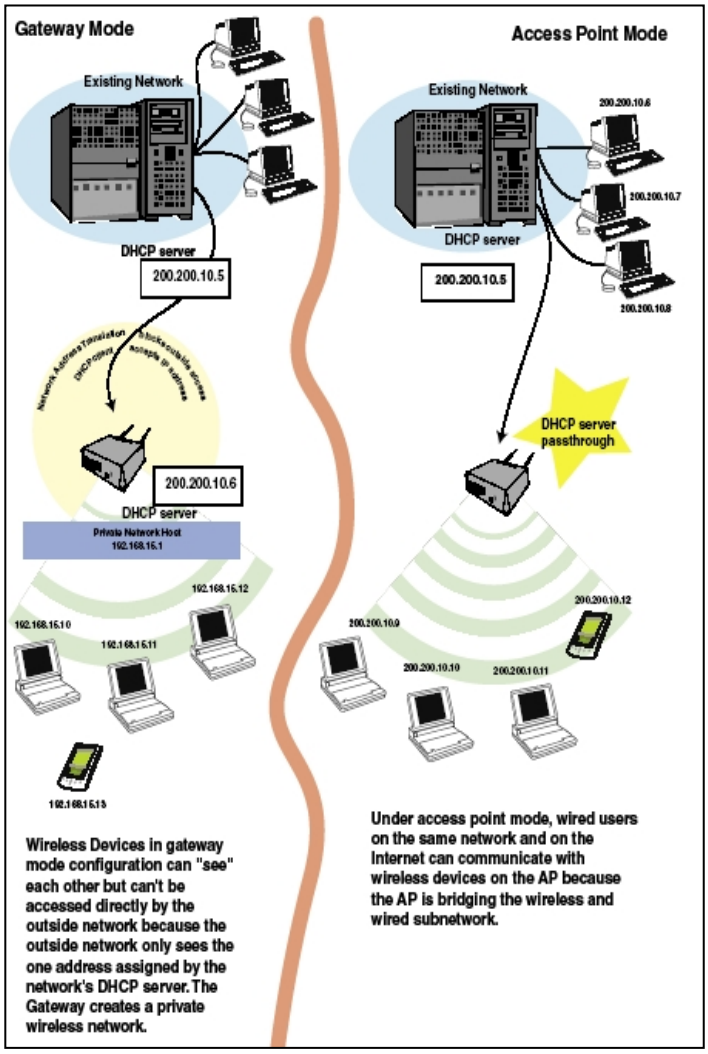
• System Time: You can manual key in the time and day, or get them automatically from NTP server. The 9100MESH serial products are with RTC chip to keep date and time data. It can keep system date and time data for 5 days.

• Login Banner:

When you are satisfied with your changes, click Apply.

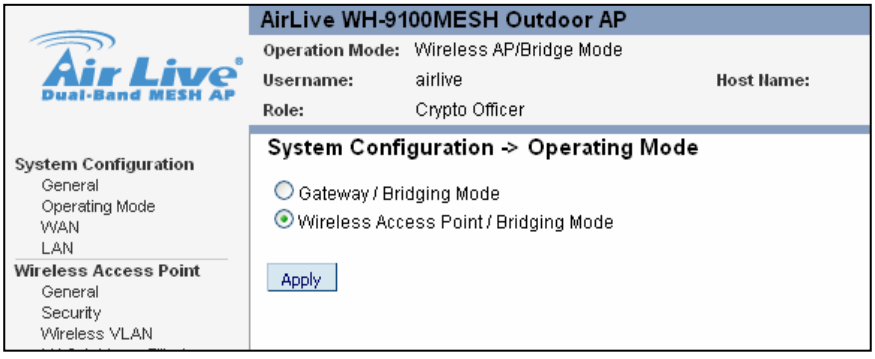
5.3 System Configuration – Operation Mode

At 9100MESH model, it adds a selection item - Operation mode. You can set up 9100MESH as standard Access Point function, or Gateway.



At AP mode, it virtually connects wireless users to the host wired network. The IP addresses for wireless devices are typically assigned by the wired network's DHCP server. All wireless devices connected to the AP are configured on the same sub network as the wired network interface and can be accessed by devices on the wired network.

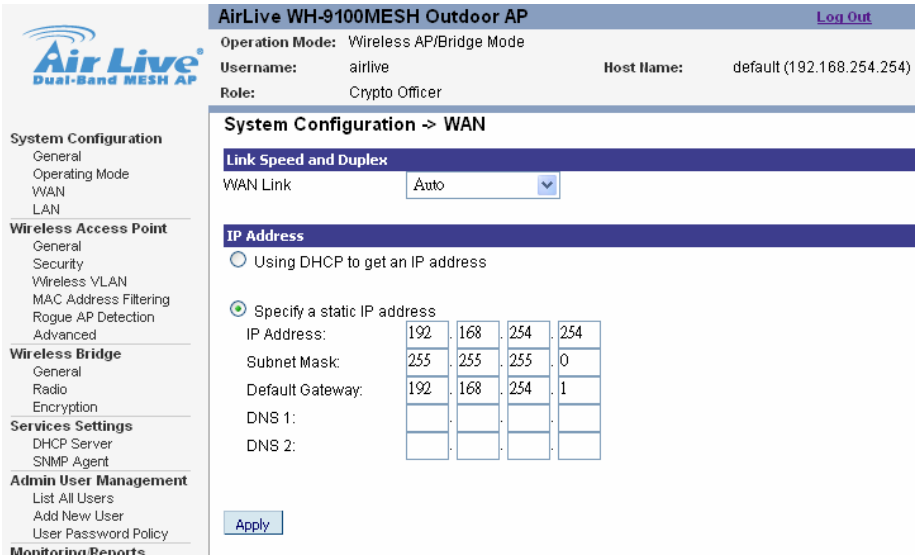
If additional security for the wireless network is desired (differentiating it from the wired network to which it is connected), or the wired network can not provide enough IP to wireless devices, you can set up device in gateway mode. Unlike the AP mode that the wireless clients get IP address from upstream network equipment and is at the same sub-network with wired network interface. Gateway mode provides private IP address for the wireless clients and is different sub-network from wired network interface. Gateway mode takes advantage of some built-in "router" function, such as the Network Address Translation (NAT) and



Firewall. The NAT provides private IP address for the wireless clients and the Firewall enhance the security of wireless network.

5.4 System Configuration – WAN

Click the entry on the left hand navigation panel for System Configuration – WAN. This directs you to the System Configuration – WAN page.



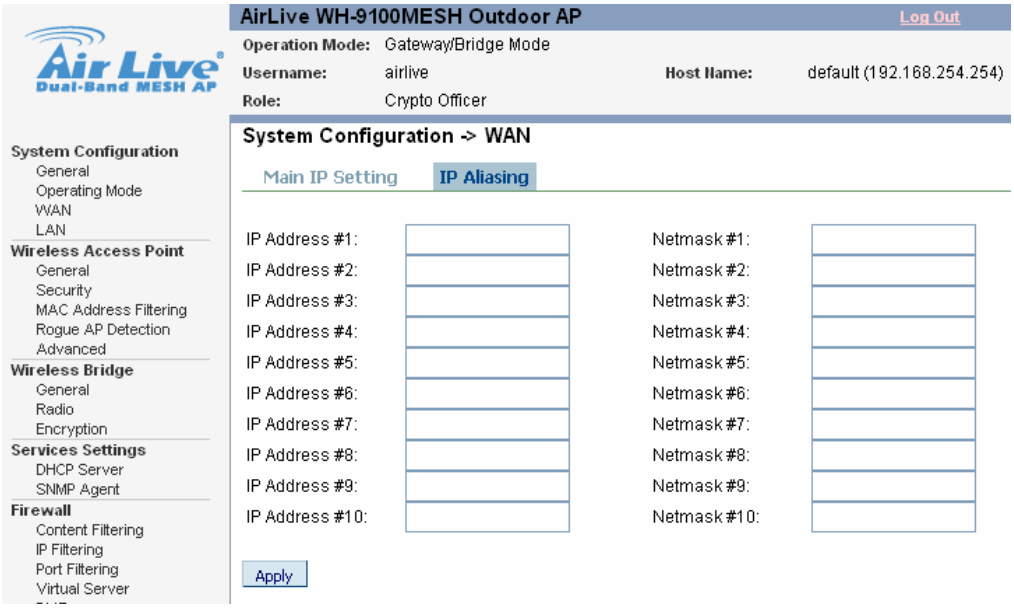
The default IP of WAN is as static IP. You need input the information that the AP requires in order to allow the wireless devices (9100MESH) access to the wired LAN. This will be the IP address, Subnet Mask, Default Gateway, and, where needed, DNS1 and 2. The default WAN port value is IP Address: 192.168.254.254, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.254.1.

You also can choose “Using DHCP to get an IP address”. By this way, the 9100MESH will get an IP address from DHCP server.

Click Apply to accept changes.

5.4.1 IP Aliasing

You can add up to ten additional IP aliases on the WAN port, if you use WH-9100MESH product and set up its operation mode as Gateway mode.



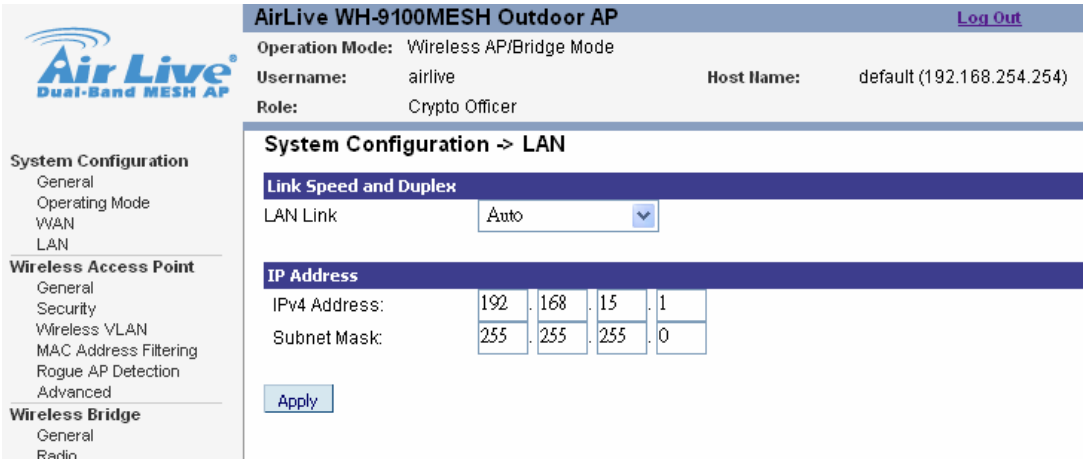
The IP aliasing entries can be used by the virtual server to map a public IP address to a private IP address. If the virtual server needs to map multiple public IP addressed to multiple private IP address,

the IP aliasing entries an be used to create additional public IP address. These entries are always static entries and can not use DHCP.

Click Apply to accept changes.

5.5 System Configuration – LAN

Click the entry on the left hand navigation panel for System Configuration – LAN. This directs you to the System Configuration – LAN page.



This set up the default numbers for the four octets for a possible private LAN function for the AP. It also allows changing the default numbers for the LAN Subnet Mask. The Local LAN port provides local access for configuration. It is not advisable to change the private LAN address while doing the initial setup as you are connected to that LAN. If you do change DHCP IP address as new one, you need use the IP you key in to enter configure screen again after clicking Apply button.

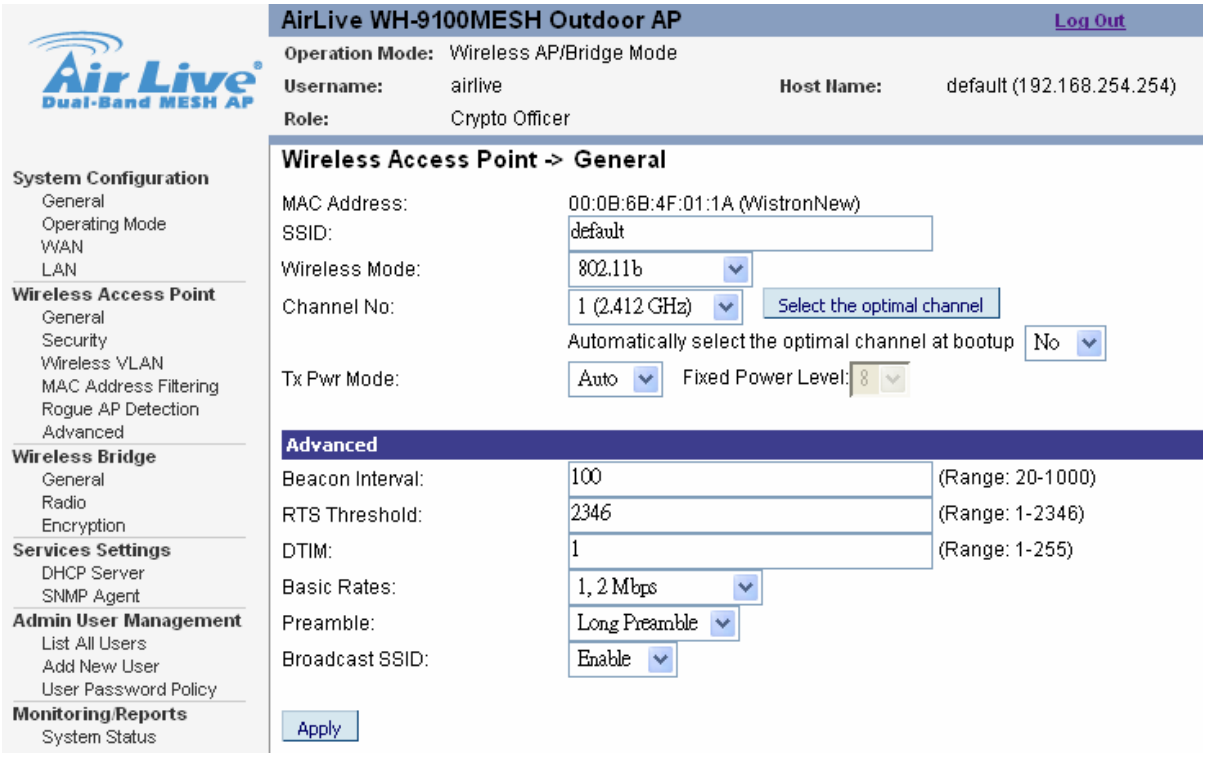
Chapter 6: Wireless Access Point Configuration

This chapter describes the items about set up AP function. Those items are under the Wireless Access Point Configuration menu. If you don't know how to enter configuration screen, chapter 4 describes how to do it. Please keep in mind that you need click Apply to save all settings.

6.1 Wireless Access Point – General

Click the entry on the left hand navigation panel for Wireless Access Point – General. This directs you to the Wireless Access Point – General page.

Figure 6-1 Wireless Access Point – General screen



6.1.1 MAC address

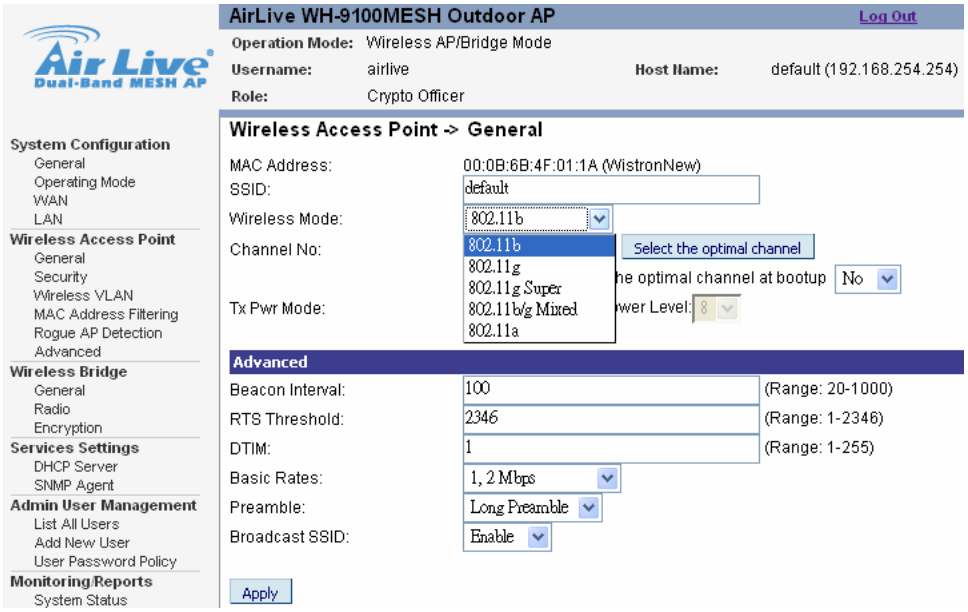
The MAC address list here is AP's wireless interface. This is not the BSSID for bridging setup. The BSSID for bridging is found on the Wireless Bridge – General page.

6.1.2 SSID

If you will be using an SSID for a wireless LAN, enter it here and in the setup of each wireless client. This nomenclature has to be set on the AP and each wireless device in order for them to communicate.

6.1.3 Wireless Mode

The wireless Mode menu allows you to specify whether you want AP to operate solely in the 802.11a, 802.11b, 802.11g or in a combination of 802.11b/g. The 802.11b/g use 2.4GHz ISM (**I**ndustrial, **S**cientific and **M**edical) frequency band and the 802.11a use the 5GHz UNII (**U**nlicensed **N**ational **I**nformation **I**nfrastructure) frequency band.



- **802.11b:**

  The 802.11b will accommodate legacy system and support 1, 2, 5.5 and 11Mbps data rate.

- **802.11g:**

  The 802.11g support data rates up to 54Mbps (6, 9, 12, 18, 24, 36, 48, 54Mbps) at 2.4GHz frequency band by using the 802.11a OFDM techniques. This mode limits use to those WLANs that have only 802.11g clients.

- **802.11b/g Mixed**

  The 802.11b/g Mixed allows you to use both 802.11b and 802.11g clients. At this mode, all transmissions will be at the highest data rates available if the environment is with only 802.11g devices. However, if an 802.11b device links to this network, the header information needs to back down to 802.11b rates for all of 802.11g and 802.11b devices. It will little slow down the network throughput. The side effect is an overall increase in overhead, so a small price is paid in 802.b/g Mixed mode.

  If you make sure all of WLAN devices are 802.11g clients, then you can chooses 802.11g mode to gain a higher performance.

- **802.11g Super**

  The 802.11g Super mode can support data rate up to 108Mbps (72, 96, 108 Mbps). Although you can gain a highest data rate, you need to use this function carefully because it occupies large bandwidth and may corrupt the adjacent channels' radio signal.

Note: Super G's channel bonding feature can significantly degrade the performance of neighboring 2.4GHz WLANs. Moreover, Super G doesn't check to see if 11b or 11g standard-compliant devices are in range before using its non-standard techniques.

- **802.11a**

  The 802.11a mode can support data rate up to 54Mbps (6, 9, 12, 18, 24, 36, 48, 54Mbps). The 802.11a uses 5-GHz UNII (Unlicensed National Information Infrastructure) frequency band. The

use of 5-GHz UNII frequency band provides some distinct advantages over the 2.4GHz band. In addition to providing a greater amount of bandwidth for transmission, the 5-GHz band has less potential interference because lots of wireless device working in the 2.4GHz band (Bluetooth, cordless telephone, microwave ovens, and so on)

- **802.11a Turbo (This mode is not allowed for outdoor use, so has been removed from wireless mode menu)**
  The 802.11a Turbo mode can support data rate up to 108Mbps (72, 96, 108 Mbps).

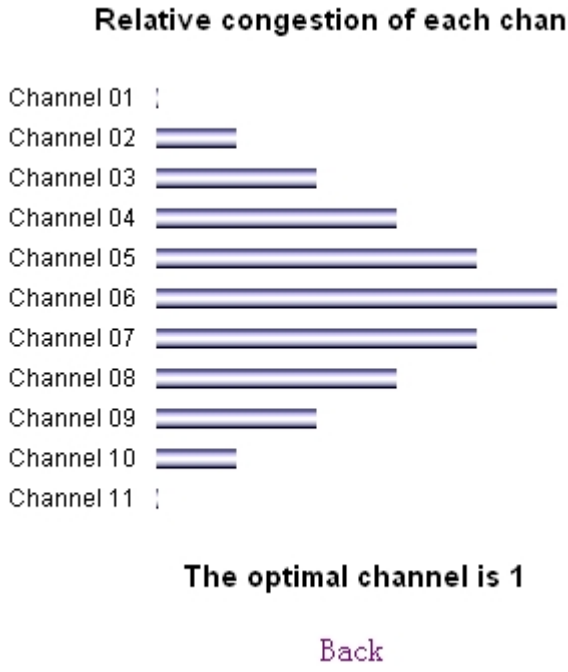
6.1.4 Channel Number

The channel number is a means of assigning frequencies to a series of access points. If you are using the WH-9100MESH as both an AP and bridge, the channel number set for the AP and the one for bridge should be sufficiently different to avoid interference. Generally, it has been found that the selection channel 4 for bridging and channel 11 for AP gives a good spread at 2.4GHz band, or one use 2.4GHz band and another one use 5GHz band.

Before you setting the channel, you had better to use the optimal channel function to detect the environment's radio signal and choose the best one for using.

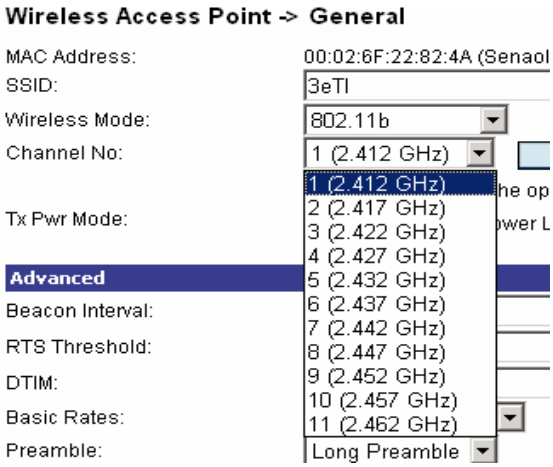
- **Optimal channel**

If you click on the button "**Select the optimal channel"**, a popup screen will display the choices. After enter this function, the WH-9100MESH detects the environment's radio signal at each channel and show them at this screen. This action does not select the channel for you but shows you what will most probably be channel selected if you leave the following dropdown menu at Yes.



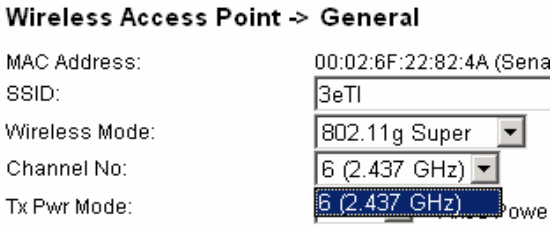
- **802.11b, 802.11g and 802.11b/g Mixed mode**

There are 11 (13 for ETSI) channel numbers that may be assigned. Because the 802.11b signal bandwidth is 22MHz, there are 3 non-overlapping channels for 802.11b at 2.4GHz ISM band. To reduce the interference problem, you may be able to establish up to 3 wireless networks at the same area. If you need establish 3 wireless networks, you may assign channel number 1 to the first wireless network. Then the channel 6 will be better for second wireless networks and channel 11 will be the third one.



- **802.11g Super**

The 802.11g Super mode occupies larger frequency bandwidth. To avoid interfere another wireless network operation, it is fixed at channel 6.

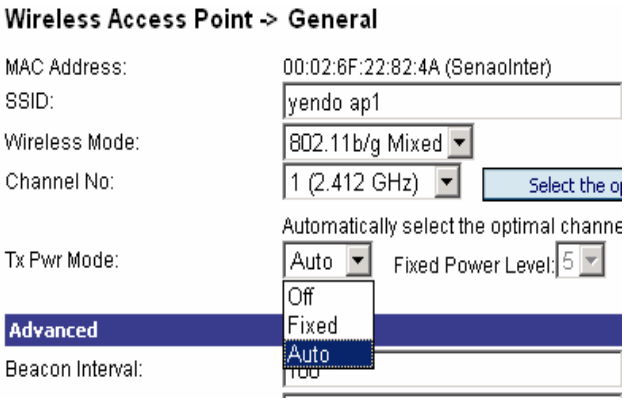


- **802.11a and 802.11a Turbo**

The frequency band of IEEE 802.11a will vary according to individual country regulations. The FCC (U.S) has allocated three bands, UNII1(5.15~5.25GHz), UNII2(5.25 ~ 5.35GHz) and UNII3(5.725~5.825GHz). Each band has 4 non-overlapping channels. For Pan-Europe, there are the 5.15GHz~5.35GHz, 5.425GHz ~ 5.725GHz. At Taiwan, the 802.11a device use the 5.725GHz ~ 5.875GHz frequency band. Refer to Appendix A to get more information.

6.1.5 TX Power Mode

The Tx Power Mode let you can set the radio power as you wanted. It defaults to Auto, giving the larger range of radio transmission available under normal conditions. As an option, the AP's cover range can be limited by setting the TX Power Mode to Fixed and choosing from 1~5 for fixed power level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission, set Tx Pwr Mode to off.



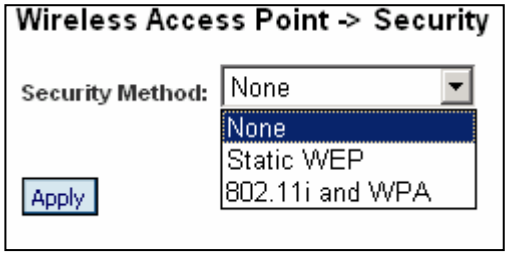
6.1.6 Advanced Option

There are a number of advanced options described in the following chart:

Advanced Options		
Beacon interval	0 ~ 4095	The frequency in milliseconds in which the 802.11 beacon is transmitted by AP
RTS Threshold	0 ~ 3000	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed
DTIM	1~65535	The number of beacon intervals between successive Delivery Traffic Identification Maps (DTIMs). This feature is used for Power Save Mode
Basic Rate	Basic Rate for 802.11b	
	1 and 2 Mbps 1, 2, 5.5 and 11Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames
	Basic Rate for 802.11a, 802.11g, or 802.11b/g mixed	
	1 and 2 Mbps 1, 2, 5.5 , 6 , 11, 12, and 24 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames
Preamble	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble.
Broadcast SSID	Enabled/Disabled	When disabled, the AP hides the SSID in outgoing beacon frames and client can not obtain the SSID through passive scanning. Also, when it is disable, the AP doesn't send probe responses to probe requests with unspecified SSIDs.

6.2 Wireless Access Point – Security

Click the entry on the left hand navigation panel for Wireless Access Point – Security. This directs you to the Wireless Access Point – Security page.



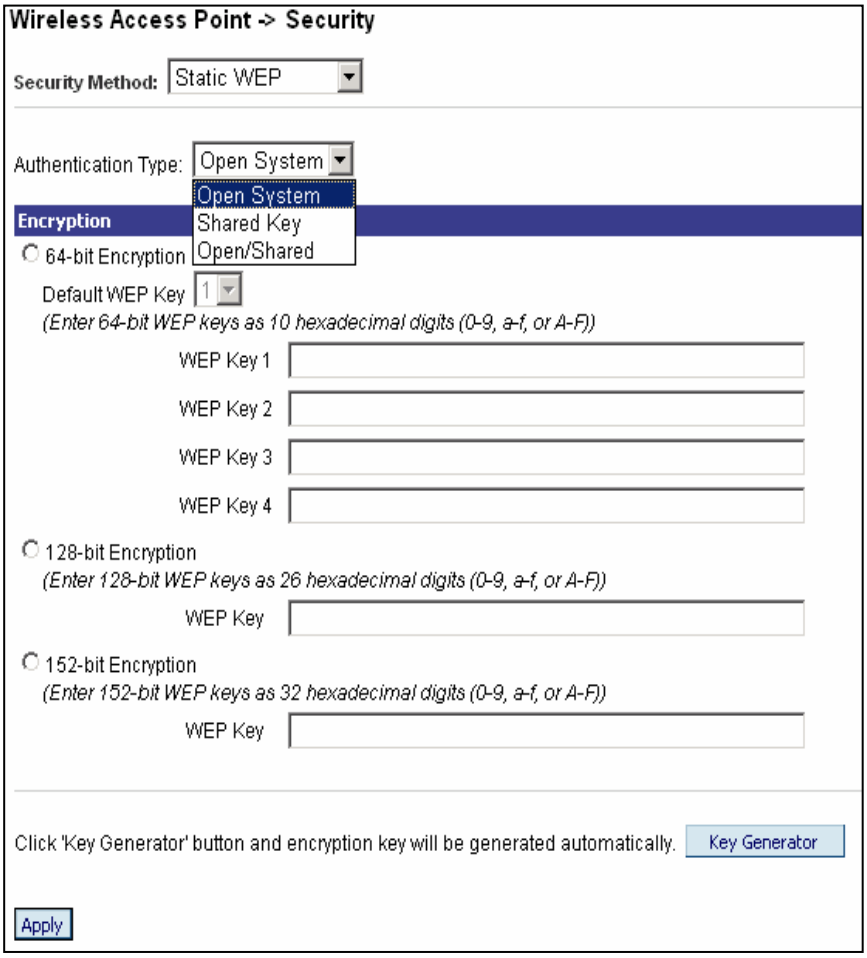
The WH-9100MESH will display a default factory setting of no encryption, but for security reasons will not communicate to any clients unless the encryptions set by administrator. You must select the wireless encryption that you want to use and click Apply. If you want to leave the encryption set to No Encryption, chooses "None" and clicks Apply. A popup dialog box will ask "are you sure you want to proceed to BYPASS mode?" Click OK to enter BYPASS mode with no encryption setting.

6.2.1 WEP

WEP (Wired Equivalent Privacy) was originally designed to provide the same level of security for wireless LANs as that of a wired LAN but is not now state-of-the-art. But the use of WEP encryption can still provides some measure of security. WEP relies on the use of identical static keys deployed on client stations and access points. In WEP, you can set the Authentication Type for **Open System**, **Shared Key**, or **Open/Shared**. Select 64.bit, 128bit or 152.bit encryption and enter the WEP key as appropriate. ".

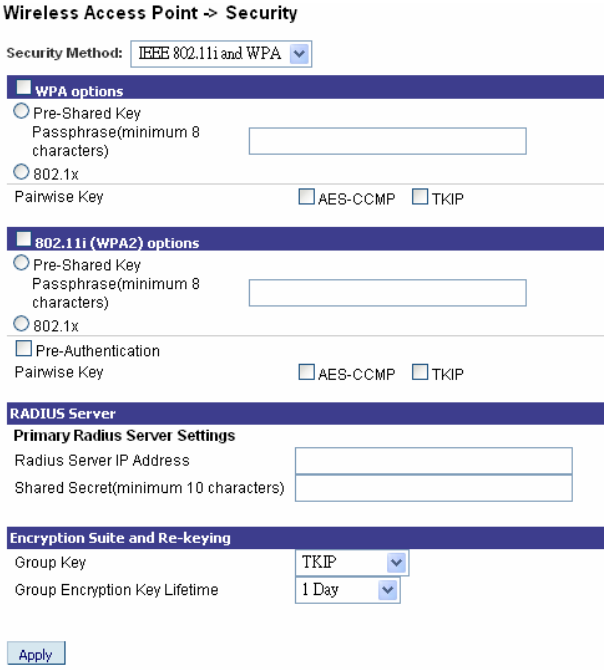
- Key Generator: The “Key generator” function generates a randomized encryption key of the appropriate length automatically. The key is initially shown in plain text so the user has the opportunity to copy the key. Once the Key is applied, there is no longer displayed in plain text.

That same WEP key must also be set on each wireless clients those are to become part of the wireless network. For greater security, set authentication type to “shared Key, and if "shared key" is accepted, then each wireless device must also be coded for "shared key”.



6.2.2 802.11i and WPA

The WH-9100MESH supports 802.11i (WPA2)



- **WPA**

WPA (Wi-Fi Protected Access) uses Temporal Key Integrity Protocol (TKIP) to improved data encryption. WPA was designed to enable use of wireless legacy systems employing WEP while improving security. In addition, user authentication is enabled using the Extensible Authentication Protocol (EAP).

- **TKIP or AES-CCMP:**

TKIP scrambles keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. The TKIP improves security especially for legacy hardware, and then the AES-CCMP is a stronger encryption algorithm for newer hardware.

Simply input up to 63 character /numeric /hexadecimals in the Passphrase field. If your clients use WPA-TKIP select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMR.

- **Pre-Share Key or 802.1x:**

If you don't have Radius Server, selecting pre-shared key.

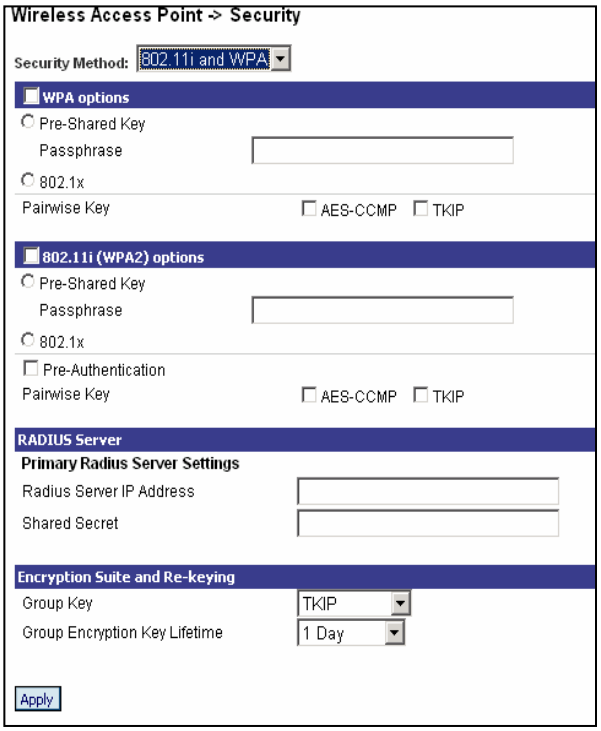
If you have installed Radius Servers, select WPA 802.1x and input the Radius Server setting. Use of Radius Server for key management and authentication requires that you have installed a separate certification system and each client must have been issued an authentication certificate.

- **Re-keying time:**

This is the frequency in which new encryption keys are generated and distributed to the client. The more frequent re-keying time, the security will be better. For highest security, select the lowest re-keying interval.

- **802.11i (WPA2)**

The IEEE 802.11i is a new standard that enhances the 802.11 MAC security and authentication by stronger encryption, authentication, and key management. The WPA2 and 802.11i are virtually identical. The WPA2 is the Wi-Fi Alliance base on the IEEE 802.11i and runs a certification program that grants the WPA2 brand based on equipment's support of the important feature of 802.11i.



Besides the Pre-authentication function, setting WPA2 is most same as WPA,

- **Pre-authentication**

  Enable pre-authentication to allow a client to authenticate in advance with the AP before the client is associated with it. Allowing the AP to pre-authenticate a client decreases the transition time when a client roams between APs.

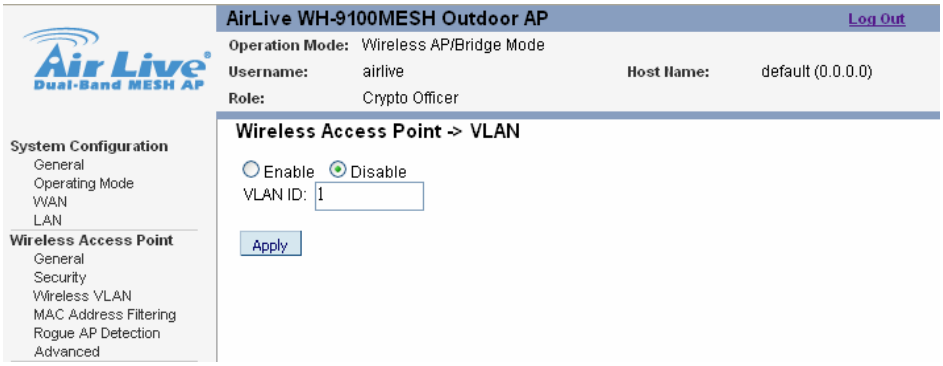
Once you have selected the options you will use, click Apply to save all setting.

6.3 Wireless VLAN

When VLAN is enabled, all data coming out the WAN port is VLAN-tagged, which means an external network unit such as router, switch , or a VLAN-enable computer had to be sure to terminate the VLAN traffic. Data originating from or targeting to wireless network client is tagged with the VLAN ID corresponding to an SSID it is associated with. Data generated by an Access Point itself is tagged with the management VLAN ID.

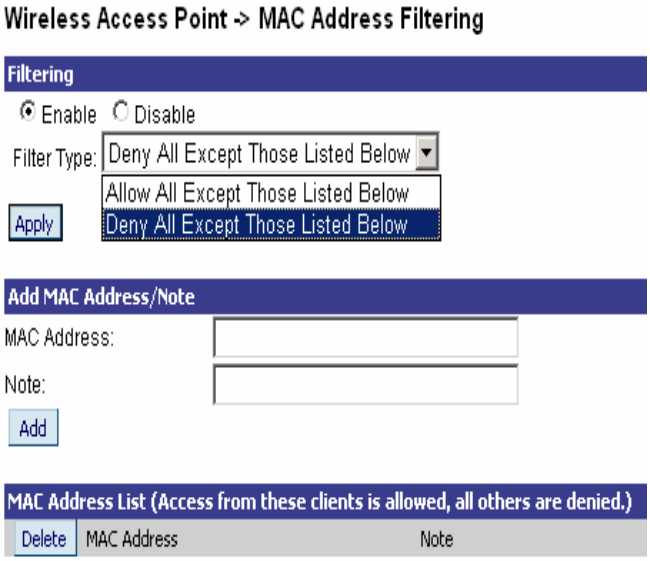
To create a new VLAN, enter a VLAN ID (range form 1 to 4094) and an SSID. Set the security to None, Static, or IEEE 802.11i and WPA.

After you create a VLAN you can modify it by selecting the VLAN from existing VLAN list.



6.4 MAC address Filtering

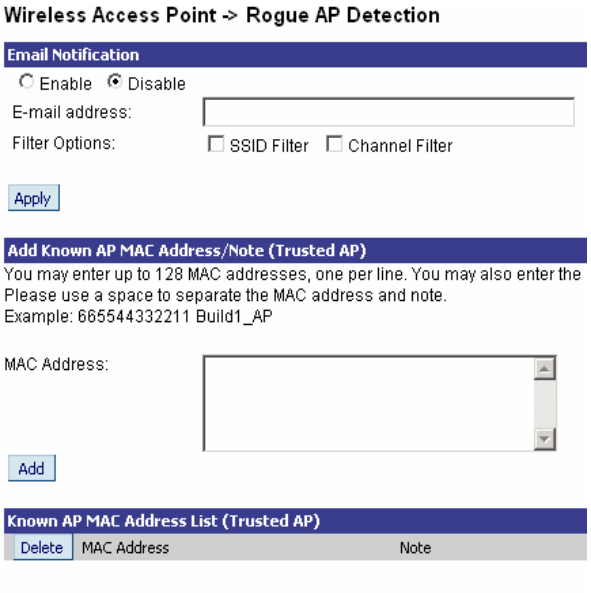
The factory default for MAC Address filtering is Disabled. If you enable MAC Address filtering, you should also set the toggle for Filter Type. This works as follows:



- If Filtering is enabled and Filter Type is "**Deny All Except Those Listed Below**" , only those devices equipped with the authorized MAC addresses will be able to communicate with the AP. In this case, input the MAC addresses of all the PC cards that will be authorized to access this AP.
- If Filtering is enabled and Filter Type is "**Allow All Except Those Listed Below**", those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the AP.In this case, navigate to the report: Wireless Clients and copy the MAC address of any wireless Client that you want to exclude from communication with the AP and input those MAC Addresses to the MAC Address list.

6.5 Rogue AP Detection

This function allows the network administrator to detect in band rogue AP. Enable rogue AP detection and enter the MAC Address of each AP in the network that you want the AP being configured to accept as trusted AP (You may add up to 20 APs). Enter an email address for notification of any rogue or non- trusted APs when WH-9100MESH find it. You can also select the following filter options.



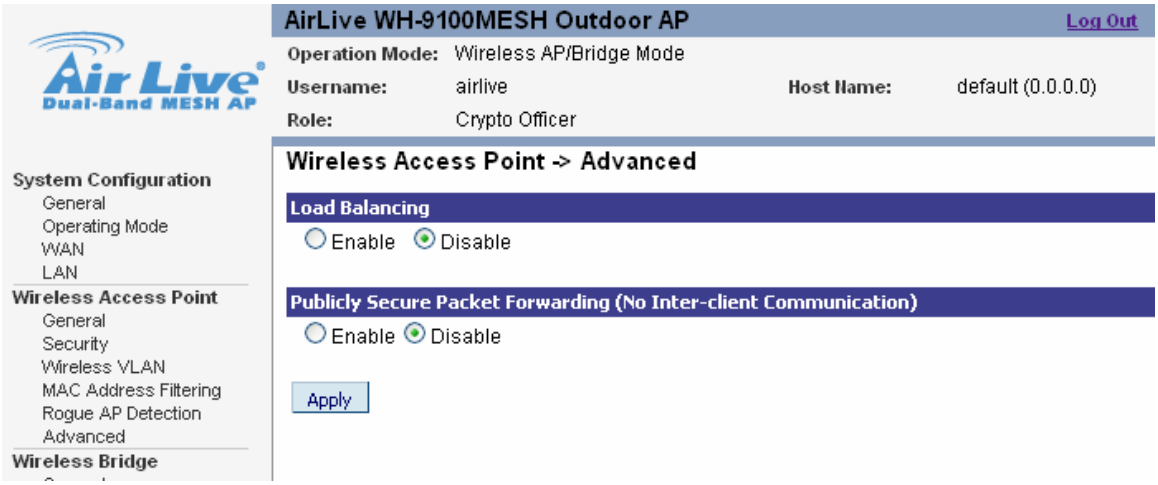
- SSID Filter: Check the SSID option to only send rogue APs that match the AP's SSID or wireless bridge's SSID.
- Channel Filter: Check the channel filter option to only send rogue APs that match the AP's channel or the wireless bridge's channel.
- If both options are checked, only APs that match both the SSID and channel are sent.

The Adjacent AP lists under Monitoring/Reports on the navigation menu, will detail any APs'

information.

6.6 Wireless Access Point – Advanced

Click the entry on the left hand navigation panel for Wireless Access Point – Advanced. This directs you to the Wireless Access Point – Advanced page. The Advanced page allows you to enable or disable load balancing and Layer 2 Isolation



6.6.1 Load Balancing

Load balancing is enabled by default to distribute traffic efficiently among network servers so that no individual server is overburdened. For example, if two APs with similar settings are in a conference room, depending on the location of the APs, all wireless clients could potentially associate with the same AP, leaving the other AP unused. Load balancing attempts to evenly distribute the wireless clients on both APs.

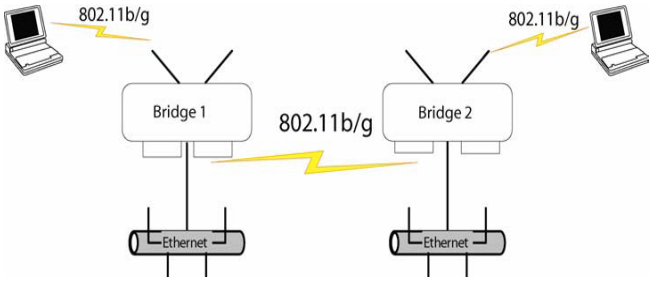
6.6.2 Publicly Secure Packet Forwarding

The Publicly Secure Packet Forwarding selection item is the Layer 2 Isolation function. Layer 2 isolation prevents wireless clients that associate with the same AP from communication with each other.

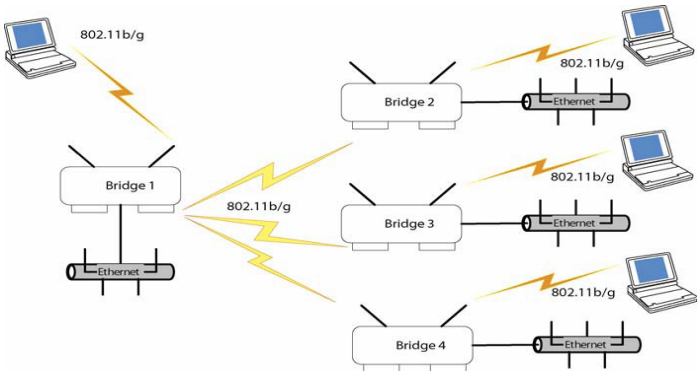
Chapter 7: Wireless Bridge Configuration

In the 9100MESH, wireless bridging uses a second WLAN card (WLAN2) to set up an independent wireless bridge connection. Thus, the 9100MESH can work AP and Bridge simultaneously and with no loss efficiency. Since wireless bridging provides a mechanism for AP to collaborate, it is possible to extend the basic service set (BSS) of a standalone AP and to connect two separate LANs without installing my cabling. The 9100MESH model support manual bridge function and **auto bridge mode**. The manual bridging function in the WH-9100MESH allows you to set a number of alternate bridging configurations. We discuss some of the most popular settings in this chapter. The auto bridging function will be discussed at next chapter (Chapter 8).

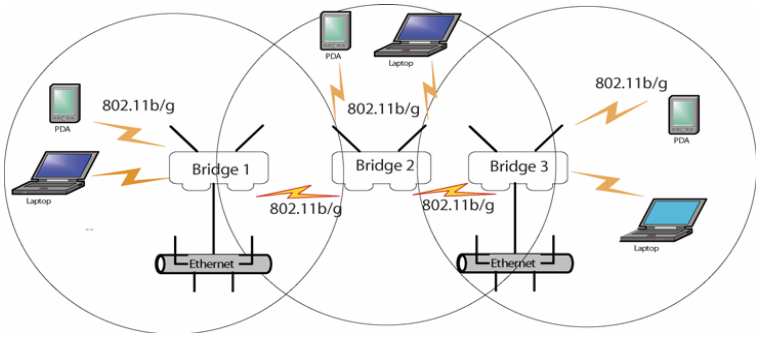
- Point-to-Point bridging of two Ethernet Links



- Point-to-Multipoint bridging of several Ethernet links



- Repeater mode

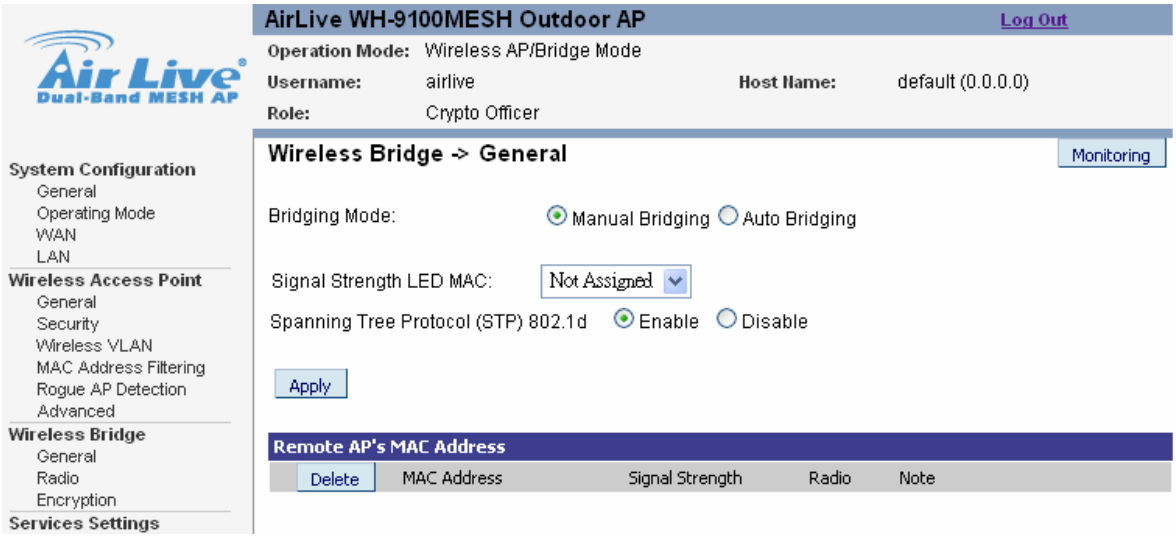


7.1 Wireless Bridge – General

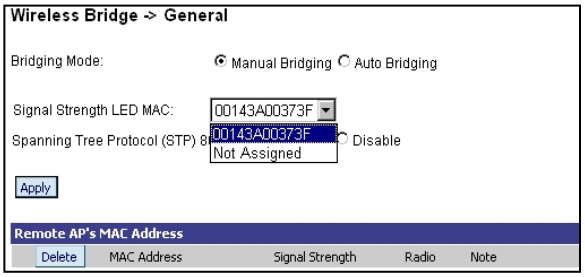
Click the entry on the left hand navigation panel for Wireless Bridge - General. This directs you to the

Wireless Access Point – Bridging page.

7.1.1 Manual Bridging



- **Signal strength LED MAC:**



Signal strength LED MAC allows you set up the SS (Signal Strength) LED to indicate the received bridge signal strength (RSSI, Received Signal Strength Indication) of remote device the. When you key in the BSSID at "Add Remote's AP BSSID/Note" section and click "Add", this BSSID will be indicated here. Choosing the BSSID that you want to know the received signal strength, the SS LED will indicate the signal strength by different flicker frequency. If you don't wish to display any connection signal, select "Not Assigned". You need click "Apply" after you change this value.

- **Spanning Tree Protocol (STP) 802.1d:**

  It should be enabled if there is any possibility that a bridging loop could occur. If you are certain that there is no possibility that a bridging loop will occur, you can disable Spanning Tree Protocol, because the bridge will be more efficient (faster) without it. However, if not sure, the safest solution is to enable Spanning Tree Protocol.

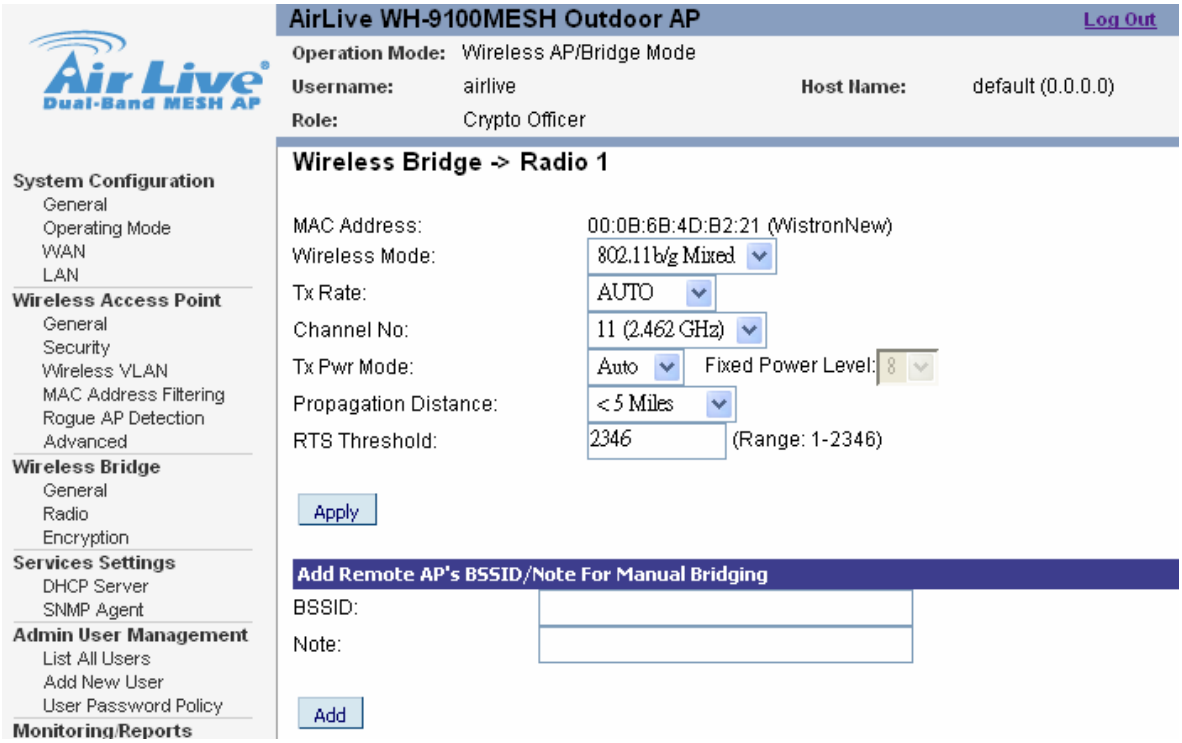
- **Remote AP's MAC Address**

  This section list the remote bridge's information, port number, signal strength and note. Moreover, if you don't want to link with some remote bridges, click the check box at the left side of port number and confirm by clicking "Delete".

7.1.2 Auto Bridging

The detail function of Auto Bridging describes at Chapter 8.

7.2 Wireless Bridge – Radio



- **MAC Address:**
  This is the MAC Address for WLAN card and as BSSID for the bridge devices at the other end that want to link with this unit. The Wireless Bridging uses the BSSID for purposes of establishing contact.

- **Wireless Mode:**

  WH-9100MESH supports 802.11 b/g Mixed, 802.11g Super and 802.11a modes

  Note: When the WH-9100MESH's AP is working, we don't suggest you set up the bridge's Wireless mode as 802.11g Super mode. This is because the 802.11g Supper mode occupy large frequency bandwidth, it may interfere the AP's radio signal.

- **Tx Rates:**
  When set to AUTO, the unit attempts to select the optimal rate for the channel. If a fixed rate is used, the unit will only transmit at that rate.

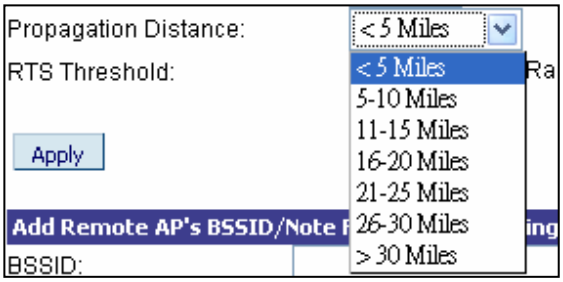
- **Channel No:**
  The channel number is a means of an assigning frequency that device uses it to transmit/receive data. The channel number should be same as the one using on the devices those will be bridge together.

- **Tx Pwr Mode:**

  It is same as AP, support Off, Fix and Auto modes. At Fix mode, there are 5 signal levels you can select (1 being the smallest power level). If you want to prevent any radio frequency transmission, set Tx Pwr Mode to off.

- **Propagation Distance**

  This parameter relates to adjust the timing of WLAN MAC. To make sure the radio signal can reach to the device at other end, set the distance based on the distance between this bridge and furthest bridge that is connected to it



- **RTS Threshold**

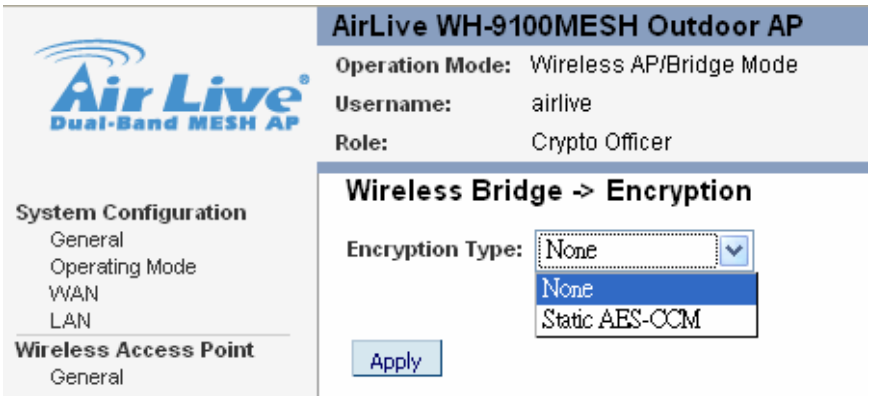
  This function uses for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed

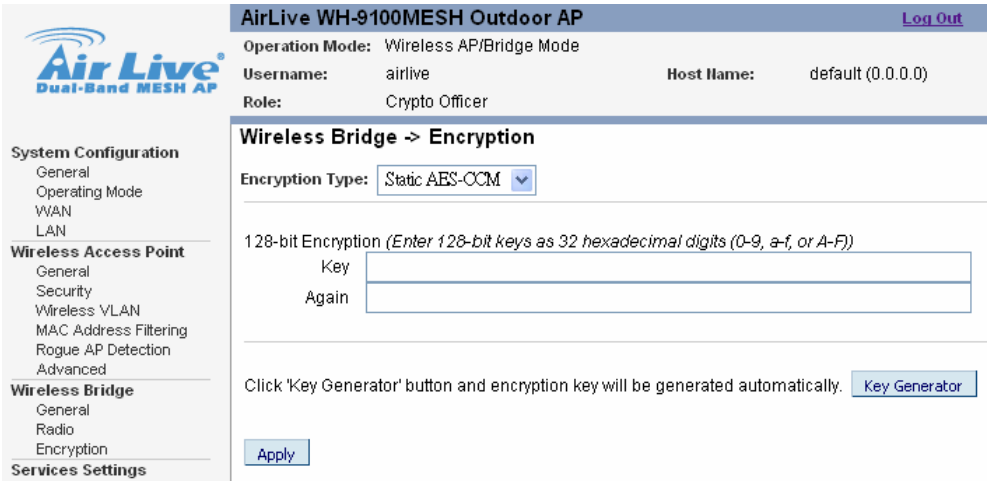
- **Add Remote's AP BSSID/Note for manual bridging**

  The BSSID corresponds to that bridge's MAC address. The Wireless Bridging uses the BSSID for purposes of establishing contact. You need to enter the BSSID of remote bridge, enter hexadecimal with colons. Data entry is not case sensitive. You may also enter a note that defines the location of the remote bridge. Then click Add to accept. The remote bridge's BSSID will now appear in the **Remote AP's MAC Address** section of previous page Wireless Bridge - General.

7.3 Wireless Bridge - Encryption

This page is used to configure static encryption keys for the wireless bridge. On this screen, you can either select Off- No Data Encryption or Static AES Key of 128 bit. The "Key generator" function generates a randomized encryption key of the appropriate length automatically. You can use this function to get a randomized key number from one device and use it to all of other devices those are on the same bridge network. The encryption key that you use on this screen must be the same for any bridge connect to your bridging network in order for communication to occur.

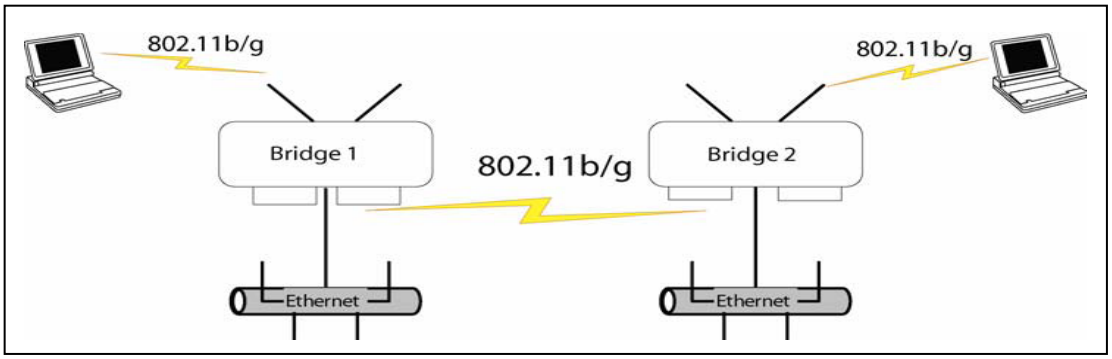




7.4 Point-to-Point Bridge Setup Guide

A point-to-point link is a direct connection between tow, and only two, locations or nodes. Because the WH-9100MESH's bridge function uses a separate WLAN card for bridge. Thus, the 9100MESH can work AP and Bridge function simultaneously.

Figure 7-1 Point-to-Point Bridge scene



For the two bridges that are to be linked to communicate properly, they have to be set up with compatible commands in setup screens. Below is the list

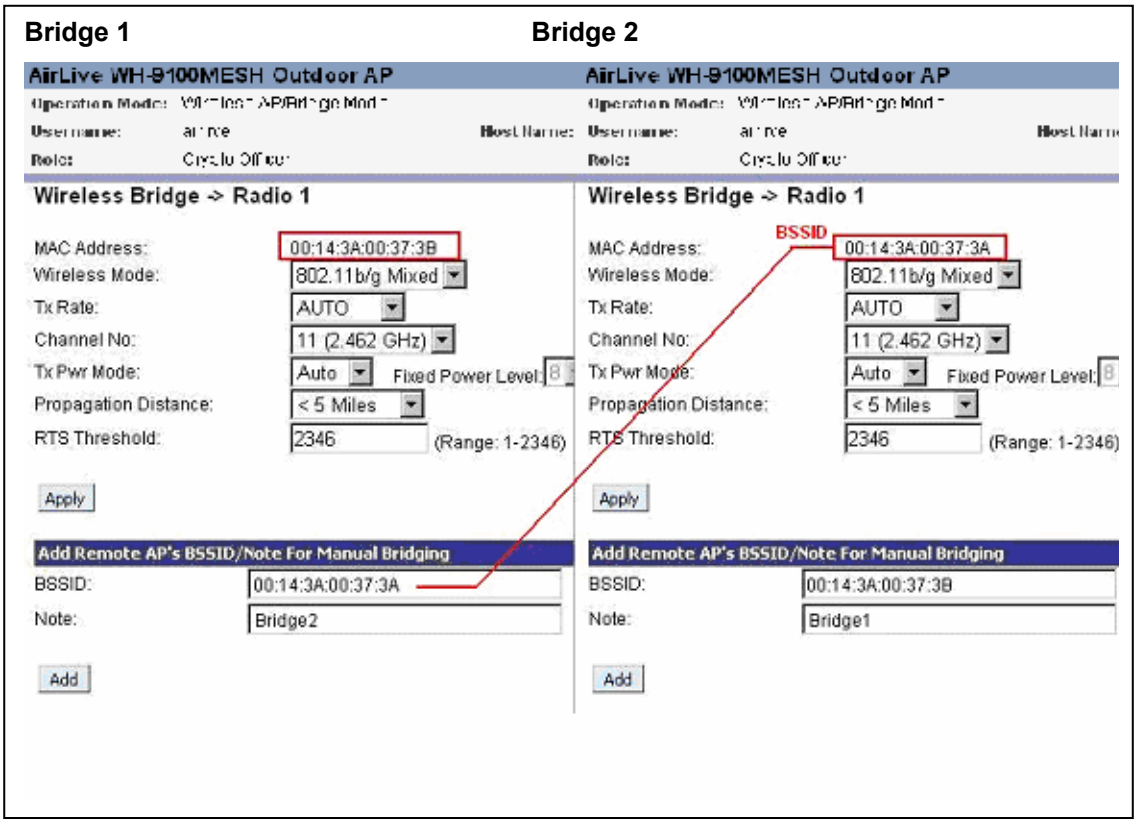
- **Channel number:**
  - The bridges must have the same channel number.
  - The channel number doesn't be same as using for AP.
- **Wireless Mode:**
  - Choose 802.11g for high data rate
  - Choose 802.11b for high transmit distance
- **Spanning Tree Protocol (802.1d):**
  - Enable, if there is any possibility of a bridging loop, or
  - Disable, if there is no possibility of bridging loop to gain higher efficient
- **Bridge signal strength LED port:**
  - Set up the SS LED map to which remote bridge

- **BSSID:**
  - Entering remote bridge's MAC address at the BSSID field of "Add remote AP's BSSID/Note" section. Although it is option item, entering a note that defines the location of the remote bridge may be helpful for your management lots of remote bridges. After you key in BSSID and Note, clock the "Add" to list this item at "Remote AP's MAC Address" section.
- **Encryption:**
  - Setting Encryption type: Off or Static AES Key
  - Each bridge must have the same encryption type. And if using Static AES Key, the key of each bridge must be the same.

Click apply to accept your changes

7.4.1 Example: Point-to-Point Bridge configuration

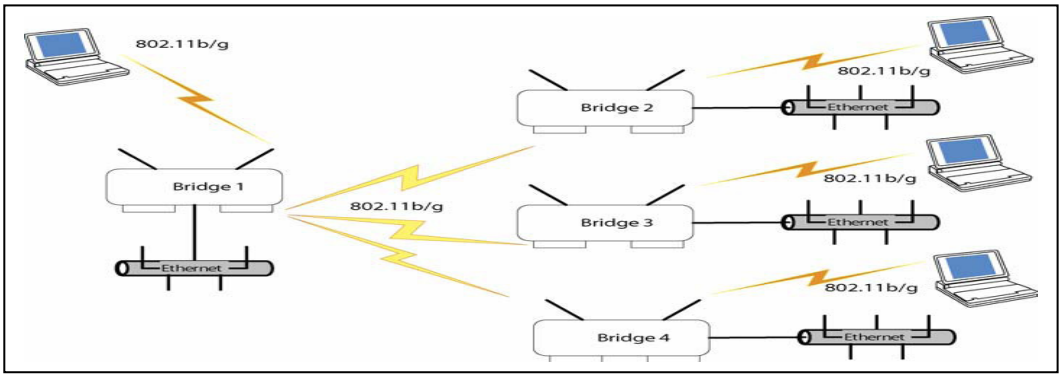
Direction	**Bridge 1**	**Bridge 2**
Wireless Bridge - General		
Bridge Mode	Manual Bridge	Manual Bridge
Spanning Tree Protocol	Enable (or Disable if no bridging loop)	Enable (or Disable if no bridging loop)
Wireless Bridge - Radio		
Channel	4	4
Wireless Mode	802.11g (for high data rate)	802.11g (for high data rate)
TX Power	Auto	Auto
Propagation distance	Select appropriate value	Select appropriate value
BSSID	Add Bridge 2 BSSID (MAC address)	Add Bridge 1 BSSID (MAC address)
Wireless Bridge – Encryption		
Encryption	Select appropriate Key type and Key. Must be the same key as Bridge 2	Select appropriate Key type and Key. Must be the same key as Bridge 1



7.5 Point-to-Multipoint Bridge Setup Guide

A Point-to-Multipoint configuration allows you to set up three or more 9100MESH in bridging mode and accomplish bridging between 3 or more locations wirelessly. Figure 7-3 illustrates a Point-to-Multipoint topology as an example

Figure 7-3 Point-to-Multipoint Bridge scene



Same as Point-to-Point Bridge Setup procedure, you need to set up with compatible commands in setup screens. Using Figure 7-3 as a example, Bridge 1 must contain all of the other's BSSID, while Bridge 2 and 3 must contain Bridge 1's BSSID.

Direction	Bridge 1	Bridge 2~3
Wireless Bridge - General		

Bridge Mode	Manual Bridge	Manual Bridge
Spanning Tree Protocol	Enable (or Disable if no bridging loop)	Enable (or Disable if no bridging loop)
Wireless Bridge - Radio		
Channel	4	4
Wireless Mode	802.11g (for high data rate)	802.11g (for high data rate)
TX Power	Auto	Auto
Propagation distance	Select appropriate value	Select appropriate value
BSSID	Add Bridge 2 BSSID (MAC address)	Add Bridge 1 BSSID (MAC address)
Wireless Bridge – Encryption		
Encryption	Select appropriate Key type and Key. Must be the same key as Bridge 2	Select appropriate Key type and Key. Must be the same key as Bridge 1

The above recommended setup requires only Bridge 1 to be set in point-to-multipoint mode. It is possible to set all bridges in point-to-multipoint mode, in which case, each bridge would have to contain the BSSID for each of the other bridges and Spanning Tree Protocol must be enabled.

7.6 Repeater Bridge Setup Guide

A repeater setup can be used to extend the wireless signal from one bridge connected to an Ethernet LAN wirelessly so that another bridge can control a wireless LAN at a distance. Figure 7-4 illustrates this topology.

Figure 7-4 Point-to-Multipoint Bridge scene

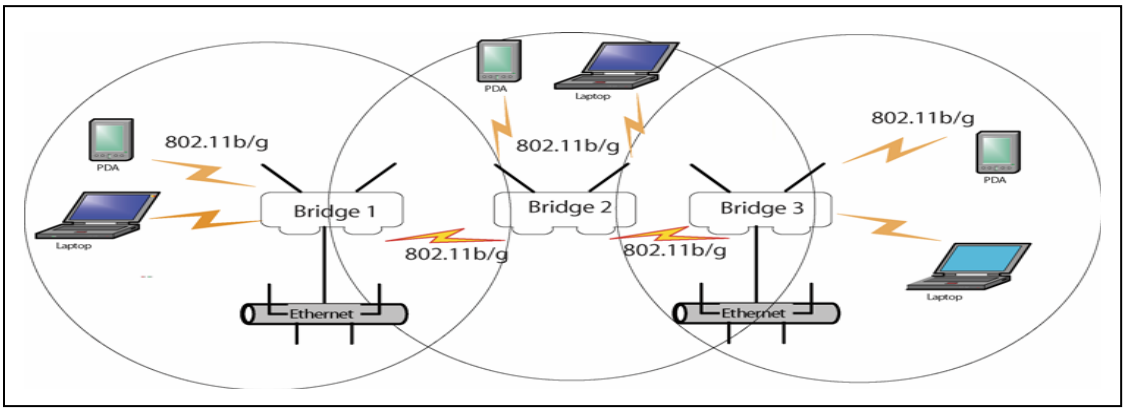


Table 7-3 describes the basic attributes for the network topology illustrate at Figure 7-4.

Table 7-3 Repeater Configuration table

Direction	Bridge 1	Bridge 2	Bridge 3

Wireless Configuration - General			
Bridge Mode	Manual Bridge	Manual Bridge	Manual Bridge
Spanning Tree Protocol	Enable (Disable if no loop)	Enable Disable if no loop)	Enable Disable if no loop)
Wireless Bridge - Radio			
Channel	4	4	4
Wireless Mode	802.11g (for high data rate)	802.11g (for high data rate)	802.11g (for high data rate)
TX Power	Auto	Auto	Auto
Propagation distance	Appropriate value	Appropriate value	Appropriate value
BSSID	Add Bridge2's BSSID (MAC address)	Add Bridge1's and 3's BSSID(MAC address)	Add Bridge2's BSSID (MAC address)
Wireless Configuration – Bridging Encryption			
Encryption	Select appropriate Key type and Key. Must be the same key as Bridge 2	Select appropriate Key type and Key. Must be the same key as Bridge 1	Select appropriate Key type and Key. Must be the same key as Bridge 1

Chapter 8: Auto Bridge (Wireless Mesh Network)

This chapter describes the feature of 9100MESH, Auto-forming wireless bridging. If you don't know how to enter configuration screen, chapter 4 describes how to do it. Please keep in mind that you need click Apply to save all settings.

8.1 Auto Bridge Wireless (Mesh) Network

At manual bridge mode, you need to write down each bridge devices' BSSID, wasting time to find out their network topology and then key in the BSSID in every device. If on of device out of order, the original network topology is useless and the bridging network is broken. You need take time to find out which device is broken, find out the new topology and key in the new BSSID to every device again.

The Auto bridge Wireless (Mesh) Network technology is a auto-forming, auto-hearing network solution. When the wireless bridge mode is in auto bridge mode, you can form the up to 40 bridges devices' network topology automatically. Using the Auto Bridge function, the devices will bridge together automatically when their SSID and Radio Parameters are the same. Those devices will calculate the bridge network topology and also monitor the bridge network status automatically. Thus, if some of devices are out of order or change location, a new bridge network topology will be made and let those devices bridge together again. The feature is called auto-hearing.

8.2 Rule of Auto Bridge mode

8.2.1 Root device

The lowest priority number plus BR MAC address will be selected to be the root device of bridging network. The priority number is a setting parameter at Wireless Bridge – General (Bridging Mode as Auto Bridging) screen. The BR information is the LOWEST MAC address of all the MAC address on this unit. They include LAN, WAN, WLAN1 and WLAN2.

However, if the wireless network is connected to an Ethernet switch which might has STP (Spanning Tree Protocol) devices on the same network. The root will be assign to the lowest MAC address of the STP device on the network.

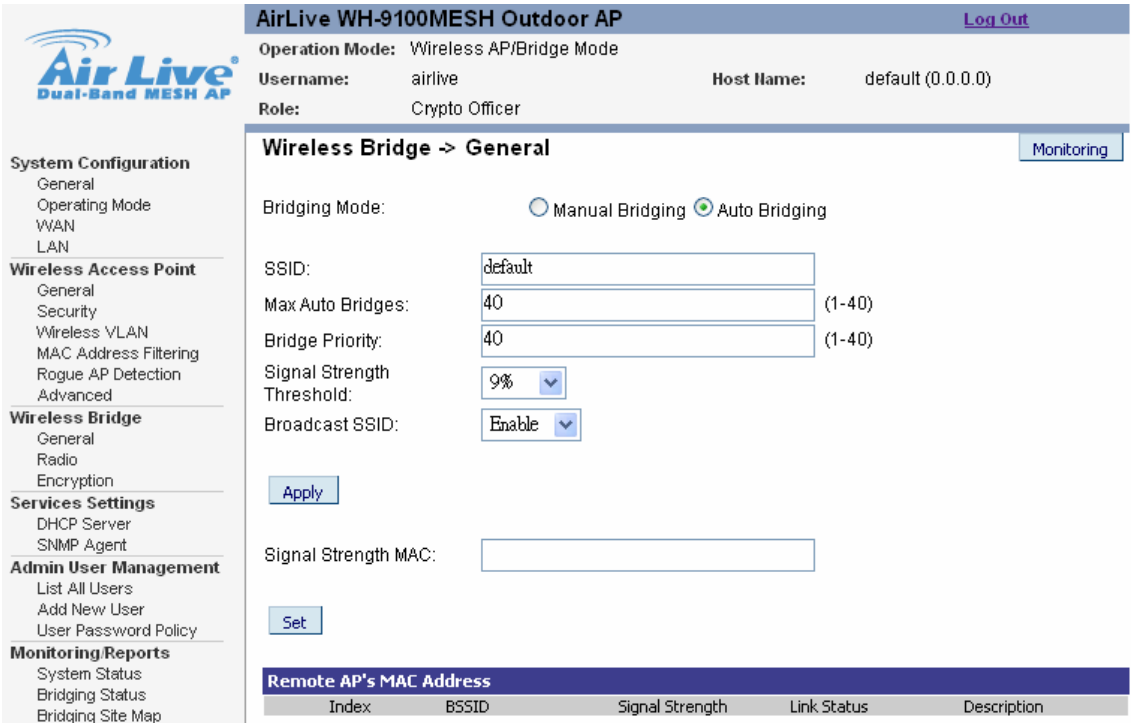
8.2.2 Routing Path

The routing path of auto bridging network is defined a node select the lowest path cost to the root device. The path cost is base on the Signal Strength and Priority. If the higher Signal Strength will be selected as routing path. If the Signal Strength is happen to be the same, then the lower priority number will be the routing path. If the priority number is same, the lower MAC address will be assigned to the routing path.

8.3 Auto Bridge GUI Screen

8.3.1 Wireless Bridge – General GUI Screen

Click the entry on the left hand navigation panel for Wireless Bridge-General and choose Auto Bridging, directs you to this page.



- **SSID:**

  The SSID can be treated as a nickname of Auto Bridge network. The SSID of bridges those you want to link together need be same.

- **Max Auto Bridges:**

  Maximum number of auto bridge allowed

- **Bridge Priority:**

  Determining the root device and routing path cost, the lowest bridge priority in the network will become the root device of bridge network topology.

- **Signal Strength Threshold:**

  If the signal strength of remote node is blow this threshold. The link will be dropped.

- **Broadcast SSID**

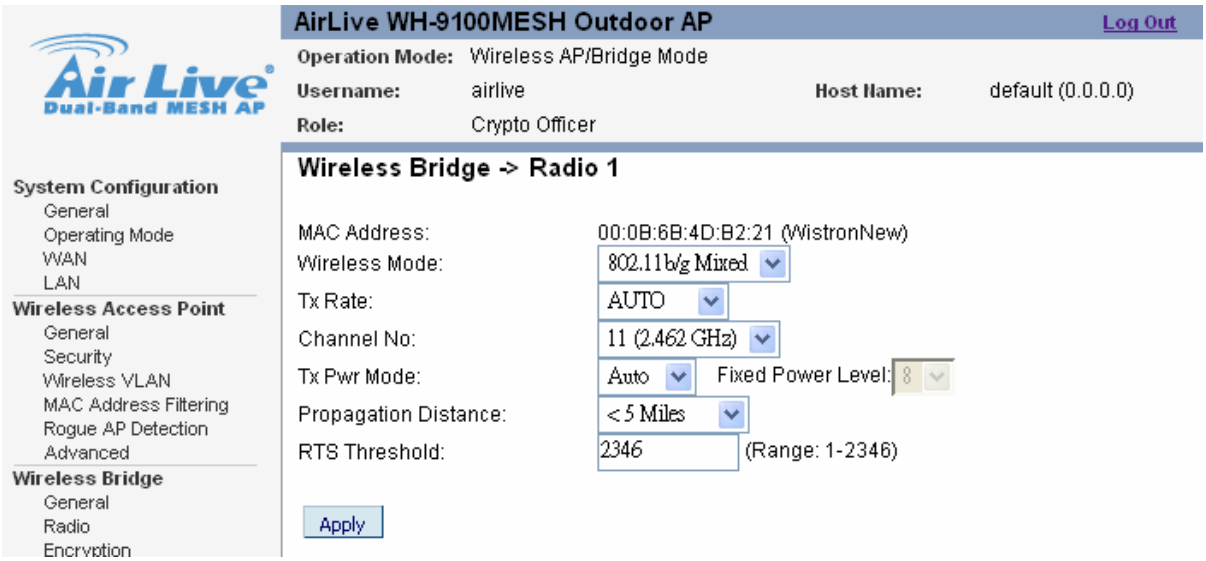
  It on by default to enabled bridge will use SSID for token for communication. If don't like SSID be exposed, it can be disable. However both setting must be same, otherwise the devices cannot bridge together.

- **Signal Strength MAC:**

  Choosing the BSSID that you want to know the received signal strength, the SS LED will indicate the signal strength by different flicker frequency. If you don't wish to display any connection signal, just leave it as empty. You need click "Set" after you change this value.

8.3.2 Wireless Bridge – Radio GUI Screen

Click the entry on the left hand navigation panel for Wireless Bridge - Radio when bridge mode set as Auto Bridging, directs you to this page



- **MAC Address:**

  This is the MAC Address for WLAN card that is for bridge function.

- **Wireless Mode:**

  WH-9100MESH supports 802.11 b/g Mixed, 802.11g Super and 802.11a modes

  Note: When the WH-9100MESH's AP is working, we don't suggest you set up the bridge's Wireless mode as 802.11g Super mode. This is because the 802.11g Supper mode occupy large frequency bandwidth, it may interfere the AP's radio signal.

- **Tx Rates:**

  When set to AUTO, the unit attempts to select the optimal rate for the channel. If a fixed rate is used, the unit will only transmit at that rate.

- **Channel No:**

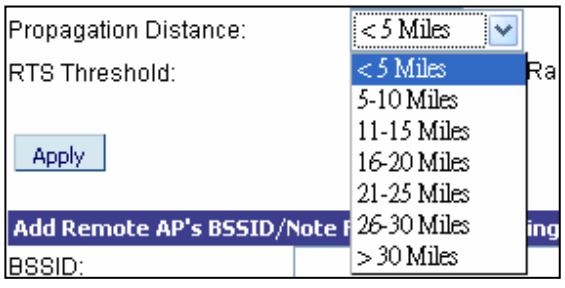
  The channel number is a means of an assigning frequency that device uses it to transmit/receive data. The channel number should be same as the one using on the devices those will be bridge together.

- **Tx Pwr Mode:**

  It is same as AP, support Off, Fix and Auto modes. At Fix mode, there are 5 signal levels you can select (1 being the smallest power level). If you want to prevent any radio frequency transmission, set Tx Pwr Mode to off.

- **Propagation Distance**

  This parameter relates to adjust the timing of WLAN MAC. To make sure the radio signal can reach to the device at other end, set the distance based on the distance between this



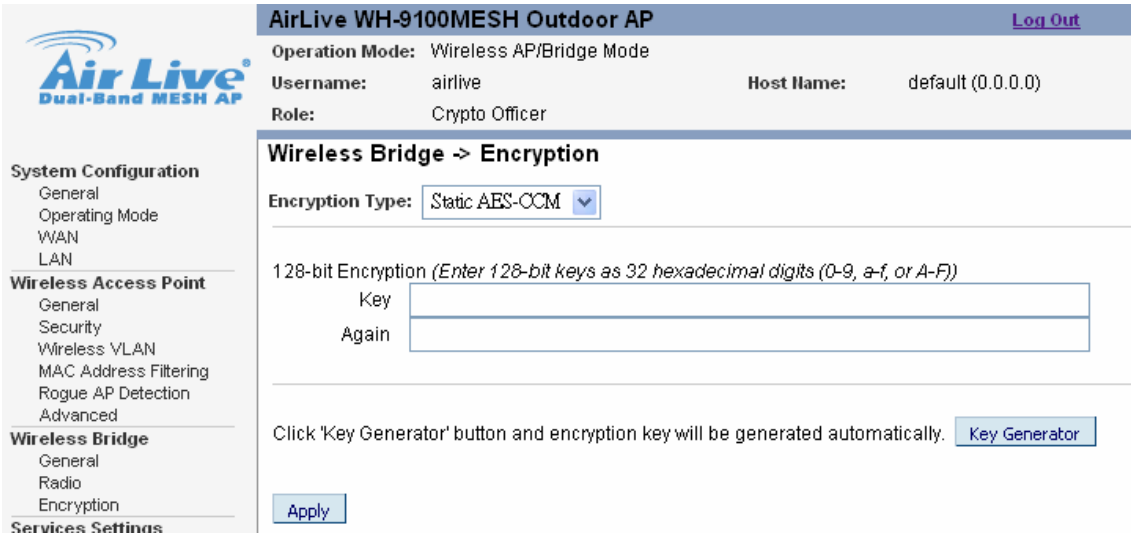
bridge and furthest bridge that is connected to it

- **RTS Threshold**

  This function uses for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed

8.3.3 Wireless Bridge – Encryption Screen

Click the entry on the left hand navigation panel for Wireless Bridge - Encryption when bridge mode set as Auto Bridging, directs you to this page.

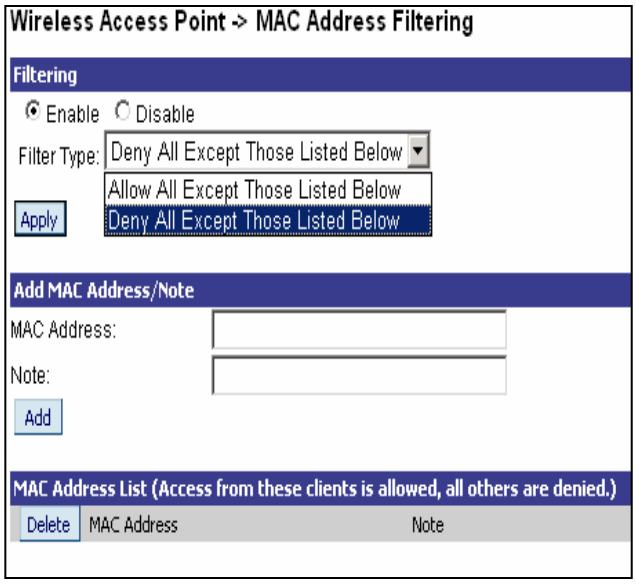


This page is used to configure static encryption keys for the wireless bridge. On this screen, you can either select Off- No Data Encryption or Static AES Key of 128 bit. The “Key generator” function generates a randomized encryption key of the appropriate length automatically. You can use this function to get a randomized key number from one device and use it to all of other devices those are on the same bridge network. The encryption key that you use on this screen must be the same for any bridge connect to your bridging network in order for communication to occur.

8.3.4 Wireless Bridge – MAC Address filtering

The factory default for MAC Address filtering is Disabled. If you enable MAC Address filtering, you should also set the toggle for Filter Type. This works as follows:

- If Filtering is enabled and Filter Type is “**Deny All Except Those Listed Below**” , only those devices equipped with the authorized MAC addresses will be able to communicate with the AP. In this case, input the MAC addresses of all the PC cards that will be authorized to access this AP.



- If Filtering is enabled and Filter Type is "**Allow All Except Those Listed Below**", those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the AP.In this case, navigate to the report: Wireless Clients and copy the MAC address of any wireless Client that you want to exclude from communication with the AP and input those MAC Addresses to the MAC Address list.

8.4 Auto Bridge General Settings

Items	Parameters	Description
Wireless Bridge – General Page		
SSID		The SSID of bridges those you want to link together need be same.
Max Auto Bridges	1 ~ 40	Maximum number of auto bridge allowed
Bridge Priority	1 ~ 40	Determines the root device. The lowest bridge priority in the network will become the root device of bridge network topology.
Signal Strength Threshold		If the signal strength of remote node is blow this threshold. The link will be dropped.
Broadcast SSID		Default on to enabled bridge will use SSID for token for communication. If don't like SSID be exposed, it can be disable. However both setting must be same, otherwise the devices cannot bridge together.
Wireless Bridge – Radiol Page		
Wireless Mode	802.11b/g Mixed 802.11g Super 802.11a 802.11a Turbo	
Tx Rate	Auto 6, 9, 12, 24, 36, 48, 54 Mbps	When set to AUTO, the unit attempts to select the optimal rate for the channel. If a fixed rate is used, the unit will only transmit at that rate.
Channel Number		Set the channel frequency for the wireless bridge. The bridges those you want to link together need be same channel frequency
Tx Pwr Mode		It is same as AP, support Off, Fix and Auto modes. At Fix mode, there are 5 signal levels you can select (1 being the smallest power level). If you want to prevent any radio frequency transmission, set Tx Pwr Mode to off.
Propagation Distance	< 5Miles 5~10 Miles 11~15 Miles 16~20 Miles 21~25 Miles 26~30 Miles > 30 Miles	Set the distance based on the distance between this bridge and furthest bridge that is connected to it

Chapter 9: Service Settings Menu

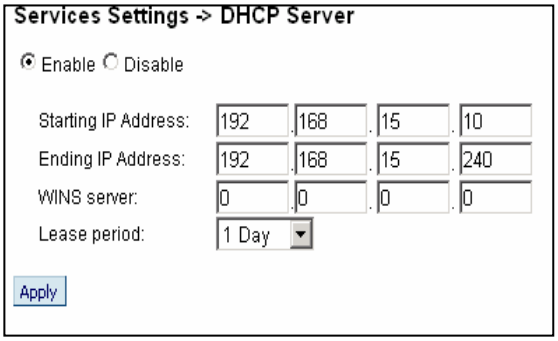
This chapter describes the items about Service Setting. If you don't know how to enter configuration screen, chapter 4 describes how to do it. Please keep in mind that you need click Apply to save all settings. Please keep in mind that you need click Apply to save all settings.

Click the entry on the left hand navigation panel for Service Setting. This directs you to this page.

9.1 DHCP server

This page allows configuration of the DHCP server function. The DHCP server function, accessible only from the Local LAN port, is used for initial configuration of the management function.

The default factory setting for the DHCP server function is enabled. You can disable the DHCP server function, if you wish. You can also set the range of address to be assigned.

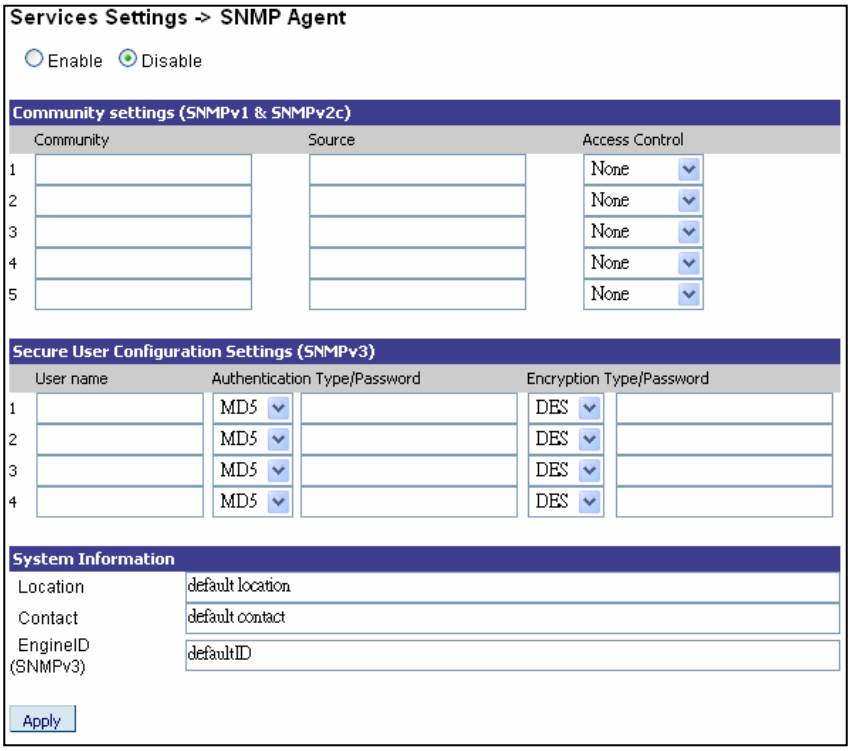


WNS server: The WNS (Windows Internet Naming Service) server is used for name resolution. It is similar in function to DNS. It allows you to search for resources by computer name instead of IP address

Lease period is for the DHCP server function. The lease times you can select are: 1 hour, 2 hours, 1 day, 2 days, or 1 week.

9.2 SNMP

The SNMP collects and stores management information for use in a network management system. The Wh-9100MESH integrated SNMP agent software module translates the device management information into a common form for interpretation by the SNMP manager, which usually resides on a network administrator's computer.



The SNMP manager function interacts with the SNMP agent execute applications to control

and manage object variables (interface features and devices) in the gateway. Components of managed information include number of packets received on an interface, port status, dropped packets, and so forth.

The SNMP configuration consists of several fields, which are explained below:

- **Community:**
  This is simply the SNMP terminology for “password” for SNMP functions.
- **Source:**
  This field is for Key in the IP address or name where the information is obtained.
- **Access Control:**
  Define the level of management interaction permitted.

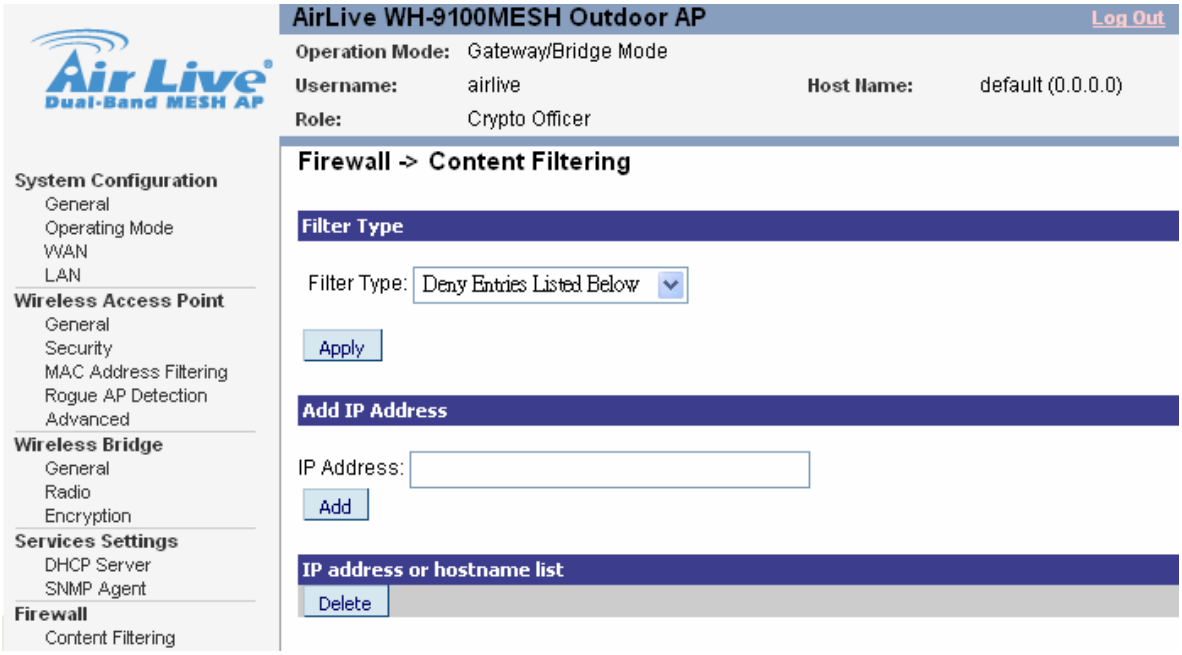
Chapter 10: Firewall (for Gateway mode)

10.1 Content Filtering

Click the entry on the left hand navigation panel for Firewall – Content Filtering. The Content Filtering screen allows the system administrator to identify particular hosts or IPs that will be blocked form access by the gateway. Simply input the IP address and click Add.

Entries can be added as:

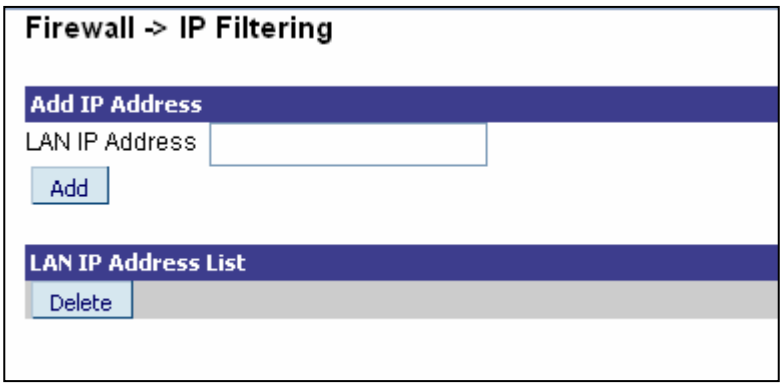
- Individual IP addressed (192.168.204.10)
- IP address range (192.168.204.0/24)
- Exact URL (www.yahoo.com)
- Wildcard URL (*.gov)



10.2 IP Filtering

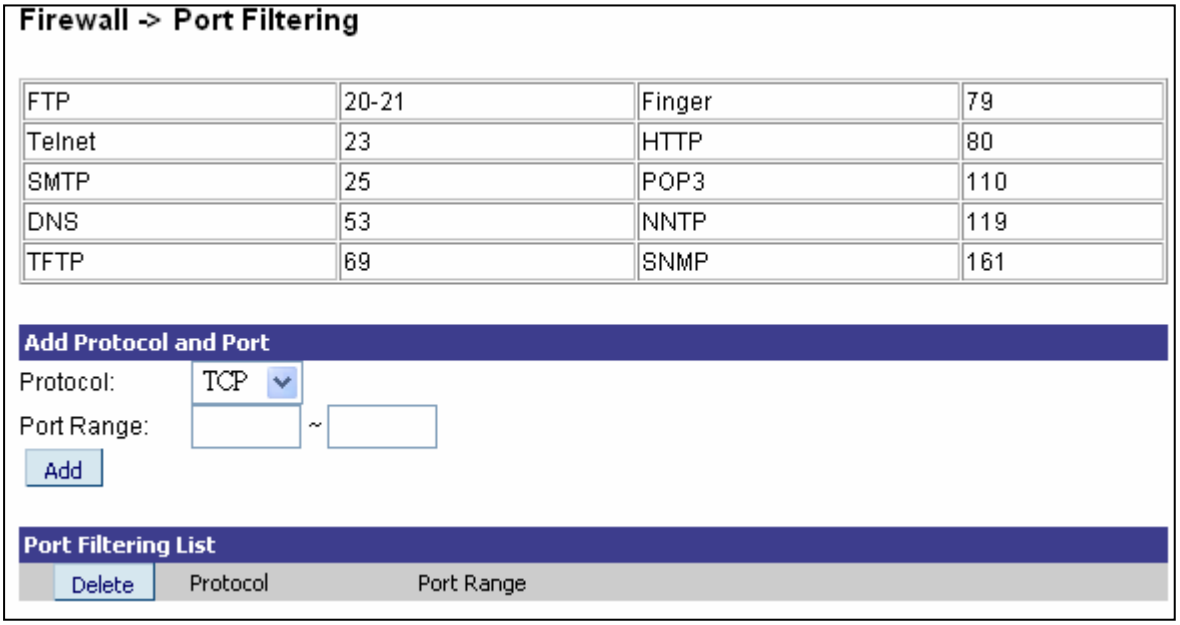
Click the entry on the left hand navigation panel for Firewall – IP Filtering.

The IP Filtering screen blocks certain IPs on the Private LAN from accessing your internet connection. It restricts clients to those with a specific IP address.



10.3 Port Filtering

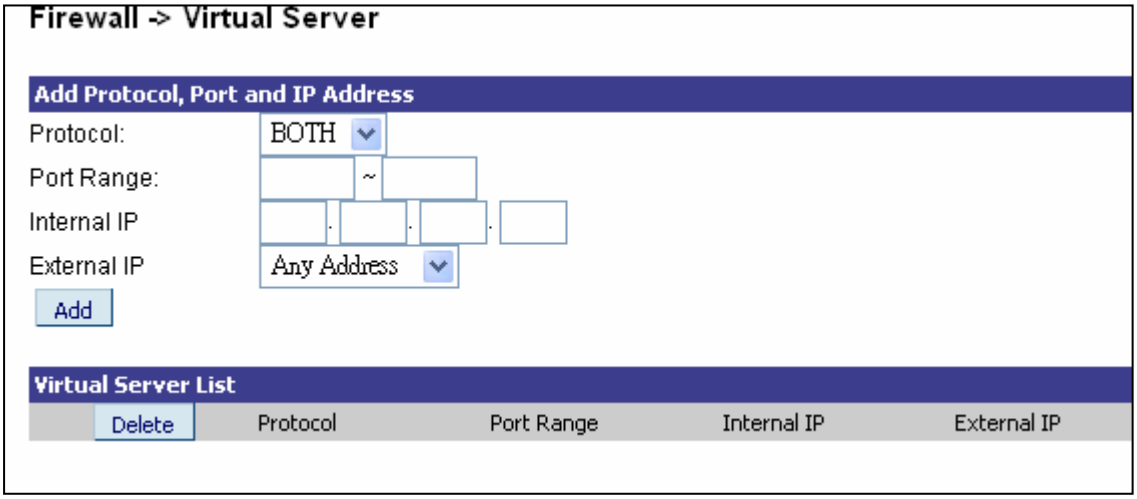
Click the entry on the left hand navigation panel for Firewall – Port Filtering. Port Filtering permits you to configure the Gateway to block outbound traffic on specific ports. It can be used to block the wireless network from using specific protocols on the network.



10.4 Virtual Server

Click the entry on the left hand navigation panel for Firewall – Virtual Server.

In order to protect the Private Network, the built-in NAT firewall filter out traffic to the private network. Since all clients on the Private Network are normally not visible to outside users, the virtual server function allows some clients on the Private Network to be accessed by outside users by configuring the application mapping function offered on the this Telnet (Port23), FTP (Port 21) , and Web server (Port 80).Client computers on the Private LAN can host these applications, and allow users from the Internet to access these applications hosted on the virtual servers.



This is done by mapping virtual servers to private IP addressed, according to the specific TCP port application. As the planning table below shows, we have identified a Telnet (port23) virtual server for private IP 192.168.15.56, a SMTP Mail (Port 25) virtual server for private IP 192.168.15.33, and Web (port 80) virtual server for private IP 192.168.15.64. For example, all Internet requests to the gateway for SMTP Mail services (port25) to the WAN IP address will redirected to the Private Network computer specified by the server IP 192.168.15.33.

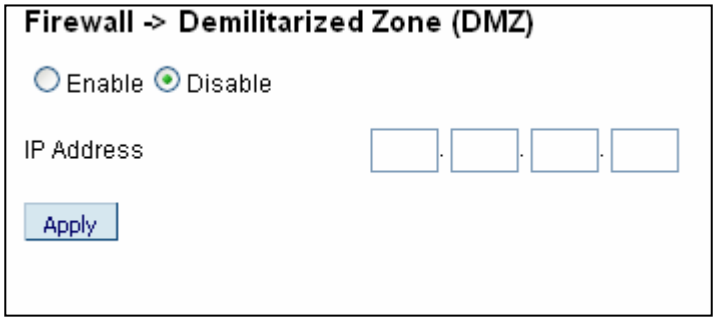
Service Port	Server IP
23	192.168.15.56
25	192.168.15.33
80	192.168.15.64

It is Recommend that IP address of virtual server computer hosted on the Private Network be manually (statically) assigned to coincide with a static server mapping to that specific IP address. Virtual servers should not rely on the dynamic IP assignment of the DHCP server function which could create unmapped IP address assignments.

Protocol – Selection of UDP, TCP, or Both (TCP and UDP) allows these specified network protocols to pass through during the TCP port communication with each virtual server IP address.

10.5 DMZ

Click the entry on the left hand navigation panel for Firewall – DMZ. The Demilitarize Zone (DMA) host allows one computer on the Private Network to be to tall expose to the wired network or Internet for unrestricted two-way communication.



This configuration is typically used when a computer is operation proprietary client software or 2-way communication such as video-teleconferencing, where multiple TCP port assignments are required for communication. To assign a PC the DMA host status, fill in the Private IP address which is identified as the exposed host and click the Apply button. However, any Internet user who knows the WAN IP address of the gateway can connect to the DMZ host since the firewall feature is disabled for this device, causing a potential security risk to data residing on the that host.

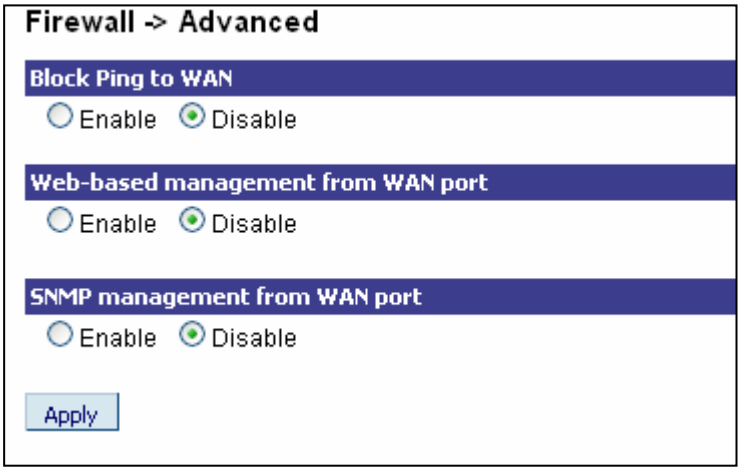
Again, it is recommended that IP addressed of DMA host computers on the Private Network be manually (statically) assigned to coincide with a static DMZ host mapping to that specific IP address. DMZ hosts should not rely on the dynamic IP assignment of DHCP server function which could create incorrectly mapped IP address assignments to non-DMZ hosts.

10.6 Advanced

As advanced firewall functions, you can enable/disable

- Block Ping to WAN
- Web-based management from WAN port
- SNMP management from WAN port

These options allow you more control over your environment



Chapter 11: Admin User Management

This chapter describes the items about Admin User Management page. If you don't know how to enter configuration screen, chapter 4 describes how to do it.

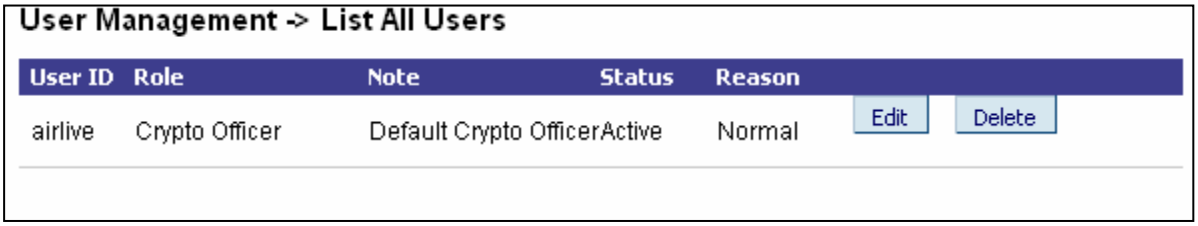
There are two user roles for WH-9100MESH, crypto officer and administrator.

- **Crypto Officer:** The crypto officer has the highest authority to set up all of functions of WH-9100MESH.
- **Administrator:** The administrator has most of right to set up WH-9100MESH, however, he can not set up the encryption function.

The WH-9100MESH default username is **airlive** (password is airlive) and its role is crypto officer to allow you initial the configuration job.

11.1 List All Users

Click the entry on the left hand navigation panel for Admin User Management – List All Users. This directs you to this page. The List All Users page simply lists all administrator accounts configured for the unit.

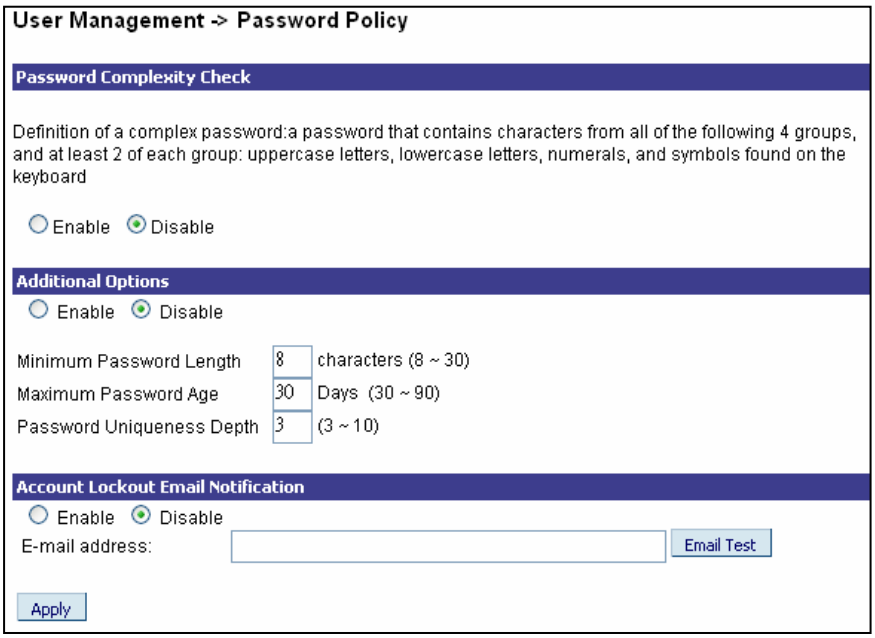


11.2 Add New User

The Add New User screen allows you to add new Crypto Officer or Administrators, assigning and confirming the password for each. The password can not be less than 8 characters. After you key in user ID, password, and choose Role, click Add to add this new user.

11.3 User Password Policy

The WH-9100MESH password policy allow you to enable Password Complexity Check, Additional Option and Account Lockout Email Notification



Chapter 12: Monitoring/Reports Menu

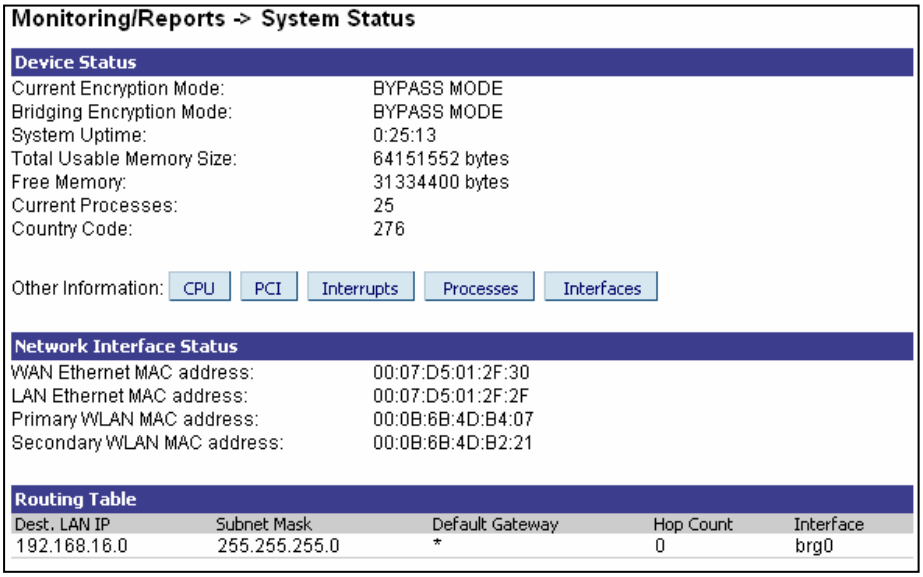
This chapter describes the items about Monitor/Reports page. If you don't know how to enter configuration screen, chapter 4 describes how to do it.

The Monitoring/Reports section gives you a variety of lists and status reports. Most of there are self-explanatory.

12.1 System Status

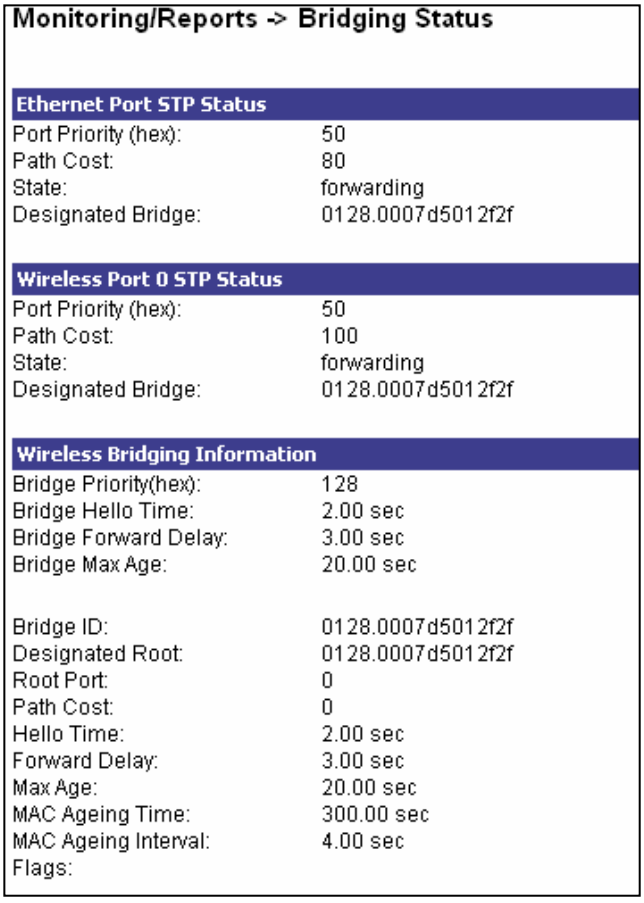
Click the entry on the left hand navigation panel for Monitor/Reports – System status. This directs you to this page. This screen displays the status of the WH-9100MESH device and network interface details and the routing table.

There are also some pop-up informational menus on this screen that give detailed information about CPU, PCI, Interrupts, Process and Interfaces.



12.2 Bridging Status

Click the entry on the left hand navigation panel for Monitor/Reports –Bridging Status. This screen displays the Ethernet Port STP status, wireless port STP status, and wireless bridging information.



Monitoring/Reports -> Bridging Status

Ethernet Port STP Status

Port Priority (hex):	50
Path Cost:	80
State:	forwarding
Designated Bridge:	0128.0007d5012f2f

Wireless Port 0 STP Status

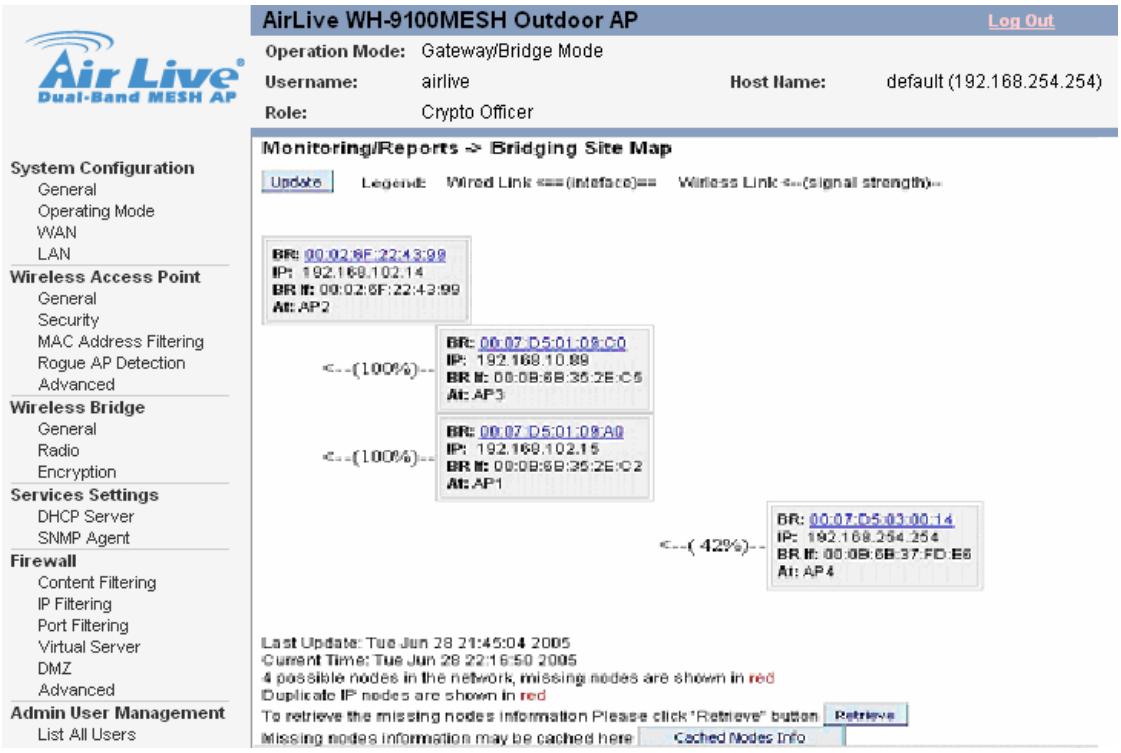
Port Priority (hex):	50
Path Cost:	100
State:	forwarding
Designated Bridge:	0128.0007d5012f2f

Wireless Bridging Information

Bridge Priority(hex):	128
Bridge Hello Time:	2.00 sec
Bridge Forward Delay:	3.00 sec
Bridge Max Age:	20.00 sec
Bridge ID:	0128.0007d5012f2f
Designated Root:	0128.0007d5012f2f
Root Port:	0
Path Cost:	0
Hello Time:	2.00 sec
Forward Delay:	3.00 sec
Max Age:	20.00 sec
MAC Ageing Time:	300.00 sec
MAC Ageing Interval:	4.00 sec
Flags:	

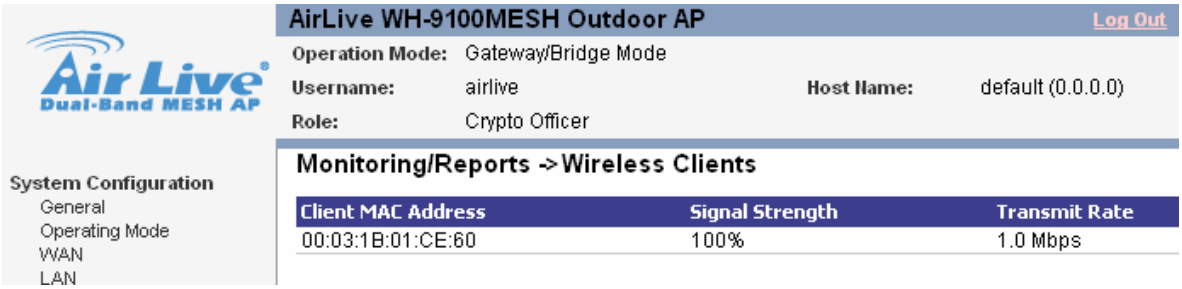
12.3 Bridge Site Map

Click the entry on the left hand navigation panel for Monitor/Reports – Bridge Site Map. This screen displays the graphology of Bridges Network topology with some useful information – IP, Signal Strength and so on.



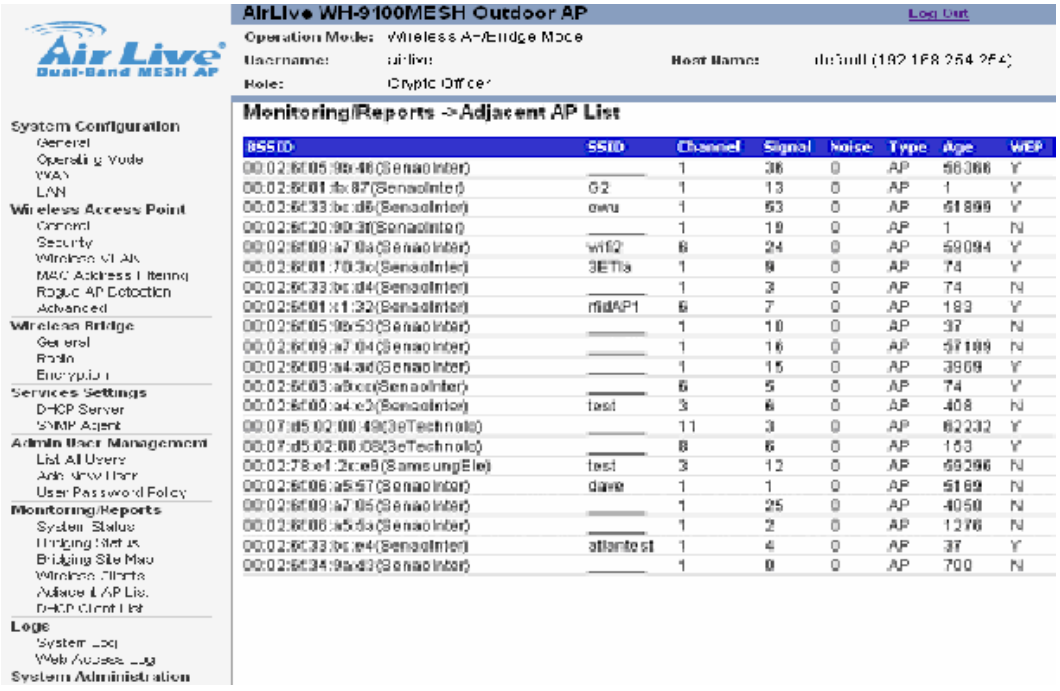
12.4 Wireless Clients

Click the entry on the left hand navigation panel for Monitor/Reports – Wireless Client. This screen displays the MAC address of all wireless clients and their signal strength and transmit rate.



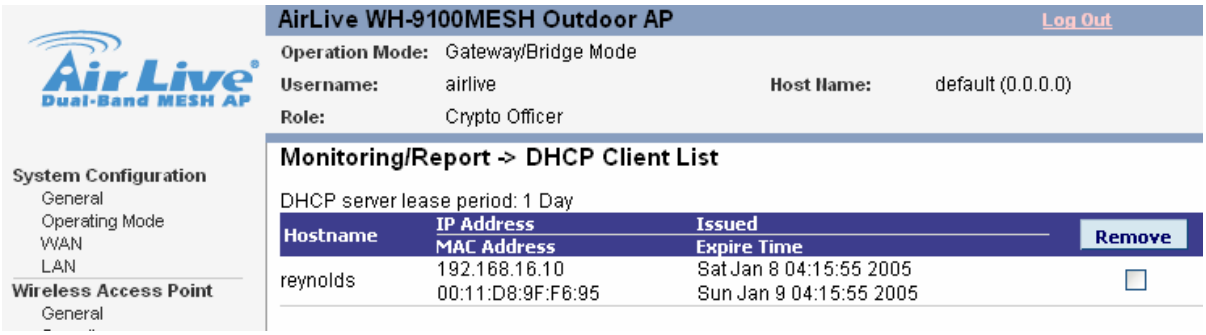
12.5 Adjacent AP list

Click the entry on the left hand navigation panel for Monitor/Reports – DHCP Client List. The Adjacent AP list shows all the APs on the network.



12.6 DHCP Client List

Click the entry on the left hand navigation panel for Monitor/Reports – DHCP Client List. This directs you to this page. The DHCP client list displays all clients currently connected to the WH-9100MESH via DHCP server, including their hostnames, IP addresses, and MAC addresses. Use the Remove button to clear any DCHP client entries you wish to remove.

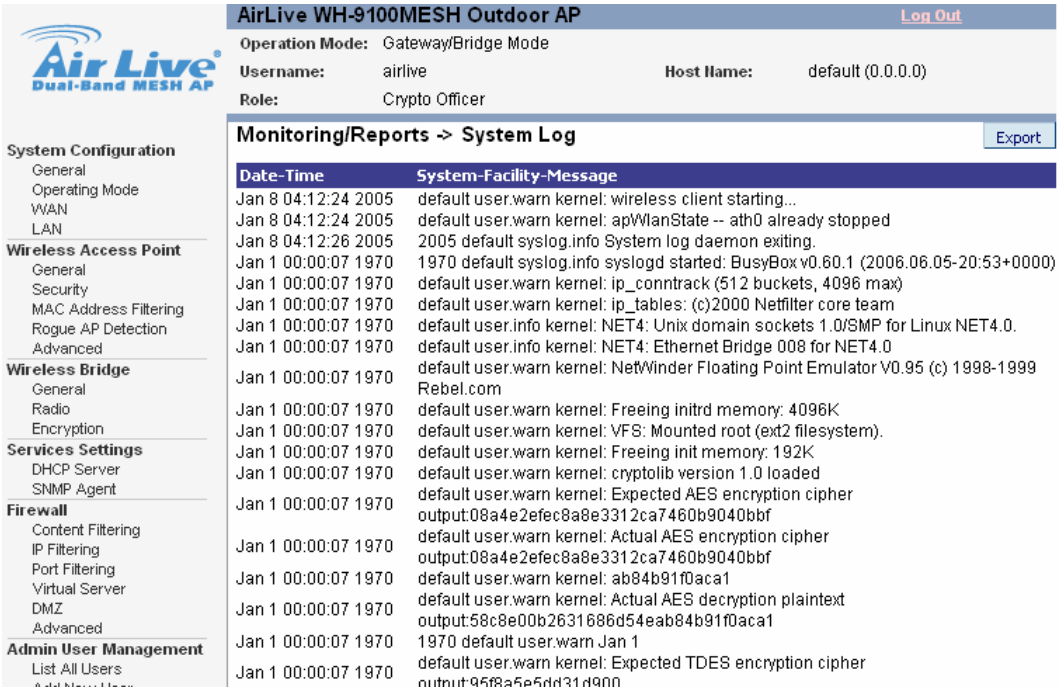


Chapter 13: Logs

This chapter describes the items about Monitor/Reports page. If you don't know how to enter configuration screen, chapter 4 describes how to do it.

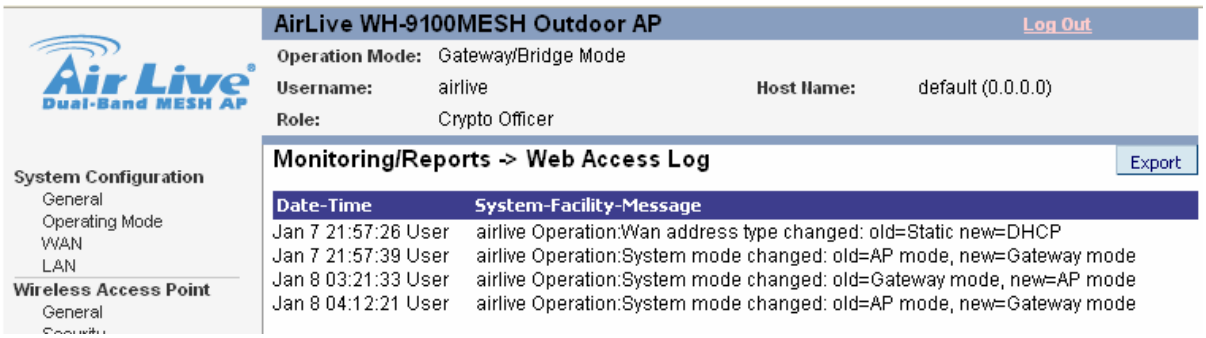
13.1 System Log

Click the entry on the left hand navigation panel for Logs – System Log. This directs you to this page. The system log display system-facility-messages with date and time stamp. There are messages documenting functions performed internal to system, based on the system's functionality. Generally, the network administrator would only use this information if trained as or working with a field engineer or as information provide to technical support. The system log will continue to accumulate listing. If you wish to clear listings manually, use the Clear button.



13.2 Web Access Log

Click the entry on the left hand navigation panel for Logs – Web Access Log to enter this page.



This screen displays system facility messages with date and time stamp for any actions involving web access. For example, this log records when you set encryption mode, change operating mode, etc., using the web browser. It establishes a running record regarding what actions were performed and by whom. The Web Access Log will continue to accumulate listing. Using the Clear button to clear listings manually,

Chapter 14: System Administration Menu

This chapter describes the items about System Administration page. If you don't know how to enter configuration screen, chapter 4 describes how to do it.

14.1 System Upgrade

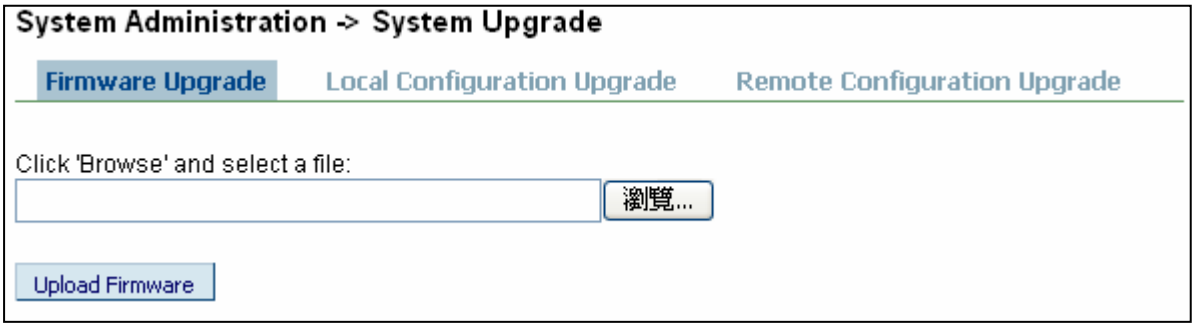
Click the entry on the left hand navigation panel for System Administration – Firmware Upgrade to enter this page. It provides the ability to upload to the WH-9100MESH device's firmware as they become available. When a new upgrade file becomes available, you can do a firmware upgrade from the Firmware Upgrade window.

There is also a configuration file transfer option which allows the system configuration file from one AP to be transferred to another AP, in order to minimize the administration of the APs. Only configuration parameters that can be shared between APs are downloaded in the configuration file. WAN IP address and hostname are not transferred in the configuration file. Click on the Local Configuration Upgrade and Remote Configuration Upgrade tabs to perform file transfers. Only the Crypto Officer role can access this function.

14.1.1 Firmware Upgrade

On the **System Administration – System Upgrade** screen, the Firmware Upgrade tab is the default view.

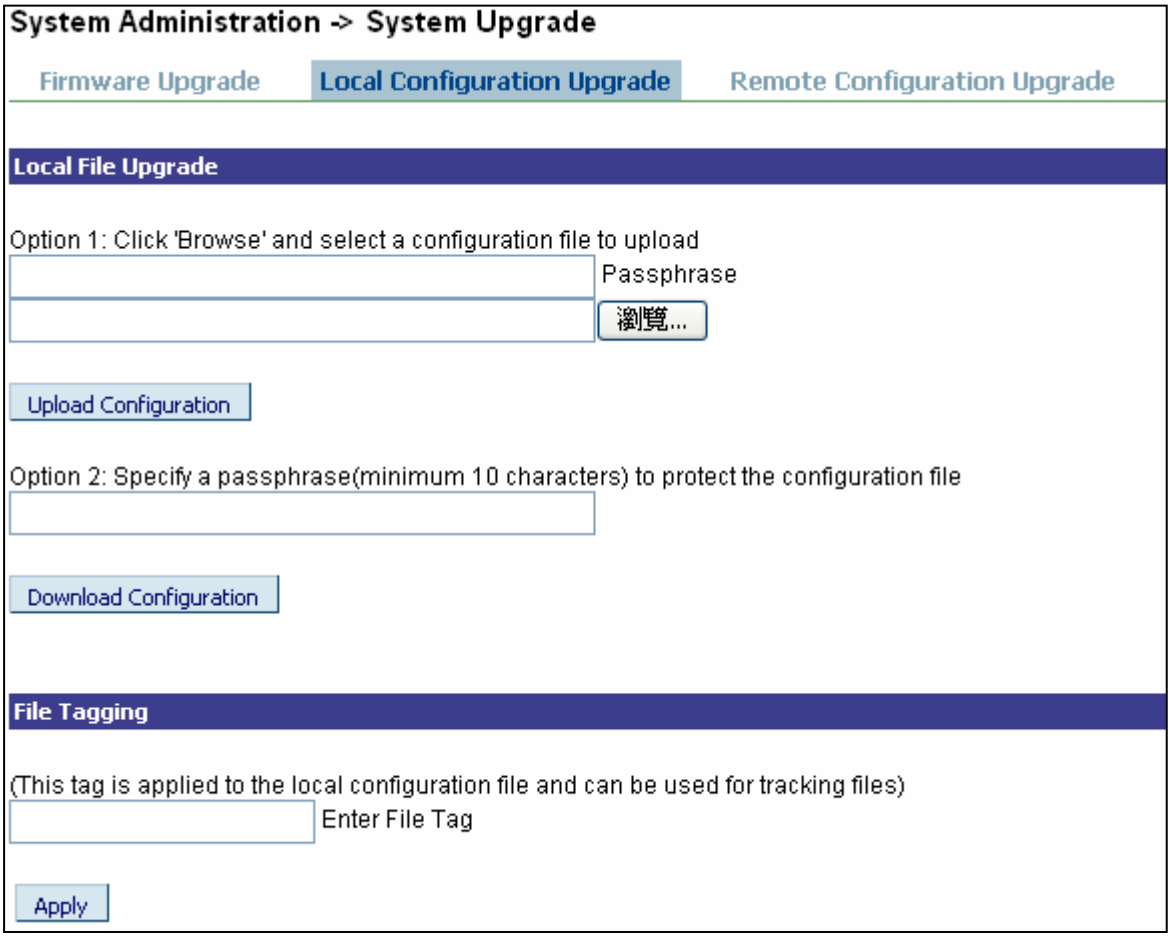
Click browse and select the firmware file to be uploaded. Click on the Upload Firmware button.



14.1.2 Location Configuration Upgrade

On the **System Administration – System Upgrade** screen, click on the **Local Configuration Upgrade** tab to upload and download configuration files to APs connected to the network.

To upload a configuration file, select the file using the browse button and enter the passphrase for that file. The passphrase protects the file from unauthorized users. It prevents unauthorized user from applying the system configuration file to an unauthorized AP to gain access to the network. Before downloading the system configuration file to a local computer, the use must enter a passphrase to protect the file. Before the system configuration file can be uploaded onto another AP, the passphrase must be entered on the remote AP.



14.1.3 Remote Configuration Upgrade

On the **System Administration – System Upgrade** screen, click on the **Remote Configuration Upgrade** tab to upload and download configuration files to APs in remote location which are not configured.

This remote configuration upgrade feature allows you to selectively transfer a configuration file to other APs. The process of using Remote configures function as following:

Step 1: Choose remote devices

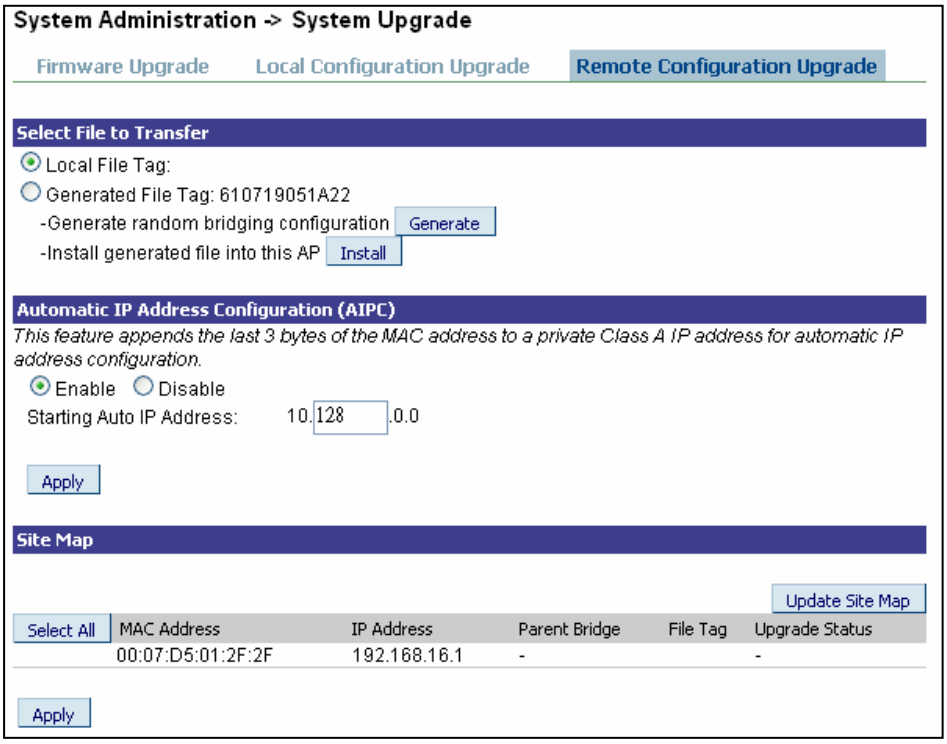
Click **Update Site Map** button to find out the remote devices and then select which are you want to configure.

Step 2: Select File to Transfer

You can click the **Local File Tag** that set up remote AP same as local one or as different by choosing **Generated File**. It will generate a random configuration file is used to update the bridging SSID and bridging encryption on other devices using the existing bridging link. If the bridging key or the bridging SSID is changed on the normal configuration screen, then the bridging link to the other devices will be terminated and the configuration can not be updated.

Step 3: Click Apply button

Once the file is transferred, the remote AP will be rebooted. Once the remote units are rebooted, the site map can be updated and the File Tag will show the status of the units. If the tab matches the local tag, the unit was updated successfully.

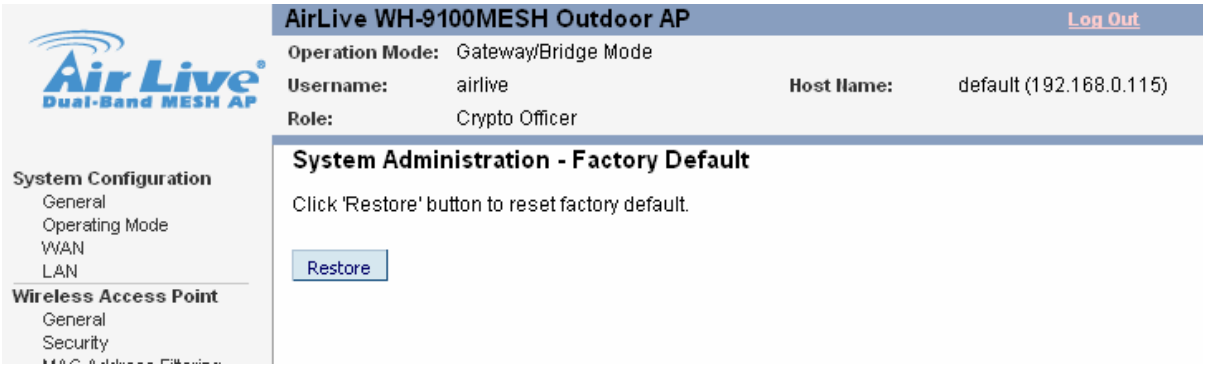


- Automatic IP address Configuration

  The automatic IP address configuration feature uses the last three bytes of the WAN MAC address for the last three bytes of the IP address. For example, the WAN MAC address of 00:07:D5:01:02:03 will translate to an IP address of 10.1.2.3. fi the starting range of the automatic IP address configuration is set to 10.128.0.0 and the WAN MAC address is 00:07:D5:01:02:03 (Basically the second byte add 128+1). The MAC address on the WAN port is from the AirLive's address pool of 16 million addresses. There is a small chance for duplicate MACs. However, if a duplicate IP address is detected, the bridge site map will show this device with a red IP address. The distributed default gateway is the first IP address in the valid range. For example: for 10.128.0.9, the default gateway is 10.128.0.1. The distribute netmask is 255.0.0.0.

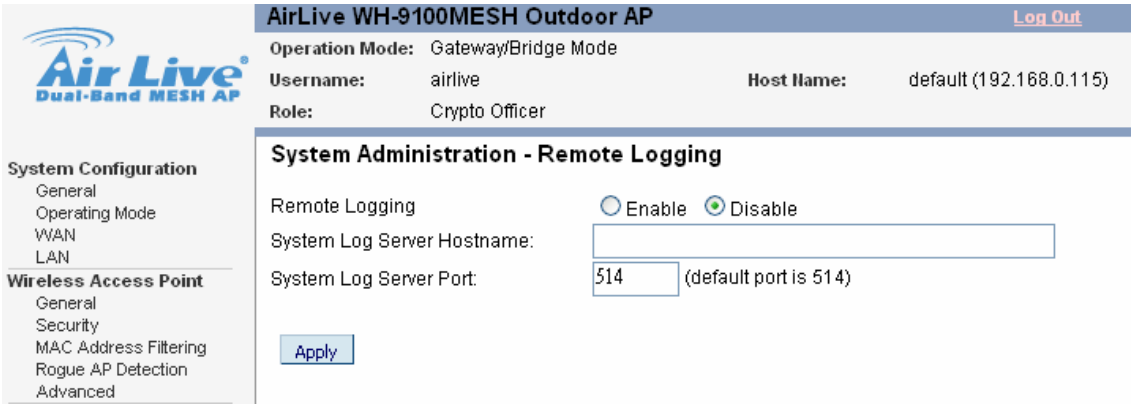
14.2 Factory Default

Click the entry on the left hand navigation panel for System Administration – Factory Default to enter this page. The "Restore" button is a fallback troubleshooting function that should only be use to reset system to original settings.



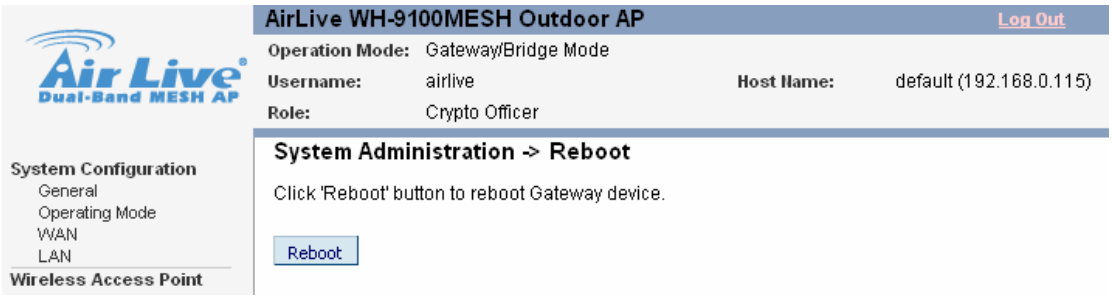
14.3 Remote Logging

Click the entry on the left hand navigation panel for System Administration – Remote Logging to enter this page. Remote logging allows you to forward the syslog data from each machine to a central remote logging server. In the WH-9100MESH, this function uses the syslogd daemon. You can find more information about syslogd by searching for “syslogd” in an Internet search engine (such as Google®) to find a versin compatible with your operation system. If you enable Remote logging, input a System Log Server IP Address and System Log Server Port, click Apply to accept these values.



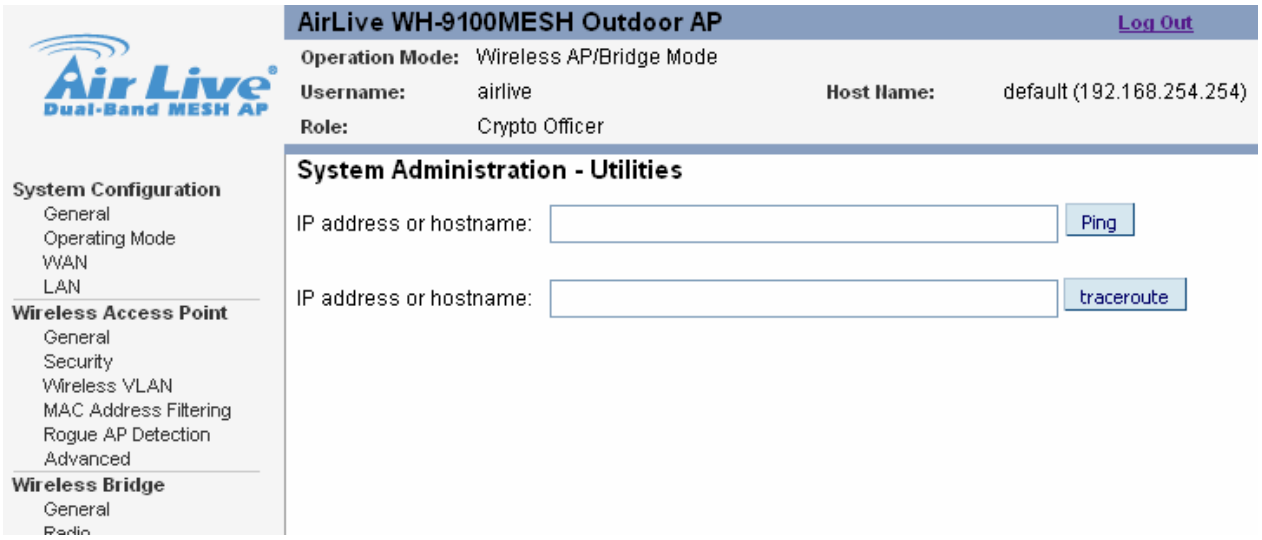
14.4 Reboot

Click the entry on the left hand navigation panel for System Administration – Reboot to enter this page. The Reboot utility allows you to reboot the WH-9100MESH without changing any preset functionality.



14.5 Utilities

Click the entry on the left hand navigation panel for System Administration – Utilities to enter this page. This screen gives you ready access to two useful utilities: Ping and Traceroute. Simply enter the IP address or hostname you wish to ping or traceroute and click either the Ping or Traceroute button, as appropriate.



Chapter 15: Reset and Rest to Factory Default Setting

The WH-9100MESH is with two kind of reset behavior. One is reset system without changing any preset functionality and the other one is reset system to factory default settings that will change any preset functionality. There are two ways to do reset function. One is by enter configure screen (introduce at chapter 12.2 and chapter 12.4) and another way is done by press reset button at the front panel of case. The behaviors of reset button are as below:

- No action: if press button less than 3 seconds
- Reset system: if press button between 3 ~ 8 seconds
- Reset to Factory Default setting: if press button longer than 8 seconcs

Chapter 16: Technical Support

Manufacturer's Statement

The WH-9100MESH is provided with warranty. It is not desired or expected that the user open the device. If malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.

If you are experiencing trouble with this unit, the point of contact is: your manufacturer or sales representative.

Radio Frequency Interference Requirements

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the Federal Communications Commission's Rules and Regulations. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may came harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense-

Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user authority to operate thee equipment.

Channel Separation and WLAN Cards

There are two WLAN cards in this device. One is used for the Access Point function; the other is used for the Bridge. Channel Separation is required to reduce interference between the AP and Bridge WLAN cards. We have found that assigning 11 to the AP and 4to the Bridge has given the optimum channel separation in test installations.

Appendix A: Channel information at 5 GHz frequency band

Table 6-1: US FCC UNII

Frequency band	Channel No.	Carrier Frequency
UNII 1	36	5.180 GHz
(5.15~5.25 GHz)	40	5.200 GHz
	44	5.220 GHz
	48	5.240 GHz
UNII 2	52	5.260 GHz
(5.25~5.35 GHz)	56	5.280 GHz
	60	5.300 GHz
	64	5.320 GHz
UNII 3	149	5.745 GHz
(5.725~5.825 GHz)	153	5.765 GHz
	157	5.785 GHz
	161	5.805 GHz

Table 6-2 Taiwan DGT

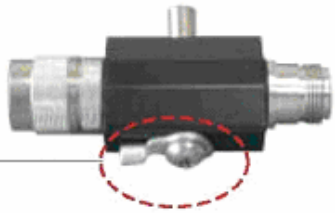
Frequency band	Channel No.	Carrier Frequency
DGT	149	5.745 GHz
(5.725~5.875 GHz)	153	5.765 GHz
	157	5.785 GHz
	161	5.805 GHz
	165	5.825 GHz
	169	5.845GHz

Table 6-2 Europe (CEPT)

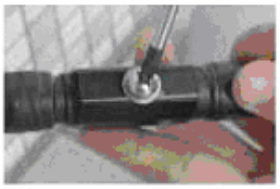
Frequency band	Channel No.	Carrier Frequency
ETSI	36	5.180 GHz
(5.15~5.725 GHz)	40	5.200 GHz
	44	5.220 GHz
	48	5.240 GHz
	52	5.260 GHz
	56	5.280 GHz
	60	5.300 GHz
	64	5.320 GHz
	100	5.500 GHz
	104	5.520 GHz
	108	5.540 GHz
	112	5.560 GHz
	116	5.580 GHz
	120	5.600 GHz
	124	5.620 GHz
	128	5.640 GHz
	132	5.660 GHz
	136	5.680 GHz
	140	5.700 GHz
	144	5.720 GHz

Appendix B: Lightning Arrestor Installation Guide

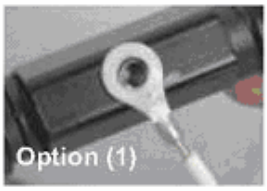
Air Live
Daul-Band MESH AP

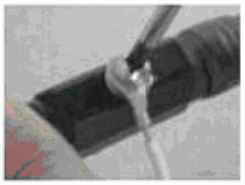


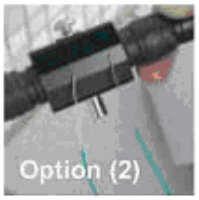
Lightning Arrestor Installation guide for outdoor antenna-kit

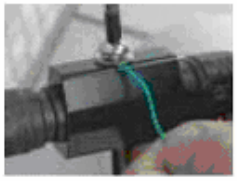


Step 1
loosen the screw from the surge protector.

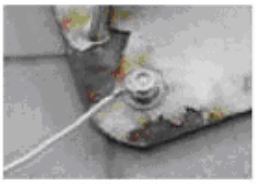


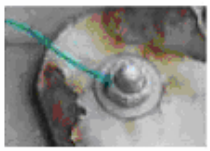


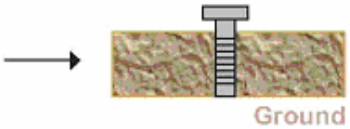




Step 2
get a normal conductive copper wire with 2 sides stripped long enough to be conductive, these wires can lead high voltage surges into the grounding.







Step 3
find a conductive material nearby the antenna installation sites, connect another end of the wire into position, there are several options:
(1) Use a long screw to stick into the ground tightly, connect another wire onto.
(2) fix or solder another end of wire onto a steel material/ bar under steel construction, such as wall for buildings, railings or other conductive materials which set up from the ground.

Remark:
(1) for the ground screw you use, we suggest the longer (deeper into ground) the better performance it has.
(2) please use a copper wire with diameter at least from 2.0mm, the thicker the diameter, the higher voltage it can sustain.