



# **AIR FORCE ONE 5**

## **User Manual**

**V1.08**

# ***Table of Contents***

Chapter 1. System Overview.....	1
1.1 Introduction of Air Force One 5(AFO-5).....	1
1.2 System Concept.....	2
1.3 Applications in Wireless Network.....	3
1.4 Product Benefit.....	6
1.5 Specification.....	7
Chapter 2. Basic Installation.....	10
2.1 Hardware Installation.....	10
2.1.1 Package Contents.....	10
2.1.2 Panel Function Descriptions.....	10
2.1.3 Hardware Installation Steps.....	12
2.2 Web Management Interface Instructions.....	13
Chapter 3. AP Mode Configuration.....	15
3.1 External Network Connection.....	15
3.1.1 Network Requirement.....	15
3.1.2 Configure LAN IP.....	16
3.2 Wireless LAN Network Creation.....	18
3.2.1 Wireless General Setup.....	18
3.2.2 Wireless Advanced Setup.....	20
3.2.3 Create Virtual AP (VAP).....	25
3.2.3.1 Virtual AP Overview.....	25
3.2.3.2 Virtual AP Setup.....	26
3.2.4 Access Control List.....	30
3.3 Wireless Network Expansion.....	31
3.4 System Management.....	32
3.4.1 Configure Management.....	32
3.4.2 Configure System Time.....	34
3.4.3 Configure UPnP.....	35
3.4.4 Configure SNMP Setup.....	36
3.4.5 Backup / Restore and Reset to Factory.....	38
3.4.6 Firmware Upgrade.....	39
3.4.7 Network Utility.....	40
3.4.8 Reboot.....	41
3.5 System Status.....	42
3.5.1 System Overview.....	42
3.5.2 Associated Clients Status.....	44
3.5.3 Show WDS Link Status.....	45
3.5.4 Extra Information.....	46
3.5.5 Event Log.....	48
Chapter 4. WDS Mode Configuration.....	49
4.1 External Network Connection.....	49
4.1.1 Network Requirement.....	49
4.1.2 Configure LAN IP.....	50
4.2 Wireless Network Expansion.....	52
4.2.1 General Setup.....	52
4.2.2 Advanced Setup.....	54

4.2.3 WDS Setup.....	59
4.3 System Management.....	60
4.3.1 Configure Management.....	60
4.3.2 Configure System Time.....	62
4.3.3 Configure UPnP.....	63
4.3.4 Configure SNMP Setup.....	64
4.3.5 Backup / Restore and Reset to Factory.....	66
4.3.6 Firmware Upgrade.....	67
4.3.7 Network Utility.....	68
4.3.8 Reboot.....	69
4.4 System Status.....	70
4.4.1 System Overview.....	70
4.4.2 WDS List.....	72
4.4.3 Extra Information.....	73
4.4.4 Event Log.....	75
Chapter 5. CPE Mode Configuration.....	76
5.1 External Network Connection.....	76
5.1.1 Network Requirement.....	76
5.1.2 Configure WAN Setup.....	77
5.1.3 Configure DDNS Setup.....	79
5.1.4 Configure LAN Setup.....	80
5.2 Access Point Association.....	82
5.2.1 Configure Wireless General Setting.....	82
5.2.2 Site Survey.....	84
5.2.3 Create Wireless Profile.....	85
5.3 System Management.....	88
5.3.1 Configure Management.....	88
5.3.2 Configure System Time.....	90
5.3.3 Configure UPnP.....	91
5.3.4 Configure SNMP Setup.....	92
5.3.5 Backup / Restore and Reset to Factory.....	94
5.3.6 Firmware Upgrade.....	95
5.3.7 Network Utility.....	96
5.3.8 Reboot.....	97
5.4 Access Control List.....	98
5.4.1 IP Filter Setup.....	98
5.4.2 MAC Filter Setup.....	100
5.4.3 QoS Setup.....	101
5.5 Resource Sharing.....	103
5.5.1 DMZ.....	103
5.5.2 Virtual Server (Port Forwarding).....	104
5.6 System Status.....	106
5.6.1 Overview.....	106
5.6.2 Station Statistics.....	109
5.6.3 Extra Info.....	111
5.6.4 Event Log.....	113
Chapter 6. Client Bridge + Universal Repeater Configuration.....	114
6.1 External Network Connection.....	114

6.1.1 Network Requirement.....	114
6.1.2 Configure LAN IP.....	115
6.2 Access Point Association.....	117
6.2.1 Configure Wireless General Setting.....	117
6.2.2 Wireless Advanced Setup.....	119
6.2.3 Site Survey.....	124
6.2.4 Create Wireless Profile.....	125
6.3 Wireless LAN Network Creation.....	127
6.3.1 Repeater AP Setup.....	127
6.3.2 MAC Filter Setup.....	131
6.4 System Management.....	132
6.4.1 Configure Management.....	132
6.4.2 Configure System Time.....	134
6.4.3 Configure UPnP.....	135
6.4.4 Configure SNMP Setup.....	136
6.4.5 Backup / Restore and Reset to Factory.....	138
6.4.6 Firmware Upgrade.....	139
6.4.7 Network Utility.....	140
6.4.8 Reboot.....	141
6.5 System Status.....	142
6.5.1 System Overview.....	142
6.5.2 Associated Clients Status.....	145
6.5.3 Remote AP.....	146
6.5.4 Extra Information.....	147
6.5.5 Event Log.....	149
Appendix A. Windows TCP/IP Settings.....	150
Appendix B. WEB GUI Valid Characters .....	152
Appendix C. MCS Data Rate.....	156
Appendix D. System Manager Privileges.....	157
Appendix E. Enabling UPnP in Windows XP .....	158

# ***Chapter 1. System Overview***

## **1.1 Introduction of Air Force One 5(AFO-5)**

Kozumi outdoor high power WiFi-N Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. Kozumi outdoor CPE/AP utilizes a 200mW output Tx Power connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

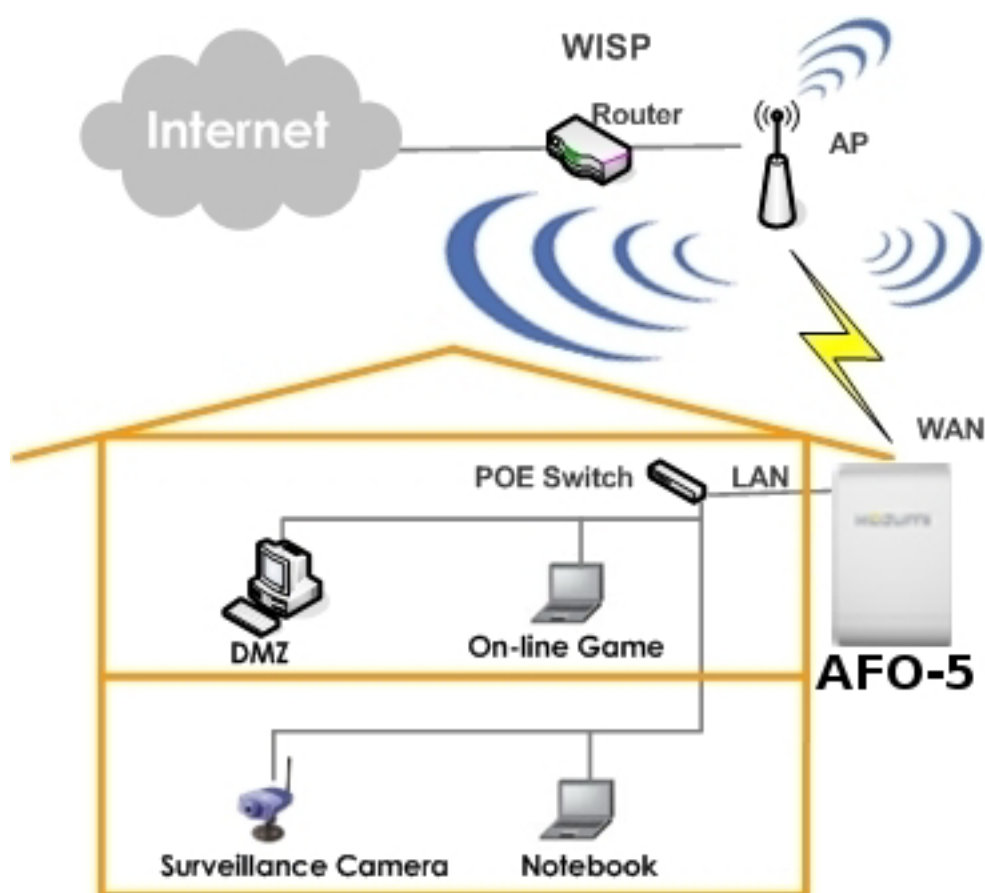
Kozumi outdoor high power Bridge can be used for seven different purposes in four different modes. In the AP mode, it can be deployed either as traditional fixed wireless Access Point(AP), or combination of AP and WDS(AP+WDS). In the WDS mode, it's only used to expand or bridge Ethernet networks and deployed as a main base, relay based or remote base station. In the CPE mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless WAN gateway to access to Internet. In the Client Bridge + Universal Repeater mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless or wired bridge to access to Internet

1. Access Point : It can be deployed as a traditional fixed wireless Access Point
2. Repeater: To expand wireless service by repeating prior AP
3. WDS : It can be used to expand Ethernet network via wireless WDS Link
4. AP+WDS: Not only to extend Ethernet network, but also provide wireless access to the expanded network
5. CPE (Customer Premises Equipment): It is a wireless gateway with NAT and DHCP Server functions to connects to Wireless Internet Service Provider's (WISP)
6. Client Bridge + Universal Repeater : It is a wireless repeater or bridge to connects to Wireless Internet Service Provider's (WISP)

## 1.2 System Concept

The AFO-5 is not only designed and used as traditional outdoor AP, but also with rich features tailored for WISP applications. The two-level management capability and access control ease WISP and owners to maintain and manage wireless network in a more controllable fashion. Main applications are listed as follows with illustration:

- Wireless CPE for Multi Dwelling Unit/Multi Tenant Unit(MDU/MTU) complexes including apartments, dormitories, and office complexes.
- Outdoor Access Point for school campuses, enterprise campuses, or manufacture plants.
- Indoor Access Point for hotels, factories, or warehouses where industrial grade devices are preferred.
- Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
- Wireless coverage for indoor and outdoor grounds in private resorts, home yards, or gulf course communities.



## 1.3 Applications in Wireless Network

AFO-5 is a multiple mode system which can be configured either as a wireless gateway or an access point as desired. It also can be used WDS link for Ethernet network expansion. This section depicts different applications on **AP Mode**, **WDS Mode**, **CPE Mode** and **Client Bridge + Universal Repeater Mode**.



### ■ Configuration in AP Mode (including Access Point + WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly.

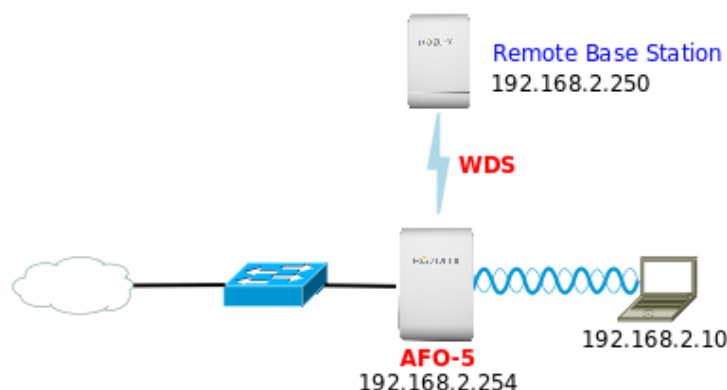
#### ➔ Example 1 : Access Point without WDS

- ✓ It can be deployed as a tradition fixed wireless Access Point



#### ➔ Example 2 : Access Point with WDS

- ✓ It can be deployed as a tradition fixed wireless Access Point and provides WDS link to expand network

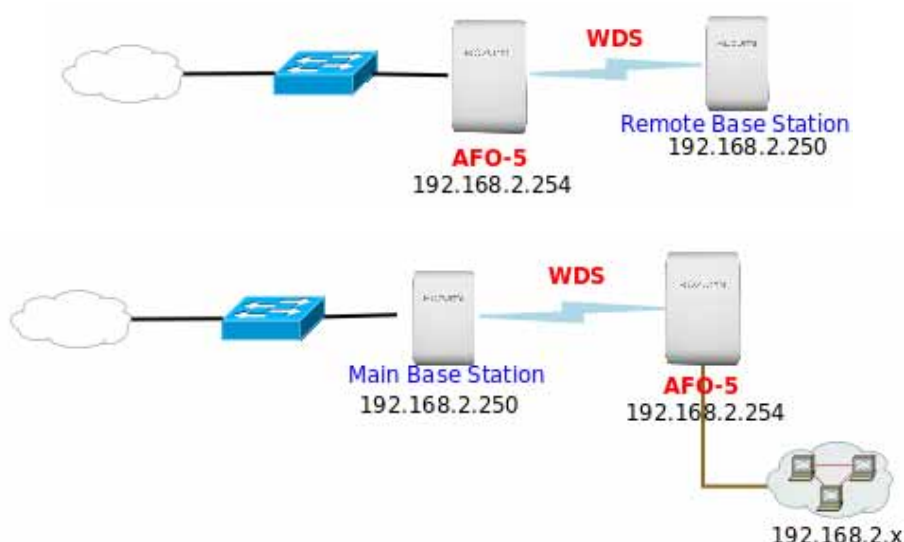




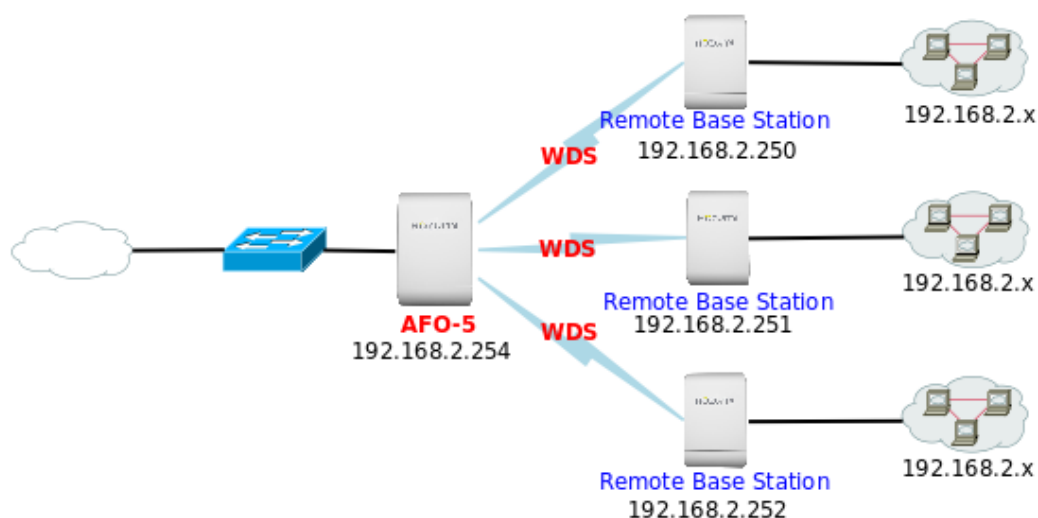
## ■ Configuration in WDS Mode (Pure WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly. In this mode, it can support single or multiple WDS links and no wireless clients **can** associate with it though.

### → Example 1 : Point-to-Point



### → Example 2 : Point-to-Multi-Point



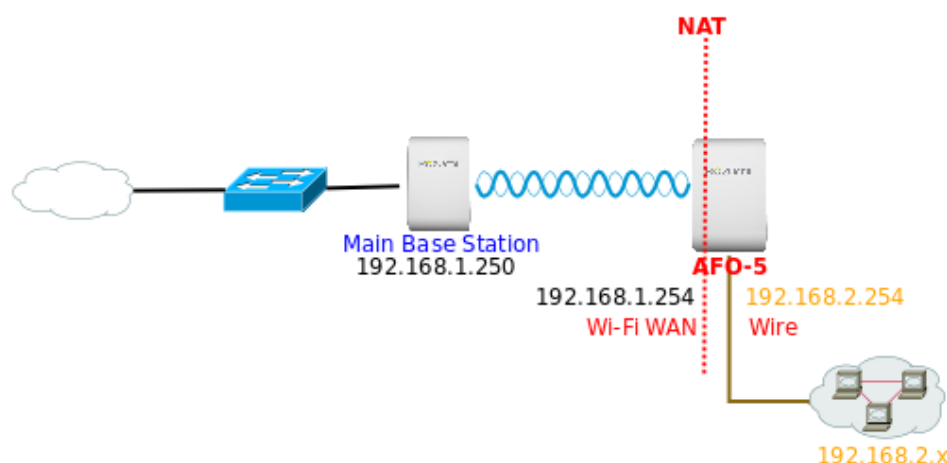


### → Example 3 : Multi-Point Repeating bridge



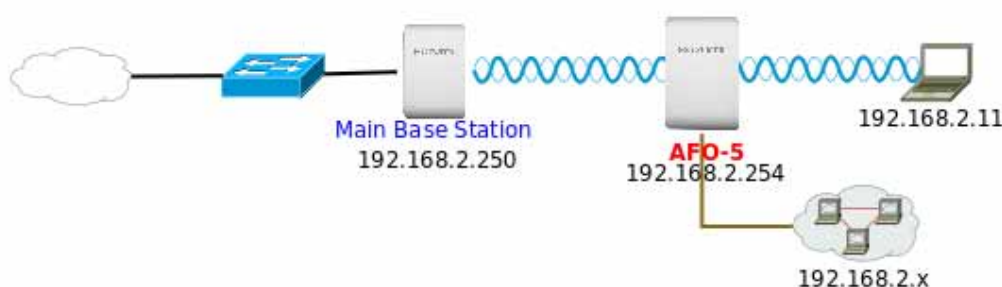
## ■ Configuration in CPE Mode

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, AFO-5 is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to AFO-5 are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.



## ■ Configuration in Client Bridge + Universal Repeater Mode

It can be used as an Client Bridge + Universal Repeater to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, AFO-5 is enabled with DHCP Server functions. The wired clients of AFO-5 are in **the same** subnet from Main Base Station and it **accepts** wireless connections from client devices.



## 1.4 Product Benefit

- IEEE 802.11n Draft 2.0 Compliance in 2Tx / 2Rx Design
- Support IEEE 802.11n and 802.11a
- Operates in the 5GHz ISM Band
- **Built in 14dBi, 5GHz (H35, E20) Directional Antenna**
- Enables Bandwidth of up to 300Mbps(Tx), 300Mbps(Rx) link rate
- Topology : Point to Point ; Point to Multi Point
  - ➔ Access Point Mode : Pure Access Point Function and Access Point /Bridge(WDS) Function
  - ➔ WDS Mode
  - ➔ CPE Mode (Router Client )
  - ➔ Client Bridge + Universal Repeater
- Security with 802.1X, WPA, and WPA2
- Support QoS(Quality of Service) & WMM
- Integrated Power over Ethernet (PoE)
- Multiple Virtual AP & Capability of Client Isolation
- Business-class WLAN Security and Client Authentications
- Provide Advanced Wireless Setting
- Support Web Management and SNMP MIB II
- Over Load Current Protection
- Wide Range Voltage Support (12-68VDC)
- Weather-Proof Housing (IP 68 Approved), M-13 RJ45 and N-Type Connector
- Client Isolation Through Layer 2 VLAN Technology
- Two administrator accounts for manager authorities
- QoS for bandwidth management and traffic prioritization

AFO-5 outdoor high power WiFi-A/N Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers.. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. AFO-5 outdoor bridge utilizes a 200mW output Tx Power to connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

AFO-5 outdoor high power Bridge supports four operational modes, the AP mode, the WDS mode, the CPE mode and Client Bridge + Universal Repeater mode, respectively with built-in remote management features.

## 1.5 Specification

### ■ Wireless Architecture Mode

#### ➔ AP Mode

##### ✓ Pure AP Mode

- It can be deployed as a tradition fixed wireless Access Point
- It allow wireless clients or Stations(STA ) to access

##### ✓ AP/WDS Mode

- This enables the wireless interconnection of Access Point in an IEEE802.11 network .and accept wireless clients at the same time

#### ➔ WDS Mode

- ✓ This enables the wireless interconnection of Access Point in an IEEE802.11 network.
- ✓ It allows a wireless network to be expanded using multiple access point without the need for a wired backbone to link them.
- ✓ This also be referred to as repeater mode.
- ✓ It can't allow wireless clients or Stations (STA) to associate.

#### ➔ CPE Mode

- ✓ WiFi connection as WAN , in CPE mode , the device run as DHCP server to assign IP address to clients out of a private IP address pool behind a NAT

#### ➔ Client Bridge + Universal RepeaterMode

- ✓ A wireless repeater and bridge with DHCP server enabled, clients on the same subnet as host AP(Primary Router).

### ■ Networking

- ➔ Support Static IP, Dynamic IP(DHCP Client) and PPPoE on WiFi WAN Connection
- ➔ Support PPTP/L2TP/IP Sec Pass Through
- ➔ PPPoE Reconnect – Always On , On demand, Manual
- ➔ MAC Cloning
- ➔ DHCP Server in CPE and Client Bridge + Universal Repeater Mode
- ➔ 802.3 Bridging
- ➔ Masquerading (NAT)
- ➔ Proxy DNS
- ➔ Dynamic DNS
- ➔ NTP Client
- ➔ Virtual DMZ
- ➔ Virtual Server (Port Forwarding)
- ➔ Support MAC Filter

- ➔ Support IP Filter
- ➔ Bandwidth traffic Shaping

## ■ Wireless Feature

- ➔ Transmission power control : 1~100 %
- ➔ Channel selection : Manual or Auto
- ➔ No of associated clients per AP : 32
- ➔ Setting for max no associated clients : Yes
- ➔ No. of ESSID (Virtual AP ) : 7
- ➔ No. of Max. WDS setting : 4
- ➔ Preamble setting : Short/ Long
- ➔ Setting for 802.11a/n mix or 802.11a only
- ➔ Setting for transmission speed
- ➔ Dynamic Wireless re-transmission
- ➔ IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- ➔ IEEE 802.11i Preauth (PMKSA Cache )
- ➔ IEEE 802.11h - TPC(Transmission Power Control) and DFS(Dynamic Frequency Select)
- ➔ IEEE 802.11d -Multi country roaming
- ➔ Wireless Site Survey
- ➔ Channel Bandwidth setting : 20MHz or 20/40MHz
- ➔ HT Tx/Rx Stream selection : 1 or 2
- ➔ A-MSDU and A-MPDU support
- ➔ Maximal MPDU density for TX aggregation setting
- ➔ Short Slot support
- ➔ RTS Threshold and Fragment Threshold support

## ■ Authentication/ Encryption (Wireless Security)

- ➔ Layer 2 User Isolation and AP Isolation
- ➔ Blocks client to client discovery within a specified VLAN
- ➔ WEP 64/ 128 Bits
- ➔ EAP-TLS + Dynamic WEP
- ➔ EAP-TTLS + Dynamic WEP
- ➔ PEAP/ MS-PEAP+Dynamic WEP
- ➔ WPA (PSK +TKIP)
- ➔ WPA (802.1x certification + TKIP)
- ➔ 802.11i WPA2 (PSK + CCMP/ AES)
- ➔ 802.11i WPA2 (802.1x certification + CCMP/ AES)
- ➔ Setting for TKIP/ CCMP/ AES key's refreshing period

- ➔ Hidden ESSID support
- ➔ Setting for “Deny ANY “ connection request
- ➔ MAC Address filtering (MAC ACL)
- ➔ No. of registered RADIUS servers : 1
- ➔ VLAN assignment on ESSID
- ➔ Support WEP, AES and TKIP data encryption over WDS link

#### ■ **Quality of Service**

- ➔ Download and Upload traffic control
- ➔ Packet classifications via DSCP (Differentiated Services Code Point)
- ➔ Control Policy by IP/IP Ranges/ MAC Group/ Service
- ➔ Layer-7 Protocol Support
- ➔ Traffic Analysis and Statistics
- ➔ No. of Max. Policy setting : 10
- ➔ DiffServ/ ToS
- ➔ IEEE802.1p/ CoS
- ➔ IEEE 802.1Q Tag VLAN priority control
- ➔ IEEE802.11e WMM

#### ■ **System Administration**

- ➔ Intuitive Web Management Interface
- ➔ Password Protected Access
- ➔ Firmware upgrade via Web
- ➔ Reset to Factory Defaults
- ➔ Profiles Configuration Backup and Restore
- ➔ One-button-click to reset factory default
- ➔ Two administrator accounts
- ➔ Remote Link Test – Display connect statistics
- ➔ Full Statistics and Status Reporting
- ➔ NTP Time Synchronization
- ➔ Even Log
- ➔ Support SNMP v1, v2c, v3
- ➔ SNMP Traps to a list of IP Address
- ➔ Support MIB II
- ➔ CLI access via Telnet and SSH
- ➔ Administrative Access : HTTP and HTTPS
- ➔ UPnP (Universal Plug and Play)

## Chapter 2. Basic Installation

### 2.1 Hardware Installation

#### 2.1.1 Package Contents

The standard package contents of AFO-5 :

■ Air Force One 5	x 1
■ Quick Installation Guide	x 1
■ CD-ROM (with User Manual and QIG)	x 1
■ Power Adapter DC24V 0.5A	x 1
■ PoE Injector	x 1
■ Mounting Kit	x 2



*It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

#### 2.1.2 Panel Function Descriptions

##### AIR FORCE ONE 5

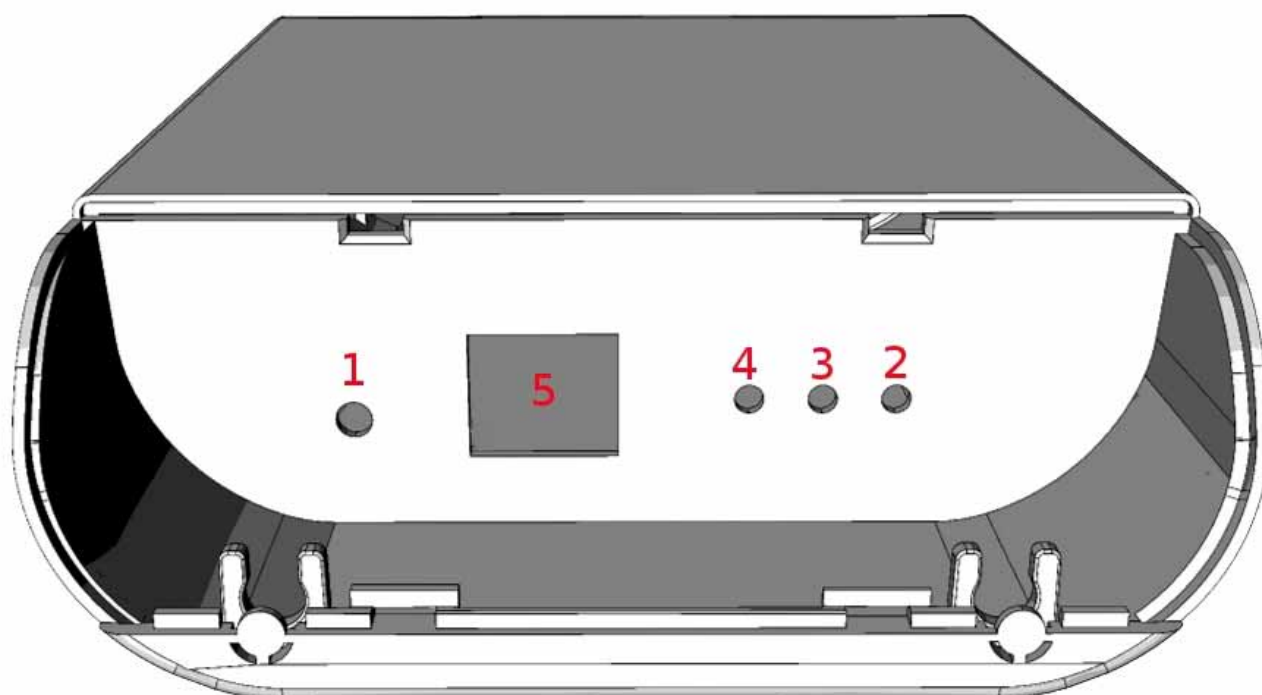
Front Panel



Rear Panel



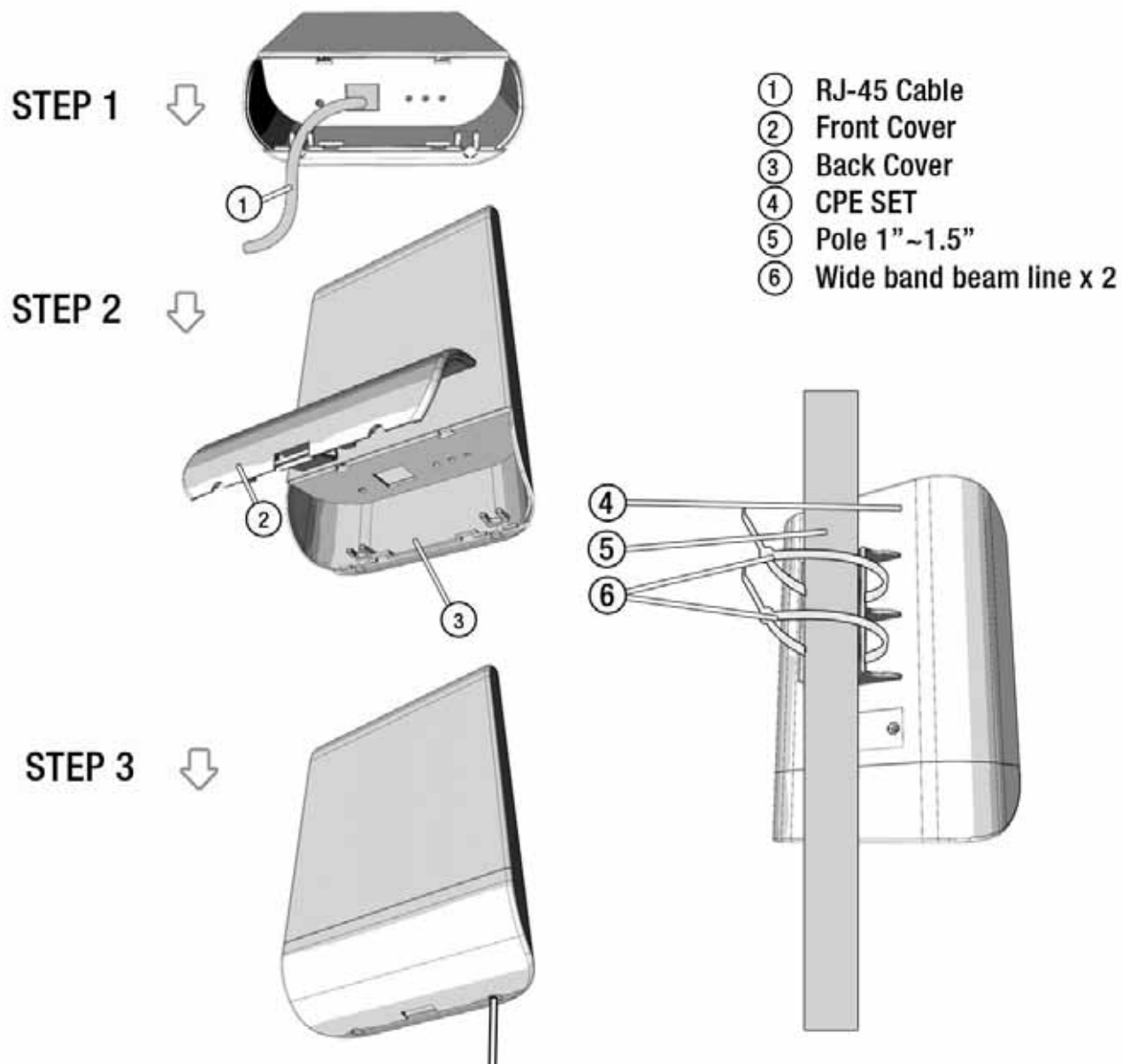
## Bottom Panel



1. Reboot Button :      Unscrew the screw and click Reset button to restart system or reset to default configurations.
  - ➔ Press and hold the Reset button for 2 seconds and release to restart system. The LED except Power indicator will be off before restarting.
  - ➔ Press and hold the Reset button for more than 10 seconds to reset the system to default configurations.
2. Power :              Green LED ON indicates power on, and OFF indicates power off.
3. WLAN :              Green LED FLASH indicates Wireless Transmit.
4. Ethernet :           Green LED ON indicates connection, OFF indicates no connection, FLASH indicates Packets transmit
5. PoE Connector :    For connecting to PSE

### 2.1.3 Hardware Installation Steps

Please follow the steps mentioned below to install the hardware of AFO-5 :





## 2.2 Web Management Interface Instructions

AFO-5 supports web-based configuration. Upon the completion of hardware installation, AFO-5 can be configured through a PC/NB by using its web browser such as Internet Explorer version 6.0.

- **Default IP Address :** 192.168.2.254
- **Default IP Netmask :** 255.255.255.0
- **Default User Name and Password :**

The default user name and password for both root manager account and admin manager account are as follows :

Mode	CPE Mode		AP Mode	WDS Mode	Universal Repeater + Client Bridge Mode
<b>Management Account</b>	Root Account	Admin Account	Root Account	Root Account	Root Account
<b>User Name</b>	root	admin	root	root	root
<b>Password</b>	default	admin	default	default	default

### Step

#### ■ IP Segment Set-up for Administrator's PC/NB

Set the IP segment of the administrator's computer to be in the same range as AFO-5 for accessing the system. Do not duplicate the IP Address used here with IP Address of AFO-5 or any other device within the network

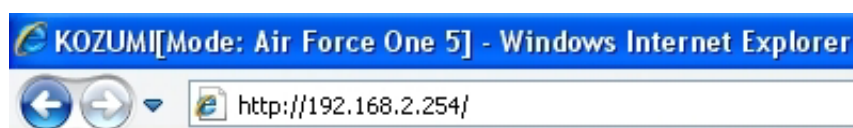
#### **Example of Segment :**

The valid range is 1 ~ 254 and 192.168.2.254 shall be avoided because it is already assigned to AFO-5 . 192.168.2.10 is used in the example below.

- IP Address : 192.168.2.10
- IP Netmask : 255.255.255.0

#### ■ Launch Web Browser

Launch web browser to access the web management interface of system by entering the default IP Address, <http://192.168.2.254>, in the URL field, and then press **Enter**.



## ■ System Login

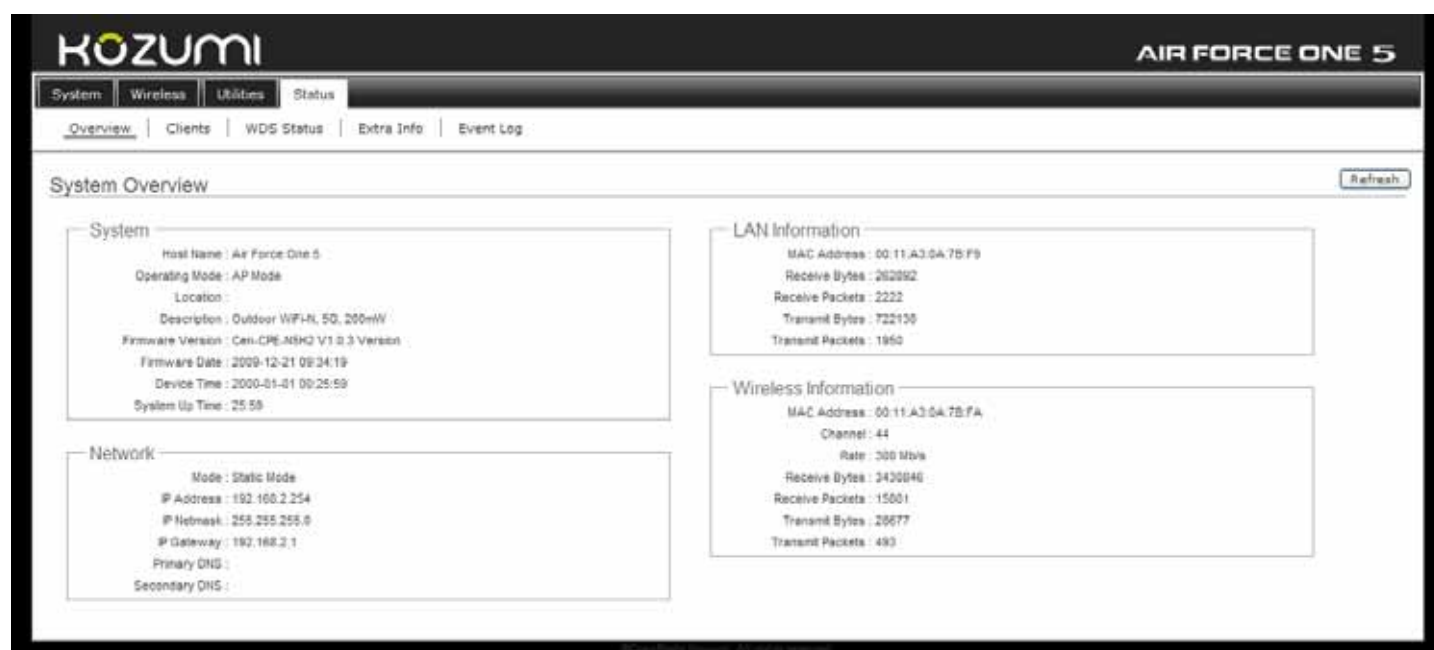
The system manager Login Page then appears.

Enter **“root”** as **User name** and **“default”** as **Password**, and then click OK to login to the system; the root manager account is used as an example here.



## ■ Login Success

System Overview page will appear after successful login.



## Chapter 3. AP Mode Configuration

When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

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

**Table 3-1: AP Mode Functions**

## 3.1 External Network Connection

### 3.1.1 Network Requirement

Normally, AFO-5 connects to a wired LAN and provides a wireless connection point to associate with wireless client as shown in Figure 3-1. Then, Wireless clients could access to LAN or Internet by associating themselves with AFO-5 set in AP mode.



Figure 3-1 Access Point on a Wired LAN Configuration

### 3.1.2 Configure LAN IP

Here are the instructions to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

#### LAN Setup

Ethernet Connection Type  
Mode : ☒ Static IP ☐ Dynamic IP

Static IP  
IP Address : 192.168.2.254  
IP Netmask : 255.255.255.0  
IP Gateway : 192.168.2.1

DNS  
DNS : ☒ No Default DNS Server ☐ Specify DNS Server IP  
Primary :   
Secondary :

802.1d Spanning Tree  
STP : ☐ Enable ☒ Disable

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .

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

- ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
- ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1

➔ **Dynamic IP** : This configuration type is applicable when the AFO-5is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

Dynamic IP  
Hostname :

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

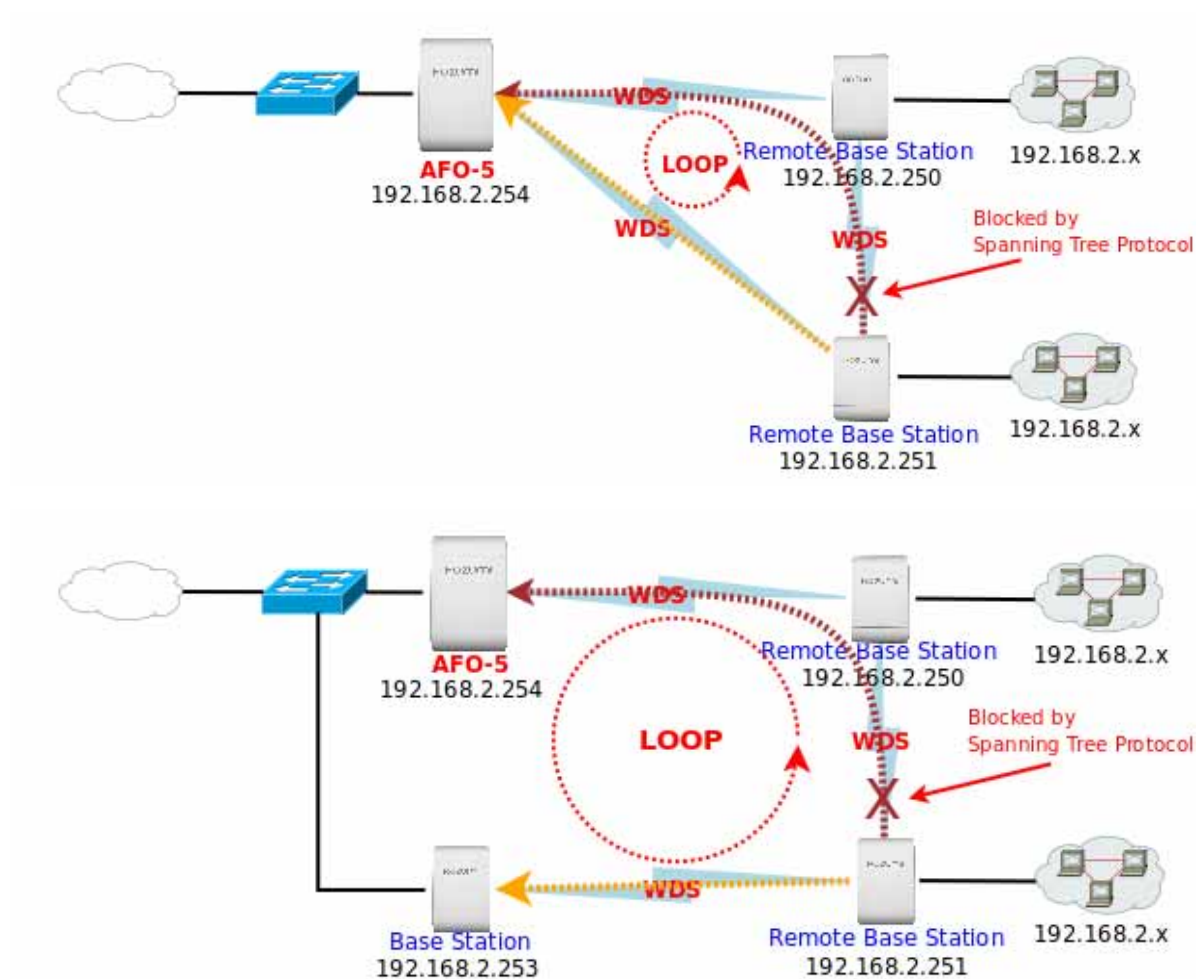
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.

➔ **Primary** : The IP address of the primary DNS server.

➔ **Secondary** : The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 4 WDS interfaces from wds0 to wds3. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. Below Figures depict a loop for a bridged LAN between LAN and WDS link



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

## 3.2 Wireless LAN Network Creation

The network manager can configure related wireless settings, **General Settings**, **Advanced Settings**, **Virtual AP(VAP) Setting**, **Security Settings**, and **MAC Filter Settings**.

### 3.2.1 Wireless General Setup

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

Wireless Setup

- **MAC address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **AP Isolation** : Select **Enable**, all clients will be isolated from each VAP, that means different VAP's clients can not reach to each other.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Channel** : The channel range will be changed by selecting different country code. Below depicts the channel range for different **Country**.

Country	Channel
US	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
JP	36, 40, 44, 48
NONE	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161

- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between **1** to **100** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, 10%.

When **Band Mode** select in **802.11a/n mixed mode**, the **HT(High Throughput)** settings should be shown-up immediately.

HT Other

HT TxStream :

HT RxStream :

- **HT TxStream/RxStream** : By default, it's 2.

HT Physical Mode

Operating Mode : ☒ Mixed Mode ☐ Green Field

Channel BandWidth : ☐ 20 ☒ 20/40

Guard Interval : ☐ Long ☒ Auto

MCS :

Reverse Direction Grant (RDG) : ☐ Disable ☒ Enable

Extension Channel :

A-MSDU : ☒ Disable ☐ Enable

Auto Block ACK : ☐ Disable ☒ Enable

Decline BA Request : ☒ Disable ☐ Enable

- **Operating Mode** : By default, it's Mixed Mode.
  - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
  - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "Auto" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG)** : Disable or enable reserve direction grant. Default is enabled.
- **Extension Channel** : When "20/40" channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **A-MSDU** : **Aggregated** Mac Service Data Unit. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU Default is disabled.
- **Auto Block ACK** : Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request** : Disable or enable decline BA request. Default is disabled.

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

### 3.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

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

#### Wireless Setup

Advanced Setup

Beacon Interval: 100 ms

DTIM Interval: 1 ms

Fragment Threshold: 2346

RTS Threshold: 2347

Short Preamble: ☒ Enable ☐ Disable

Short Slot: ☒ Enable ☐ Disable

Tx Burst: ☒ Enable ☐ Disable

Pkt\_Aggregate: ☒ Enable ☐ Disable

IEEE 802.11H: ☒ Enable ☐ Disable

WMM: ☐ Enable ☒ Disable

Save

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

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

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

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

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

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

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

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and



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

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

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

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

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

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

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet.

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

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

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

- **Pkt\_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H** : By default, it's "**Disable**". To **Enable** is to use IEEE802.11H

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

<b>DFS Channels</b>	52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140
---------------------	--

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

- ➔ **WMM Parameters of Access Point** : This affects traffic flowing from the access point to the client station

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : This affects traffic flowing from the client station to the access point.

Queue	Data Transmitted Clients to AP	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **all VAPs** and **WDS Links**.

### 3.2.3 Create Virtual AP (VAP)

The AFO-5 support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **7** logical access points, each of which can have a different set of security, VLAN tag(ID) and network settings. **Figure 3-2** shows multiple SSIDs with different security type and VLAN settings.

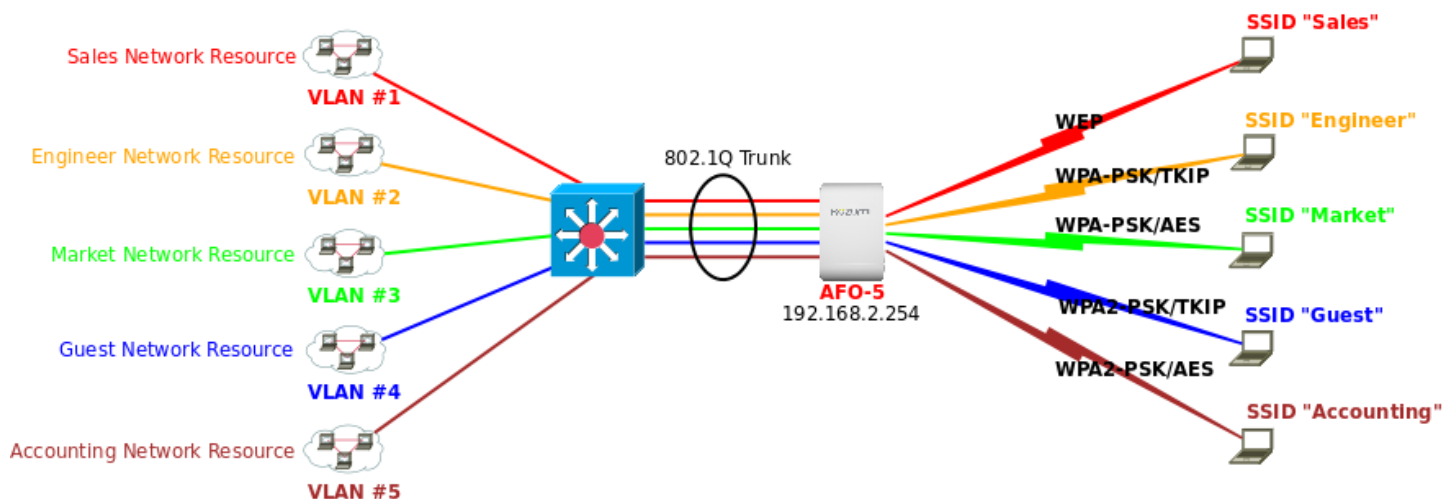


Figure 3-2 Multiple SSIDs with different Security Type and VLAN Tag

#### 3.2.3.1 Virtual AP Overview

The administrator can view all of the Virtual AP's settings via this page.

Please click on **Wireless -> Virtual AP Setup** and the Virtual AP Overview Page appears.

#### Virtual AP Overview

VAP List					
VAP	ESSID	Status	Security Type	MAC Filter	Edit
Primary AP	Main_AP	On	Disable	Disable	<a href="#">Edit</a>
VAP1		Off	Disable	Disable	<a href="#">Edit</a>
VAP2		Off	Disable	Disable	<a href="#">Edit</a>
VAP3		Off	Disable	Disable	<a href="#">Edit</a>
VAP4		Off	Disable	Disable	<a href="#">Edit</a>
VAP5		Off	Disable	Disable	<a href="#">Edit</a>
VAP6		Off	Disable	Disable	<a href="#">Edit</a>

- **VAP** : Indicate the system's Virtual AP.
- **ESSID** : Indicate the ESSID of the respective Virtual AP
- **Status** : Indicate the Status of the respective Virtual AP. The **Primary AP** always on.
- **Security Type** : Indicate an used security type of the respective Virtual AP.
- **MAC Filter** : Indicate an used MAC filter of the respective Virtual AP.
- **Edit** : Click **Edit** button to configure Virtual AP's settings, including security type and MAC Filter.

### 3.2.3.2 Virtual AP Setup

For each Virtual AP, administrators can configure SSID, VLAN tag(ID), SSID broadcasting, Maximum number of client associations, security type settings.

Click **Edit** button on the Edit column, and then a Virtual AP setup page appears.

#### VAP 1 Setup

Security

Enable AP : ☐ Enable ☒ Disable

ESSID :

Client Isolation : ☐ Enable ☒ Disable

Hidden SSID : ☐ Enable ☒ Disable

Maximum Clients :

VLAN Tag(ID) : ☐ Enable ☒ Disable  (1-4094)

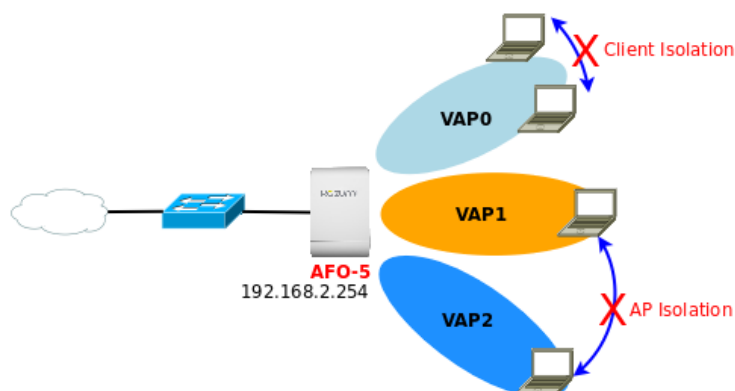
Security Type :

MAC Filter

Action :

Save

- **Enable AP** : By default, it's "**Disable**" for VAP1 ~ VAP6. **The Primary AP always enabled.**  
Select "**Enable**" to activate VAP or click "**Disable**" to deactivate this function
- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified VAP.
- **Client Isolation** : Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients. Below Figures depict Client Isolation and AP Isolation



- **Hidden SSID** : By default, it's "**Disable**".  
Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.
- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.

■ **VLAN Tag(ID)** : By default, it's selected "**Disable**".

This system supports tagged Virtual LAN(VLAN). A valid number of **1** to **4094** can be entered after it's enabled. If your network utilize VLANs you could tie a VLAN ID to a specific SSID, and packets from/to wireless clients belonging to that SSID will be tagged with that VLAN ID. This enables security of wireless applications by applying VLAN ID.

■ **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.

- ➔ **Disable** : Data are unencrypted during transmission when this option is selected.
- ➔ **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

■ **Authentication Method** : Enable the desire option among **OPEN**, **SHARED** or **WEPAUTO**.

- ➔ **Key Index** : Key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ➔ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite** : By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.



*Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.*

- ✓ **Group Key Update Period** : By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.

The image shows two configuration panels. The top panel, titled 'WPA General', contains the following settings: 'Cipher Suite' is set to 'AES' via a dropdown menu; 'Group Key Update Period' is set to '3600' seconds; 'PMK Cache Period' is set to '10' minute; and 'Pre-Authentication' has the 'Disable' radio button selected. The bottom panel, titled 'Authentication RADIUS Server', contains: 'Authentication Server' (empty text field); 'Port' is set to '1812'; 'Shared Secret' (empty text field); and 'Session Timeout' is set to '0'.

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.



*PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise*

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.  
Amount of time before a client will be required to re-authenticate.



- ➔ **WEP 802.1X** : When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

**802.1x WEP**  
Dynamic WEP : Enable

**Authentication RADIUS Server**  
Authentication Server :   
Port :   
Shared Secret :   
Session Timeout :

✓ **Radius Server Settings :**

- **IP Address** : Enter the IP address of the Authentication RADIUS server.
- **Port** : By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret** : A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout** : The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

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

### 3.2.4 Access Control List

Continue **3.2.3.2 Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.

- **MAC Filter Setup** : By default, it's "**Disable**". Options are **Disable**, **Only Deny List MAC** or **Only Allow List MAC**.

Two ways to set MAC filter rules :

➔ **Only Allow List MAC.**

The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

➔ **Only Deny List MAC.**

The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

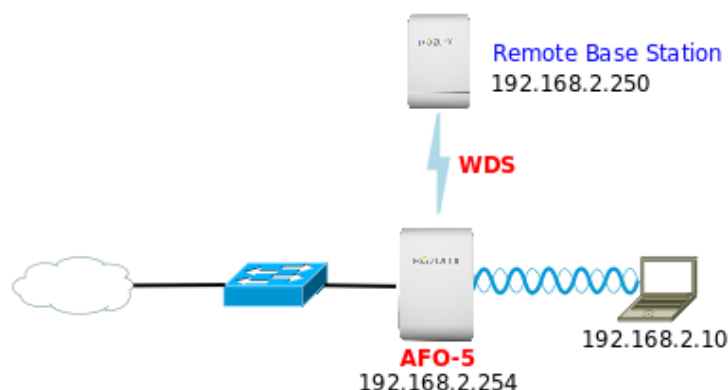
Click **Reboot** button to activate your changes



*MAC Access Control is the weakest security approach. WPA and WPA2 security method is highly recommended.*

### 3.3 Wireless Network Expansion

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



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

#### WDS Setup

Security

Security Type: Disable

WDS MAC List

Enable	WDS Peer's MAC Address	Description
<input type="checkbox"/>	01 <input type="text"/>	<input type="text"/>
<input type="checkbox"/>	02 <input type="text"/>	<input type="text"/>
<input type="checkbox"/>	03 <input type="text"/>	<input type="text"/>
<input type="checkbox"/>	04 <input type="text"/>	<input type="text"/>

Save

- **Security Type** : Option is "**Disable**", "**WEP**", "**TKIP**" or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
  - ➔ **WEP Key** : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
  - ➔ **TKIP Key** : Enter **8 to 63 ASCII** or **64 HEX** format TKIP key.
  - ➔ **AES Key** : Enter **8 to 63 ASCII** or **64 HEX** format AES key.
- **WDS MAC List**
  - ➔ **Enable** : Click **Enable** to create WDS link.
  - ➔ **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
  - ➔ **Description** : Description of WDS link.



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

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

## 3.4 System Management

### 3.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

#### Management Setup

The screenshot shows the 'Management Setup' page. On the left, under 'System Information', there are input fields for 'System Name' (filled with 'Air Force One 5'), 'Description' (filled with 'Outdoor WiFi-N, 5G, 200mW'), and 'Location'. Below this is a 'Root Password' section with 'New Root Password' and 'Check Root Password' fields. At the bottom left is an 'Admin Password' section with 'New Admin Password' and 'Check New Password' fields. On the right, under 'Admin Login Methods', there are four rows: 'Enable HTTP' with a checked box and 'Port: 80'; 'Enable HTTPS' with a checked box, 'Port: 443', and an 'UploadKey' button; 'Enable Telnet' with a checked box and 'Port: 23'; and 'Enable SSH' with a checked box, 'Port: 22', and a 'GenerateKey' button. Below the SSH section is a text box containing an SSH key: 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgOXYI'. A 'Save' button is located at the bottom center.

#### ■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

- **Root Password** : Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password** : Enter a new password if desired
  - ➔ **Check New Password** : Enter the same new password again to check.
- **Admin Password** : Log in as a admin user and is allowed to change its own,
  - ➔ **New Password** : Enter a new password if desired
  - ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.

- **Enable HTTP** : Check to select HTTP Service.
- **HTTP Port** : The default is **80** and the range is between 1 ~ 65535.
- **Enable HTTPS** : Check to select HTTPS Service
- **HTTPS Port** : The default is **443** and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

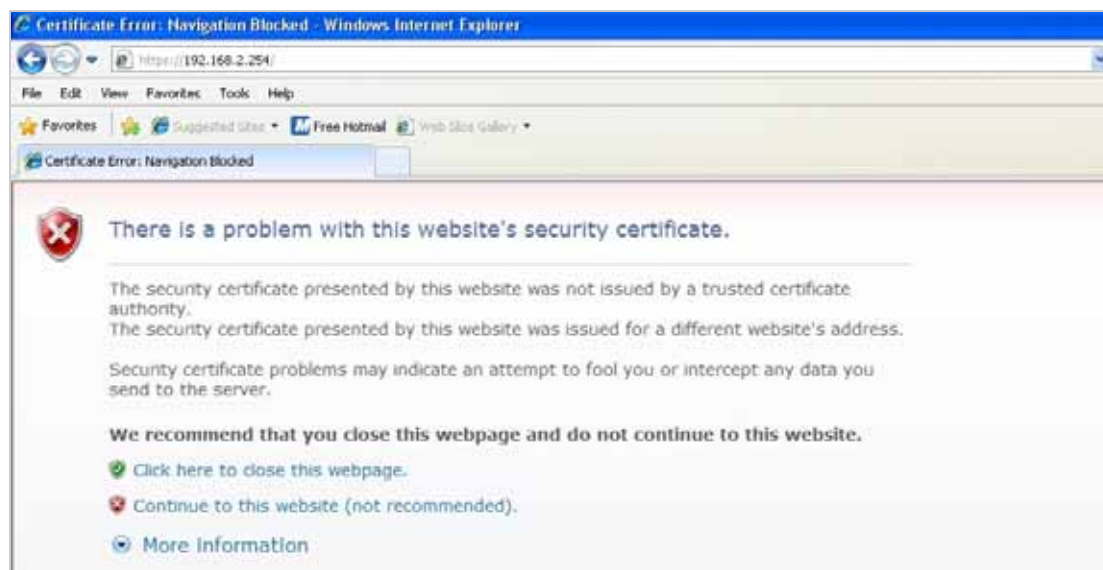
- **Enable Telnet** : Check to select Telnet Service
- **Telnet Port** : The default is **23** and the range is between 1 ~ 65535.
- **Enable SSH** : Check to select SSH Service
- **SSH Port** : Please The default is **22** and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

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

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254>). There will be a "Certificate Error", because the browser treats system as an illegal website.



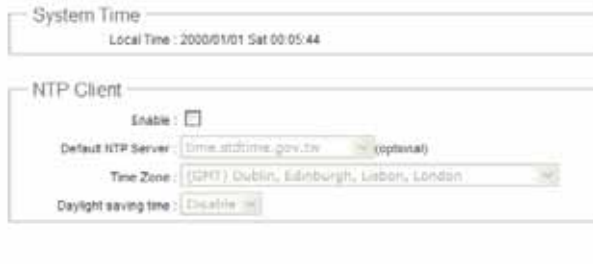
Click "**Continue to this website**" to access the system's WMI. The system's Overview page will appear.

### 3.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

#### Time Server Setup



- **Local Time** : Display the current system time.
- **NTP Client** : To synchronize the system time with NTP server.
  - ➔ **Enable** : Check to select NTP client.
  - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
  - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time** : Enable or disable Daylight saving.



*If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings*

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

### 3.4.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

#### UPNP Setup



UPNP : ☐ Enable ☒ Disable

Save

- **UPnP** : By default, it's "**Disable**". Select "**Enable**" or "**Disable**" of UPnP Service.

Click **Save** button to save changes and click **Reboot** button to activate changes

For UPnP to work in Windows XP, the "Air Force One 5" must be available in "**My Network Places**", as shown here: (your specific model may vary)



If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to **Appendix E. Using UPnP on Windows XP**

### 3.4.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

#### SNMP Setup

The image shows the 'SNMP Setup' configuration page. It contains three main sections, each with an 'Enable' checkbox:

- SNMP v2c**: Enable ☐
- SNMP v3**: Enable ☐
- SNMP Trap**: Enable ☐

A **Save** button is located at the bottom center of the page.

- **SNMP v2c Enable:** Check to enable SNMP v2c.

The image shows the 'SNMP v2c' configuration details. The 'Enable' checkbox is checked. Below it are two text input fields:

- ro community :
- rw community :

→ **ro community** : Set a community string to authorize read-only access.

→ **rw community** : Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

The image shows the 'SNMP v3' configuration details. The 'Enable' checkbox is checked. Below it are four text input fields:

- SNMP ro user :
- SNMP ro password :
- SNMP rw user :
- SNMP rw password :

→ **SNMP ro user** : Set a community string to authorize read-only access.

→ **SNMP ro password** : Set a password to authorize read-only access.

→ **SNMP rw user** : Set a community string to authorize read/write access.

→ **SNMP rw password** : Set a password to authorize read/write access.

- **SNMP Trap** : Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Enable : ☒

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

### 3.4.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

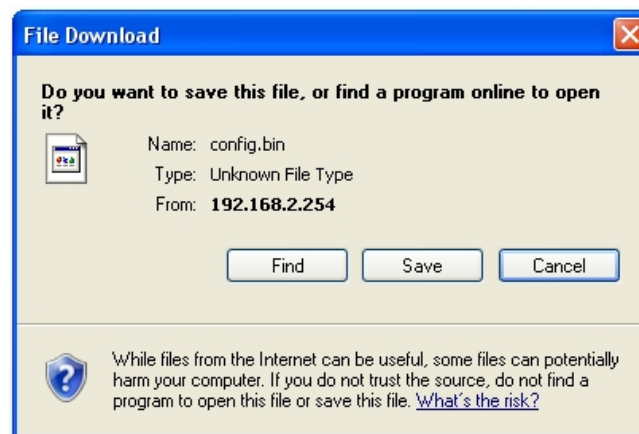
Please click on **Utilities -> Profile Setting** and follow the below setting.

#### Profile Save



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

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



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

### 3.4.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

#### Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version

Firmware Date : 2009-09-03 09:26:27

Update Firmware :

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



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.

### 3.4.7 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility.

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

Network Utility

The screenshot shows a web-based interface for network utilities. On the left, there are two sections: 'Ping' and 'Traceroute'. The 'Ping' section has a text input for 'Destination IP/Domain', a 'Count' dropdown set to '5', and a 'ping' button. The 'Traceroute' section has a text input for 'Destination Host', a 'MAX Hop' dropdown set to '6', and 'Start' and 'Stop' buttons. On the right, there is a large, empty rectangular area labeled 'Result' at the top, which is intended to display the output of the network tests.

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. [www.google.com](http://www.google.com), or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute** : Allows tracing the hops from the AFO-5 device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test
  - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - ➔ **MAX Hop** : Specifies the maximum number of hops( max time-to-live value) traceroute will probe.

### 3.4.8 Reboot

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

#### Reboot



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



The **System Overview** page appears upon the completion of reboot.

## 3.5 System Status

This section breaks down into subsections of **System Overview**, **Associated Clients Status**, **WDS Link Status**, **Extra Information** and **Event Log**.

### 3.5.1 System Overview

Display detailed information of **System**, **Network**, **LAN** and **Wireless** in the System Overview page.

- **System** : Display the information of the system.

System	
Host Name :	Air Force One 5
Operating Mode :	AP Mode
Location :	
Description :	Outdoor WiFi-N, 5G, 200mW
Firmware Version :	Cen-CPE-N5H2 V1.0.3 Version
Firmware Date :	2009-12-21 09:34:19
Device Time :	2000-01-01 00:25:59
System Up Time :	25:59

- ➔ **System Name** : The name of the system.
- ➔ **Operating Mode** : The mode currently in service.
- ➔ **Location** : Deployed geographical location.
- ➔ **Description** : A description of the system.
- ➔ **Firmware Version** : The current installed firmware version.
- ➔ **Firmware Date** : The build time of installed firmware.
- ➔ **Device Time** : The current time of the system.
- ➔ **System Up Time** : The time period that system has been in service since last reboot.

- **Network Information** : Supports Static or Dynamic modes on the LAN interface.

Network	
Mode :	Static Mode
IP Address :	192.168.2.254
IP Netmask :	255.255.255.0
IP Gateway :	192.168.2.1
Primary DNS :	
Secondary DNS :	

- ➔ **IP Address** : The management IP of system. By default, it's 192.168.2.254.
- ➔ **IP Netmask** : The network mask. By default, it's 255.255.255.0.
- ➔ **IP Gateway** : The gateway IP address and by default, it's 192.168.2.1.
- ➔ **Primary DNS** : The primary DNS server in service.
- ➔ **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.

LAN Information	
MAC Address :	00:0C:43:28:60:30
Receive Bytes :	75821
Receive Packets :	585
Transmit Bytes :	113309
Transmit Packets :	375

- ➔ **MAC Address** : The MAC address of the LAN port.
- ➔ **Receive bytes** : The total received packets in bytes on the LAN port.
- ➔ **Receive packets** : The total received packets of the LAN port.
- ➔ **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- ➔ **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display total received and transmitted statistics on available Virtual AP.

Wireless Information	
MAC Address :	00:11:A3:0A:7B:FA
Channel :	44
Rate :	300 Mb/s
Receive Bytes :	3430846
Receive Packets :	15801
Transmit Bytes :	28677
Transmit Packets :	493

- ➔ **MAC Address** : The MAC address of the Wireless port.
- ➔ **Channel** : The current channel on the Wireless port.
- ➔ **Rate** : The current Bit Rate on the Wireless port.
- ➔ **Receive bytes** : The total received packets in bytes on the Wireless port.
- ➔ **Receive packets** : The total received packets on the Wireless port.
- ➔ **Transmit bytes** : The total transmitted packets in bytes on the Wireless port.
- ➔ **Transmit packets** : The total transmitted packets on the Wireless port.

### 3.5.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with all Virtual AP.

[Refresh](#)

VAP Information					
VAP	ESSID	MAC Address	State	Security Type	Clients
Primary AP	Main_AP	00:11:A3:0A:7B:FA	On	Disable	1
VAP1		00:00:00:00:00:00	Off	Disable	0
VAP2		00:00:00:00:00:00	Off	Disable	0
VAP3		00:00:00:00:00:00	Off	Disable	0
VAP4		00:00:00:00:00:00	Off	Disable	0
VAP5		00:00:00:00:00:00	Off	Disable	0
VAP6		00:00:00:00:00:00	Off	Disable	0

Primary AP Clients						
MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth	Idle Time	Connect Time	Disconnect
00:06:B1:13:35:EF	100%(-33dBm)	100%(-38dBm)	20MHz	11	134	<a href="#">Delete</a>

- **VAP Information** : Highlights key VAP information.
  - ➔ **VAP** : Available VAP from Primary AP to VAP6.
  - ➔ **ESSID** : Display name of ESSID for each VAP.
  - ➔ **MAC Address** : Display MAC address for each VAP.
  - ➔ **Status** : On/Off
  - ➔ **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients** : Display total number of wireless connections for each VAP.
  
- **VAP Clients** : Display all associated clients on each Virtual AP.
  - ➔ **MAC Address** : MAC address of associated clients
  - ➔ **Signal Strength ANT0/ANT1** : Signal Strength of from associated clients.
  - ➔ **Bandwidth** : Channel bandwidth of from associated clients
  - ➔ **Idle Time** : Last inactive time period in seconds for a wireless connection.
  - ➔ **Connect Time** : Total connection time period in seconds for a wireless connection.
  - ➔ **Disconnect** : Click “**Delete**” button to manually disconnect a wireless client in a Virtual AP.



### 3.5.3 Show WDS Link Status

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

#### WDS Information

WDS Link Status						
MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:7B:F2	100% (-5 dBm)	100% (-6 dBm)	HTMIX	40M	15	1

- **MAC Address** : Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1** : Indicate the signal strength of the respective WDS links.
- **Phy Mode** : Indicate the phy mode of the respective WDS linked.
- **BandWidth** : Indicate the channel bandwidth of the respective WDS linked.
- **MCS** : Indicate the MCS of the respective WDS linked.
- **SGI** : Indicate the SGI (Short Guard Interval) of the respective WDS linked. "1" indicate the Short Guard Interval, "0" indicate the Long Guard Interval.



If display "**no signal**" Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address**, **Channel** and **Security type**. Also, adjust antenna angle and Tx Power.

### 3.5.4 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

#### Extra Information

Refresh

Extra Information  
Information: Route Information

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	bre0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	bre0

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

AFO-5 could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	bre0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	bre0

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

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

IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.2.22	0x1	0x2	00:1A:92:9F:A4:9B	*	bre0

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

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0~ra6 and wds0~wds3).

Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000c432880b0	no	eth2 ra0

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

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

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

Bridge MACs Information			
Port	MAC Address	Local	Ageing Timer
PrimaryAP	00:06:b1:13:35:ef	no	157.50
WDS0	00:11:a3:0a:7b:f1	no	2.05
LAN	00:11:a3:0a:7b:f9	yes	0.00
PrimaryAP	00:11:a3:0a:7b:fa	yes	0.00
LAN	00:1a:92:9f:a4:9b	no	0.10

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

Bridge STP Information			
<b>bre0</b>			
bridge id	8000.000c43288008		
designated root	8000.000c43288008		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00		
hello timer	0.84	tcn timer	0.00
topology change timer	0.00	gc timer	2.83
flags			
<b>eth2 (1)</b>			
port id	8001	state	forwarding
designated root	8000.000c43288008	path cost	100
designated bridge	8000.000c43288008	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.85
flags			
<b>ra0 (2)</b>			
port id	8002	state	forwarding
designated root	8000.000c43288008	path cost	100
designated bridge	8000.000c43288008	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.85
flags			

### 3.5.5 Event Log

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

#### System Log

[Refresh](#) [Clear](#)

Result			
Time	Facility	Severity	Message
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: started, version 2.40 cachesize 150
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-i18N TFTP
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: reading /etc/resolv.conf
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: using nameserver 192.168.2.1#53
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: cleared cache
2000 Jan 1 00:00:38	System	Info	Authentication successful for root from 192.168.2.22

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

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

## Chapter 4. WDS Mode Configuration

Please refer to illustrations of the section 1.3 for possible applications in the WDS mode. This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

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

**Table 4-1: WDS Mode Functions**

## 4.1 External Network Connection

### 4.1.1 Network Requirement

You could expand your Ethernet network via WDS link. In this mode, the AFO-5 connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in Figure 4-1. In the mode, it can't associate with any wireless clients.



**Figure 4-1 Point to Point Configuration**

## 4.1.2 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

### LAN Setup

Ethernet Connection Type  
Mode : ☒ Static IP ☐ Dynamic IP

Static IP  
IP Address : 192.168.2.254  
IP Netmask : 255.255.255.0  
IP Gateway : 192.168.2.1

DNS  
DNS : ☒ No Default DNS Server ☐ Specify DNS Server IP  
Primary :   
Secondary :

802.1d Spanning Tree  
STP : ☐ Enable ☒ Disable

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .

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

- ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
- ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1

➔ **Dynamic IP** : This configuration type is applicable when the AFO-5 is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

Dynamic IP  
Hostname :

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

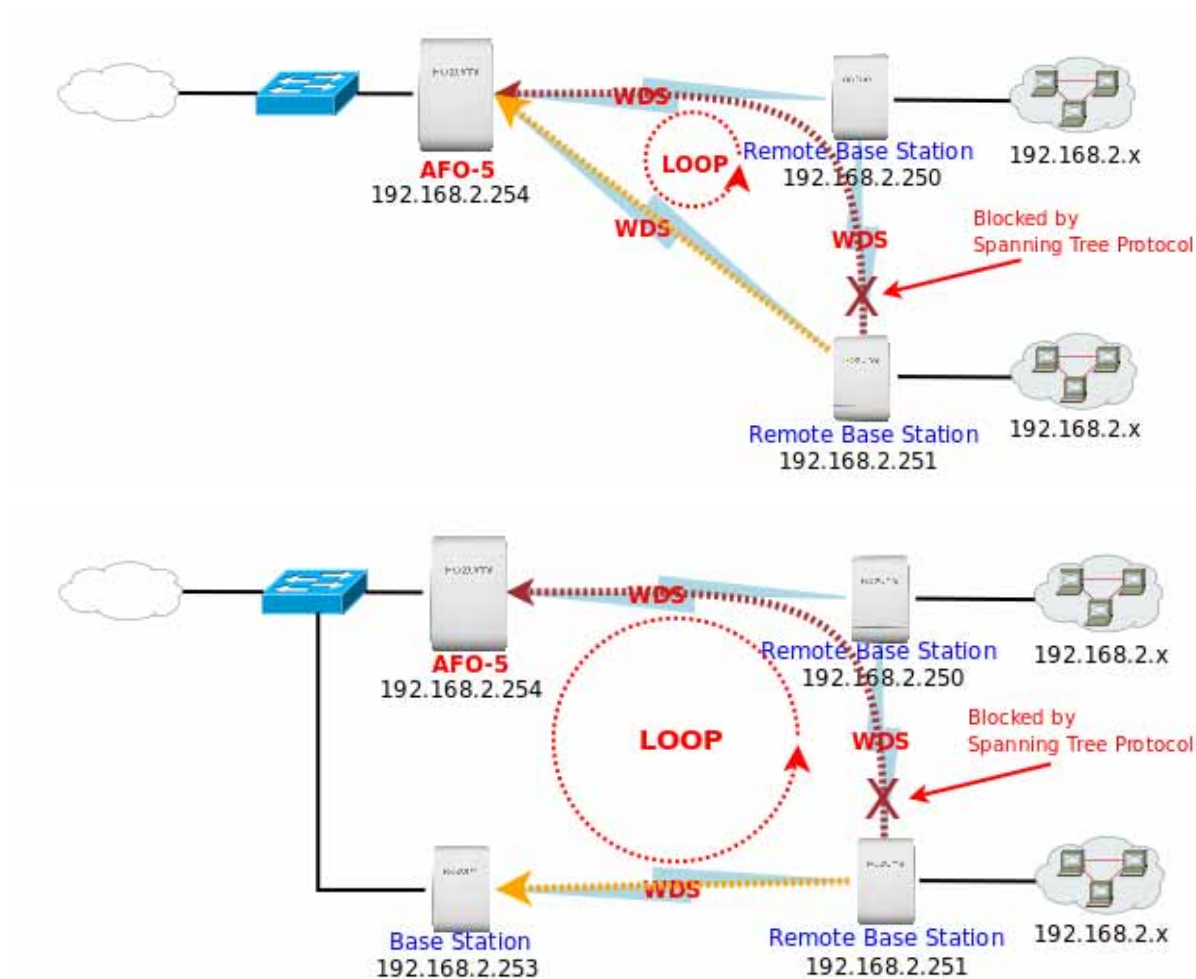
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.

➔ **Primary** : The IP address of the primary DNS server.

➔ **Secondary** : The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. Below Figures depict a loop for a bridged LAN between LAN and WDS link



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

## 4.2 Wireless Network Expansion

The network manager can configure related wireless settings, **General Settings**, **Advanced Settings** and **WDS Settings**.

### 4.2.1 General Setup

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

Wireless Setup

- **MAC address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Channel** : The channel range will be changed by selecting different country code. Below depicts the channel range for different **Country**.

Country	Channel
US	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
JP	36, 40, 44, 48
NONE	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161

- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between **1** to **100** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, 10%.

When **Band Mode** select in **802.11a/n mixed mode**, the **HT(High Throughput)** settings should be shown-up immediately.



HT Other

HT TxStream : 2

HT RxStream : 2

- **HT TxStream/RxStream** : By default, it's 2.

HT Physical Mode

Operating Mode : ☒ Mixed Mode ☐ Green Field

Channel BandWidth : ☐ 20 ☒ 20/40

Guard Interval : ☐ Long ☒ Auto

MCS : Auto

Reverse Direction Grant (RDG) : ☐ Disable ☒ Enable

Extension Channel : Auto Select

A-MSDU : ☒ Disable ☐ Enable

Auto Block ACK : ☐ Disable ☒ Enable

Decline BA Request : ☒ Disable ☐ Enable

- **Operating Mode** : By default, it's Mixed mode
  - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
  - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "Auto" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG)** : Disable or enable reserve direction grant. Default is enabled.
- **Extension Channel** : When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **A-MSDU** : **Aggregated** Mac Service Data Unit . Select **Enable** to allow aggregation for multiple MSDUs in one MPDU Default is disabled.
- **Auto Block ACK** : Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request** : Disable or enable decline BA request. Default is disabled.

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

## 4.2.2 Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

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

### Wireless Setup

Advanced Setup

Beacon Interval: 100 ms

DTIM Interval: 1 ms

Fragment Threshold: 2346

RTS Threshold: 2347

Short Preamble: ☒ Enable ☐ Disable

Short Slot: ☒ Enable ☐ Disable

Tx Burst: ☒ Enable ☐ Disable

Pkt\_Aggregate: ☒ Enable ☐ Disable

IEEE 802.11H: ☒ Enable ☐ Disable

WMM: ☐ Enable ☒ Disable

Save

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

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

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

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

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

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

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

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and

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

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

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

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

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

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

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time.

Slot time is the amount of time a device waits after a collision before retransmitting a packet.

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

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

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

- **Pkt\_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H** : By default, it's "**Disable**". To **Enable** is to use IEEE802.11H

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

<b>DFS Channels</b>	52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140
---------------------	--

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

- **WMM Parameters of Access Point** : This affects traffic flowing from the access point to the client station

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : This affects traffic flowing from the client station to the access point.

Queue	Data Transmitted Clients to AP	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC\_VI and AC\_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

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

### 4.2.3 WDS Setup

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

WDS Setup

Enable	WDS Peer's MAC Address	Description
<input type="checkbox"/>	01	
<input type="checkbox"/>	02	
<input type="checkbox"/>	03	
<input type="checkbox"/>	04	

Save

- **Security Type** : Option is “**Disable**”, “**WEP**”, “**TKIP**” or “**AES**” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
  - ➔ **WEP Key** : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
  - ➔ **TKIP Key** : Enter **8 to 63 ASCII** or **64 HEX** format TKIP key.
  - ➔ **AES Key** : Enter **8 to 63 ASCII** or **64 HEX** format AES key.
- **WDS MAC List**
  - ➔ **Enable** : Click **Enable** to create WDS link.
  - ➔ **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
  - ➔ **Description** : Description of WDS link.



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

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

## 4.3 System Management

### 4.3.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

**System Information**

System Name:

Description:

Location:

**Root Password**

New Root Password:

Check Root Password:

**Admin Password**

New Admin Password:

Check New Password:

**Admin Login Methods**

Enable HTTP: ☒ Port:

Enable HTTPS: ☒ Port:

Enable Telnet: ☒ Port:

Enable SSH: ☒ Port:

`ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgOXYI`

#### ■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

- **Root Password** : Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password** : Enter a new password if desired
  - ➔ **Check New Password** : Enter the same new password again to check.
- **Admin Password** : Log in as a admin user and is allowed to change its own,
  - ➔ **New Password** : Enter a new password if desired
  - ➔ **Check New Password** : Enter the same new password again to check.



- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.

- ➔ **Enable HTTP** : Check to select HTTP Service.
- ➔ **HTTP Port** : The default is 80 and the range is between 1 ~ 65535.
- ➔ **Enable HTTPS** : Check to select HTTPS Service
- ➔ **HTTPS Port** : The default is 443 and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

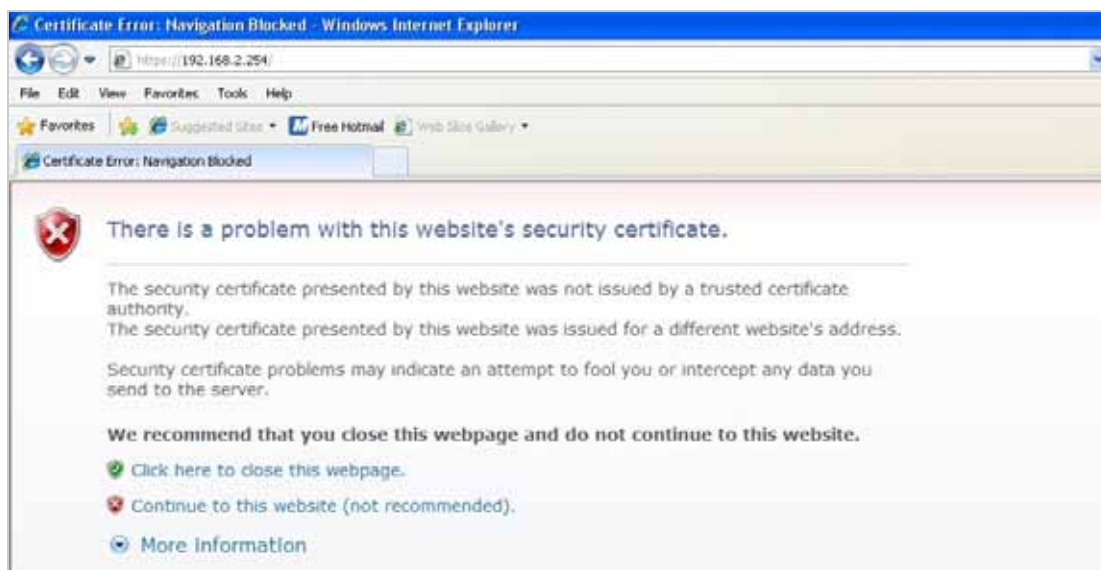
- ➔ **Enable Telnet** : Check to select Telnet Service
- ➔ **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- ➔ **Enable SSH** : Check to select SSH Service
- ➔ **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

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

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click "**Continue to this website**" to access the system's WMI. The system's Overview page will appear.

### 4.3.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

#### Time Server Setup



Save

- **Local Time** : Display the current system time.
- **NTP Client** : To synchronize the system time with NTP server.
  - ➔ **Enable** : Check to select NTP client.
  - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
  - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time** : Enable or disable Daylight saving.



*If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings*

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

### 4.3.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

#### UPNP Setup



UPNP : ☐ Enable ☒ Disable

Save

- **UPnP** : By default, it's "**Disable**". Select "**Enable**" or "**Disable**" of UPnP Service.

Click **Save** button to save changes and click **Reboot** button to activate changes

For UPnP to work in Windows XP, the "Air Force One 5" must be available in "**My Network Places**", as shown here: (your specific model may vary)



If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to **Appendix E. Using UPnP on Windows XP**

### 4.3.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

The image shows the 'SNMP Setup' configuration page. It contains three main sections: 'SNMP v2c', 'SNMP v3', and 'SNMP Trap'. Each section has an 'Enable' checkbox. Below these sections is a 'Save' button.

- **SNMP v2c Enable** : Check to enable SNMP v2c.

The image shows the 'SNMP v2c' configuration details. The 'Enable' checkbox is checked. There are two text input fields: 'ro community' and 'rw community'.

➔ **ro community** : Set a community string to authorize read-only access.

➔ **rw community** : Set a community string to authorize read/write access.

- **SNMP v3 Enable: Check to enable SNMP v3.**

SNMPv3 supports the highest level SNMP security.

The image shows the 'SNMP v3' configuration details. The 'Enable' checkbox is checked. There are four text input fields: 'SNMP ro user', 'SNMP ro password', 'SNMP rw user', and 'SNMP rw password'.

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

➔ **SNMP ro password** : Set a password to authorize read-only access.

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

➔ **SNMP rw password** : Set a password to authorize read/write access.

- **SNMP Trap** : Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

SNMP Trap

Enable : ☒

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.


### 4.3.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

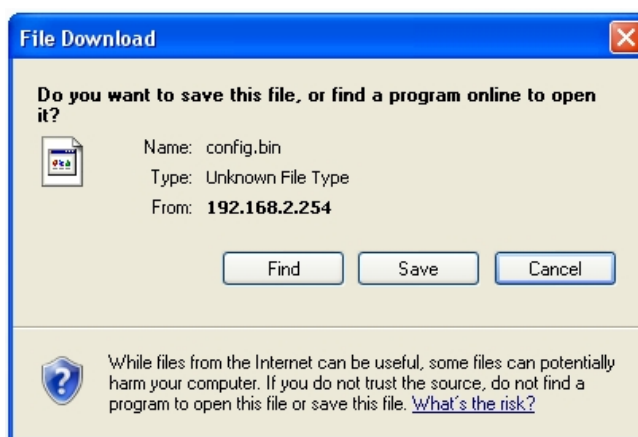
Please click on **Utilities -> Profile Setting** and follow the below setting.

#### Profile Save



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

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



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

### 4.3.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

#### Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-NSM2 V0.0.4 Beta Version  
Firmware Date : 2009-09-03 09:26:27  
Update Firmware :

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



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding.
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.

### 4.3.7 Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

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

Network Utility

The screenshot shows a web-based interface for network utilities. On the left, there are two sections: 'Ping' and 'Traceroute'. The 'Ping' section has a text input for 'Destination IP/Domain', a 'Count' dropdown set to '5', and a 'ping' button. The 'Traceroute' section has a text input for 'Destination Host', a 'MAX Hop' dropdown set to '6', and 'Start' and 'Stop' buttons. On the right, there is a large, empty rectangular area labeled 'Result' at the top, which is intended to display the output of the network tests.

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. [www.google.com](http://www.google.com), or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute** : Allows tracing the hops from the AFO-5 device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
  - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - ➔ **MAX Hop** : Specifies the maximum number of hops( max time-to-live value) traceroute will probe.



### 4.3.8 Reboot

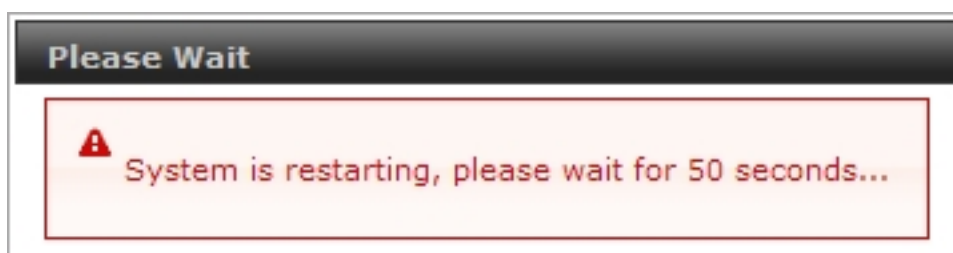
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

#### Reboot

 You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Reboot

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



The **System Overview** page appears upon the completion of reboot.

## 4.4 System Status

This section breaks down into subsections of **System Overview**, **WDS Link Status**, **Extra Information** and **Event Log**.

### 4.4.1 System Overview

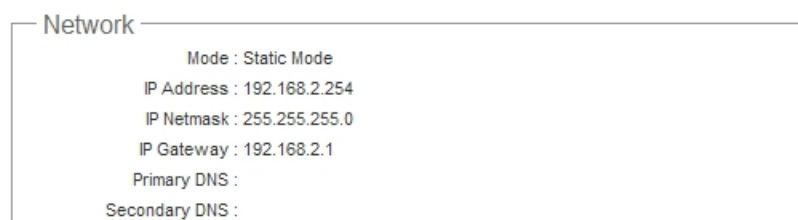
Detailed information on **System**, **Network**, **LAN Information** and **Wireless Information** can be reviewed via this page.

- **System** : Display the information of the system.



- ➔ **System Name** : The name of the system.
- ➔ **Operating Mode** : The mode currently in service.
- ➔ **Location** : The reminding note on the geographical location of the system.
- ➔ **Description** : The reminding note of the system.
- ➔ **Firmware Version** : The current firmware version installed.
- ➔ **Firmware Date** : The build time of the firmware installed.
- ➔ **Device Time** : The current time of the system.
- ➔ **System Up Time** : The time period that system has been in service since last reboot.

- **Network Information** : Display the information of the Network.



- ➔ **Mode** : Supports Static or Dynamic modes on the LAN interface.
- ➔ **IP Address** : The management IP of system. By default, it's 192.168.2.254.
- ➔ **IP Netmask** : The network mask. By default, it's 255.255.255.0.
- ➔ **IP Gateway** : The gateway IP address and by default, it's 192.168.2.1.
- ➔ **Primary DNS** : The primary DNS server in service.
- ➔ **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.

LAN Information	
MAC Address :	00:0C:43:28:60:30
Receive Bytes :	2888
Receive Packets :	22
Transmit Bytes :	3610
Transmit Packets :	22

- ➔ **MAC Address** : The MAC address of the LAN port.
- ➔ **Receive bytes** : The total received packets in bytes on the LAN port.
- ➔ **Receive packets** : The total received packets of the LAN port.
- ➔ **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- ➔ **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display the detailed receive and transmit statistics of Wireless interface.

Wireless Information	
MAC Address :	00:11:A3:0A:7B:FA
Channel :	44
Rate :	300 Mb/s
Receive Bytes :	167110
Receive Packets :	706
Transmit Bytes :	15373
Transmit Packets :	104

- ➔ **MAC Address** : The MAC address of the Wireless port.
- ➔ **Channel** : The current channel on the Wireless port.
- ➔ **Rate** : The current Bit Rate on the Wireless port.
- ➔ **Receive bytes** : The total received packets in bytes on the Wireless port.
- ➔ **Receive packets** : The total received packets of the Wireless port.
- ➔ **Transmit bytes** : The total transmitted packets in bytes of the Wireless port.
- ➔ **Transmit packets** : The total transmitted packets of the Wireless port.

### 4.4.2 WDS List

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

#### WDS Information

WDS Link Status						
MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:7B:F2	100% (-5 dBm)	100% (-6 dBm)	HTMIX	40M	15	1

- **MAC** : Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1** : Indicate the signal strength of the respective WDS links.
- **Phy Mode** : Indicate the phy mode of the respective WDS linked.
- **BandWidth** : Indicate the channel bandwidth of the respective WDS linked.
- **MCS** : Indicate the MCS of the respective WDS linked.
- **SGI** : Indicate the SGI (Short Guard Interval) of the respective WDS linked. "1" indicate the Short Guard Interval, "0" indicate the Long Guard Interval.



If display "**no signal**" Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address**, **Channel** and **Security type**. Also, adjust antenna angle and Tx Power.

### 4.4.3 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information

Refresh

Extra Information

Information: Route Information

Route Information

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	bre0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	bre0

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

AFO-5 could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

Route Information							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	bre0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	bre0

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

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

ARP Table Information					
IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.2.22	0x1	0x2	00:1A:92:9F:A4:9B	*	bre0

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

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0 and wds0~wds3).

Bridge Table Information			
Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000c432880b0	no	eth2 ra0

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

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

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

Bridge MACs Information			
Port	MAC Address	Local	Ageing Timer
WDS0	00:11:a3:0a:7b:f1	no	1.69
LAN	00:11:a3:0a:7b:f9	yes	0.00
LAN	00:12:cf:51:ea:27	no	68.68
LAN	00:16:d4:33:32:6b	no	15.71
LAN	00:1a:4b:1e:e5:15	no	273.04
LAN	00:1a:92:9f:a4:9b	no	0.19
LAN	00:21:9b:df:d9:31	no	24.29

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

Bridge STP Information			
<b>bre0</b>			
bridge id	8000.000c43288008		
designated root	8000.000c43288008		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00		
hello timer	0.84	tcn timer	0.00
topology change timer	0.00	gc timer	2.83
flags			
<b>eth2 (1)</b>			
port id	8001	state	forwarding
designated root	8000.000c43288008	path cost	100
designated bridge	8000.000c43288008	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.85
flags			
<b>ra0 (2)</b>			
port id	8002	state	forwarding
designated root	8000.000c43288008	path cost	100
designated bridge	8000.000c43288008	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.85
flags			

### 4.4.4 Event Log

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

#### System Log

[Refresh](#) [Clear](#)

Result			
Time	Facility	Severity	Message
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: started, version 2.40 cachesize 150
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-i18N TFTP
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: reading /etc/resolv.conf
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: using nameserver 192.168.2.1#53
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: cleared cache
2000 Jan 1 00:00:38	System	Info	Authentication successful for root from 192.168.2.22

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

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

## Chapter 5. CPE Mode Configuration

When CPE mode is chosen, the system can be configured as a Customer Premises Equipment(CPE). This section provides detailed explanation for users to configure in the CPE mode with help of illustrations. In the CPE mode, functions listed in the table below are also available from the Web-based GUI interface.

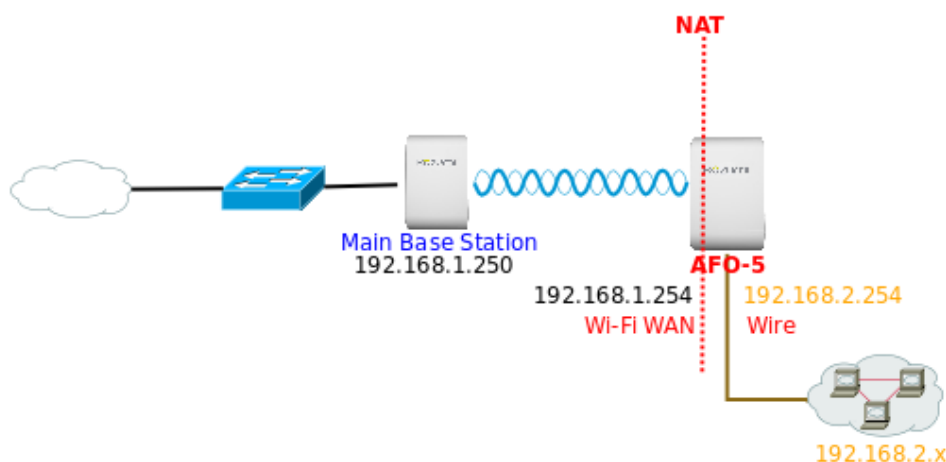
OPTION	System	Wireless	Advance	Utilities	Status
Functions	Operating Mode	General Setup	DMZ	Profiles Settings	System Overview
	WAN	Wireless Profile	IP Filter Setup	Firmware Upgrade	Station Statistics
	LAN	Site Survey	MAC Filter Setup	Network Utility	Extra Info
	DDNS Setup		Virtual Server	Reboot	Event Log
	Management		QoS		
	Time Server				
	UPNP				
	SNMP				

**Table 5-1: CPE Mode Functions**

## 5.1 External Network Connection

### 5.1.1 Network Requirement

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, AFO-5 is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to AFO-5 are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.



**Figure 5-1 CPE mode configuration**