

## 5.1.2 Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP** and **PPPoE**,

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

### WAN Setup



*In CPE mode, the WAN Port is the Wireless interface.*

- **Mode** : By default, it's "**Static IP**". Check "Static IP", "Dynamic IP" or "PPPoE" to set up system WAN IP.

➔ **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.

- ✓ **IP Address** : The IP address of the WAN port; default IP address is 192.168.1.254
- ✓ **IP Netmask** : The Subnet mask of the WAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway** : The default gateway of the WAN port; default Gateway is 192.168.1.1

➔ **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click **Release** button to release IP address and click **Renew** button to renew IP address again.

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

➔ **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.

- ✓ **User Name** : Enter User Name for PPPoE connection
- ✓ **Password** : Enter Password for PPPoE connection
- ✓ **Reconnect Mode** :
  - **Always on** – A connection to Internet is always maintained.
  - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “Reconnect Mode” will turn out “Always on”
- ✓ **MTU** : By default, it's **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **DNS** : Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.
  - ➔ **Primary** : The IP address of the primary DNS server.
  - ➔ **Secondary** : The IP address of the secondary DNS server.
- **MAC Clone** : The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.

MAC Clone

☒ Keep Default MAC Address

☐ Clone MAC Address: 00:1A:92:9F:A4:9B

☐ Manual MAC Address:  :  :  :  :  :

- ➔ **Keep Default MAC Address** : Keep the default MAC address of WAN port on the system.
- ➔ **Clone MAC Address** : If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.



The Clone MAC Address field will display MAC address of the PC connected to system. Click “Save” button can make clone MAC effective.

- ➔ **Manual MAC Address** : Enter the MAC address registered with your ISP.

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

### 5.1.3 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

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

#### Dynamic DNS Setup



- **Enabled:** By default, it's "**Disable**". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

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

## 5.1.4 Configure LAN Setup

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

LAN IP

IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

DHCP Server

DHCP: ☐ Enable ☒ Disable

802.1d Spanning Tree

STP: ☐ Enable ☒ Disable

Save

- **LAN IP** : The administrator can manually setup the LAN IP address.
  - ➔ **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

### ■ 802.1d Spanning Tree

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

DHCP Server

DHCP: ☒ Enable ☐ Disable

Start IP: 192.168.2.10

End IP: 192.168.2.70

DNS1 IP:

DNS2 IP:

WINS IP:

Domain:

Lease Time:

- ➔ **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- ➔ **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain** : Enter the domain name for this network.

- **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

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

## 5.2 Access Point Association

### 5.2.1 Configure Wireless General Setting

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

#### Wireless Setup

**General Configuration**

Band Mode:

Country:

Tx Power:  %

**HT Physical Mode**

Operating Mode: ☒ Mixed Mode ☐ Green Field

Channel BandWidth: ☐ 20 ☒ Auto

Guard Interval: ☐ Long ☒ Auto

MCS:

**11n Configuration**

MPDU Enable: ☐ Enable ☒ Disable

A-MPDU: ☐ Manual ☒ Auto

MPDU Density:

A-MSDU: ☐ Enable ☒ Disable

- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **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 of which setting to choose, then keep the default setting, **10%**.

When **Band Mode** select in **802.11a/n mixed mode**, the **HT(High Throughput) Physical Mode** and **11n Configuration** settings should be shown-up immediately.

**HT Physical Mode**

Operating Mode: ☒ Mixed Mode ☐ Green Field

Channel BandWidth: ☐ 20 ☒ Auto

Guard Interval: ☐ Long ☒ Auto

MCS:

**11n Configuration**

MPDU Enable: ☐ Enable ☒ Disable

A-MPDU: ☐ Manual ☒ Auto

MPDU Density:

A-MSDU: ☐ Enable ☒ Disable

- **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 "**Auto**" 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**)
- **MPDU Enable** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **A-MPDU** : A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select "Manual" to set "MPDU Density"
- **MPDU Density** : Minimum separation of MPDUs in an A-MPDU.

0	1	2	3	4	5	6	7
No Restriction	$\frac{1}{4} \mu s$	$\frac{1}{2} \mu s$	$1 \mu s$	$2 \mu s$	$4 \mu s$	$8 \mu s$	$16 \mu s$

- **A-MSDU : Aggregated** Mac Service Data Unit, A-MSDU. Select **Enable** to allows aggregation for multiple MSDUs in one MPDU. Default is disabled.

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

## 5.2.2 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.

### Station Site Survey

#### Scan Result

ESSID	MAC Address	Signal	Channel	Security	Band	Network Type	Select
Main_AP	00:11:a3:0a:7c:3a	50%	44	NONE	11a/n	Infrastructure	<a href="#">Select</a>
Main_AP-253	00:11:a3:0a:7b:f2	100%	44	NONE	11a/n	Infrastructure	<a href="#">Select</a>
253AP1	00:11:a3:0a:7b:f3	100%	44	WEP	11a/n	Infrastructure	<a href="#">Select</a>
253AP2	00:11:a3:0a:7b:f4	100%	44	WPAPSK/AES	11a/n	Infrastructure	<a href="#">Select</a>
253AP3	00:11:a3:0a:7b:f5	100%	44	WPAPSK/TKIP	11a/n	Infrastructure	<a href="#">Select</a>
253AP4	00:11:a3:0a:7b:f6	100%	44	WPA2PSK/AES	11a/n	Infrastructure	<a href="#">Select</a>
253AP5	00:11:a3:0a:7b:f7	100%	44	WPA2PSK/TKIP	11a/n	Infrastructure	<a href="#">Select</a>

- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Signal :** Received signal strength of all found Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Security :** Security type by all found Access Points.
- **Band :** Wireless band used by all found Access Points.
- **Network Type :** Network type used by all found Access Points.
- **Select :** Click “**Select**” to configure settings and associate with chosen AP.



While clicking “Select” button in the Site Survey Table, the “**ESSID**” and “**Security Type**” will apply in the Wireless Profile Setup. However, more settings are needed including Security Key.



### 5.2.3 Create Wireless Profile

The administrator can configure station profiles via this page.

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

- **Profile Name** : Set different profiles for quick connection uses.
- **ESSID** : Assign Service Set ID for the wireless system.
- **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** : RTS 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 "**Auto**". To **Disable** is to use Long 128-bit Preamble Synchronization field.  
The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
  - **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.  
With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
  - **WMM** : By default, it's "**Disable**". Select Enable, the packets with QoS WMM will have higher priority.
  - **Security Type** : Select an appropriate security type for association, the Security Type can be selected in "**NONE**", "**OPEN**", "**SHARED**", "**WPA-PSK**", or "**WPA2-PSK**" from drop-down list; the type needs to be the same as that associated access point.
- ➔ **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.

WEP

Key Index :

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- ✓ **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.

WPA

Cipher Suite :

Pre-shared Key :

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.

- **Profile List** : The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List

Profile List

Active	#	Profile Name	ESSID	Security Type	Delete	Edit
<input type="radio"/>	1	Profile0	default	NONE	<a href="#">Delete</a>	<a href="#">Edit</a>
<input checked="" type="radio"/>	2	Profile-Test	253AP1	OPEN	<a href="#">Delete</a>	<a href="#">Edit</a>

- ➔ Click “**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.
- ➔ Click “**Delete**” to remove profile.

- Click and Select a profile from list, then click the **“Connect”** button to connecting to the wireless network with the profile setting.



*If you only click “Connect” button and does not click “Save” button. The selected profile would not be saved on the Profile List after rebooting*

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

## 5.3 System Management

### 5.3.1 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

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. Further down 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 checkbox and 'Port: 80'; 'Enable HTTPS' with a checked checkbox, 'Port: 443', and an 'UploadKey' button; 'Enable Telnet' with a checked checkbox and 'Port: 23'; and 'Enable SSH' with a checked checkbox, 'Port: 22', and a 'GenerateKey' button. Below the SSH section is a text box containing an SSH key: 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgOXYI'. At the bottom center is a 'Save' button.

#### ■ 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.*

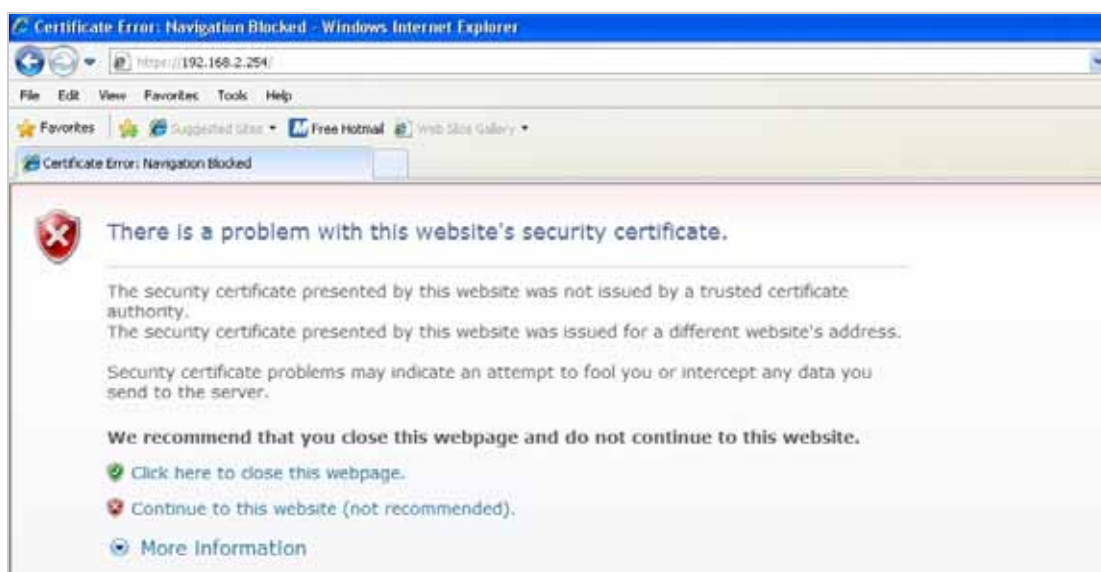
- ➔ **Enable Telnet** : Check to select Telnet Service
- ➔ **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- ➔ **Enable SSH** : Check to select SSH Service
- ➔ **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



*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://192.168.10.100>). There will be a "Certificate Error", because the browser treats system as an illegal website.



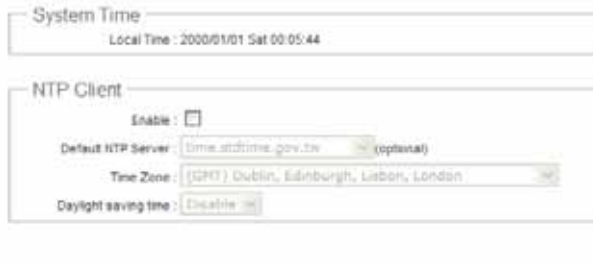
Click "**Continue to this website**" to access the system's WMI. The system's Overview page will appear.

### 5.3.2 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



- **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

### 5.3.3 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



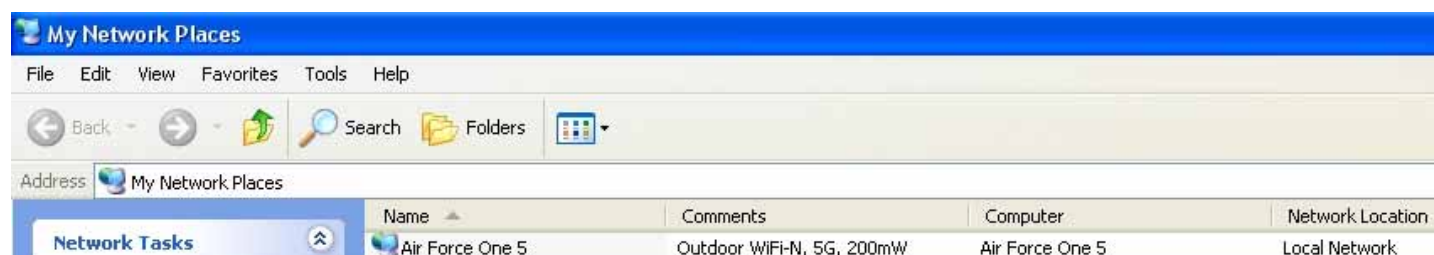
UPNP : ☐ Enable ☒ Disable

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**

### 5.3.4 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.

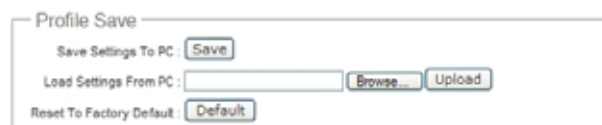
Click **Save** button to save changes and click **Reboot** button to activate.


### 5.3.5 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.

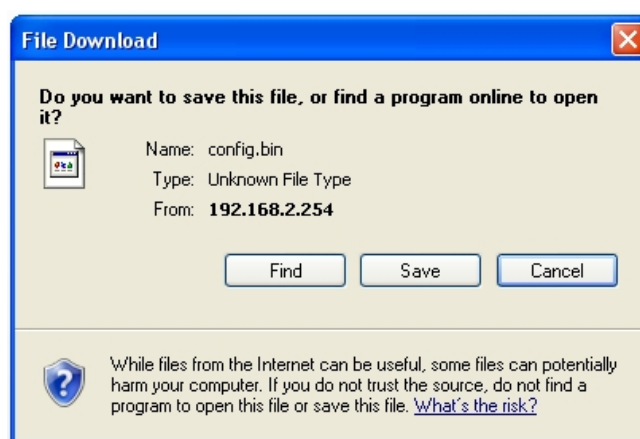
Please click on **Utilities -> Profile Setting** and follow the below setting.

#### 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.

### 5.3.6 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 Browse 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.

### 5.3.7 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' for displaying the test outcomes.

- **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.

### 5.3.8 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.

## 5.4 Access Control List

### 5.4.1 IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.

IP Filter Setup

#### IP Rules

Source Address/Mask:

Source Port:

Destination Address/Mask:

Destination Port:

In/Out: ☐ In ☒ Out

Protocol: ☒ TCP ☐ UDP ☐ ICMP

Listen: ☐ Yes ☒ No

Action: ☒ Deny ☐ Pass

Interface: ☐ LAN ☐ WAN ☒ Both

#### IP Filter List

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

- **Source Address/Mask** : Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **Destination Address/Mask** : Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **In/Out** : Applies to Ingress or egress packets
- **Protocol** : Supports **TCP**, **UDP** or **ICMP**.
- **Listen** : Click **Yes** radial button to match TCP packets only with the SYN flag.
- **Active** : **Deny** to drop and **Pass** to allow per filter rules
- **Interface** : The interface that a filter rule applies



All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

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

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

- **Example 1 :** Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

- **Example 2 :** All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	pass	LAN

## 5.4.2 MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.

### MAC Filter Setup

**MAC Rules**

Action: Disabled Save

MAC Address:  Add

**MAC Filter List**

#	MAC Address	Delete
No MAC Rule in the List!		

- **MAC Filter Rule** : By default, it's "**Disable**". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click **Save** button to save your change.

Two ways to set the Access Control List:

➔ **Only Allow List MAC.**

The wireless clients in the ACL List will be **allowed** to access to Access Point; All others will be denied.

➔ **Only Deny List MAC.**

The wireless clients in the ACL List will be **denied** to access to Access Point; All others will be allowed.

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

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

Click **Reboot** button to activate your changes



### 5.4.3 QoS Setup

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.

#### QoS Setup

**Rules**

Comment:

MAC Address:

Local IP:  ~

Destination IP:  ~

DSCP Class:

Protocol:

Local Port:

Destination Port:

**Action**

Remark DSCP:

Bandwidth: ☐ Enable ☒ Disable

Upload:  Kbps

Download:  Kbps

**QoS List**

#	Comment	Remark DSCP	Bandwidth(U/D)	Delete	Edit
No QoS Rule in the List!					

- **Rules** : Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
  - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
  - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click “**Add**” button to add in the MAC group of each rule. Click “**Remove**” button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
  - ➔ **Source / Destination IP** : Specify source/ destination IP addresses range required for this rule. If you specify source IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of source IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
  - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list.

The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.

- ✓ **BE** : *Default* PHB, which is typically best-effort traffic
- ✓ **EF** : *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
- ✓ **AF** : *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

DROP Precedence	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

- ➔ **Protocol** : Select **Any** or specify protocol from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Source/ Destination Port can not used.
- ➔ **Source Port** : Specify source port range required for this rule
- ➔ **Destination Port** : Specify destination port range required for this rule
- **Action** : After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
  - ➔ **Remark DSCP** : Specify a new DSCP class, if you want to replace or remark the DSCP
  - ➔ **Bandwidth** : Click “**Enable**” to activate function, and click “**Disable**” to deactivate function
  - ➔ **Upload / Download** : Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click “**Add**” button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- **Example 1** : On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1	192.168.2.10		ANY	FTP	NO	1024/8196
2			ANY	ANY	NO	512/512

- **Example 2** : On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1			ANY	ANY	NO	512/512
2	192.168.2.10		ANY	FTP	NO	1024/8196

## 5.5 Resource Sharing

### 5.5.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.

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

#### DMZ Setup

The image shows a web-based configuration interface for DMZ Setup. It features a title bar 'DMZ Setup' with a close button. Below the title bar is a form with a label 'DMZ' and two radio buttons: 'Enable' and 'Disable'. The 'Disable' radio button is selected. Below the radio buttons is a text input field labeled 'IP Address:'. To the right of the form is a 'Save' button.

DMZ

DMZ : ☐ Enable ☒ Disable

IP Address:

Save

- **DMZ :** By default, it's "**Disable**". Check **Enable** radial button to enable DMZ.
- **IP Address :** Enter IP address of DMZ host and only one DMZ host is supported.

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

## 5.5.2 Virtual Server (Port Forwarding)

“Virtual Server” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don’t repeat ports’ usage to avoid confusion.

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

### Virtual Server Setup

**Virtual Server**

Virtual Server : ☒ Enable ☐ Disable

Description :

Private IP :

Protocol Type : ☒ TCP ☐ UDP

Private Port :

Public Port :

**Virtual Server List**

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

- **Virtual Server** : By Default, It’s “**Disable**”. Check **Enable** radial button to enable Virtual Server.
- **Description** : Enter appropriate message for resource sharing via Virtual Server.
- **Private IP** : Enter corresponding IP address of internal resource to share.
- **Protocol Type** : Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80
- **Public Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80



*The Private Port and Public Port can be different. However, total number of ports need to be the same.  
Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.*

Click “**Add**” button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP **20~80** will be redirected to port TCP **20~80** of **192.168.2.11**

**DMZ Enabled : 192.168.2.12**

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.10	22	22
2	TCP	192.168.2.11	20:80	20:80

- **Example 2 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port **20~80** will be redirected to port **20~80** of **192.168.2.11**. The rule 2 won't take effect.

**DMZ Enabled : 192.168.2.12**

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.11	20:80	20:80
2	TCP	192.168.2.10	22	22

## 5.6 System Status

This section breaks down into subsections of **System Overview**, **Station Statistics**, **Extra Information** and **Event Log**.

### 5.6.1 Overview

Detailed information on **System**, **WAN Information**, **LAN Information** and **DHCP Server Status** can be reviewed via this page.

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

System	
Host Name :	Air Force One 5
Operating Mode :	CPE 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 00:20:03
System Up Time :	20:03

- ➔ **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.

- **WAN Information** : Display the information of the WAN interface.

WAN Information	
Mode :	Static Mode
MAC Address :	00:0C:43:28:60:34
IP Address :	192.168.1.254
IP Netmask :	255.255.255.0
IP Gateway :	192.168.1.1
Primary DNS :	
Secondary DNS :	
Receive Bytes :	109857
Receive Packets :	1265
Transmit Bytes :	0
Transmit Packets :	542

The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.

WAN Information

Mode : Dynamic Mode

MAC Address : 00:0C:43:28:60:14

The WAN port specified **PPPoE**, and the **Connect** and **DisConnect** button will be show up. Click **“Connect”** button to assigned IP address from PPPoE server, **“DisConnect”** button to release IP address of WAN port.

WAN Information

Mode : PPPoE Mode

Reconnect Mode : Manual

- ➔ **Mode** : Supports Static, Dynamic, and PPPoE modes.
- ➔ **Reconnect Mode** : The current reconnect mode of the PPPoE.
- ➔ **MAC Address** : The MAC address of the WAN port.
- ➔ **IP Address** : The IP address of the WAN port.
- ➔ **IP Netmask** : The IP netmask of the WAN port.
- ➔ **IP Gateway** : The gateway IP address of the WAN port.
- ➔ **Primary DNS** : The primary DNS server in service.
- ➔ **Secondary DNS** : The secondary DNS server in service.
- ➔ **Receive bytes** : The total received packets in bytes on the WAN port.
- ➔ **Receive packets** : The total received packets of the WAN port.
- ➔ **Transmit bytes** : The total transmitted packets in bytes of the WAN port.
- ➔ **Transmit packets** : The total transmitted packets of the WAN port.

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

LAN Information

MAC Address : 00:0C:43:28:60:30

IP Address : 192.168.2.254

IP Netmask : 255.255.255.0

Receive Bytes : 20576

Receive Packets : 174

Transmit Bytes : 37810

Transmit Packets : 177

- ➔ **MAC Address** : The MAC address of the LAN port.
- ➔ **IP Address** : The IP address of the LAN port.
- ➔ **IP Netmask** : The IP netmask 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.

- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.

DHCP Server Status

DHCP : Enable

Start IP : 192.168.2.10

End IP : 192.168.2.70

DNS1 IP : 192.168.2.1

DNS2 IP :

WINS IP :

Domain :

Lease Time : 86400

IP Address	MAC Address	Expired In
	none	

- ➔ **IP Address** : IP addresses to LAN devices by DHCP server.
- ➔ **MAC Address** : MAC addresses of LAN devices.
- ➔ **Expired In** : Shows how long the leased IP address will expire.



## 5.6.2 Station Statistics

Link information, Transmit and Receive Statistics for the connection with AP, Below depicts an example for Station Statistics.

Station Statistics

Refresh

Link Status

Status : Connected  
ESSID : Main\_AP-253  
BSSID : 00:11:A3:0A:7B:F2  
Extra Info : Link is Up  
Channel : 44 (5220000 KHz) ; Central Channel: 46  
Link Speed : Tx(Mbps) 270.0 Rx(Mbps) 243.0  
Link Quality : Good 100%  
Signal Strength ANT0 : Good 100%  
Signal Strength ANT1 : Good 100%

HT Status

Channel BandWidth : 40  
Guard Interval : long  
MCS : 15

Transmit Statistics

Frames Transmitted Successfully 8290  
Frames Transmitted Successfully Without Retry 8271  
Frames Transmitted Successfully After Retry(s) 19  
Frames Fail To Receive ACK After All Retries 1  
RTS Frames Successfully Receive CTS 0  
RTS Frames Fail To Receive CTS 0

Receive Statistics

Frames Received Successfully 5296  
Frames Received With CRC Error 1316  
Frames Dropped Due To Out-of-Resource 0  
Duplicate Frames Received 0

### ■ Link Status :

- ➔ **Status** : Shows the current link status. It should be “**Connected**” or “**Disconnected**”.
- ➔ **ESSID** : Shows the current SSID, which must be the same on the wireless client and AP in order for communication to be established.
- ➔ **BSSID** : Shows the associated BSSID, which can be used to identify the wireless access point.
- ➔ **Extra Info** : Shows the current link status of extra information. It should be “**Link is Up**” or “**Link is Down**”,
- ➔ **Channel** : Shows current channel and central channel, its corresponding frequency.
- ➔ **Link Speed(Mbps)** : The data transfer speed adopted by this network. (measured in Mbits per second)
- ➔ **Link Quality** : Shows the link quality of the system with an access point.
- ➔ **Signal Strength ANT0/ANT1** : Shows the wireless signal strength of the connection between system and an access point.

### ■ HT Status :

- ➔ **Channel BandWidth** : Shows the current channel bandwidth used for communication. It should be “**20**” or “**40**”
- ➔ **Guard Interval** : Shows the current GI used for communication. It should be “**short**” or “**long**”.
- ➔ **MCS** : Shows the current GI used for communication. It should be between **0** to **15** or **32**.

### ■ Transmit Statistics

- ➔ **Frames Transmitted Successfully**: The number of successfully transmitted frames.
- ➔ **Frames Transmitted Successfully Without Retry**: The number of successfully transmitted frames without any retry.
- ➔ **Frames Transmitted Successfully After Retry(s)**: The number of successfully transmitted frames with one or more retries.

- **Frames Fail To Receive ACK After All Retries:** The number of unsuccessfully transmitted frame with many retries.
- **RTS Frames Successfully Receive CTS:** The number of successful received CTS (Clear To Send) response after this AFO-5 sends out the RTS (Request To Send) message.
- **RTS Frames Fail To Receive CTS:** The number of unsuccessful received CTS response after this AFO-5 sends out the RTS message.

#### ■ Receive Statistics

- **Frames Received Successfully:** The number of successful received frames.
- **Frames Received With CRC Error:** The number of received frames with CRC (Cyclical Redundancy Checking) error.
- **Frames Dropped Due To Out-of-Resource:** The number of dropped frames.
- **Duplicate Frames Received:** The number of duplicate frames.

### 5.6.3 Extra Info

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: Netstat Information

Netstat Information

Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	119	TIME_WAIT	192.168.2.22	3423	192.168.2.254	80
tcp	113	TIME_WAIT	192.168.2.22	3419	192.168.2.254	80
udp	5		192.168.2.22	138	192.168.2.255	138
tcp	118	TIME_WAIT	192.168.2.22	3421	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3413	192.168.2.254	80
tcp	431999	ESTABLISHED	192.168.2.22	3425	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3415	192.168.2.254	80
tcp	91	TIME_WAIT	192.168.2.22	3417	192.168.2.254	80

- **Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status*, *Source/Destination IP address* and *Port*.

- **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
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	ra0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	0	ra0

- **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.

Bridge Table Information			
Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000c43288008	no	eth2

- **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
LAN	00:11:a3:0a:7b:f9	yes	0.00
LAN	00:1a:92:9fa4:9b	no	0.08

- **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	1.93	tcn timer	0.00
topology change timer	0.00	gc timer	3.92
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	0.00
flags			

## 5.6.4 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 6. Client Bridge + Universal Repeater Configuration

When Client Bridge + Universal Repeater mode is activated, the system can be configured as an **Access Point** and **Client Station** simultaneously. This section provides information in configuring the Client Bridge + Universal Repeater mode with graphical illustrations. AFO-5 provides functions as stated below where they can be configured via a user-friendly web based interface.

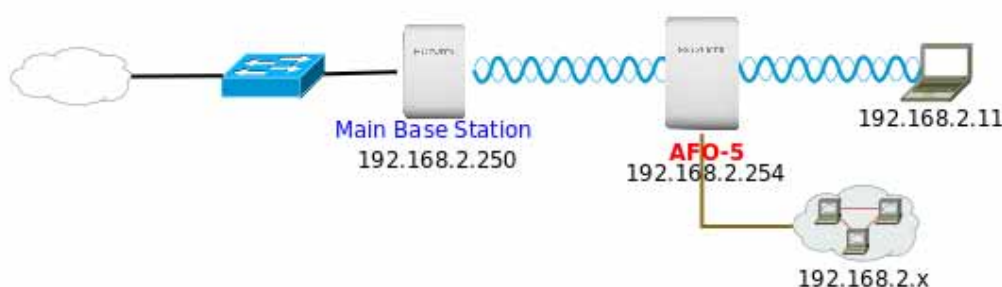
Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Setup	Profiles Settings	System Overview
	LAN	Advanced Setup	Firmware Upgrade	Clients
	Management	AP Setup	Network Utility	Remote AP
	Time Server	Wireless Profile	Reboot	Extra Info
	UPNP	Site Survey		Event Log
	SNMP			

**Table 6-1: Client Bridge + Universal Repeater Mode Functions**

### 6.1 External Network Connection

#### 6.1.1 Network Requirement

It can be used as an Client Bridge or 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.



**Figure 6-1 Client Bridge + Universal Repeater mode Configuration**



When the AFO-5 configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between AFO-5 to Main Base Station and wireless client to AFO-5, but security type can be different.

## 6.1.2 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

**DHCP Server**  
DHCP: ☐ 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. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

DHCP Server

DHCP : ☒ Enable ☐ Disable

Start IP :

End IP :

DNS1 IP :

DNS2 IP :

WINS IP :

Domain :

Lease Time :

- ➔ **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- ➔ **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain** : Enter the domain name for this network.
- ➔ **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

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



## 6.2 Access Point Association

### 6.2.1 Configure Wireless General Setting

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

Wireless Setup

**General Setup**

Band Mode:

Tx Power:  %

**HT Other**

HT TxStream:

HT RxStream:

**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

A-MSDU: ☒ Disable ☐ Enable

Auto Block ACK: ☐ Disable ☒ Enable

Decline BA Request: ☒ Disable ☐ Enable

- **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 **54** Mbps for **802.11a**
- **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 of which setting to choose, then keep the default setting, 10%.

When **Band Mode** select in **802.11a/n mixed mode**, the **HT(High Throughput) Physical Mode and 11n Configuration** settings should be shown-up immediately.

**HT Physical Mode**

Operating Mode: ☒ Mixed Mode ☐ Green Field

Channel BandWidth: ☐ 20 ☒ Auto

Guard Interval: ☐ Long ☒ Auto

MCS:

**11n Configuration**

MPDU Enable: ☐ Enable ☒ Disable

A-MPDU: ☐ Manual ☒ Auto

MPDU Density:

A-MSDU: ☐ Enable ☒ Disable

- **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 "**Auto**" 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**)
- **MPDU Enable** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **A-MPDU** : A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select "Manual" to set "MPDU Density"
- **MPDU Density** : Minimum separation of MPDUs in an A-MPDU.

0	1	2	3	4	5	6	7
No Restriction	$\frac{1}{4} \mu s$	$\frac{1}{2} \mu s$	$1 \mu s$	$2 \mu s$	$4 \mu s$	$8 \mu s$	$16 \mu s$

- **A-MSDU : Aggregated** Mac Service Data Unit, A-MSDU. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU. Default is disabled.

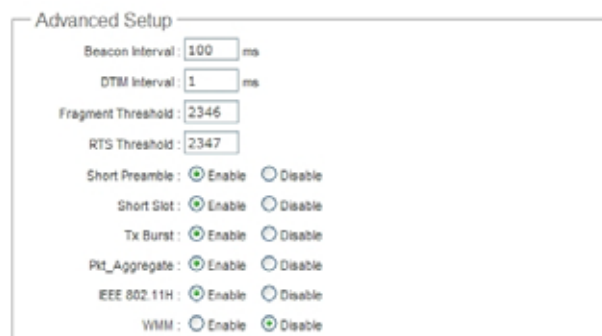
Click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **Repeater AP**

## 6.2.2 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.

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 **Repeater AP**.

### 6.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.

#### Station Site Survey

Scan Result							
ESSID	MAC Address	Signal	Channel	Security	Band	Network Type	Select
Main_AP	00:11:a3:0a:7c:3a	50%	44	NONE	11a/n	Infrastructure	<a href="#">Select</a>
Main_AP-253	00:11:a3:0a:7b:f2	100%	44	NONE	11a/n	Infrastructure	<a href="#">Select</a>
253AP1	00:11:a3:0a:7b:f3	100%	44	WEP	11a/n	Infrastructure	<a href="#">Select</a>
253AP2	00:11:a3:0a:7b:f4	100%	44	WPAPSK/AES	11a/n	Infrastructure	<a href="#">Select</a>
253AP3	00:11:a3:0a:7b:f5	100%	44	WPAPSK/TKIP	11a/n	Infrastructure	<a href="#">Select</a>
253AP4	00:11:a3:0a:7b:f6	100%	44	WPA2PSK/AES	11a/n	Infrastructure	<a href="#">Select</a>
253AP5	00:11:a3:0a:7b:f7	100%	44	WPA2PSK/TKIP	11a/n	Infrastructure	<a href="#">Select</a>

- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Signal :** Received signal strength of all found Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Security :** Security type by all found Access Points.
- **Band :** Wireless band used by all found Access Points.
- **Network Type :** Network type used by all found Access Points.
- **Select :** Click “**Select**” to configure settings and associate with chosen AP.



While clicking “Select” button in the Site Survey Table, the “**ESSID**” and “**Security Type**” will apply in the Wireless General Setup. However, more settings are needed including Security Key.



## 6.2.4 Create Wireless Profile

The administrator can configure station profiles via this page.

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

### Station Profile

- **MAC Address** : The MAC address of the Wireless Station Interface is displayed here.
- **Profile Name** : Set different profiles for quick connection uses.
- **ESSID** : Assign Service Set ID for the wireless system.
- **Lock to AP MAC** : This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.
- **Security Type** : Select the desired security type from the drop-down list; the options are **"NONE"**, **"OPEN"**, **"SHARED"**, **"WPA-PSK"** and **"WPA2-PSK"**.
  - ➔ **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.

- ✓ **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.

WPA

Cipher Suite : AES ▼

Pre-shared Key :

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.

- **Profile List** : The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List

Profile List

Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
<input type="radio"/>	1	AP_Profile0	default		44	NONE	<a href="#">Delete</a>	<a href="#">Edit</a>
<input checked="" type="radio"/>	2	Profile-Test	253AP1	00:11:a3:0a:7b:f3	44	OPEN	<a href="#">Delete</a>	<a href="#">Edit</a>

[Connect](#)

- ➔ Click **“Edit”** an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click **“Save”** button to save the profile.
- ➔ Click **“Delete”** to remove profile.
- ➔ Click and Select a profile from list, then click the **“Connect”** button to connecting to the wireless network with the profile setting.



*If you only click “Connect” button and does not click “Save” button. The selected profile would not be saved on the Profile List after rebooting.*

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

## 6.3 Wireless LAN Network Creation

The network manager can configure related wireless settings, **Repeater AP Setup**, **Security Settings**, and **Access Control Settings**.

### 6.3.1 Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and ACL settings.

- **MAC Address** : The MAC address of the Repeater AP Interface is displayed here.
- **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 AP.
- **Client Isolation** : By default, it's "**Disable**".  
Select "**Enable**", all clients will be isolated from each other, which means they can't reach each other.
- **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's 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 Repeater AP.
- **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.

WEP

Authentication Type : ☒ OPEN ☐ SHARED ☐ WEPAUTO

Key Index : 1

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- ✓ **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.

WPA General

Cipher Suite : AES

Pre-shared Key :

Group Key Update Period : 3600 seconds

- ✓ **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.

**WPA General**

Cipher Suite : AES

Group Key Update Period : 3600 seconds

PMK Cache Period : 10 minute

Pre-Authentication : ☒ Disable ☐ Enable

**Authentication RADIUS Server**

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 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.

### 6.3.2 MAC Filter Setup

Continue **6.3.1 Repeater AP Setup** section, the administrator can allow or reject clients to access Repeater 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 or WPA2 security method is highly recommended.*

## 6.4 System Management

### 6.4.1 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. Further down 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 checkbox and 'Port: 80'; 'Enable HTTPS' with a checked checkbox, 'Port: 443', and an 'UploadKey' button; 'Enable Telnet' with a checked checkbox and 'Port: 23'; and 'Enable SSH' with a checked checkbox, 'Port: 22', and a 'GenerateKey' button. Below the SSH section is a text box containing an SSH key: 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgOXYI'. At the bottom center is a 'Save' button.

#### ■ 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.*

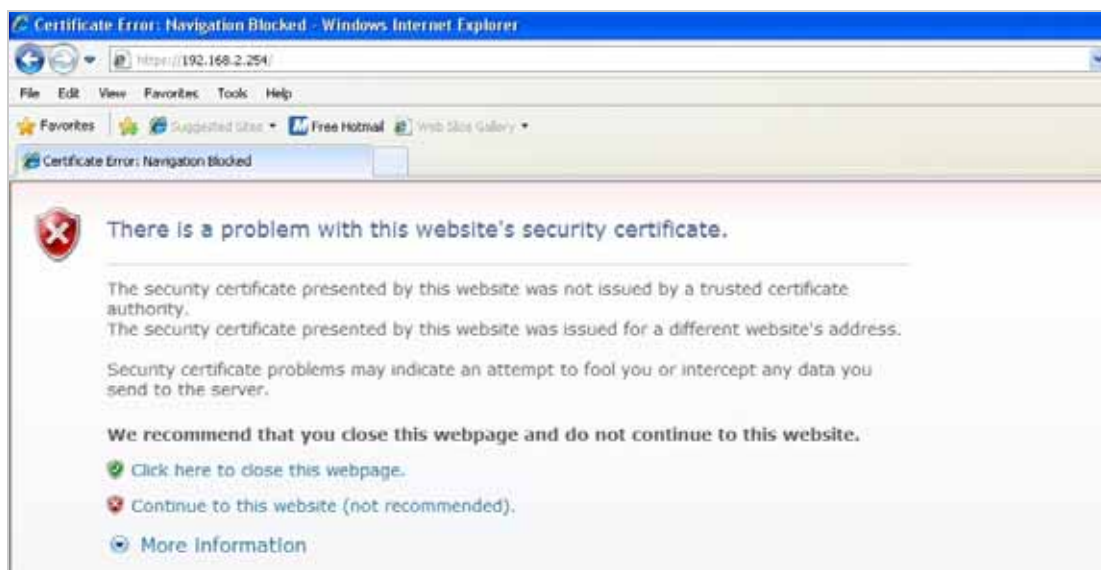
- **Enable Telnet** : Check to select Telnet Service
- **Telnet Port** : The default is **23** and the range is between 1 ~ 65535.
- **Enable SSH** : Check to select SSH Service
- **SSH Port** : Please The default is **22** and the range is between 1 ~ 65535.



*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://192.168.10.100>). There will be a "Certificate Error", because the browser treats system as an illegal website.



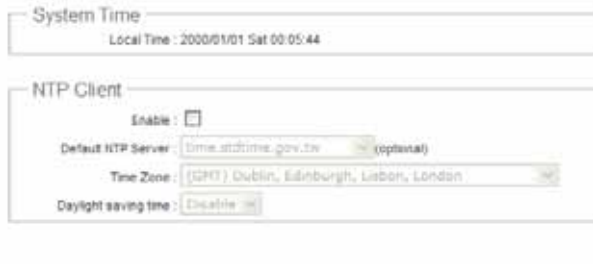
Click "**Continue to this website**" to access the system's WMI. The system's Overview page will appear.

## 6.4.2 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

### 6.4.3 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**

## 6.4.4 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 detailed configuration for **SNMP v2c**. 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 detailed configuration for **SNMP v3**. 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.


## 6.4.5 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.

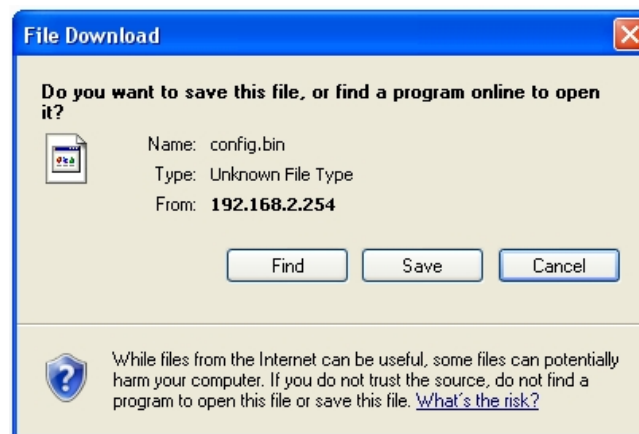
Please click on **Utilities -> Profile Setting** and follow the below setting.

### 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.

## 6.4.6 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.

## 6.4.7 Network Utility

The administrator can diagnose network connectivity via the PING utility.

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

Network Utility

The screenshot shows the 'Network Utility' interface. 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 'Result' area with a vertical scrollbar, currently empty.

- **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.



### 6.4.8 Reboot

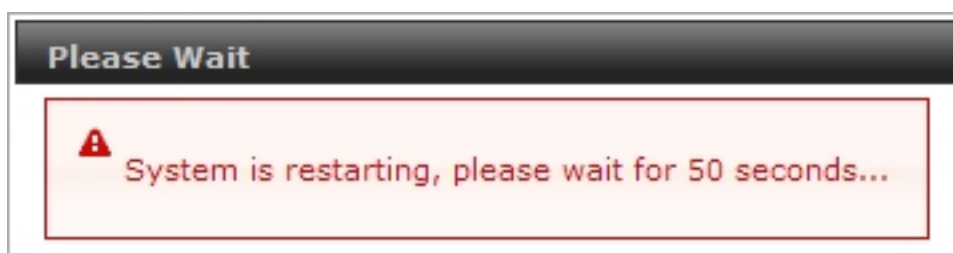
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

#### Reboot

 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.

## 6.5 System Status

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

### 6.5.1 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 :	Client Bridge + Universal Repeater 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 00:01:05
System Up Time :	01:05

- ➔ **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.

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 :	

- ➔ **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 the detailed receive and transmit statistics of 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 the detailed receive and transmit statistics of Wireless interface.

Wireless Information	
AP MAC Address :	00:11:A3:0A:7B:FA
Station MAC Address :	00:11:A3:0A:7B:FB
Channel :	44
AP Rate :	300 Mb/s
Station Rate :	300 Mb/s
Receive Bytes :	113126
Receive Packets :	526
Transmit Bytes :	2708
Transmit Packets :	88

- ➔ **MAC Address** : The MAC address of the Wireless port.
- ➔ **Channel** : The current channel on the Wireless port.
- ➔ **AP Rate** : The current Bit Rate on the Repeater AP.
- ➔ **Station Rate** : The current Bit Rate on the Wireless Client Station.
- ➔ **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.

- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.

DHCP Server Status		
DHCP : Enable		
Start IP : 192.168.2.10		
End IP : 192.168.2.70		
DNS1 IP : 192.168.2.1		
DNS2 IP :		
WINS IP :		
Domain :		
Lease Time : 86400		
IP Address	MAC Address	Expired In
	none	

- ➔ **IP Address** : IP addresses to LAN devices by DHCP server.
- ➔ **MAC Address** : MAC addresses of LAN devices.
- ➔ **Expired In** : Shows how long the leased IP address will expire.

## 6.5.2 Associated Clients Status

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

### Wireless Clients

[Refresh](#)

AP Information					
AP	ESSID	MAC Address	State	Security Type	Clients
Repeater AP	Main_AP_Repeater	00:11:A3:0A:7B:FA	On	Disable	1

Repeater AP Clients						
MAC Address	Signal Strength ANT0	Signal Strength ANT1	Band/Width	Idle Time	Connect Time	Disconnect
00:06:B1:13:35:EF	100%(-32dBm)	100%(-40dBm)	20MHz	8	67	<a href="#">Delete</a>

- **AP Information** : Highlights key Repeater AP information.
  - ➔ **AP** : Available Repeater AP.
  - ➔ **ESSID** : Display name of ESSID for Repeater AP.
  - ➔ **MAC Address** : Display MAC address for Repeater AP.
  - ➔ **Status** : On/Off
  - ➔ **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients** : Display total number of wireless connections on Repeater AP.
  
- **Repeater AP Clients** : Display all associated clients.
  - ➔ **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 Repeater AP.

### 6.5.3 Remote AP

SSID, MAC address, antenna 0/1 received signal strength and channel bandwidth for associated AP are available.

#### Remote AP

Connection Information				
ESSID	MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth
Main_AP-253	00:11:A3:0A:7B:F2	100%(-39dBm)	100%(-42dBm)	40MHz

- **ESSID** : Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.
- **MAC Address** : Display MAC address of associated AP.
- **Signal Strength ANT0/ANT1** : Shows the wireless signal strength of the connection between system and an access point.
- **BandWidth** : Shows the current channel bandwidth used for communication. It should be "20" or "40"



If display "**No Connection AP!**", you need check Wireless configuration. Things to verify are **Channel** and **Security type**. Also, adjust antenna angle and Tx Power.

## 6.5.4 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: Netstat Information

Netstat Information

Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	119	TIME_WAIT	192.168.2.22	3423	192.168.2.254	80
tcp	113	TIME_WAIT	192.168.2.22	3419	192.168.2.254	80
udp	5		192.168.2.22	138	192.168.2.255	138
tcp	118	TIME_WAIT	192.168.2.22	3421	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3413	192.168.2.254	80
tcp	431999	ESTABLISHED	192.168.2.22	3425	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3415	192.168.2.254	80
tcp	91	TIME_WAIT	192.168.2.22	3417	192.168.2.254	80

- **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 apcli0).

Bridge Table Information			
Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000c43286010	no	eth2 ra0 apcli0

- **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
Repeater-AP	00:06:b1:13:35:ef	no	0.09
WLAN-Client	00:11:a3:0a:7b:f1	no	2.80
LAN	00:11:a3:0a:7b:f9	yes	0.00
Repeater-AP	00:11:a3:0a:7b:fa	yes	0.00
WLAN-Client	00:11:a3:0a:7b:fb	yes	0.00
LAN	00:1a:92:9f:a4:9b	no	0.10
WLAN-Client	00:40:d0:3e:7b:fd	no	65.92

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

Bridge STP Information			
bre0			
bridge id	8000.000c43286010		
designated root	8000.000c43286010		
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	1.36	tcn timer	0.00
topology change timer	0.00	gc timer	3.36
flags			
eth2 (1)			
port id	8001	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			
ra0 (2)			
port id	8002	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			
apcli0 (3)			
port id	8003	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			



## 6.5.5 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

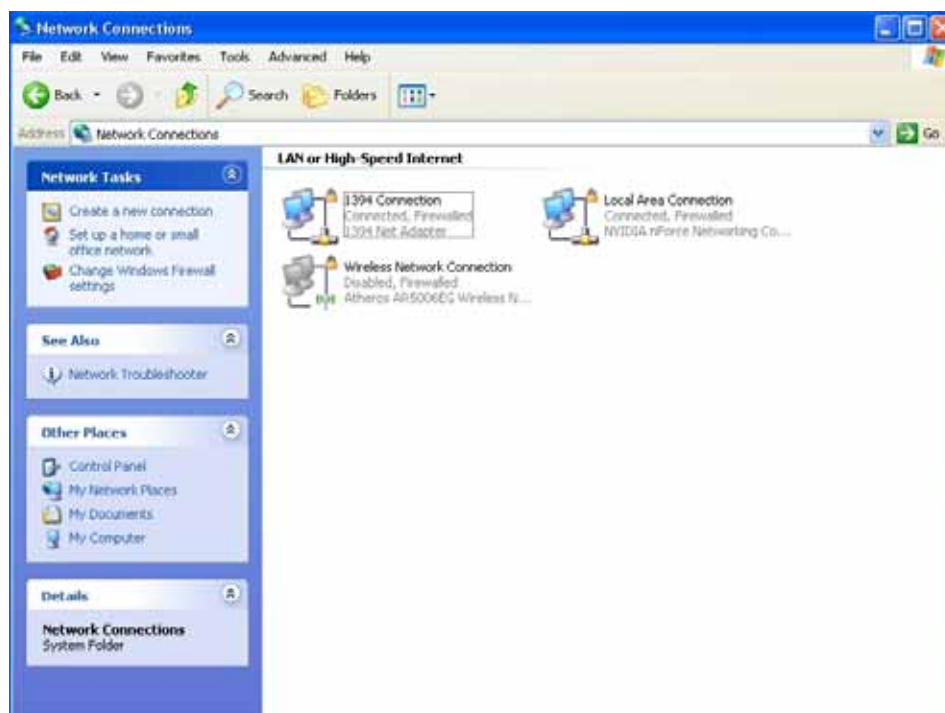
- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

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

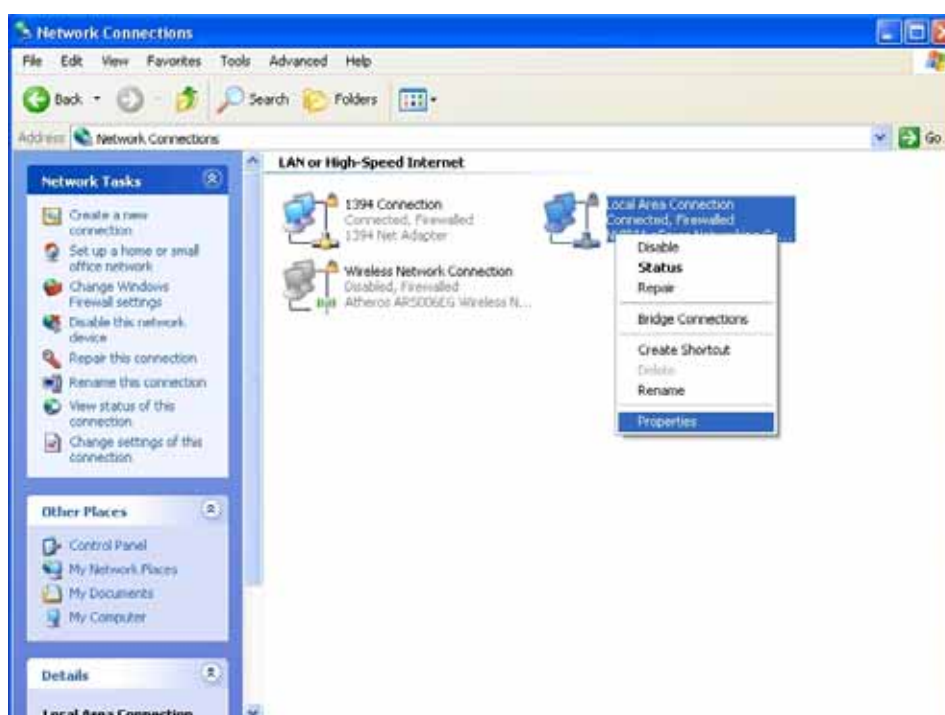
## Appendix A. Windows TCP/IP Settings

### ■ Windows XP

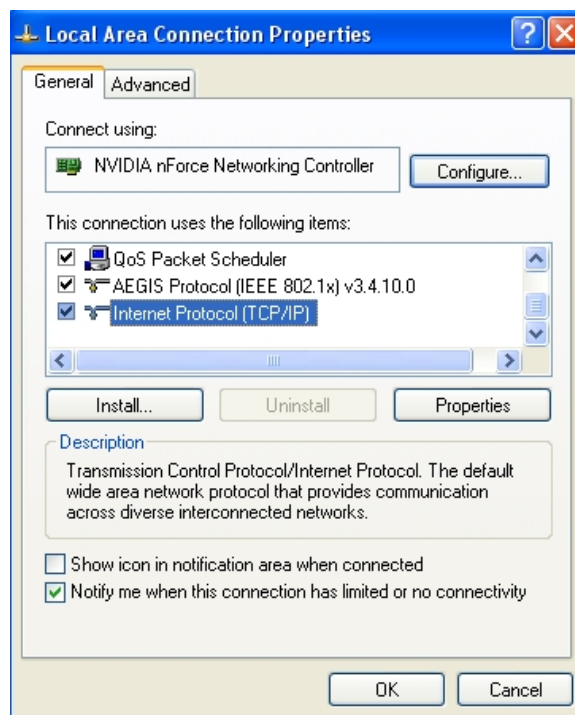
1. Click **Start -> Settings -> Control Panel**, and then “**Control Panel**” window appears. Click on “**Network Connections**”, and then “**Network Connections**” window appears.



2. Click right on “**Local Area Connection**”, and select **Properties**.



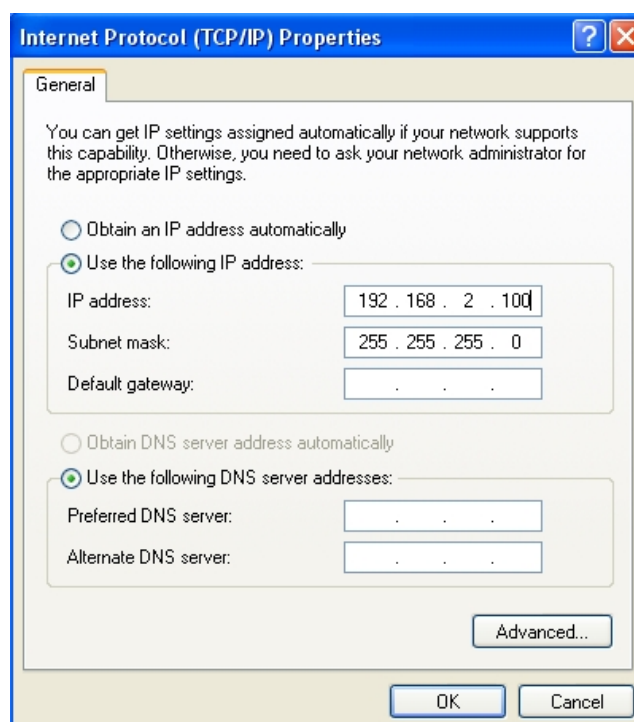
3. In “**Local Area Connection Properties**” window, select “**Internet Protocol (TCP/IP)**” and click on **Properties** button.



4. Select “Use the following IP address”, and type in

**IP address : 192.168.2.100**

**Subnet mask : 255.255.255.0**



## Appendix B. WEB GUI Valid Characters

**Table B WEB GUI Valid Characters**

Block	Field	Valid Characters
<b>LAN</b>	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary	IP Format; 1-254
	Secondary	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
<b>WAN</b>	Manual MAC Address	12 HEX chars
	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User name	Length : 32 0-9, A-Z, a-z
	Password	~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	MTU	576 ~ 1492
	Idle Time	0 ~ 60 minutes
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
<b>DDNS</b>	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User Name	Length : 32 0-9, A-Z, a-z
	Password	~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
<b>DHCP Server</b>	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP	IP Format; 1-254
	DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254
	Domain	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =

**Table B WEB GUI Valid Characters (continued)**

Block	Field	Valid Characters
<b>Management</b>	System Name	Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Description	Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	HTTP Port	1 ~ 65535
	Telnet Port	1 ~ 65535
<b>SNMP</b>	RO community	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	RO user	Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	RO password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] ; ` , . =
	IP	IP Format; 1-254

**Table B WEB GUI Valid Characters (continued)**

Block	Field	Valid Characters
<b>General Setup</b>	Tx Power	1-100 %
<b>Wireless Profile (CPE Mode)</b>	Profile Name	Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	ESSID	Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
<b>Advanced Setup</b>	Beacon Interval	20 ~ 1024
	Date Beacon Rate	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347
<b>Virtual AP Setup</b>	ESSID	Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	VLAN ID	1 ~ 4094
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Group Key Update Period	>=60 seconds
	PMK Cache Period	> 0 minute
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	8 ~ 64 characters
	Session Timeout	>= 60 seconds; 0 is disable

**Table B WEB GUI Valid Characters (continued)**

Block	Field	Valid Characters
<b>WDS Setup</b>	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	TKIP Key	8 ~ 63 ASCII chars; 64 HEX chars
	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
<b>IP Filter</b>	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
<b>MAC Filter</b>	MAC address	MAC Format; 12 HEX chars
<b>Virtual Server</b>	Description	Length : 32 0-9, A-Z, a-z space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	Private IP	IP Formate; 1-254
	Private Port	1 ~ 65535
	Public Port	1 ~ 65535
<b>DMZ</b>	IP Address	IP Format; 1-254
<b>QoS</b>	Comment	Length : 32 0-9, A-Z, a-z space ~ ! @ # \$ % ^ * ( ) _ + - { }   : < > ? [ ] / ; ` , . =
	MAC Address	MAC Format; 12 HEX chars
	Source IP	IP Formate; 1-254
	Destination IP	IP Formate; 1-254
	Source Port	1 ~ 65535
	Destination Port	1 ~ 65535
	Upload & Download	8 ~ 8192 digital number

## Appendix C. MCS Data Rate

The table below shows the relationships between the variables that allow for the maximum data rate

**Table C MCS Data Rate**

MCS Index	Modulation	Data Rate (Mb/s)			
		Channel Bandwidth = 20		Channel Bandwidth = 40	
		Long Guard Interval	Short Guard Interval	Long Guard Interval	Short Guard Interval
0	BPSK	6.5	7.2	13.5	15.0
1	QPSK	13.0	14.4	27.0	30.0
2	QPSK	19.5	21.7	40.5	45.0
3	16-QAM	26.0	28.9	54.0	60.0
4	16-QAM	39.0	43.3	81.0	90.0
5	64-QAM	52.0	57.8	108.0	120.0
6	64-QAM	58.5	65.0	121.5	135.0
7	64-QAM	65.0	72.2	135.0	157.5
8	BPSK	13.0	14.4	27.0	30.0
9	QPSK	26.0	28.9	54.0	60.0
10	QPSK	39.0	43.3	81.0	90.0
11	16-QAM	52.0	57.8	108.0	120.0
12	16-QAM	78.0	86.7	162.0	180.0
13	64-QAM	104.0	115.6	216.0	240.0
14	64-QAM	117.0	130.0	243.0	270.0
15	64-QAM	130.0	114.4	270.0	300.0

**Note :**

- ✓ When MCS=32, only Short Guard Interval option is supported, Channel Bandwidth=20 is not supported. If Channel Bandwidth=40, the HT duplicate 6Mbps.
- ✓ When MCS=0~7(One Tx Stream), Guard Interval and Channel Bandwidth are supported
- ✓ When MCS=8~15(Two Tx Stream), Guard Interval and Channel Bandwidth are supported



## Appendix D. System Manager Privileges

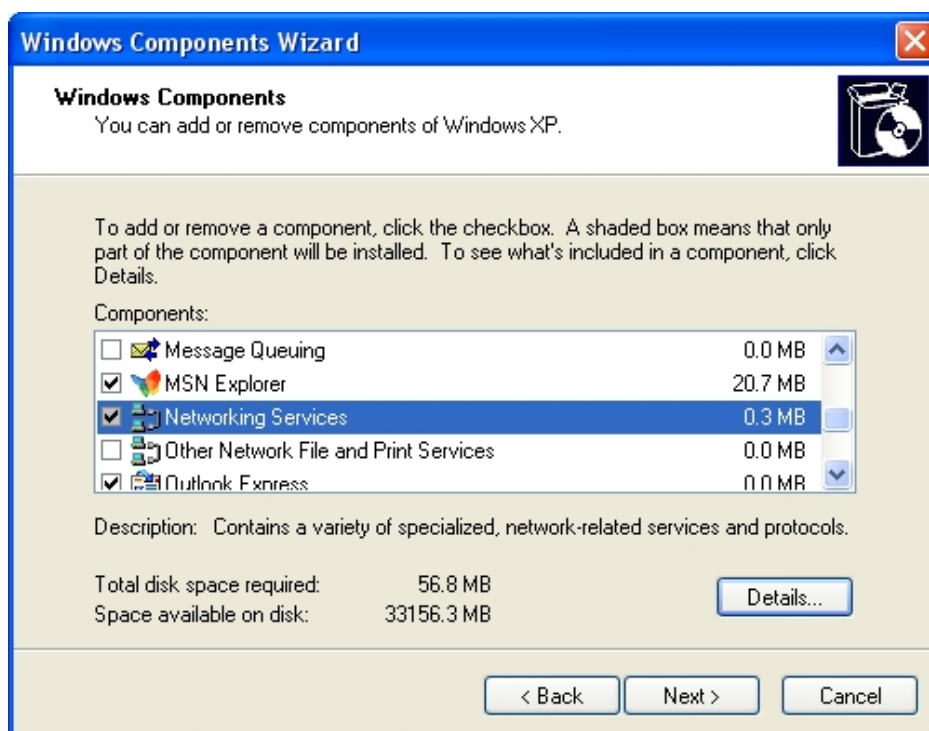
There are two system management accounts for maintaining the system; namely, the **root** and **admin** accounts are with different levels of privileges. The root manager account is empowered with full privilege to Read & Write while the admin manager account is Read only.

The following table display CPE admin account's privileges.

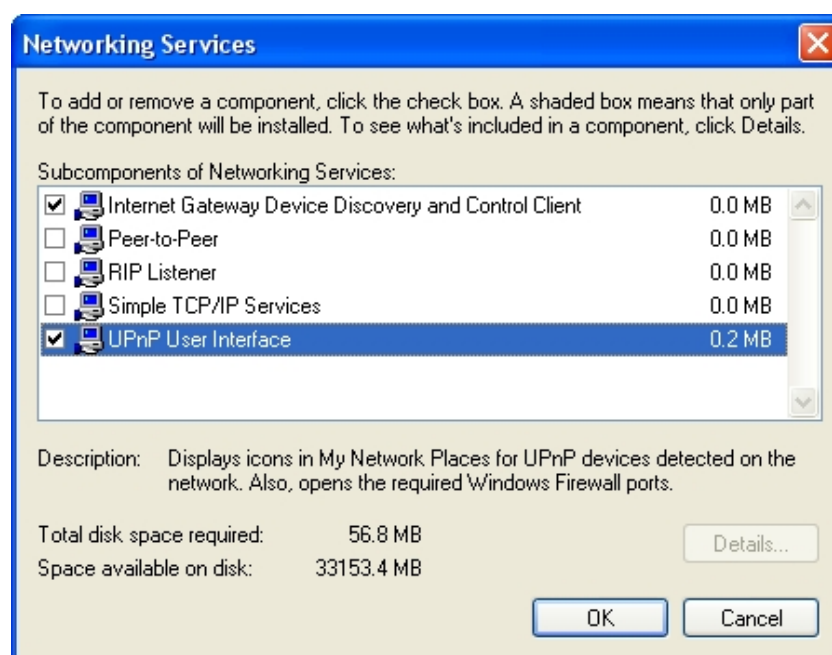
Main Menu	Sub Menu	Group	Admin Privilege
<b>System</b>	Operating Mode		Read
	WAN		Read
	LAN		Read & Write
	DDNS Setup		Read & Write
	Time		Read & Write
	SNMP Setup		Read
	UPNP		Read & Write
<b>Wireless</b>	General		Read
	Advanced		Read
	Site Survey		Read
<b>Advance</b>	DMZ		Read
	IP Filter		Read
	MAC Filter		Read
	Virtual Server		Read
	QoS		Read
<b>Administrator</b>	Management	System Information	Read
		Root Password	Read
		Admin Password	Read & Write
		Login Methods	Read
	Profile Settings	Backup Settings	Read & Write
		Restore Settings	Read
		Reset to Default	Read
	System Upgrade		Read
	Network Utility		Read & Write
	Reboot		Read & Write

## Appendix E. Enabling UPnP in Windows XP

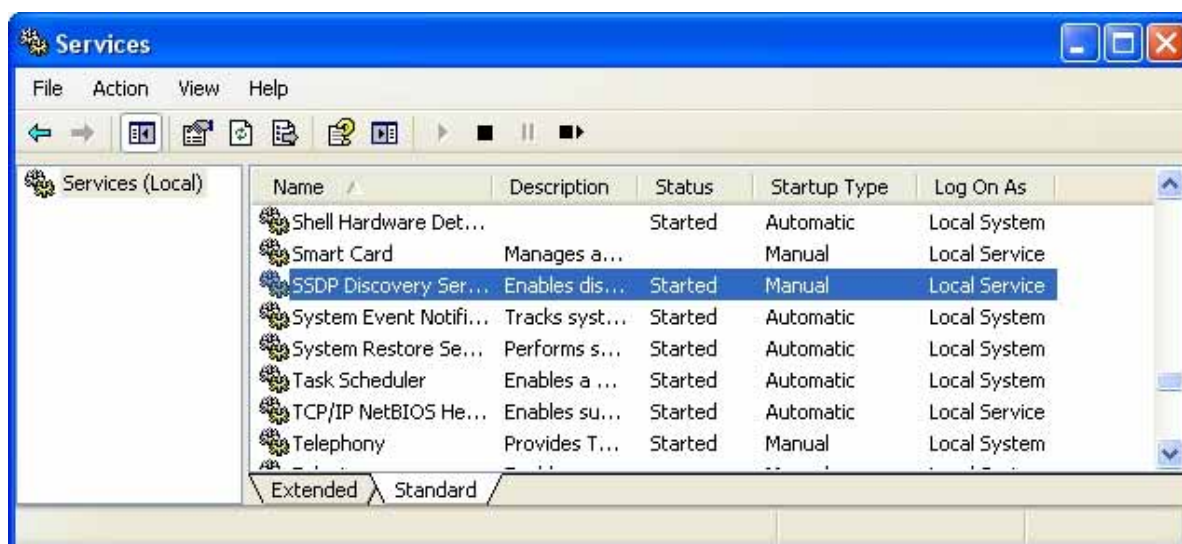
1. Open the **"Add/Remove Programs"** control panel, and then click on **"Add/Remove Windows Components"** in the sidebar. Scroll down and find **"Networking Services"**, highlight it, and then click **Details**.



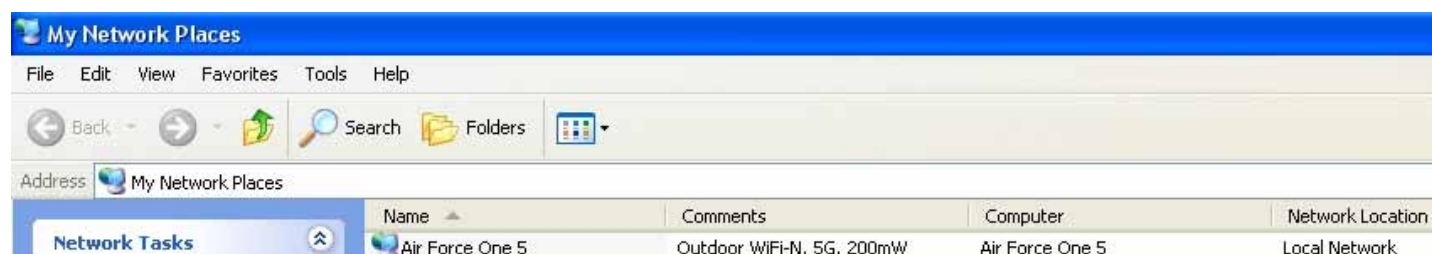
2. In the **"Networking Services"** window, ensure that the **"Internet Gateway Device"** and **"UPnP User Interface"** options are checked. If they are not, check it to enable them, as shown below, and click OK to continue.



- Next, in the **“Control panel”**, open the **“Administrative Tools”** and then open **“Services”**. Scroll down until you find the **“SSDP Discovery Interface”**. If the Status is not **Started**, double-click on *SSDP Discovery Interface* to open the service properties. Change the startup type to **Automatic**, then close the properties. Now, right-click on *SSDP Discovery Services*, and choose **Start** from the pop-up menu. The SSDP Discovery Service will then be running and start each time you boot.



- After enabling UPnP and starting the SSDP Discovery Service, it may take few minutes for the “Air Force One 5” to be discovered and appear in your **“My Network Places”**.



This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

---Reorient or relocate the receiving antenna.

---Increase the separation between the equipment and receiver.

---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

---Consult the dealer or an experienced radio/TV technician for help.

This device is restricted to INDOOR USE due to its operation in the 5.15 to 5.25GHz frequency range. According to FCC 15.407(e), requires this product to be used indoors for the frequency range 5.15 to 5.25GHz to reduce the potential for harmful interference to co-channel of the Mobile Satellite Systems.

High power radars are allocated as primary user of the 5.25 to 5.35GHz and 5.65 to 5.85GHz bands. These radar stations can cause interference with and / or damage this device

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions

- (1) This device may not cause harmful interference and
- (2) This device must accept any interference received, including interference that may cause undesired operation

FCC RF radiation exposure statement:

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

2.this equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body .

FCC NOTICE: To comply with FCC part 15 rules in the United States,

the system must be professionally installed to ensure compliance with the Part 15 certification.

It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States.

The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.