IEEE 802.11b/g/n Wireless CPE/ IEEE 802.11a/n Wireless CPE User's Manual

Model name: ZAC-1023-2-9 / ZAC-1023-5-13

ZAC-501 / ZAC-502

ZWA-3070 / ZWA-3080

ZN-7200-2EI / ZN-7200-2AEI-L

V1.0

May 2014

Copyright

About This Manual

This user manual is intended to guide professional installer to install the IEEE 802.11n ZAC Access Point series and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

✎ **Note:**

- This indicates an important note that you must pay attention to.

⚠ **Warning:**

- This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
- Verify that the ambient temperature remains between 0 to 40° C, taking into account the elevated temperatures when installed in a rack or enclosed space.
- Verify the integrity of the electrical ground before installing the device.

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

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

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

根據低功率電波輻射性電機管理辦法

(1) 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

(2) 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Warranty

Hardware warranty is for one (1) year from date of shipment from Distributor warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

IN NO EVENT SHALL DISTRIBUTOR BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE RISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者

Content

Chapter 1 Introduction

Introduction

The ZAC Series Access Point is a multi-mode 2x2 Access Point embedded with a software-based virtual access controller (VAC) for centrally managing managed APs that eliminates the need for a separate hardware controller to manage the WLAN. ZN-7200-2EI operates at 2.4GHz band while ZN-7200-2AEI-L operates at 5GHz band. Ideally for SMB or hotspot network, this breakthrough innovation provides superior Wi-Fi network solutions at significantly lower cost and easier management.

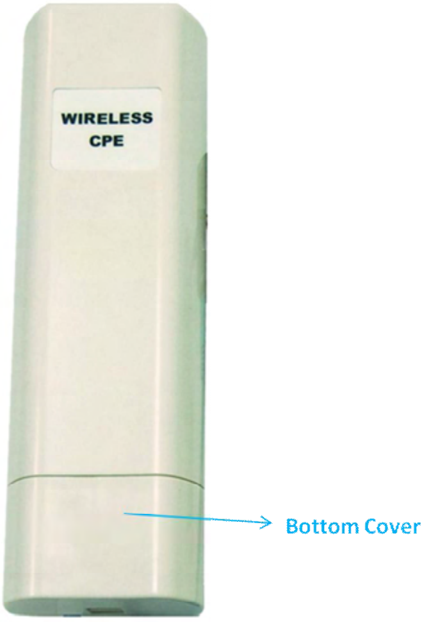
While operating as access point, the ZAC Access Point also provides centralized management and monitoring of all the managed APs on the network. In addition, the easy-to-install ZAC Access Point is also a high-performance last-mile broadband solution that provides reliable wireless network coverage for broadband application.

Key Features

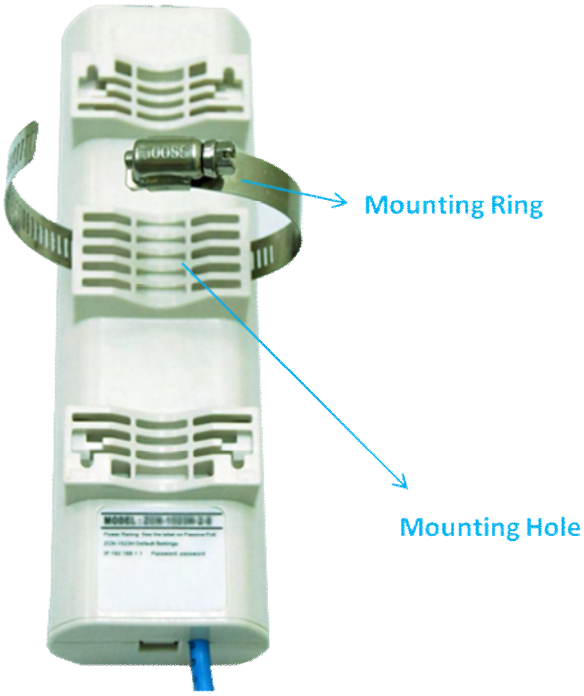
- Centralized configuration control for your network
- Compliant with IEEE 802.11n standard
- Support passive PoE supplied with 24V.
- High reliable watertight housing endures almost any harsh environments
- Three management modes including AC, AC+Thin AP, Thin AP and Fat AP.
- Four wireless operation modes in FAT AP mode including AP, Wireless Client, WDS and AP Repeater.
- Up to 8 BSSIDs available for service deployment
- Support encryption: 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK
- User-friendly Web and SNMP-based management interface

Hardware Overview

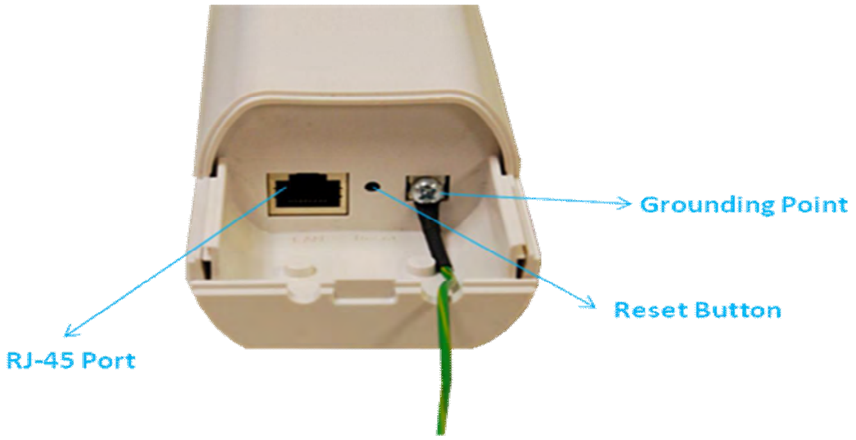
Front View



Back View



Inside the Bottom Cover

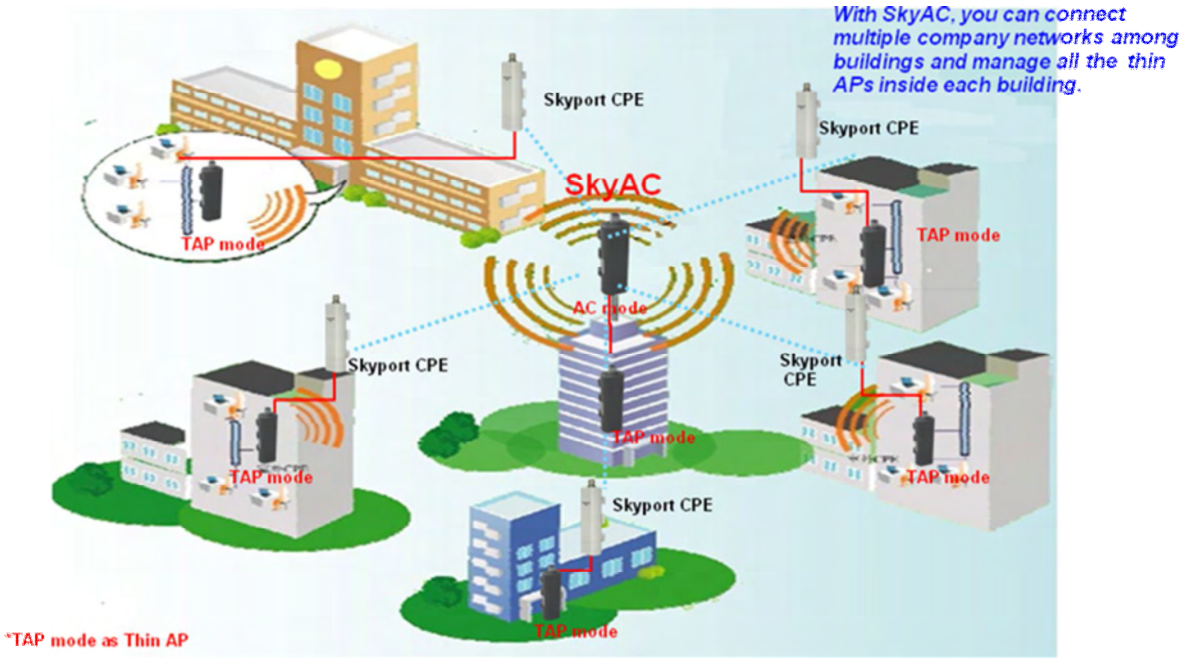


LED Indicators

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The device is powered on
		Off	The device is not receiving power
LAN	Green	On	The device has the Ethernet connection
		Off	The device has no Ethernet connection
		Blinking	Transmitting/receiving Ethernet packets
WLAN	Green	On	The WLAN is active
		Off	The WLAN is inactive
		Blinking	Transmitting/receiving wireless packets
Signal*3	Green	3 LED On	The signal strength is excellent
		2 LED On	The signal strength is good
		1 LED On	The signal strength is weak

Typical Management Scenario

This section describes the typical management of ZAC Access Point. By default, it is set to thin AP mode (managed AP) which allows it to be managed by the ZAC Access Point in AC mode. The following figure illustrates a ZAC wireless network.



When a thin AP mode joins a wired network, it will start to look for a ZAC Access Point in AC mode. If the thin AP founds the AP controller on the network, it will send the registration request to the AP controller. Once the registration is successfully made, the AP that acts as the AP controller will add the thin AP to its management list and provides it configuration information.

Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing the ZAC Access Point.

Preparation before Installation

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing the ZAC Access Point for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing the ZAC Access Point, please note the following things:
    - Do not use a metal ladder;
    - Do not work on a wet or windy day;
    - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

Installation Precautions

To keep the ZAC Access Point well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed grounding and surge arrestor with the ZAC Access Point; otherwise, a random lightening could easily cause fatal damage to ZAC Access Point. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.**
2. Users MUST use the “Power cord & PoE Injector” shipped in the box with the ZAC Access Point. Use of other options will likely cause damage to the unit.

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

● IEEE 802.11n ZAC Access Point	×1
● Pole Mounting Ring	×1
● 24VDC Power cord & PoE Injector	×1
● Ferrite Suppression Core	× 1
● Grounding Wire	×1
● Product CD	× 1

Note:

- Product CD contains Quick Installation Guide and User Manual.

Pole Mounting Ring

Ferrite Suppression Core

24VDC Power Cord & PoE Injector

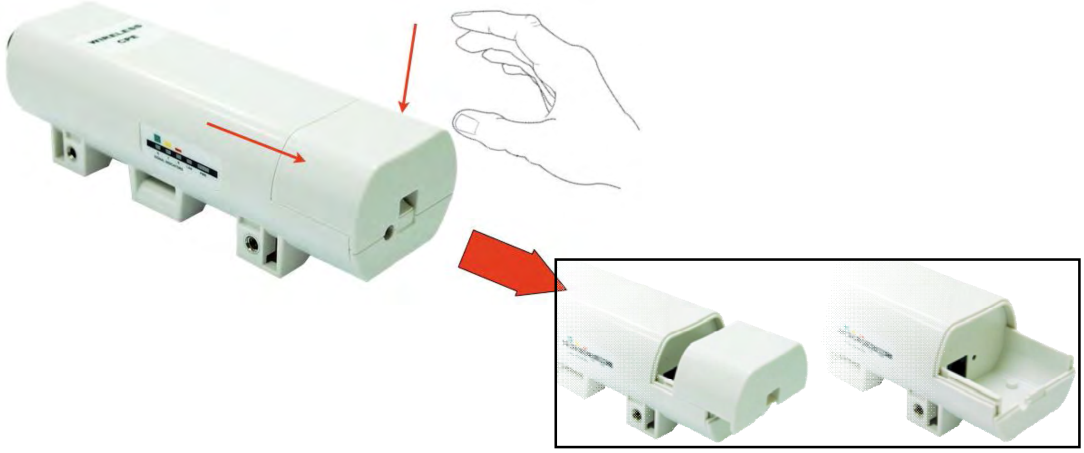
⚠ **Warning:**

- Users MUST use the “Power cord & PoE Injector” shipped in the box with the IEEE 802.11n Wireless Access Point. Use of other options will likely cause damage to the IEEE 802.11n Wireless Access Point..

Hardware Installation

Connect up

1. The bottom of the ZAC Access Point is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.



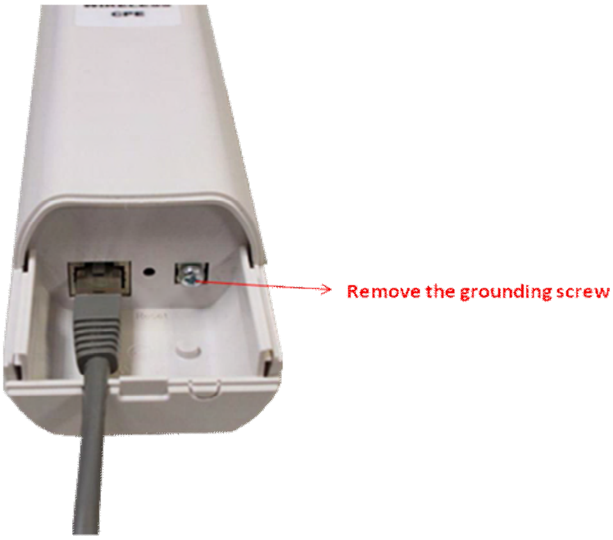
2. Plug a standard Ethernet cable into the RJ45 port.

3. Slide the cover back and press down the lock button to seal the bottom of the ZAC Access Point.

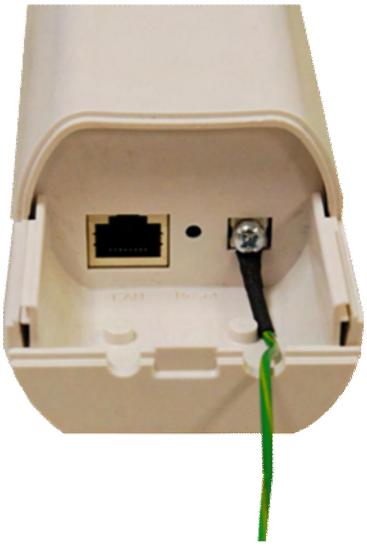
Using the Grounding Wire

The ZAC Access Point is equipped with a grounding wire. It is important that the Access Point, cables, and PoE Injector must be properly connected to earth ground during normal use against surges or ESD.

1. Remove the screw on the grounding point at the bottom of the ZAC Access Point.



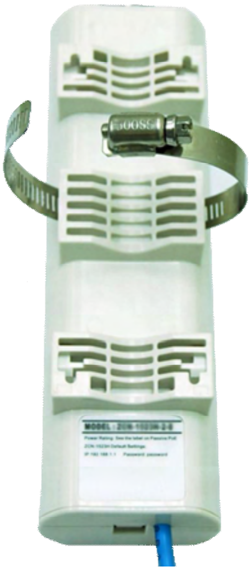
2. Put the grounding wire on the grounding point at the bottom of the ZAC Access Point. Then screw the grounding wire to tighten up.

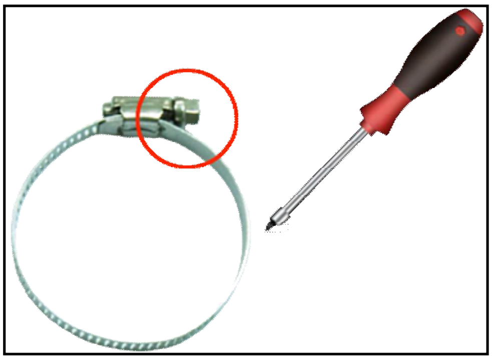


3. Connect the grounding wire to earth ground.

Mount the AP on a Pole

1. Turn the ZAC Access Point over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through the device as the following right picture shows.





2. Mount the ZAC Access Point steadily to the pole by locking the pole mounting ring tightly.

Power Up

1. Connect power cord to the PoE injector as the following right picture shows.

2. Connect the Ethernet cable that connects the Access Point to the “POE” port of the PoE injector as figured below.

3. Connect the power plug to a power socket. The Access Point will be powered up immediately.

Connect to the Access Point

To be able to configure and manage the Access Point, please do the followings:

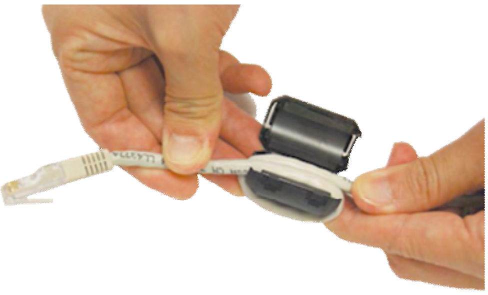
Connect to the Access Point

To be able to configure and manage the Access Point, please do the followings:

1. Open the ferrite core by unsnapping the connector latches. The core will open, revealing a concave surface.

2. Lay the Ethernet cable into the core, usually within 2 to 3 inches of the connector. You may have to experiment with the final location depending on the effectiveness of the high frequency abatement.

3. Loop the cable around and through the core. This helps "lock" the core in place, and may be required in circumstances with severe interference.

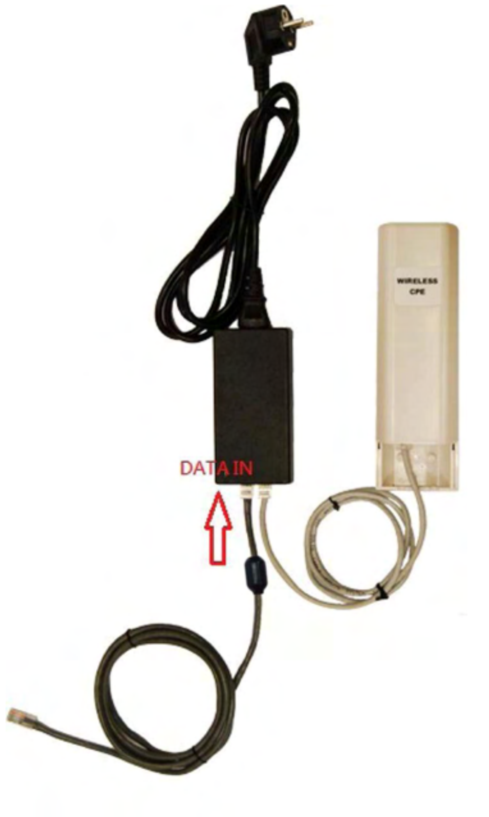


4. Close the core and snap the halves back together.

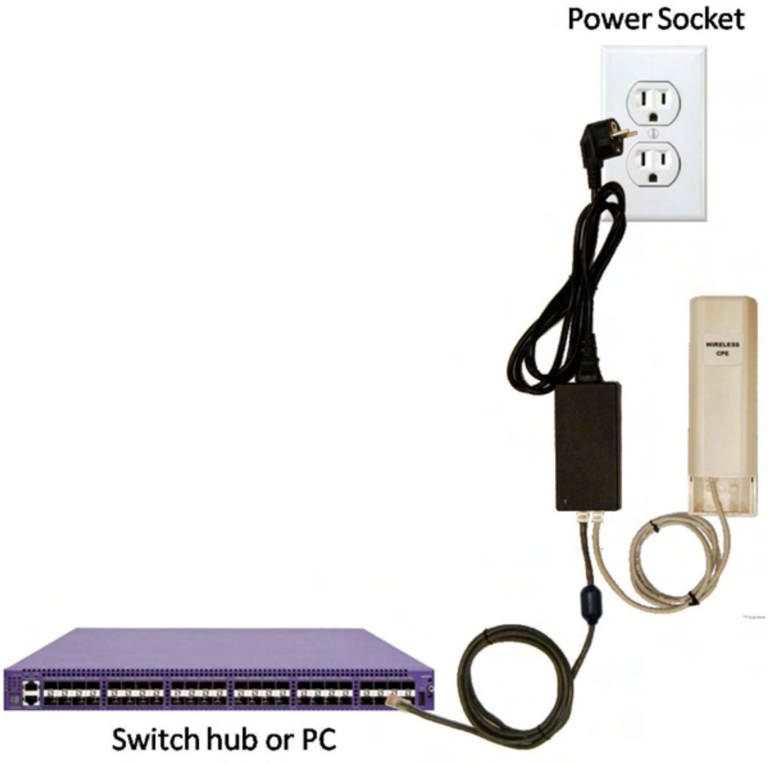
✎ **Note:**

- The ferrite is professionally installed and a shrink wrap has been put around the ferrite so the users CAN'T take the ferrite off.

5. Connect the Ethernet cable with suppression core to the "Data In" port of the PoE injector.



6. Connect the other end of Ethernet cable to a PC or a switch hub. The hardware installation is complete.

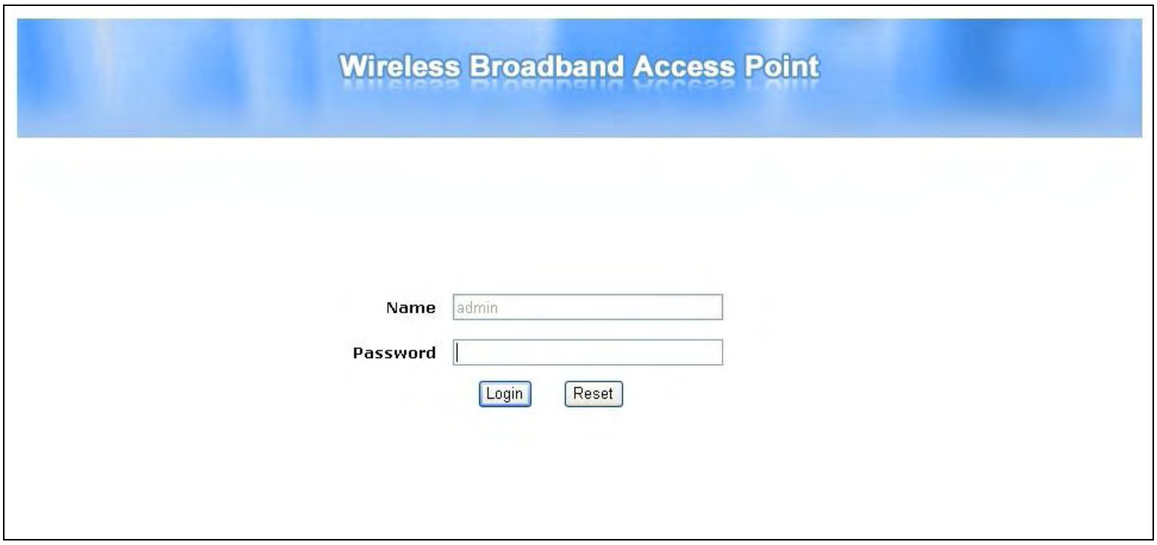


Chapter 2 Quick Setup Tutorial

Access the Web Configurator

The ZAC Access Point provides you with user-friendly Web-based management interface to easily manage the access point.

- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of the ZAC Access Point is 192.168.1.1. (X cannot be 0, 1, nor 255);
- Open Web browser and enter the IP address (Default: **192.168.1.1**) of the ZAC Access Point into the address field. You will see the login page as below.

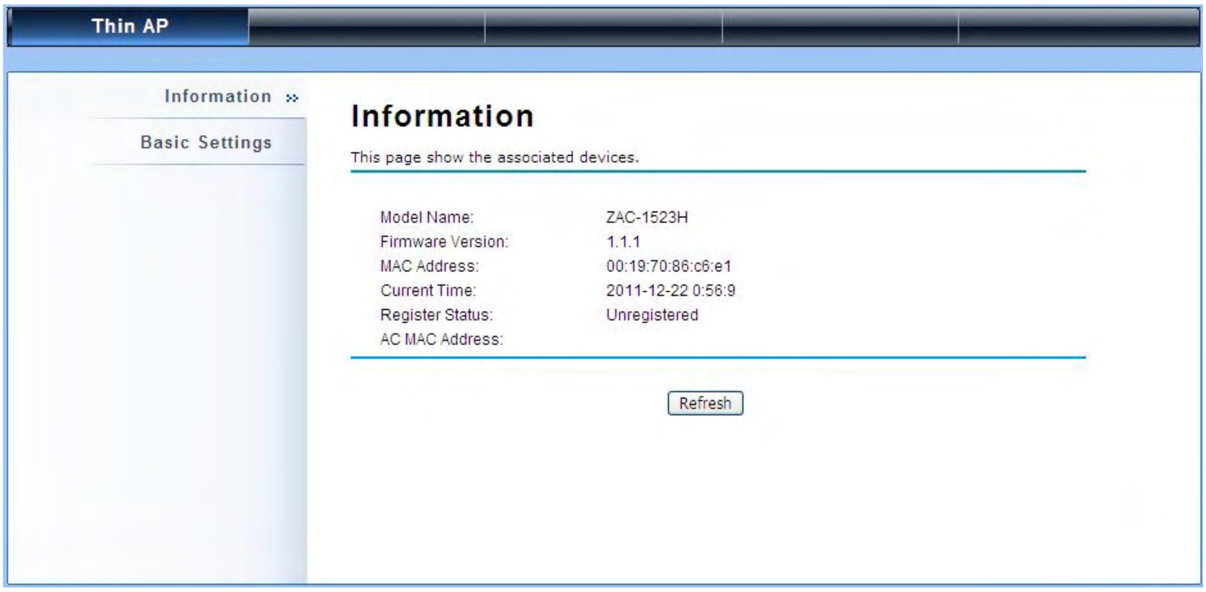


Wireless Broadband Access Point

Name admin

Password

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click "**Login**" to login the main page of the ZAC Access Point.



Information

This page show the associated devices.

Model Name:	ZAC-1523H
Firmware Version:	1.1.1
MAC Address:	00:19:70:86:c6:e1
Current Time:	2011-12-22 0:56:9
Register Status:	Unregistered
AC MAC Address:	

Note:

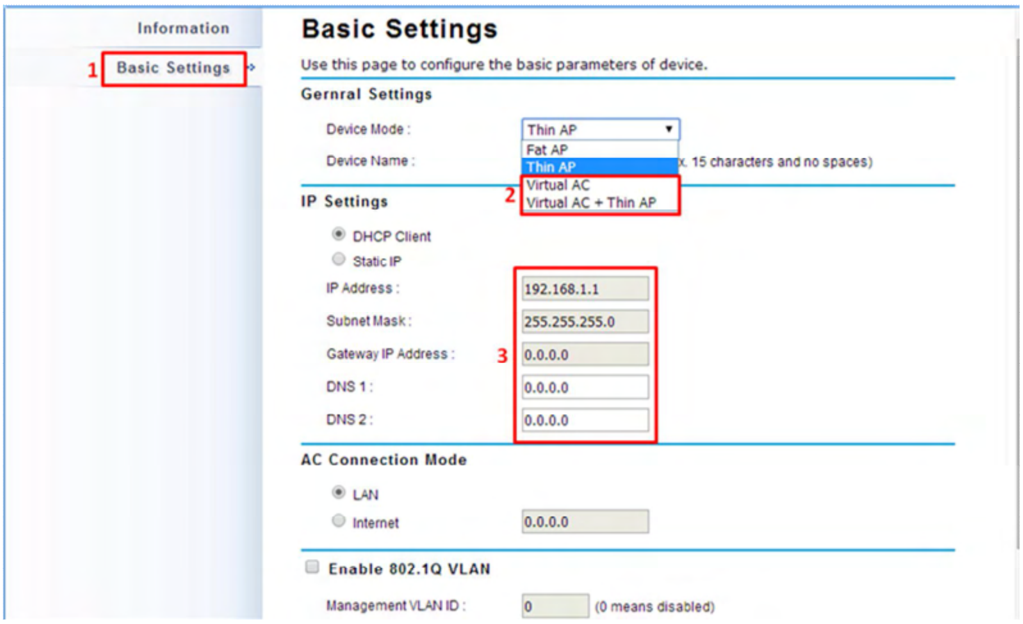
- The username and password are case-sensitive, and the password should be no more than 19 characters!

Configure the AC+Thin AP mode

The ZAC Access Point provides 4 operation modes: “**Thin AP**”, “**Virtual AC**”, “V**irtual AC+Thin AP** ”, as well as “**FAT AP**”. The default mode is “Thin AP”. To allow the ZAC Access Point to manage the thin APs, you need to switch one of the ZAC Access Points to virtual controller mode first. To change the mode, please do the following.

Configure the AC+Thin AP mode

To operate as AC+Thin AP, go to **Basic Settings**. From **Device Mode** drop-down list, select “**Virtual AC**” mode. If you would like the Access Point to perform as a virtual controller and access point concurrently, please select “**Virtual AC + Thin AP**” mode. Then assign an IP address to the ZAC Access Point and specify subnet mask, gateway and DNS address respectively. Hit **Apply** and wait for about 50 seconds to take effect.



Basic Settings

Use this page to configure the basic parameters of device.

Gernral Settings

Device Mode : Thin AP ▾
Fat AP
Thin AP
Virtual AC
Virtual AC + Thin AP

Device Name : x. 15 characters and no spaces)

IP Settings

● DHCP Client
○ Static IP

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Gateway IP Address : 0.0.0.0
DNS 1 : 0.0.0.0
DNS 2 : 0.0.0.0

AC Connection Mode

● LAN
○ Internet 0.0.0.0

□ Enable 802.1Q VLAN

Management VLAN ID : 0 (0 means disabled)

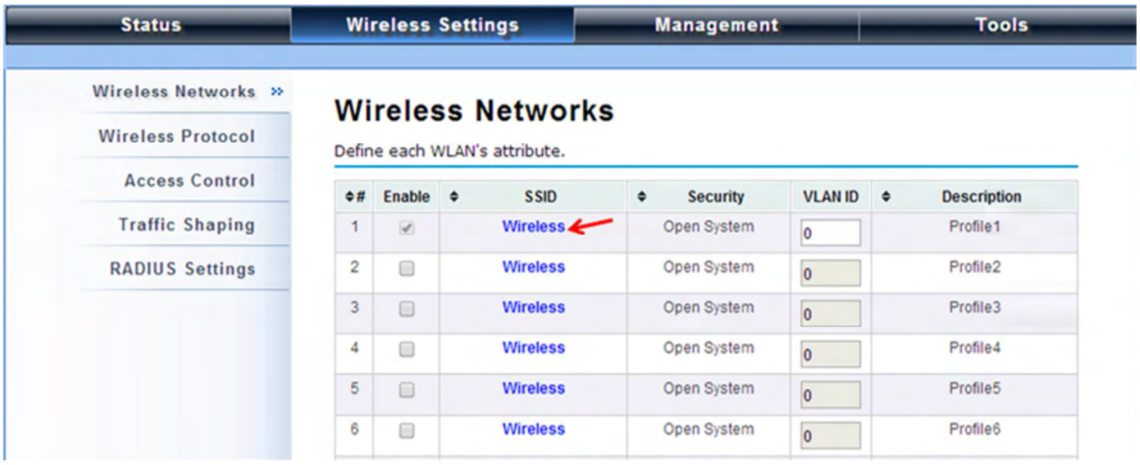
Note:

- AC+ Thin AP mode allows the ZAC Access Point to operate as access controller and thin AP concurrently.

Note:

- To operate as standalone Access Point, wireless client or bridge, please select **FAT AP** from device mode.

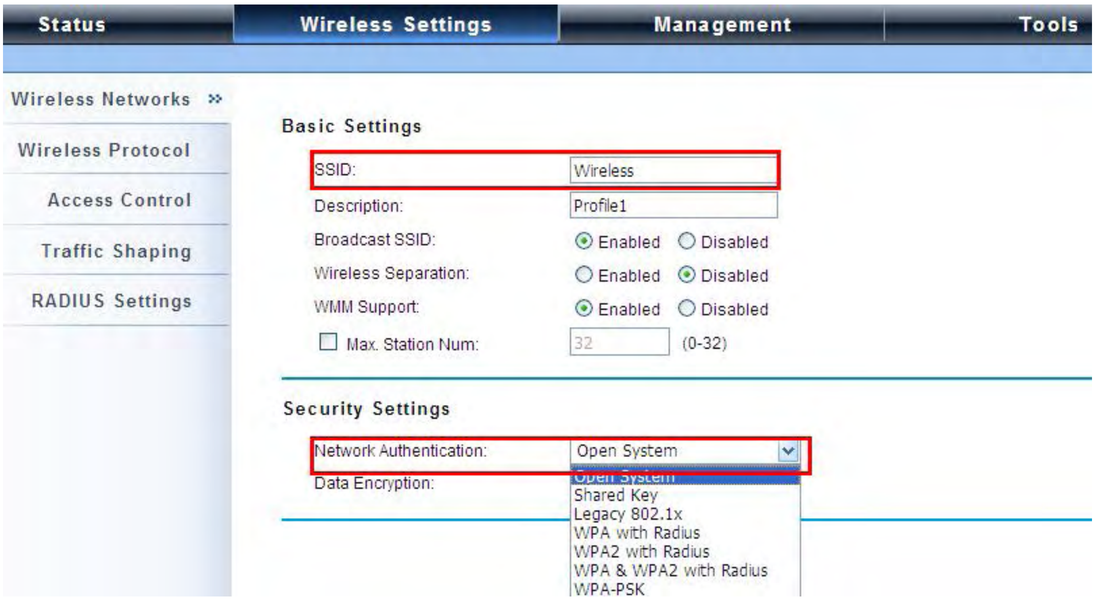
For Virtual Controller + Thin AP mode, if you need to configure the wireless settings for the ZAC Access Point especially SSID and encryption method, go to **Wireless Settings > Wireless Networks** and click on #1 **Wireless** SSID for configuration. After the configuration is made, click **Save** to save the settings.



Wireless Networks

Define each WLAN's attribute.

#	Enable	SSID	Security	VLAN ID	Description
1	☑	Wireless	Open System	0	Profile1
2	☐	Wireless	Open System	0	Profile2
3	☐	Wireless	Open System	0	Profile3
4	☐	Wireless	Open System	0	Profile4
5	☐	Wireless	Open System	0	Profile5
6	☐	Wireless	Open System	0	Profile6



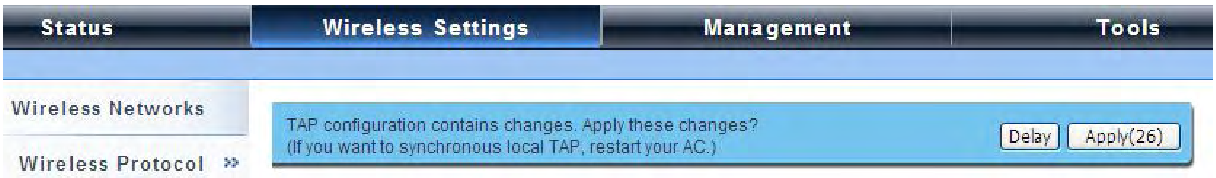
Basic Settings

SSID:	Wireless
Description:	Profile1
Broadcast SSID:	● Enabled ○ Disabled
Wireless Separation:	○ Enabled ● Disabled
WMM Support:	● Enabled ○ Disabled
☐ Max. Station Num:	32 (0-32)

Security Settings

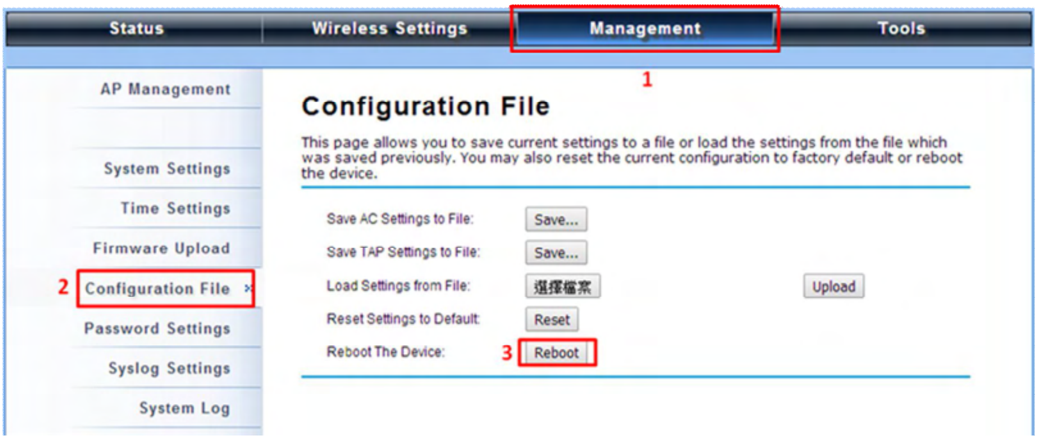
Network Authentication:	Open System
Data Encryption:	

A dialog message will pop up to remind you changes will also apply to other managed Thin APs. Click **Apply** to apply the configuration immediately.



TAP configuration contains changes. Apply these changes?
(If you want to synchronous local TAP, restart your AC.)

To make profile setting on the ZAC Access Point itself take effect, you need to reboot the AP in controller mode as well. To reboot the ZAC Access Point, go to **Management > Configuration File** and click the **Reboot** button. The reboot process will take about 50 seconds.



Status
Wireless Settings
Management
Tools
1
AP Management
System Settings
Time Settings
Firmware Upload
2
Configuration File
Password Settings
Syslog Settings
System Log

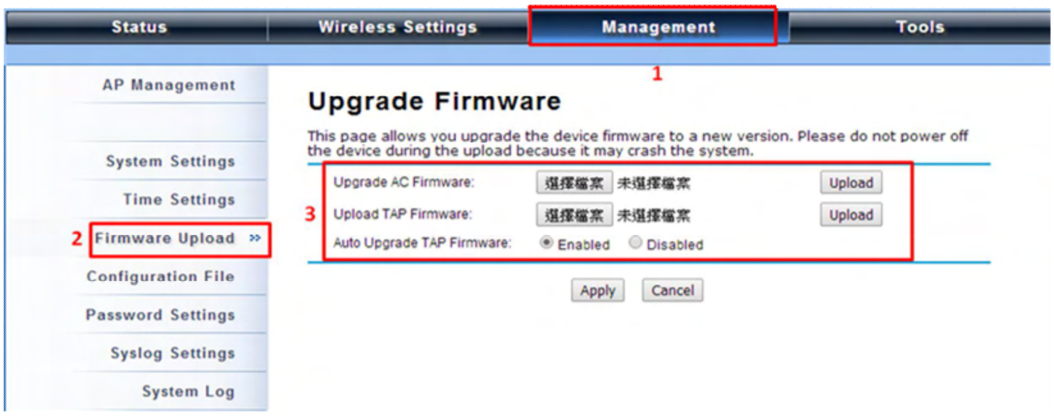
Configuration File

This page allows you to save current settings to a file or load the settings from the file which was saved previously. You may also reset the current configuration to factory default or reboot the device.

Save AC Settings to File: Save...
Save TAP Settings to File: Save...
Load Settings from File: 選擇檔案 Upload
Reset Settings to Default: Reset
Reboot The Device: 3 Reboot

Firmware Upgrade for ZAC AP in AC mode

To upgrade the firmware for the ZAC Access Point in controller mode when necessary, go to **Management > Firmware Upload** and from **Upgrade AC Firmware**, browse the firmware file where it is placed. Hit **Upload** to start the upgrade process. It will take approximately 2 minutes to complete the update.



Upgrade Firmware

This page allows you upgrade the device firmware to a new version. Please do not power off the device during the upload because it may crash the system.

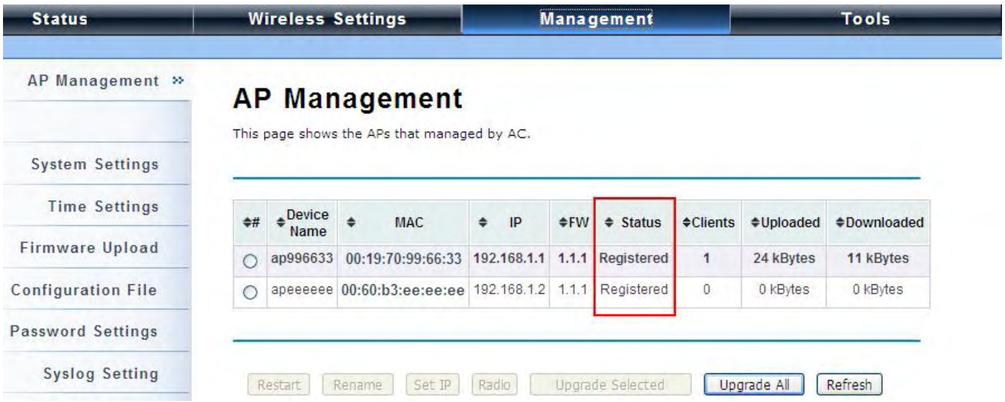
3
Upgrade AC Firmware: 選擇檔案 未選擇檔案 Upload
Upload TAP Firmware: 選擇檔案 未選擇檔案 Upload

Auto Upgrade TAP Firmware: ● Enabled ○ Disabled

Install the Managed Thin AP

Install and connect the rest of managed Access Points to your network with Ethernet cables. Power them up respectively. They will automatically discover the ZAC Access Point in controller mode and register themselves.

To check whether the thin APs are successfully registered or not, enter the web page of the ZAC Access Point master access controller and go to **Management > AP Management**. You will see "**Registered**" in **Status** column. Besides registration status, you are able to see other information such as Device Name, MAC address, IP address, FW version, number of clients that associate to each thin AP as well as upload/download speed.

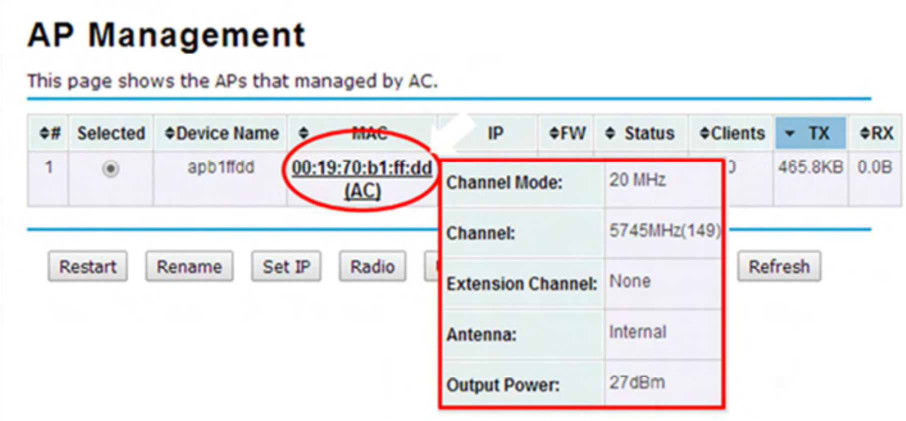


AP Management

This page shows the APs that managed by AC.

	⇕#	⇕Device Name	⇕ MAC	⇕ IP	⇕FW	⇕ Status	⇕Clients	⇕Uploaded	⇕Downloaded
○		ap996633	00:19:70:99:66:33	192.168.1.1	1.1.1	Registered	1	24 kBytes	11 kBytes
○		apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

Moving the mouse over MAC address of each managed AP will also display relevant RF information such as channel mode, current channel, antenna being used together with transmit output power.



AP Management

This page shows the APs that managed by AC.

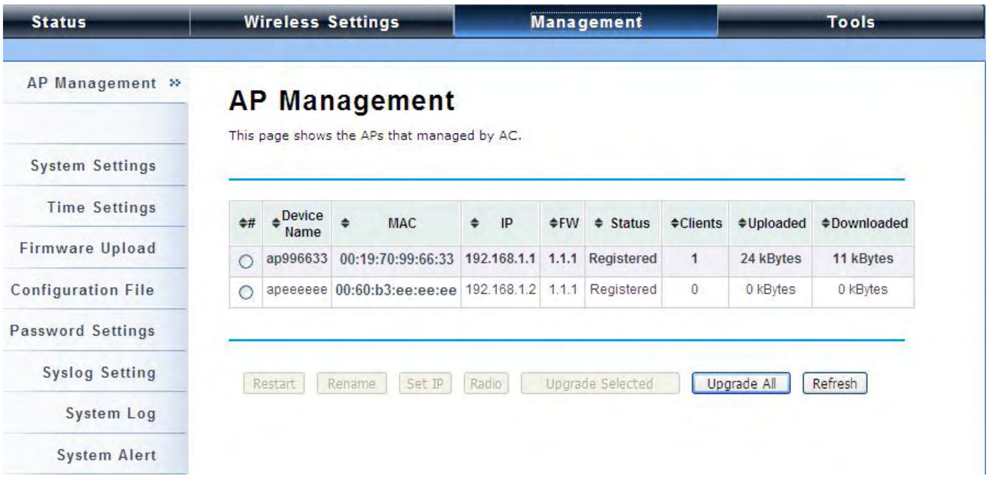
⇕#	Selected	⇕Device Name	⇕ MAC	IP	⇕FW	⇕ Status	⇕Clients	▾ TX	⇕RX
1	●	apb1ffdd	00:19:70:b1:ff:dd (AC)					465.8KB	0.0B

Channel Mode:	20 MHz
Channel:	5745MHz(149)
Extension Channel:	None
Antenna:	Internal
Output Power:	27dBm

Manage Thin APs

To configure and manage the managed APs:

1. Enter the web page of the ZAC Access Point in controller mode and go to **Management > AP Management**, the following screen shows up.

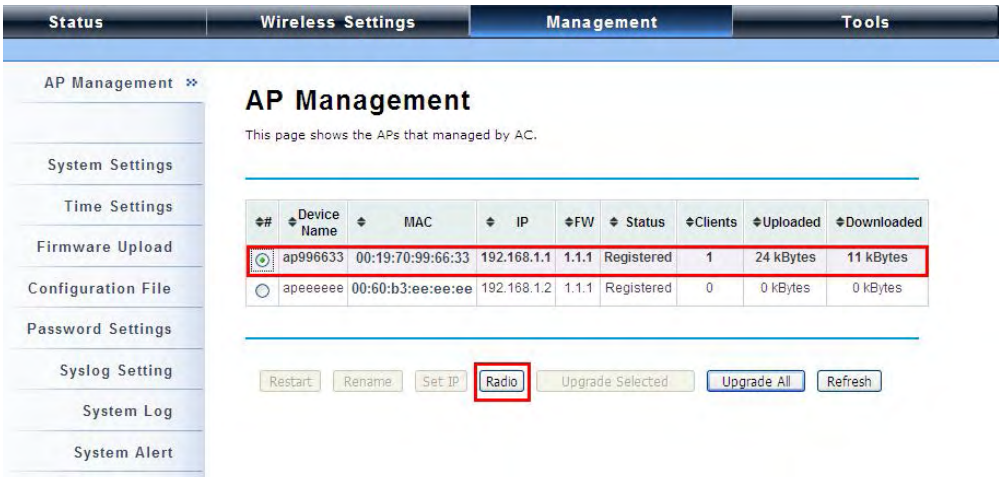


AP Management

This page shows the APs that managed by AC.

⇕#	⇕Device Name	⇕ MAC	⇕ IP	⇕FW	⇕ Status	⇕Clients	⇕Uploaded	⇕Downloaded
○	**ap996633**	**00:19:70:99:66:33**	**192.168.1.1**	**1.1.1**	**Registered**	**1**	**24 kBytes**	**11 kBytes**
○	apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

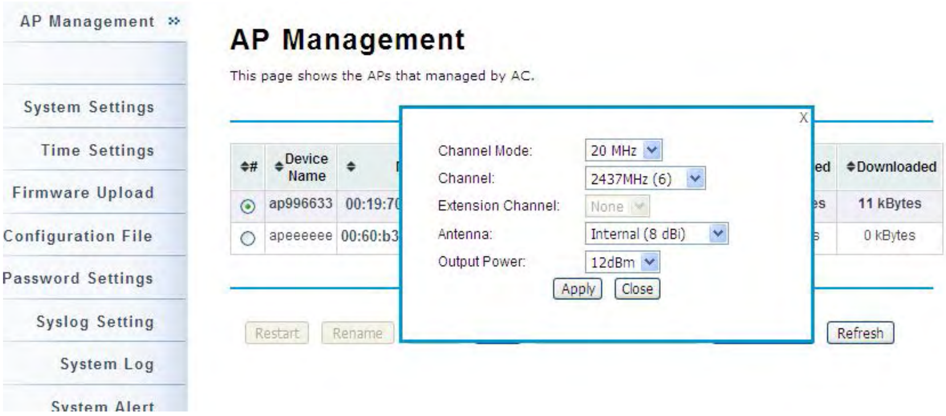
The ZAC Access Point AP in Virtual AC+Thin AP mode on the list is highlighted in bold font. By selecting it and hitting **Radio** button, you may check radio setting such as **channel bandwidth**, **channel**, **antenna** and **output power**.



AP Management

This page shows the APs that managed by AC.

⇕#	⇕Device Name	⇕ MAC	⇕ IP	⇕FW	⇕ Status	⇕Clients	⇕Uploaded	⇕Downloaded
●	**ap996633**	**00:19:70:99:66:33**	**192.168.1.1**	**1.1.1**	**Registered**	**1**	**24 kBytes**	**11 kBytes**
○	apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes



Channel Mode: 20 MHz

Channel: 2437MHz (6)

Extension Channel: None

Antenna: Internal (8 dBi)

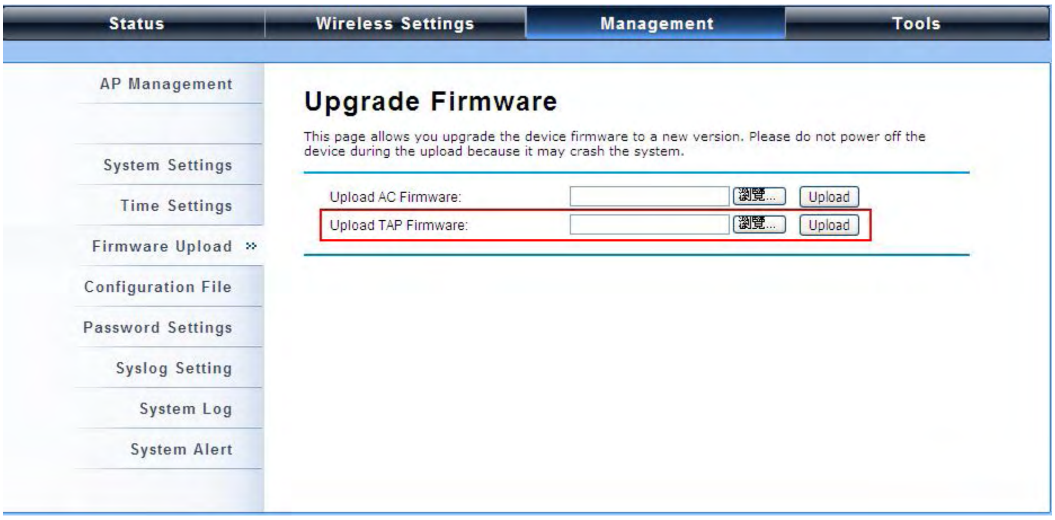
Output Power: 12dBm

Besides radio setting, you may also reboot the managed AP, change its IP address and perform firmware upgrade for managed AP.

Firmware Upgrade for Managed Thin APs

For firmware upgrade, you may choose to upgrade the selected managed AP by hitting **Upgrade Selected**, or do the group upgrade by hitting **Upgrade All**.

Before upgrading the managed AP, you need to locate the new firmware in the ZAC Access Point. Go to **Management > Firmware Upload**, browse the firmware file where it is located, click **Upload** and Click **OK**.

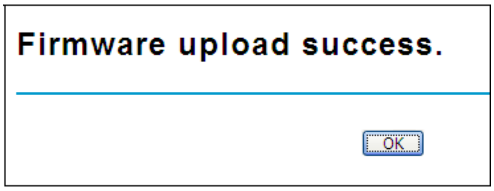


Upgrade Firmware

This page allows you upgrade the device firmware to a new version. Please do not power off the device during the upload because it may crash the system.

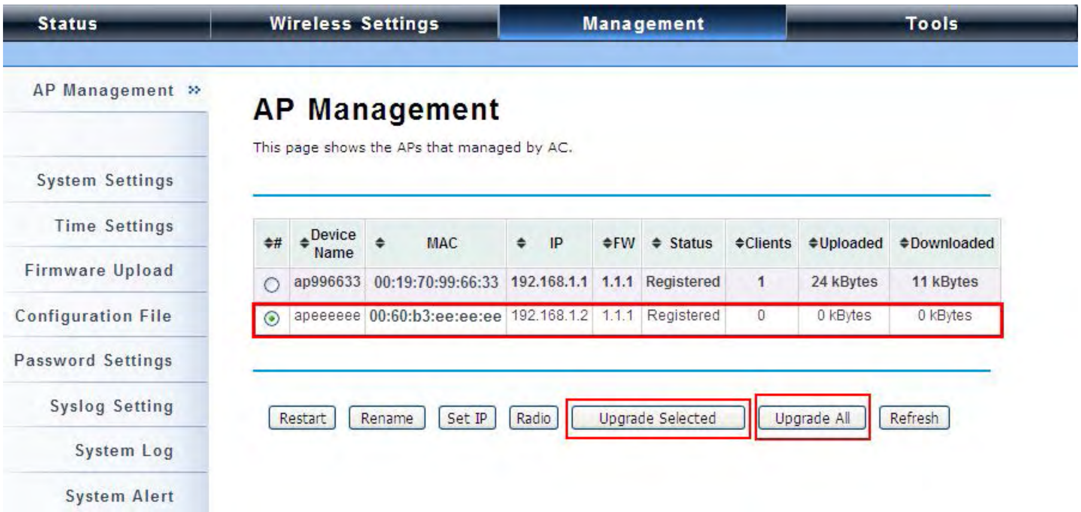
Upload AC Firmware:

Upload TAP Firmware:



Firmware upload success.

Then go back to **Management > AP Management to** do single or group update.



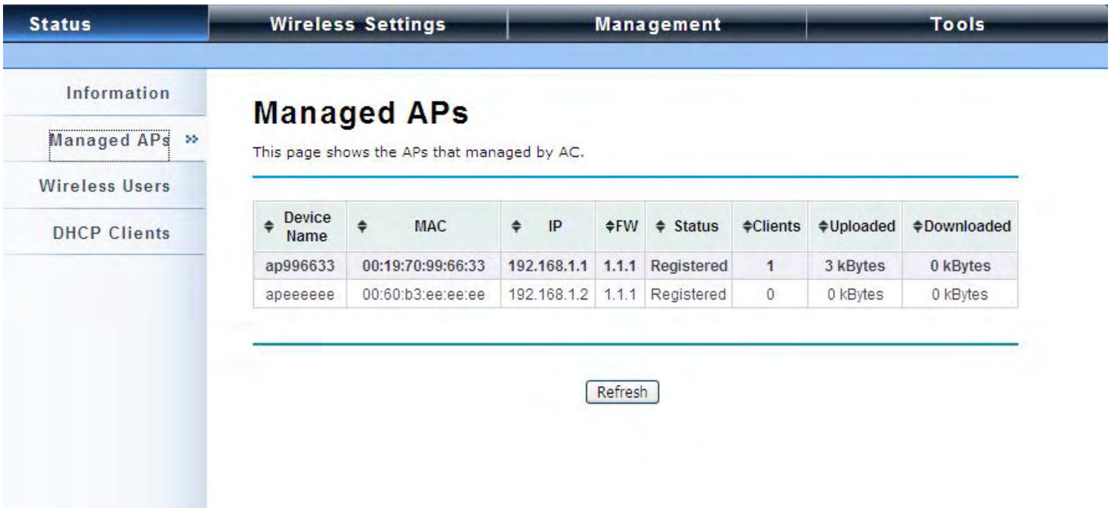
AP Management

This page shows the APs that managed by AC.

#	Device Name	MAC	IP	FW	Status	Clients	Uploaded	Downloaded
○	ap996633	00:19:70:99:66:33	192.168.1.1	1.1.1	Registered	1	24 kBytes	11 kBytes
●	apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

Monitor Managed Thin APs

To view each managed AP's status, please go to **Status > Managed APs**. Besides viewing device information such as device name, MAC address, IP address, and FW version, you may also monitor the wireless clients that are currently associated with the managed APs as well as packets statistics.



Managed APs

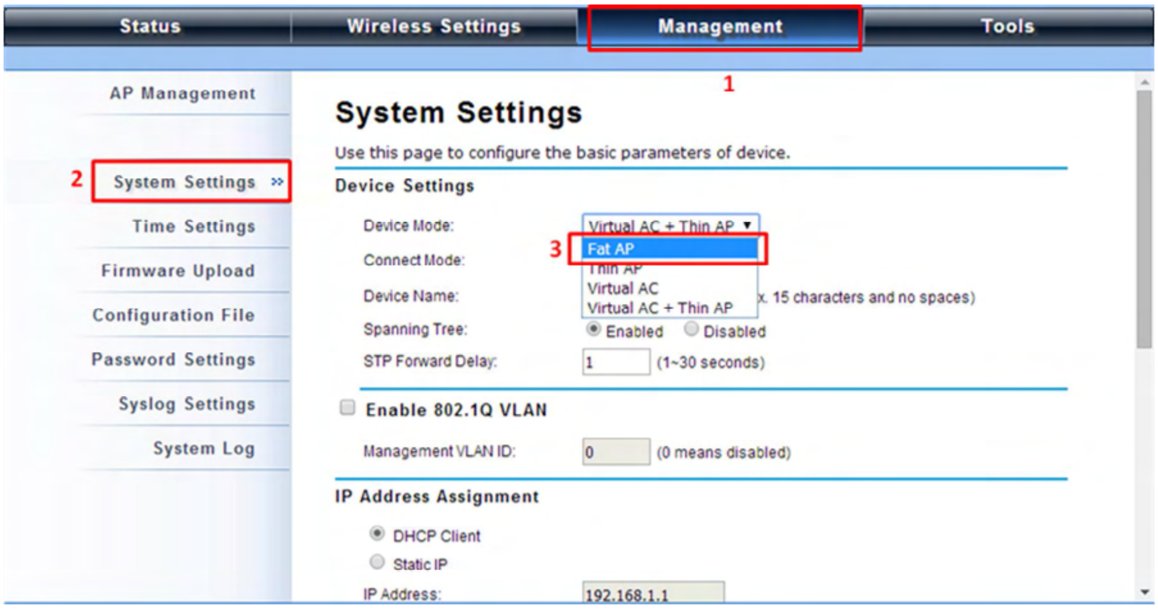
This page shows the APs that managed by AC.

Device Name	MAC	IP	FW	Status	Clients	Uploaded	Downloaded
ap996633	00:19:70:99:66:33	192.168.1.1	1.1.1	Registered	1	3 kBytes	0 kBytes
apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

Configure the Fat AP mode

Fat AP mode operates as standalone AP that cannot be managed by the ZAC Access Point.

To switch from **Virtual AC** mode to **Fat AP** mode, go to **Management > System Settings**. From the **Device Mode** drop-down list, select "**Fat AP**" and hit **YES** to make the change take effect.



System Settings

Use this page to configure the basic parameters of device.

Device Settings

Device Mode: Virtual AC + Thin AP ▾
Fat AP
Thin AP
Virtual AC
Virtual AC + Thin AP

Connect Mode:

Device Name: x. 15 characters and no spaces)

Spanning Tree: ● Enabled ○ Disabled

STP Forward Delay: 1 (1~30 seconds)

□ **Enable 802.1Q VLAN**

Management VLAN ID: 0 (0 means disabled)

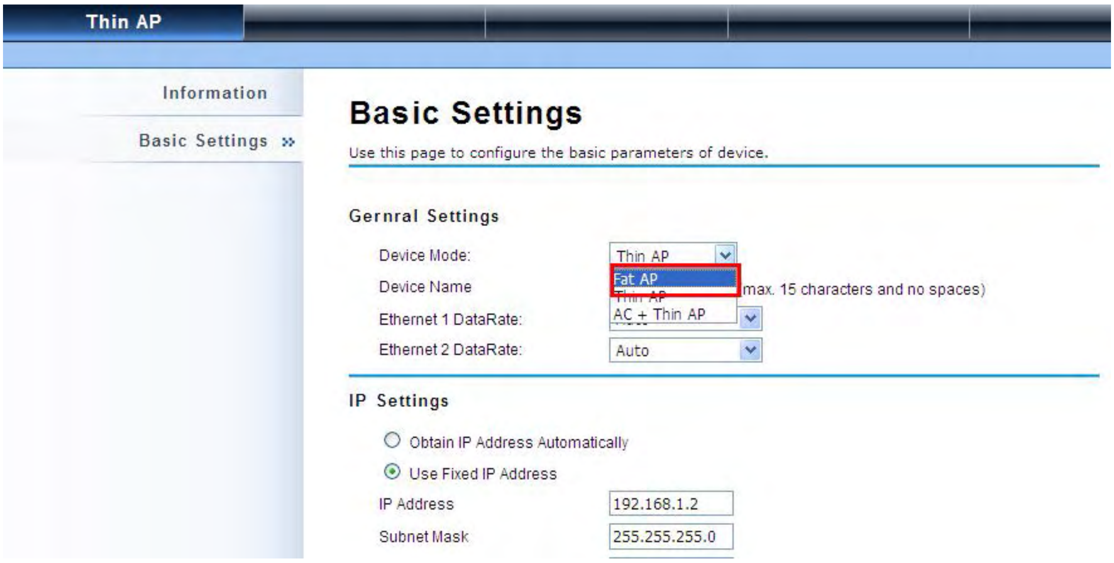
IP Address Assignment

● DHCP Client

○ Static IP

IP Address: 192.168.1.1

To switch from default mode **Thin AP** to **Fat AP** mode for the first time configuration, go to **Basic Settings.** From the **Device Mode** drop-down list, select "**Fat AP**" and hit **YES** to make the change take effect.



Basic Settings

Use this page to configure the basic parameters of device.

Gernral Settings

Device Mode:	Thin AP Fat AP Thin AP AC + Thin AP
Device Name	(max. 15 characters and no spaces)
Ethernet 1 DataRate:	
Ethernet 2 DataRate:	Auto

IP Settings

○ Obtain IP Address Automatically

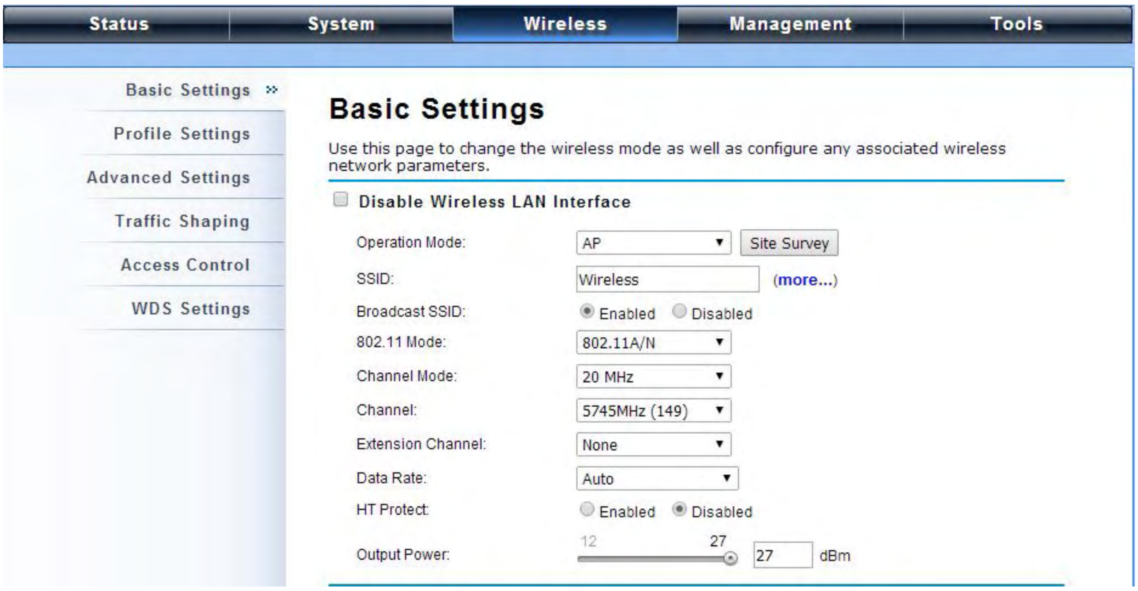
● Use Fixed IP Address

IP Address	192.168.1.2
Subnet Mask	255.255.255.0

The Fat AP covers "**AP mode**", "**Wireless Client mode**", "**Bridge mode**" as well as "**AP Repeater mode**". For details please refer to the next Chapter.

AP Mode

1. Choose **Wireless > Basic Settings**. The default is AP mode already. Here, you can change wireless SSID for your public end user. After the configuration is made, click **Apply** to save the parameters.



Basic Settings

Use this page to change the wireless mode as well as configure any associated wireless network parameters.

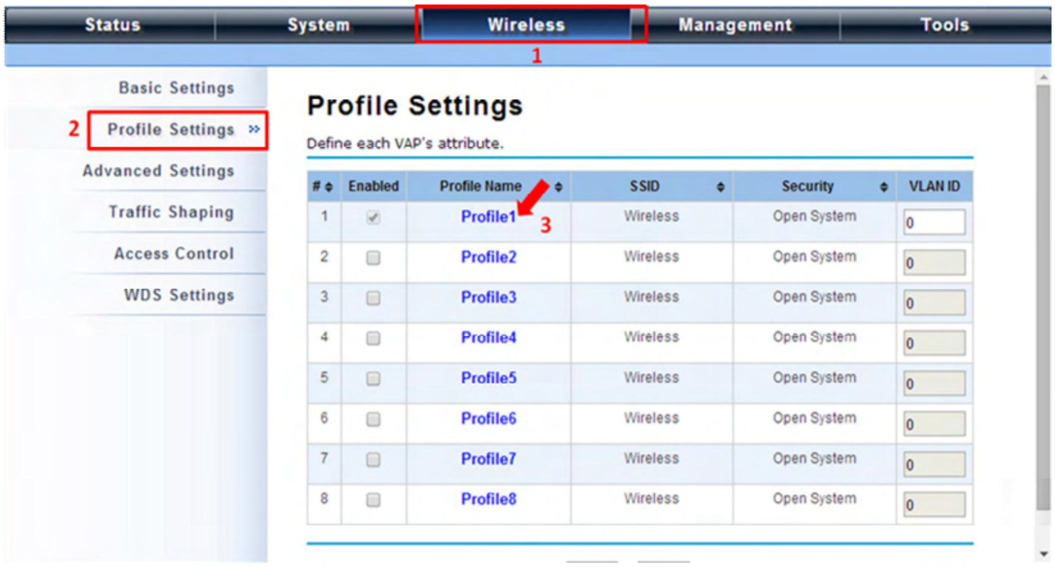
□ Disable Wireless LAN Interface

Operation Mode:	AP
SSID:	Wireless
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11A/N
Channel Mode:	20 MHz
Channel:	5745MHz (149)
Extension Channel:	None
Data Rate:	Auto
HT Protect:	○ Enabled ● Disabled
Output Power:	12 27 27 dBm

Note:

- In the example here, we only change the "Wireless Network Name (SSID)" as "Join_me".

2. If security is required, open **Wireless > Profile Setting** and click on "**Profile 1 Settings**" as below.

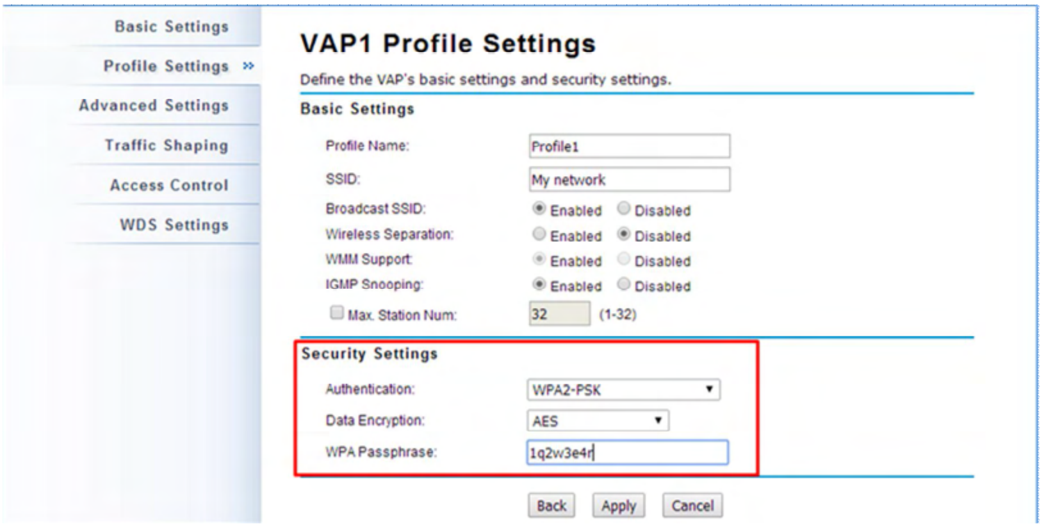


Profile Settings

Define each VAP's attribute.

#	Enabled	Profile Name	SSID	Security	VLAN ID
1	☑	Profile1	Wireless	Open System	0
2	☐	Profile2	Wireless	Open System	0
3	☐	Profile3	Wireless	Open System	0
4	☐	Profile4	Wireless	Open System	0
5	☐	Profile5	Wireless	Open System	0
6	☐	Profile6	Wireless	Open System	0
7	☐	Profile7	Wireless	Open System	0
8	☐	Profile8	Wireless	Open System	0

3. You may configure the parameters like "Network Authentication" and "Data Encryption" for more secure network communication in your application. After the configuration is made, click **Apply** to save the parameters.



VAP1 Profile Settings

Define the VAP's basic settings and security settings.

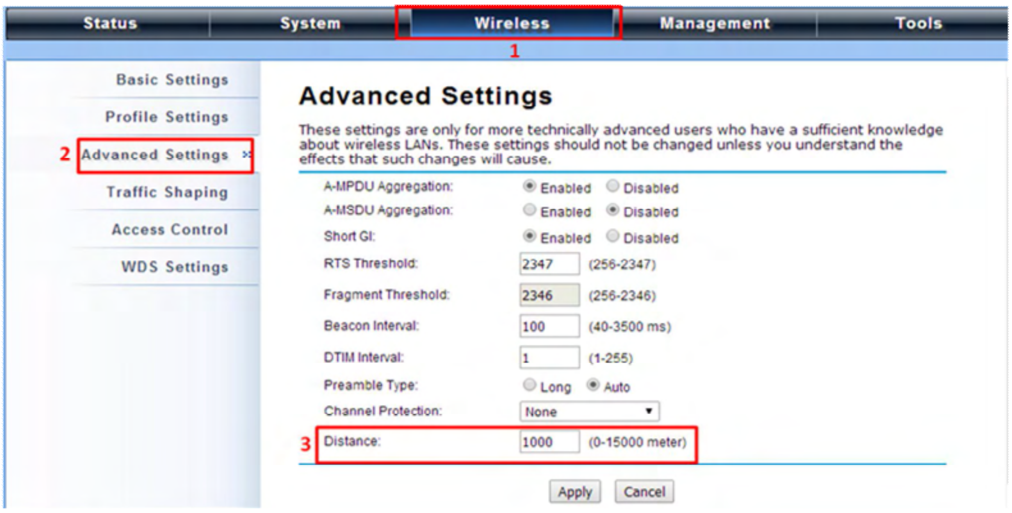
Basic Settings

Profile Name:	Profile1
SSID:	My network
Broadcast SSID:	● Enabled ○ Disabled
Wireless Separation:	○ Enabled ● Disabled
WMM Support:	● Enabled ○ Disabled
IGMP Snooping:	● Enabled ○ Disabled
☐ Max. Station Num:	32 (1-32)

Security Settings

Authentication:	WPA2-PSK
Data Encryption:	AES
WPA Passphrase:	1q2w3e4r

4. To decrease the chances of data retransmission at long distance, the ZAC Access Point can automatically adjust proper ACK timeout value by specifying distance between the nodes. By specifying the distance, go to **Wireless > Advanced Setting** and fill in the number in the Distance field. If the distance is below 1000 meters, remain the number unchanged.



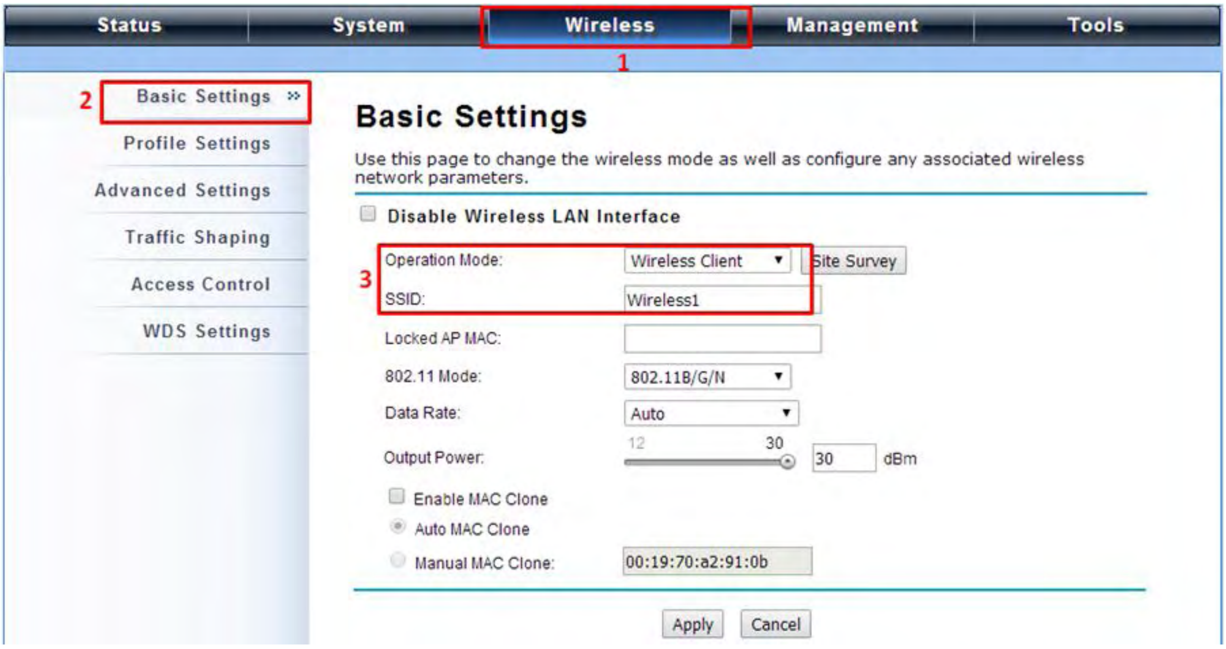
Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LANs. These settings should not be changed unless you understand the effects that such changes will cause.

A-MPDU Aggregation:	● Enabled ○ Disabled	
A-MSDU Aggregation:	○ Enabled ● Disabled	
Short GI:	● Enabled ○ Disabled	
RTS Threshold:	2347	(256-2347)
Fragment Threshold:	2346	(256-2346)
Beacon Interval:	100	(40-3500 ms)
DTIM Interval:	1	(1-255)
Preamble Type:	○ Long ● Auto	
Channel Protection:	None	
Distance:	1000	(0-15000 meter)

Wireless Client Mode

1. Go to **Wireless > Basic Settings** and choose "**Wireless Client**" from Wireless Mode. Specify the SSID that you would like connect and click **Apply** to save the configuration.



Basic Settings

Use this page to change the wireless mode as well as configure any associated wireless network parameters.

□ Disable Wireless LAN Interface

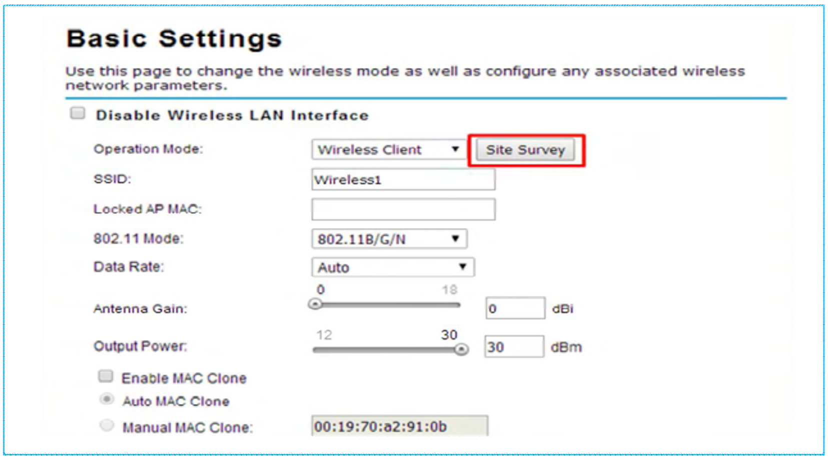
Operation Mode:	Wireless Client	
SSID:	Wireless1	
Locked AP MAC:		
802.11 Mode:	802.11B/G/N	
Data Rate:	Auto	
Output Power:	12 – 30	30 dBm

□ Enable MAC Clone

● Auto MAC Clone

○ Manual MAC Clone: 00:19:70:a2:91:0b

Besides specifying the SSID manually, you may select the preferable Access Point to connect by clicking the "**Site Survey"** button beside **Wireless Mode**. Once the button is pressed, the wireless client will scan all the available access points within coverage. Select the one you prefer to connect, and click **Select AP** to establish the connection.



Basic Settings

Use this page to change the wireless mode as well as configure any associated wireless network parameters.

□ Disable Wireless LAN Interface

Operation Mode: Wireless Client ▾ Site Survey

SSID: Wireless1

Locked AP MAC:

802.11 Mode: 802.11B/G/N ▾

Data Rate: Auto ▾

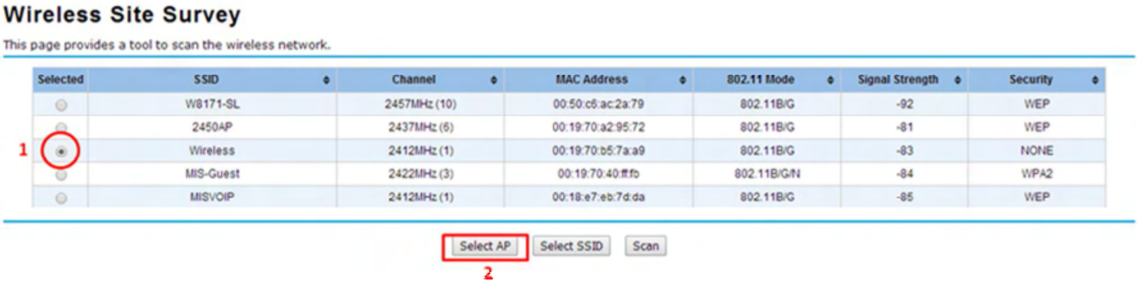
Antenna Gain: 0 dBi

Output Power: 30 dBm

□ Enable MAC Clone

● Auto MAC Clone

○ Manual MAC Clone: 00:19:70:a2:91:0b

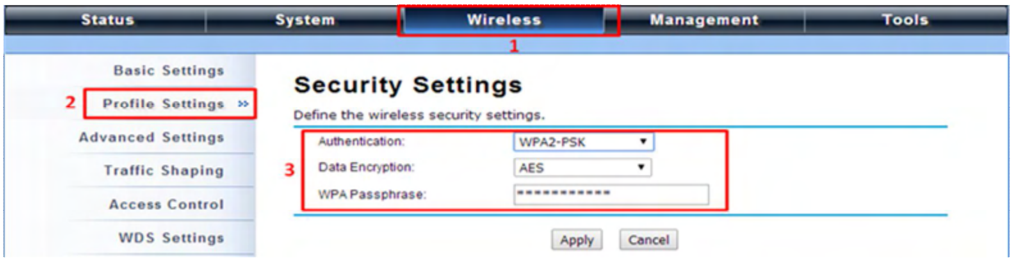


Wireless Site Survey

This page provides a tool to scan the wireless network.

Selected	SSID	Channel	MAC Address	802.11 Mode	Signal Strength	Security
○	W8171-SL	2457MHz (10)	00:50:c6:ac:2a:79	802.11B/G	-92	WEP
○	2450AP	2437MHz (6)	00:19:70:a2:95:72	802.11B/G	-81	WEP
●	Wireless	2412MHz (1)	00:19:70:b5:7a:a9	802.11B/G	-83	NONE
○	MIS-Guest	2422MHz (3)	00:19:70:40:ff:fb	802.11B/G/N	-84	WPA2
○	MISVOIP	2412MHz (1)	00:18:e7:eb:7d:da	802.11B/G	-85	WEP

3. If the AP you connect to require authentication or encryption keys, click **Profile Settings** in the left column, select the corresponding authentication and encryption options, and click “ **Apply**” to save configuration.



Security Settings

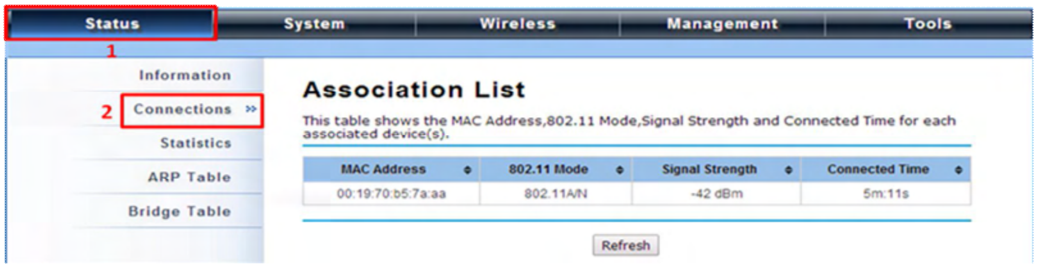
Define the wireless security settings.

Authentication: WPA2-PSK ▾

Data Encryption: AES ▾

WPA Passphrase: ***********

4. To check whether the association with the Access Point has been successfully made, go to **Status > Connections**. If the connection is established, it will display association information of the Access Point including MAC address, wireless mode, signal strength and connection time.



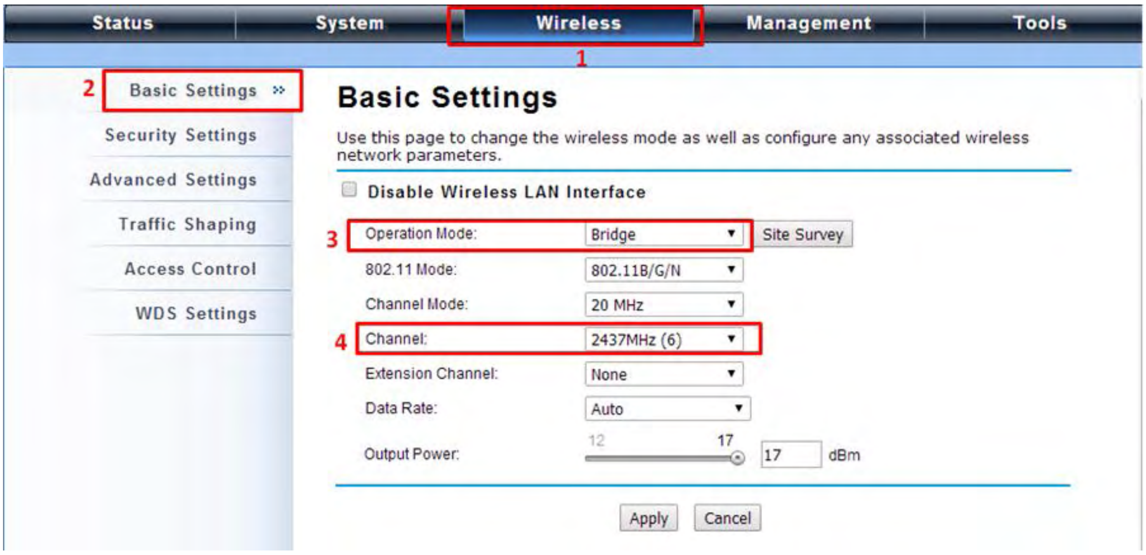
Association List

This table shows the MAC Address,802.11 Mode,Signal Strength and Connected Time for each associated device(s).

MAC Address	802.11 Mode	Signal Strength	Connected Time
00:19:70:b5:7a:aa	802.11A/N	-42 dBm	5m:11s

Bridge Mode

1. Go to **Wireless > Basic Settings**. Choose “Bridge” from Wireless Mode, check a clean channel and click **Apply** to save configuration.



Basic Settings

Use this page to change the wireless mode as well as configure any associated wireless network parameters.

□ Disable Wireless LAN Interface

Operation Mode: Bridge

802.11 Mode: 802.11B/G/N

Channel Mode: 20 MHz

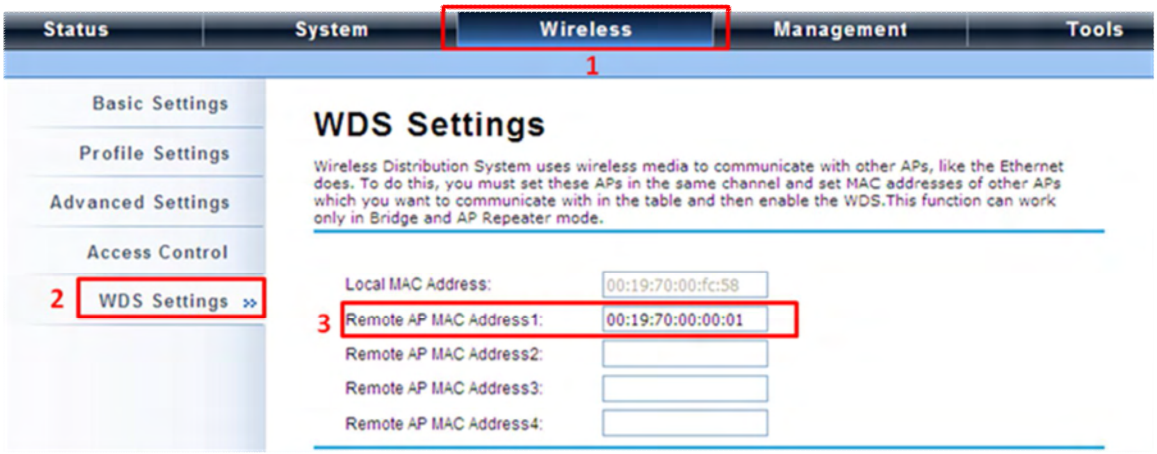
Channel: 2437MHz (6)

Extension Channel: None

Data Rate: Auto

Output Power: 12 17 17 dBm

2. Go to “**WDS Settings**” in “**Wireless**”, input the MAC address of the remote bridge to “**Remote AP MAC Address 1**” field and click “**Apply**”.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS.This function can work only in Bridge and AP Repeater mode.

Local MAC Address: 00:19:70:00:fc:58

Remote AP MAC Address1: 00:19:70:00:00:01

Remote AP MAC Address2:

Remote AP MAC Address3:

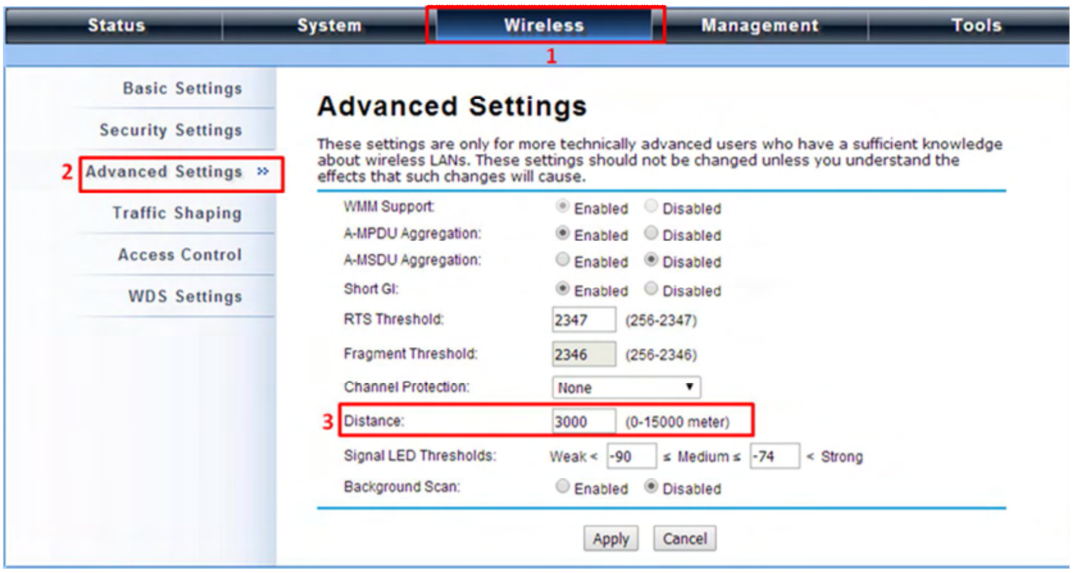
Remote AP MAC Address4:

Note:

- Bridge uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

3. Repeat the above procedures to configure the remote ZAC bridge.

4. Enter the actual distance in **Space In Meter**. For example, if the distance between the two ZAC bridges is 3 kilometers, enter 3000 in the field. Click **Apply** to save configuration.



Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LANs. These settings should not be changed unless you understand the effects that such changes will cause.

WMM Support: ● Enabled ○ Disabled

A-MPDU Aggregation: ● Enabled ○ Disabled

A-MSDU Aggregation: ○ Enabled ● Disabled

Short GI: ● Enabled ○ Disabled

RTS Threshold: 2347 (256-2347)

Fragment Threshold: 2346 (256-2346)

Channel Protection: None

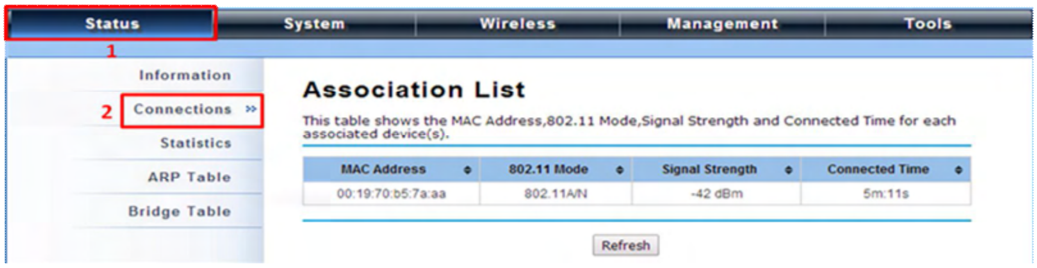
Distance: 3000 (0-15000 meter)

Signal LED Thresholds: Weak < -90 ≤ Medium ≤ -74 < Strong

Background Scan: ○ Enabled ● Disabled

5. Use ping to check whether the link between the two bridges is OK.

6. To check the wireless connectivity, go to **Status > Connections**. If the connection is established, it will display association information of the remote bridge including MAC address, wireless mode, signal strength and connection time.



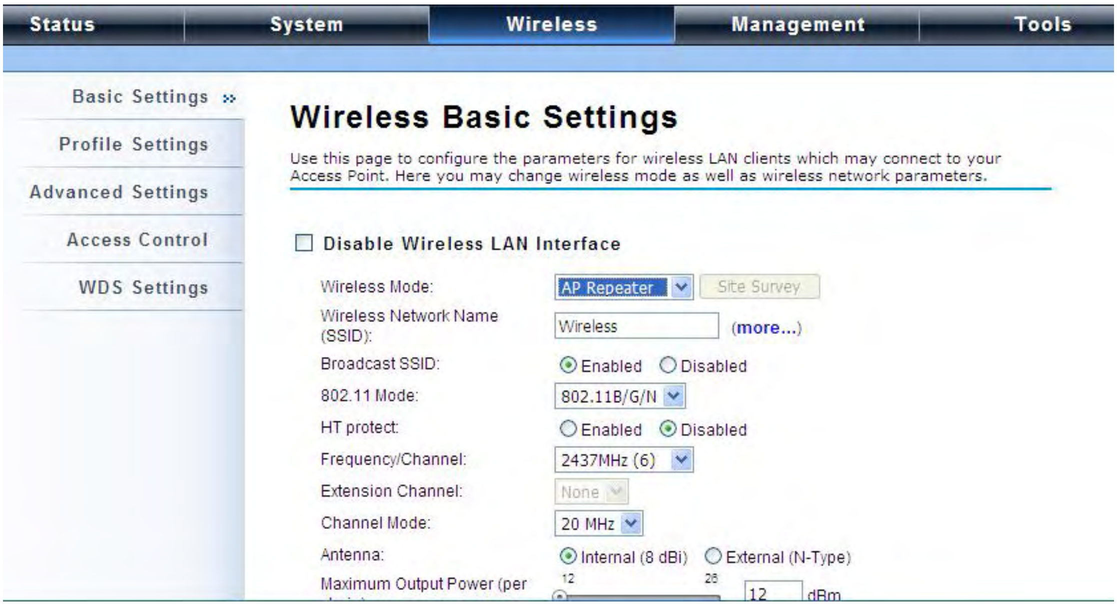
Association List

This table shows the MAC Address,802.11 Mode,Signal Strength and Connected Time for each associated device(s).

MAC Address	802.11 Mode	Signal Strength	Connected Time
00:19:70:b5:7a:aa	802.11A/N	-42 dBm	5m:11s

AP Repeater Mode

1. Go to **Wireless > Basic Settings**. Choose "**AP Repeater**" from Wireless Mode, and click **Apply** to save it.



Wireless Basic Settings

Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Wireless Mode:	AP Repeater
Wireless Network Name (SSID):	Wireless
Broadcast SSID:	● Enabled ○ Disabled
802.11 Mode:	802.11B/G/N
HT protect:	○ Enabled ● Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	None
Channel Mode:	20 MHz
Antenna:	● Internal (8 dBi) ○ External (N-Type)
Maximum Output Power (per	12 26 12 dBm

To establish point-to-point bridge connection, please follow the procedures described in Bridge mode.

To connect the wireless client to the AP, please follow the procedures described in Wireless Client mode.

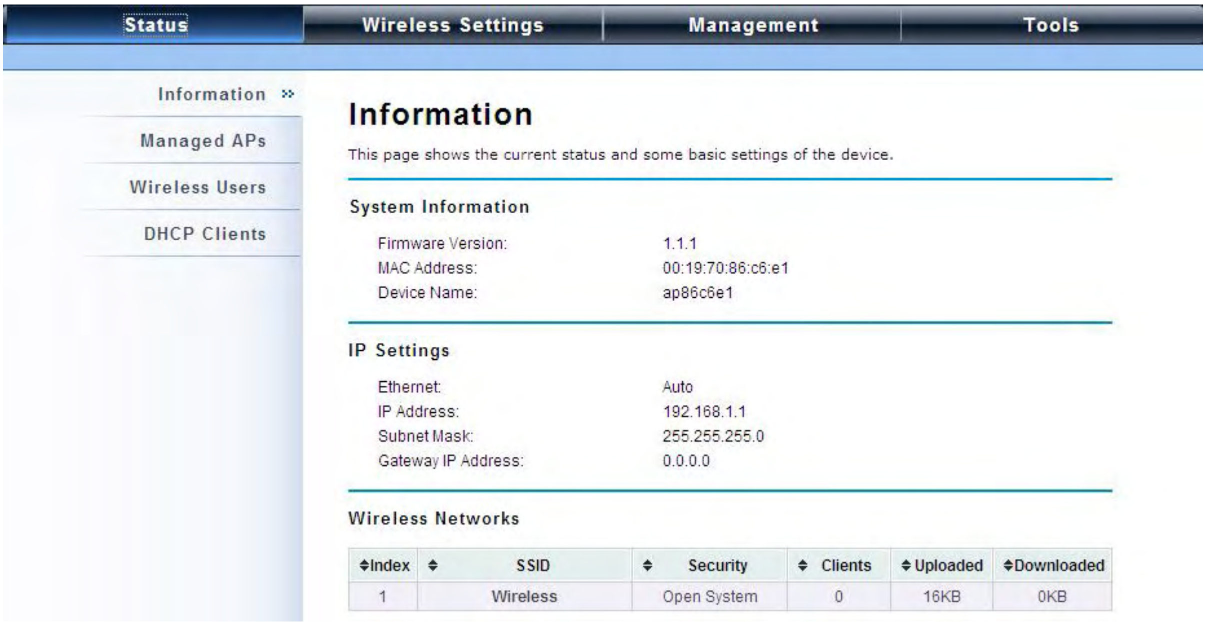
Chapter 3 Navigate the Web Configurator

Virtual AC+Thin AP Mode

Status

View Basic Information

Open “**Information**” in “**Status**” to check the basic information of the ZAC Access Point, which is read only. Information includes system information, IP settings, and wireless network setting. Click “**Refresh**” at the bottom to have the real-time information.



Information

This page shows the current status and some basic settings of the device.

System Information

Firmware Version: 1.1.1
MAC Address: 00:19:70:86:c6:e1
Device Name: ap86c6e1

IP Settings

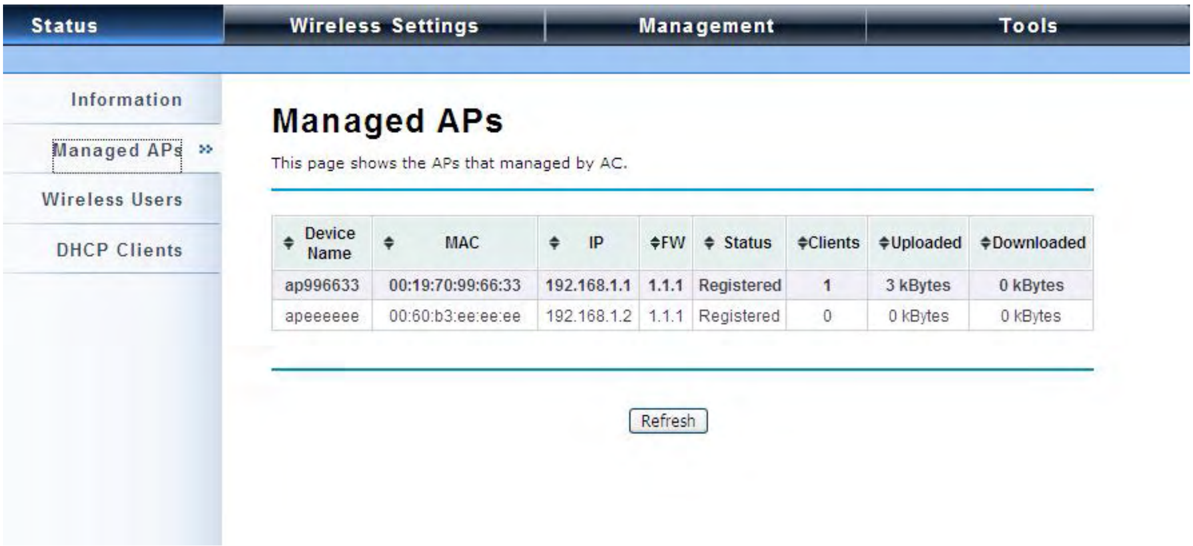
Ethernet: Auto
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0

Wireless Networks

⬍Index	⬍ SSID	⬍ Security	⬍ Clients	⬍Uploaded	⬍Downloaded
1	Wireless	Open System	0	16KB	0KB

View Managed APs

Open “**Managed APs**” in “**Status**” to check information of managed AP such as device name, MAC address, IP address, numbers of associated clients and uploaded/downloaded packets. All is read only. Click “**Refresh**” at the bottom to update the list.



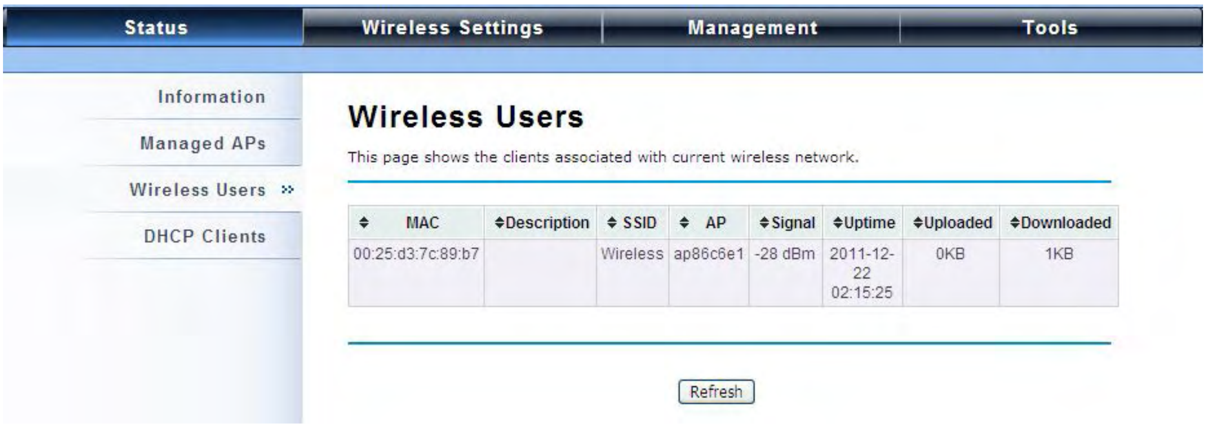
Managed APs

This page shows the APs that managed by AC.

♦ Device Name	♦ MAC	♦ IP	♦FW	♦ Status	♦Clients	♦Uploaded	♦Downloaded
ap996633	00:19:70:99:66:33	192.168.1.1	1.1.1	Registered	1	3 kBytes	0 kBytes
apeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

View Wireless Users

Open “**Wireless Users**” in “**Status**” to check the information of all the wireless clients such as MAC address, SSID of the managed APs that are associated with, signal strength, connection up time, and uploaded/downloaded packets. All is read only. Click “**Refresh**” at the bottom to update the list.



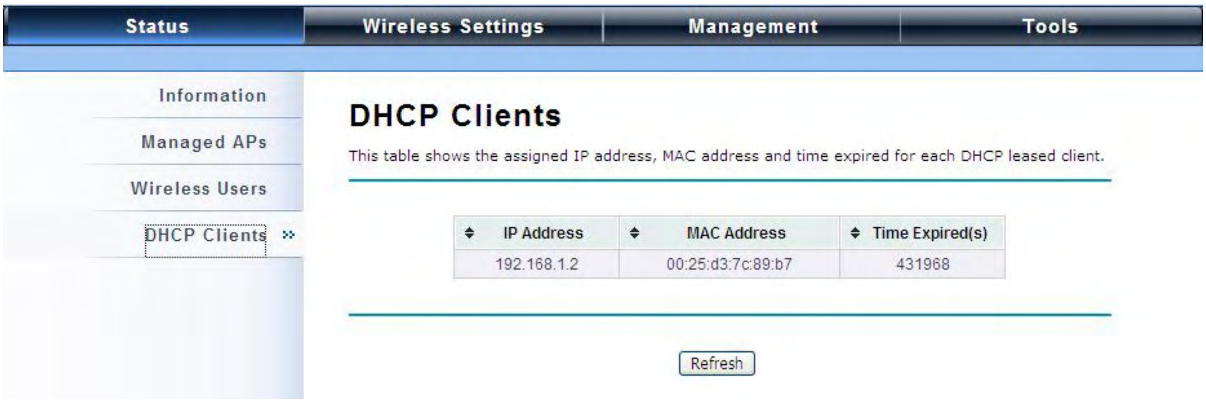
Wireless Users

This page shows the clients associated with current wireless network.

♦ MAC	♦Description	♦ SSID	♦ AP	♦Signal	♦Uptime	♦Uploaded	♦Downloaded
00:25:d3:7c:89:b7		Wireless	ap86c6e1	-28 dBm	2011-12-22 02:15:25	0KB	1KB

View DHCP Client Table

Open “**DHCP Clients**” in “**Status**” as below to check the assigned IP address, MAC address and lease time for each DHCP client. Click “**Refresh**” to update the table.



DHCP Clients

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

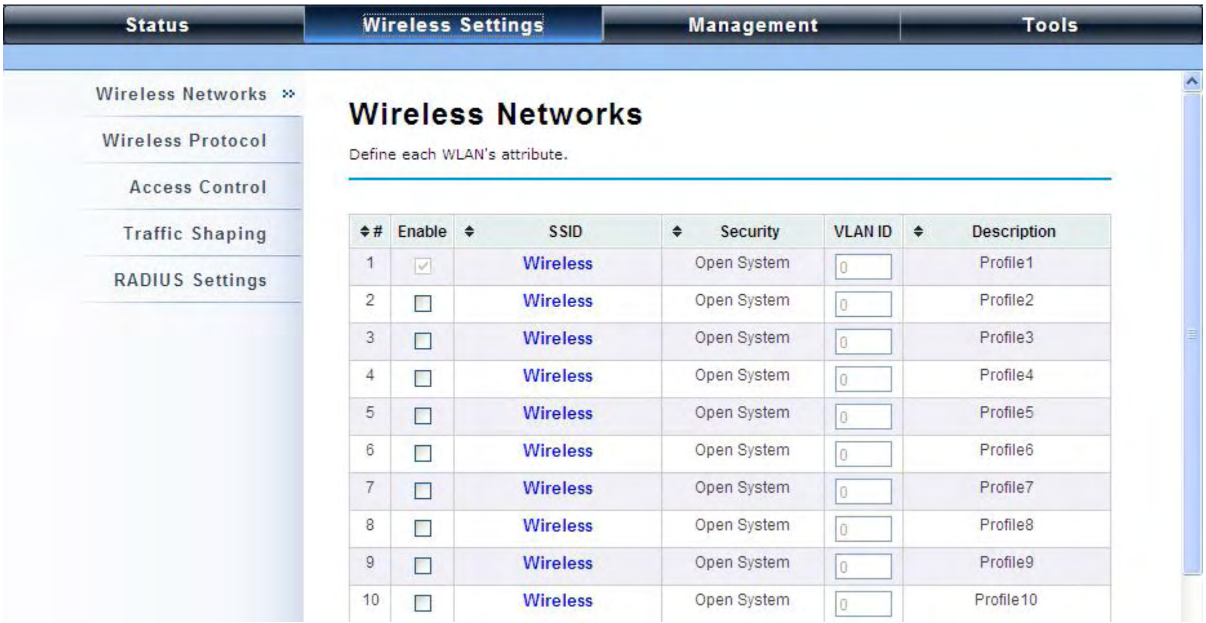
IP Address	MAC Address	Time Expired(s)
192.168.1.2	00:25:d3:7c:89:b7	431968

Wireless Settings

Wireless Setting allows you to configure wireless parameters, security method, access control and flow control for your ZAC Access Point. Note that the configuration will also apply on all the other ZAC-managed APs.

Wireless Networks (VAP Profiles Settings)

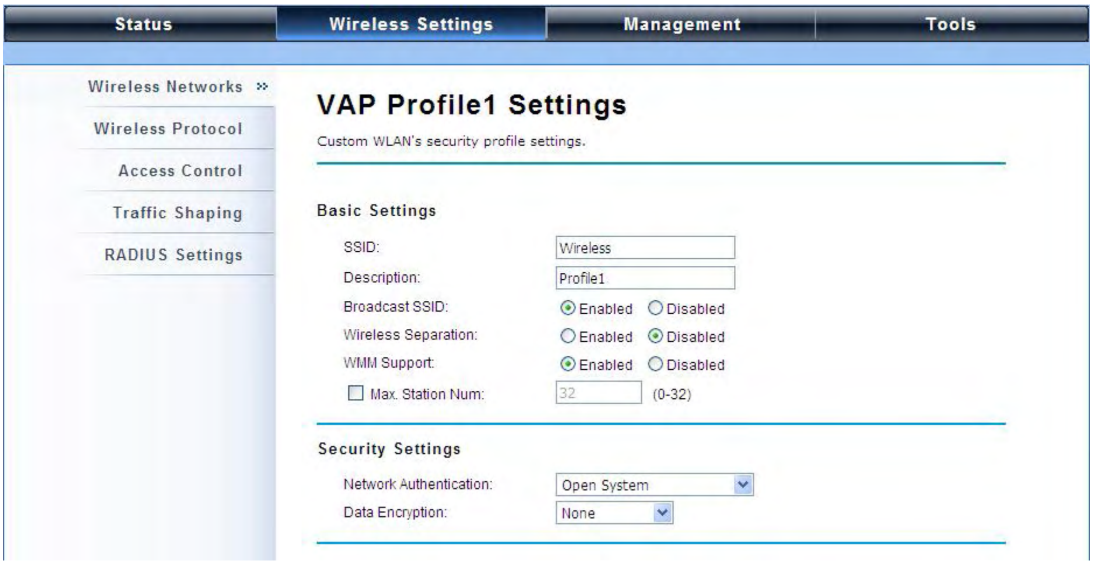
The IEEE 802.11n ZAC Access Point allows up to 8 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, you may check the **Enable** box of the profile and click on the profile (eg. Profile 2) to configure wireless and security settings. Hit **Apply** to active the profile.



Wireless Networks

Define each WLAN's attribute.

#	Enable	SSID	Security	VLAN ID	Description
1	☑	Wireless	Open System	0	Profile1
2	□	Wireless	Open System	0	Profile2
3	□	Wireless	Open System	0	Profile3
4	□	Wireless	Open System	0	Profile4
5	□	Wireless	Open System	0	Profile5
6	□	Wireless	Open System	0	Profile6
7	□	Wireless	Open System	0	Profile7
8	□	Wireless	Open System	0	Profile8
9	□	Wireless	Open System	0	Profile9
10	□	Wireless	Open System	0	Profile10



VAP Profile1 Settings

Custom WLAN's security profile settings.

Basic Settings

SSID: Wireless

Description: Profile1

Broadcast SSID: ● Enabled ○ Disabled

Wireless Separation: ○ Enabled ● Disabled

WMM Support: ● Enabled ○ Disabled

□ Max. Station Num: 32 (0-32)

Security Settings

Network Authentication: Open System

Data Encryption: None

- **Basic Setting**

SSID: This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and cannot exceed 32 characters.

Description: Name of the VAP profile

Broadcast SSID: In AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the IEEE 802.11n ZAC Access Point, so that malicious attack by some illegal STA could be avoided.

Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. By enabling "**Wireless Separation**" can prevent the communication among associated wireless clients.

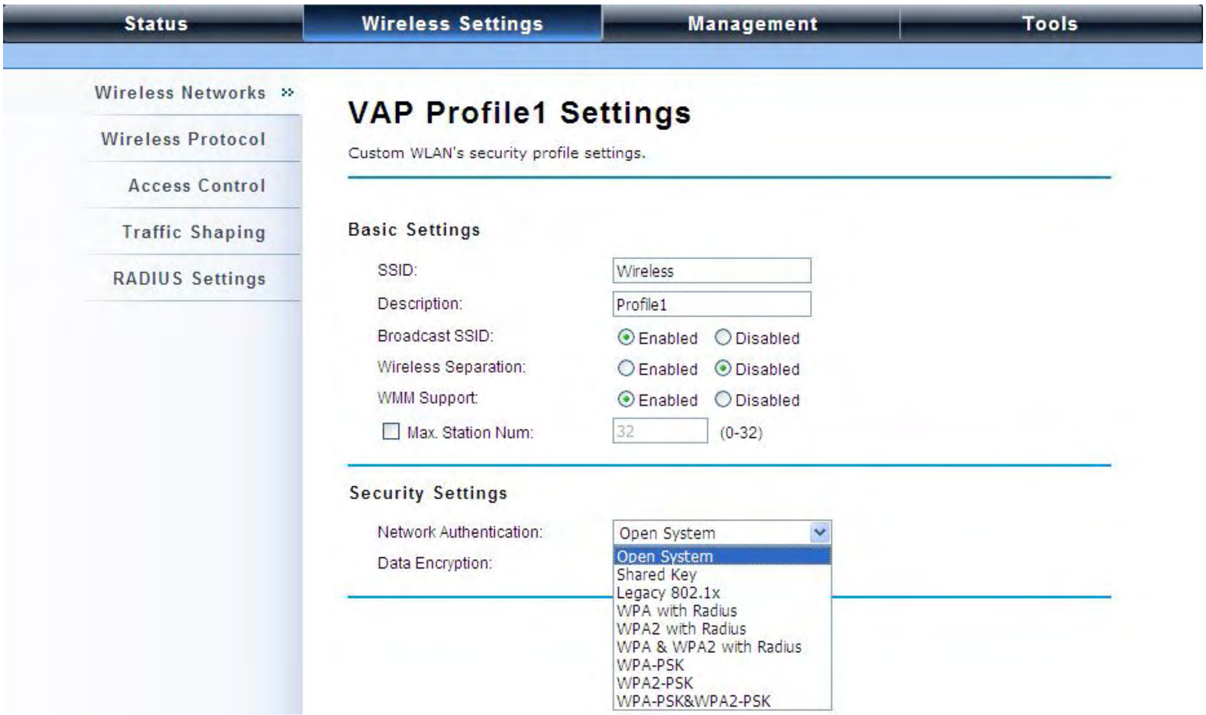
WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it. By default it is enabled and cannot be disabled in b/g/n mode.

Max. Station Number: By default the "**Max. Station Num**" the ZAC Access Point will only allow up to 32 wireless clients to associate with for better bandwidth for each client. You may tick the box and enter the preferable limits for maximum client association number.

- **Security Setting:**

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE

802.11a/n ZAC Access Point provides you with rock solid security settings.



VAP Profile1 Settings

Custom WLAN's security profile settings.

Basic Settings

SSID: Wireless

Description: Profile1

Broadcast SSID: ● Enabled ○ Disabled

Wireless Separation: ○ Enabled ● Disabled

WMM Support: ● Enabled ○ Disabled

□ Max. Station Num: 32 (0-32)

Security Settings

Network Authentication: Open System

Data Encryption:

- **Network Authentication**

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication (Not available in Bridge/AP Repeater mode).

Legacy 802.1x: It provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

WPA with RADIUS: Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. If it is selected, AES encryption and RADIUS server are required.

WPA&WPA2 with RADIUS: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

Note:

- If Radius relevant authentication type is selected, please go to **Wireless → Radius Settings** for further radius server configuration.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

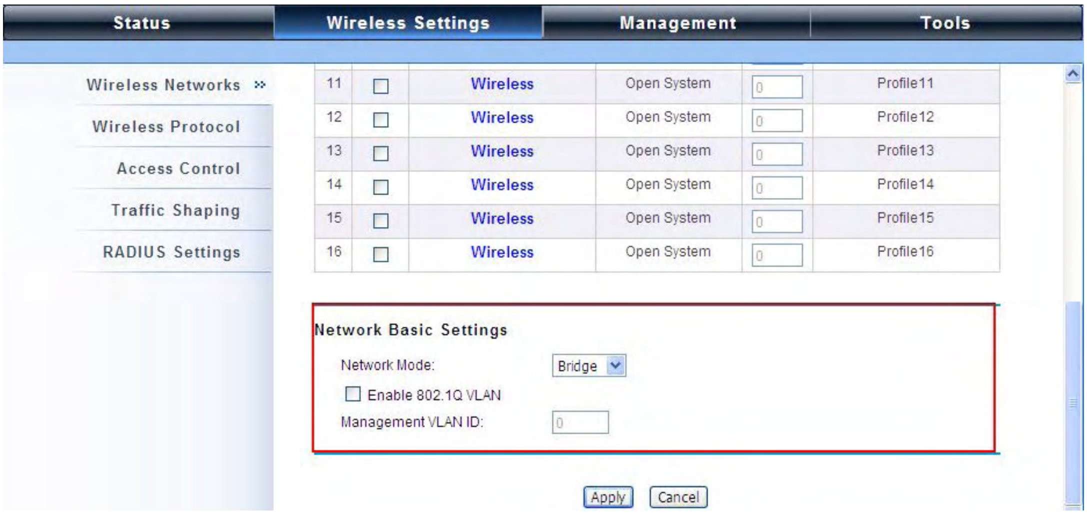
AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.

Note:

- We strongly recommend you enable wireless security on your network!
- Only the same Authentication, Data Encryption and Key among the IEEE 802.11n ZAC Access Point and wireless clients can the communication be established!

- **Network Basic Setting:**



11	□	Wireless	Open System	0	Profile11
12	□	Wireless	Open System	0	Profile12
13	□	Wireless	Open System	0	Profile13
14	□	Wireless	Open System	0	Profile14
15	□	Wireless	Open System	0	Profile15
16	□	Wireless	Open System	0	Profile16

Network Basic Settings

Network Mode: Bridge

□ Enable 802.1Q VLAN

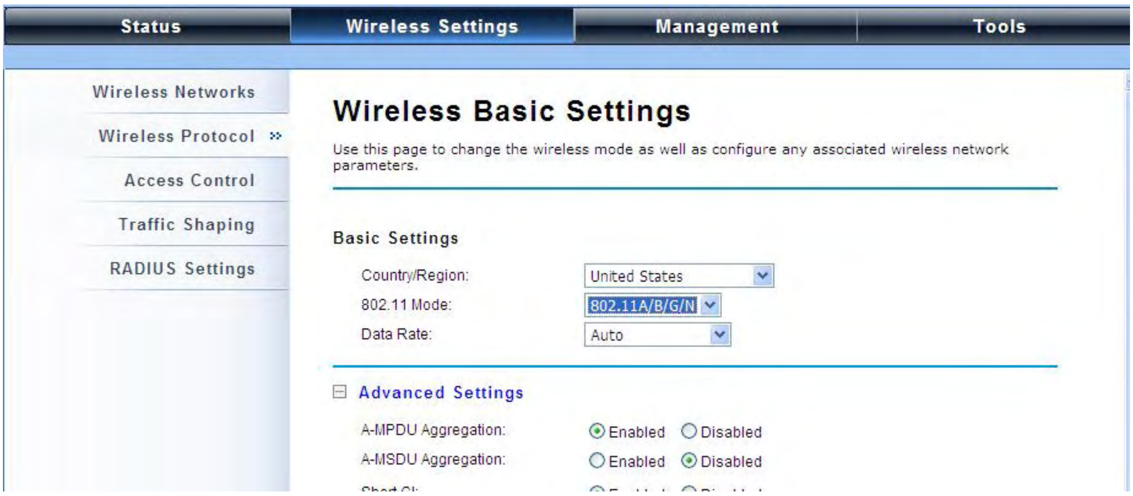
Management VLAN ID: 0

Network Mode: Specify the network mode. It includes **Bridge** and **Router**. When switch to Router mode, the LAN IP address for web page access will become 192.168.0.99.

Wireless Protocols

Allow the user to change 802.11 mode and other advanced parameters for the ZAC Access Point.

For the country region, FCC domain will support United States only.



Wireless Basic Settings

Use this page to change the wireless mode as well as configure any associated wireless network parameters.

Basic Settings

Country/Region: United States

802.11 Mode: 802.11A/B/G/N

Data Rate: Auto

⊟ Advanced Settings

A-MPDU Aggregation: ● Enabled ○ Disabled

A-MSDU Aggregation: ○ Enabled ● Disabled

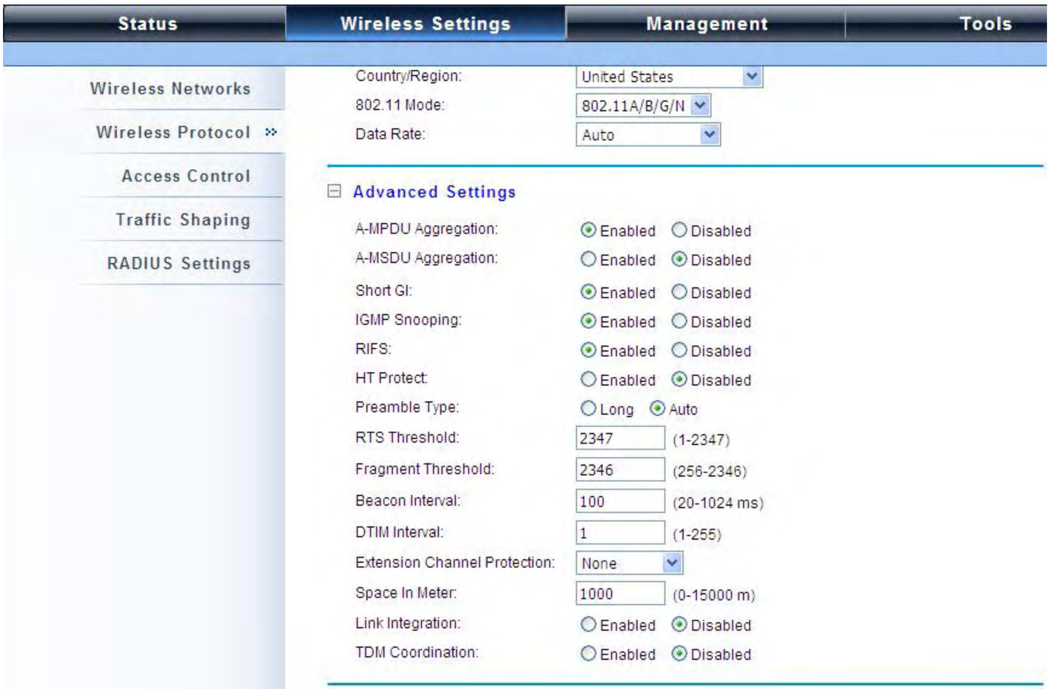
- **Basic Settings**

Country Region: The availability of some specific channels and/or operational frequency bands is country dependent. For FCC domain, the default country is **United States** only.

802.11 Mode: The IEEE 802.11n ZAC Access Point can communicate with wireless devices of 802.11b/g or 802.11b/g/n.

Data Rate: Usually "**Auto**" is preferred. Under this rate, the IEEE 802.11n ZAC Access Point will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance by fixing the data rate.

- **Advanced Settings**



Country/Region:	United States
802.11 Mode:	802.11A/B/G/N
Data Rate:	Auto

⊟ Advanced Settings

A-MPDU Aggregation:	● Enabled ○ Disabled
A-MSDU Aggregation:	○ Enabled ● Disabled
Short GI:	● Enabled ○ Disabled
IGMP Snooping:	● Enabled ○ Disabled
RIFS:	● Enabled ○ Disabled
HT Protect:	○ Enabled ● Disabled
Preamble Type:	○ Long ● Auto
RTS Threshold:	2347 (1-2347)
Fragment Threshold:	2346 (256-2346)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Extension Channel Protection:	None
Space In Meter:	1000 (0-15000 m)
Link Integration:	○ Enabled ● Disabled
TDM Coordination:	○ Enabled ● Disabled

A-MPDU/A-MSDU Aggregation: The data rate of your AP except wireless client mode could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

Short GI: Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

IGMP Snooping: IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

~~**RIFS**: RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency~~

HT Protect: Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

Preamble Type: It defines some details on the 802.11 physical layer. "**Long**" and "**Auto**" are available.

RTS Threshold: The IEEE 802.11n ZAC Access Point sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Fragmentation Threshold: Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Beacon Interval: Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

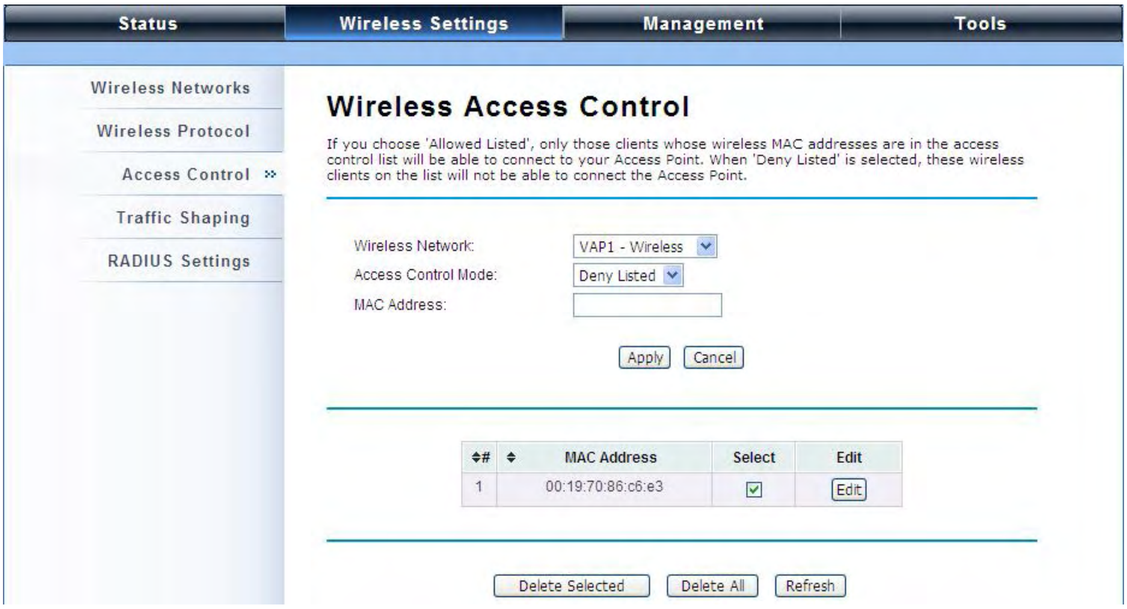
Channel Protection Mode: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Distance: To decrease the chances of data retransmission at long distance, the IEEE 802.11n ZAC Access Point can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

Access Control

The Access Control appoints the authority to wireless client on accessing IEEE 802.11n ZAC Access Point, thus a further security mechanism is provided. This function is available only under AP/Router mode.

Open “**Access Control**” in “**Wireless Settings**” as below.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Network: VAP1 - Wireless

Access Control Mode: Deny Listed

MAC Address:

#	MAC Address	Select	Edit
1	00:19:70:86:c6:e3	☑	Edit

- **Wireless Network:** Select the VAP network you would like to enable access control.
- **Access Control Mode**

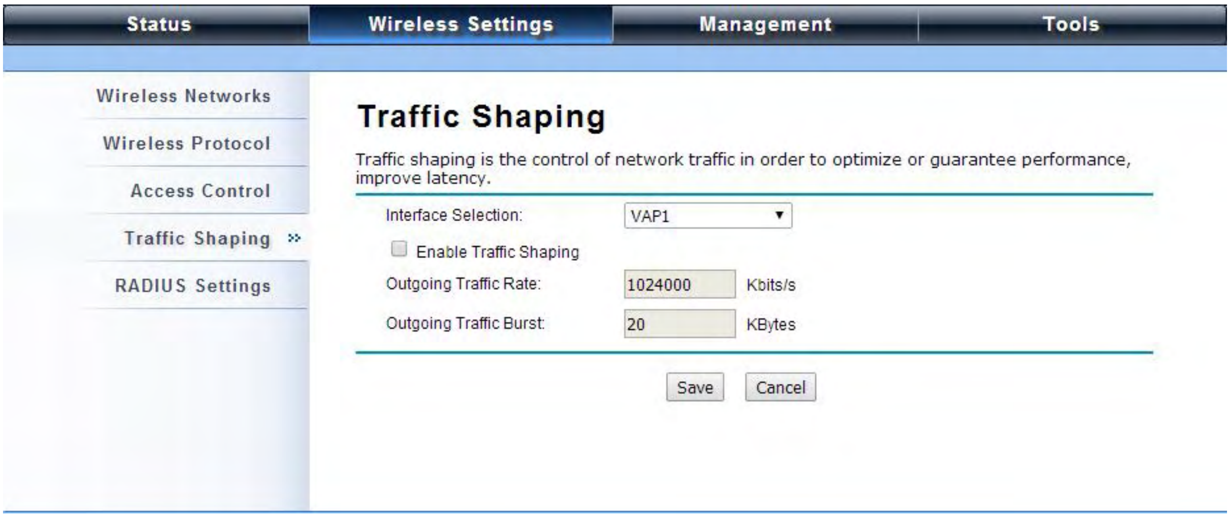
  If you select “**Allow Listed**”, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “**Deny Listed**” is selected, those wireless clients on the list will not be able to connect the AP.
- **MAC Address**

  Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.
- **Delete Selected/All**

  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click “**Delete Selected**” or “**Delete All**” to cancel that access control rule.

Traffic Shaping

It allows the administrator to manage the traffic flow to ensure optimal performance.



Traffic Shaping

Traffic shaping is the control of network traffic in order to optimize or guarantee performance, improve latency.

Interface Selection: VAP1

□ Enable Traffic Shaping

Outgoing Traffic Rate: 1024000 Kbits/s

Outgoing Traffic Burst: 20 KBytes

- **Enable Traffic Shaping**

  Check this box to control the overall bandwidth for a specific VAP network.

- **Interface Selection:** Select the VAP network you would like to enable traffic shaping.

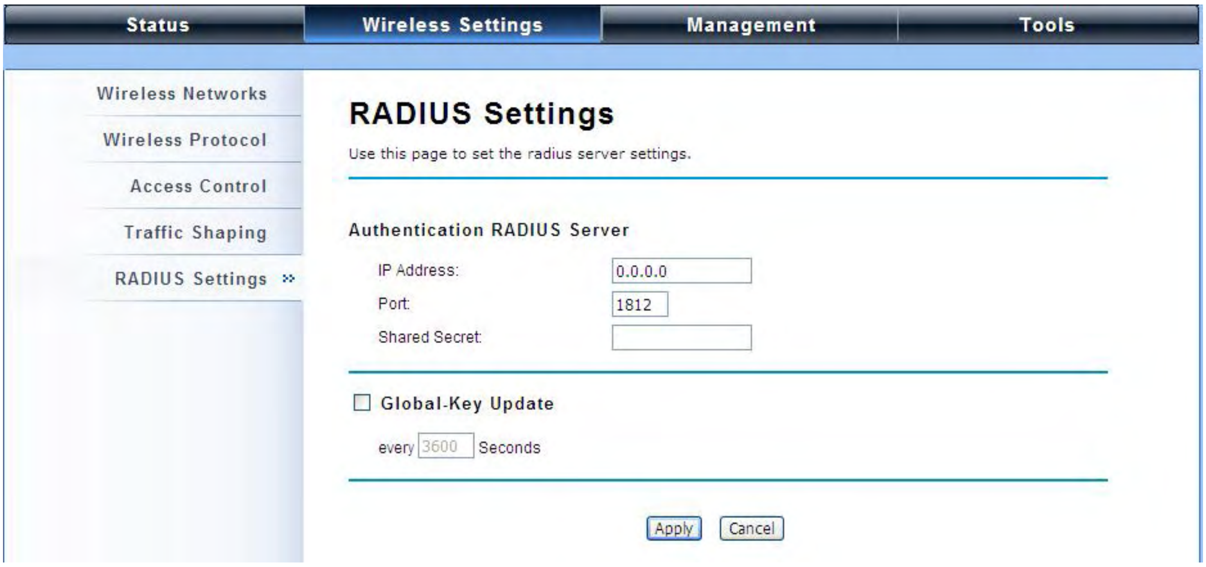
- **Outgoing Traffic Rate:** To specify maximum outgoing bandwidth to a certain rate in kbit/s.

  Outgoing Traffic Burst: To specify the buffer size for outgoing traffic that can be sent within a given unit of time. The suggested value is 20KBytes. You may just leave the default value there, and then the connection will be bound to the traffic shaping rule at all times. You may decrease it to smaller value if the incoming traffic limit is smaller.

Radius Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share. If 802.1X, WPA(2) is used, you need to configure radius settings.

Go to "**RADIUS Settings**" in "**Wireless Settings**" to make RADIUS configuration.



RADIUS Settings

Use this page to set the radius server settings.

Authentication RADIUS Server

IP Address: 0.0.0.0

Port: 1812

Shared Secret:

□ Global-Key Update

every 3600 Seconds

- **Authentication RADIUS Server**

  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

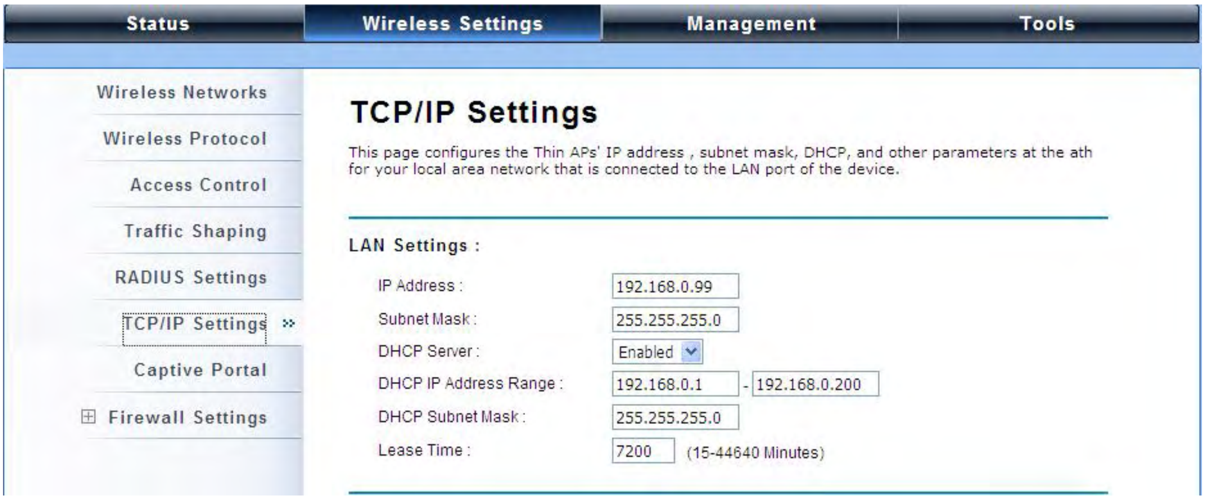
  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the IEEE 802.11n ZAC Access Point and RADIUS during authentication.

- **Global-Key Update**

  Check this option and specify the time interval between two global-key updates.   Default is 3600 seconds.

TCP/IP Settings

When the Router mode is activated, the **TCP/IP Settings** will show up in **Wireless Settings** for user to configure the TCP/IP for the ZAC-managed Access Point.



TCP/IP Settings

This page configures the Thin APs' IP address , subnet mask, DHCP, and other parameters at the ath for your local area network that is connected to the LAN port of the device.

LAN Settings :

IP Address : 192.168.0.99
Subnet Mask : 255.255.255.0
DHCP Server : Enabled
DHCP IP Address Range : 192.168.0.1 - 192.168.0.200
DHCP Subnet Mask : 255.255.255.0
Lease Time : 7200 (15-44640 Minutes)

- **LAN Settings:**

IP Address: Specify the IP address for the ZAC-managed Access Point.

Subnet Mask: Specify the Subnet mask for the ZAC-managed Access Point.

DHCP Server: Select to enable or disable DHCP server on the ZAC-managed Access Point.

DHCP IP Address Range: When the DHCP Server is enabled, users may specify DHCP IP Address Range for the ZAC-managed Access Point.

DHCP Subnet Mask: Specify the DHCP Subnet Mask for the ZAC-managed Access Point.

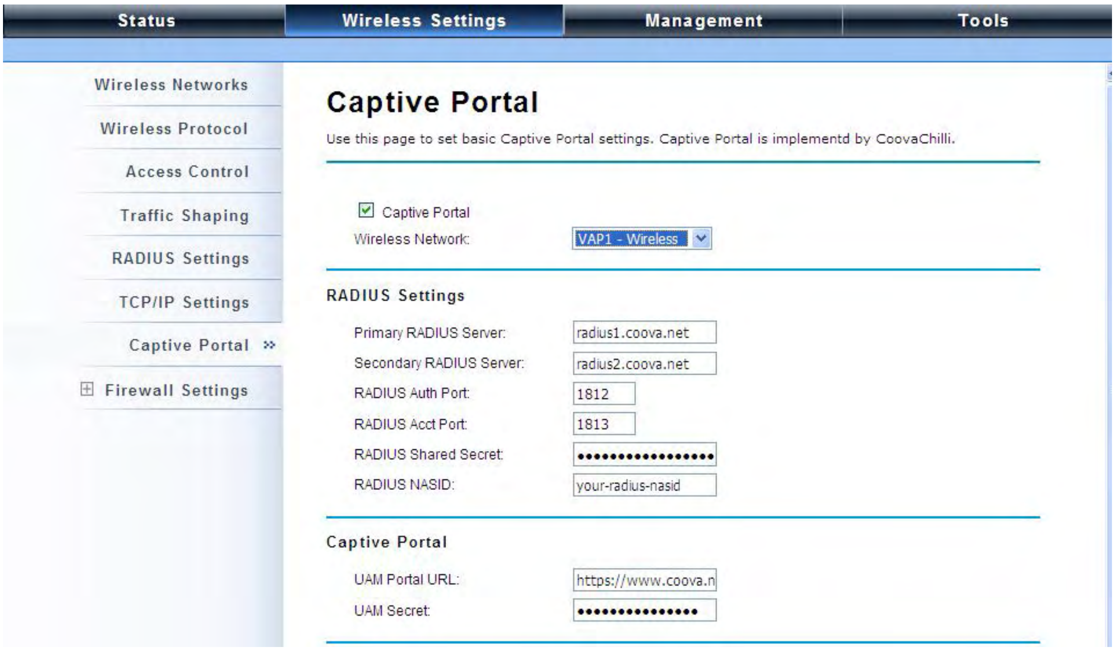
Lease Time: Specify the lease time (15-44640 minutes) for the ZAC-managed Access Point.

Note:

- For wireless clients who want to access the unit's web page in Router mode, please type the IP address here in the browser's address bar to enter the web page.

Captive Portal

Captive portal is a management which allows WLAN users to easily and securely access the Internet. Under Router mode, when captive portal is enabled, the IEEE 802.11n ZAC Access Point will redirect the client to go to an authentication web page before browsing Internet web pages. Captive portals are used on most Wi-Fi hotspots networks. Therefore, to use captive portal, you need to find the service providers that have the additional services needed to make captive portal work.



Captive Portal

Use this page to set basic Captive Portal settings. Captive Portal is implementd by CoovaChilli.

☑ Captive Portal

Wireless Network: VAP1 - Wireless

RADIUS Settings

Primary RADIUS Server: radius1.coova.net

Secondary RADIUS Server: radius2.coova.net

RADIUS Auth Port: 1812

RADIUS Acct Port: 1813

RADIUS Shared Secret: ●●●●●●●●●●●●●●●●

RADIUS NASID: your-radius-nasid

Captive Portal

UAM Portal URL: https://www.coova.n

UAM Secret: ●●●●●●●●●●●●●●●

To enable Captive Portal, check “**Captive Portal**” and select the VAP network needed for captive portal.

- **Radius Settings**

  Primary Radius Server: Enter the name or IP address of the primary radius server

  Secondary Radius Server: Enter the name or IP address of the primary radius server if any.

  Radius Auth Port: Enter the port number for authentication

  Radius Acct Port: Enter the port number for billing

  Radius Shared Secret: Enter the secret key of the radius server

  Radius NAS ID: Enter the name of the radius server if any

- **Radius Administrative-User:**

  Radius Admin Username: Enter the username of the Radius Administrator

  Radius Admin Password: Enter the password of the Radius Administrator

- **Captive Portal**

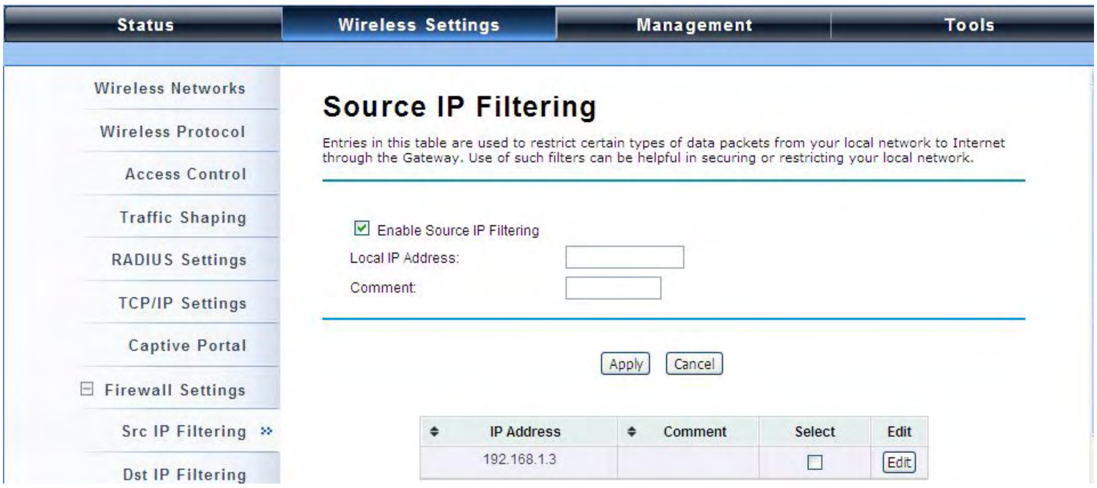
  UAM Portal URL: Enter the address of the UAM portal server

  UAM Secret: Enter the secret password between the redirect URL and the Hotspot.

Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The IEEE 802.11n ZAC Access Point has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under **Router** Mode.

- **Source IP Filtering:**



Source IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable Source IP Filtering

Local IP Address:

Comment:

IP Address	Comment	Select	Edit
192.168.1.3		□	Edit

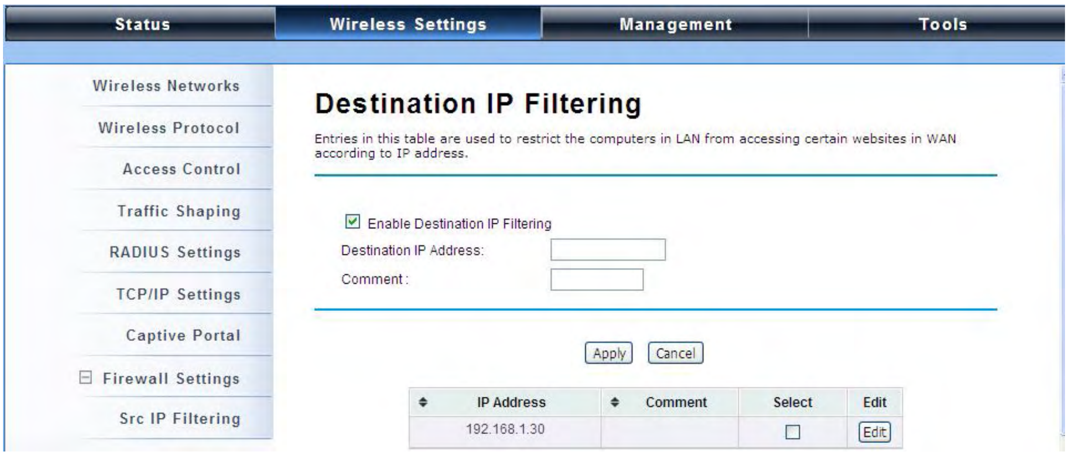
You may create and activate a rule that filters a packet based on the source IP address from your local network to Internet. Check "**Enable Source IP Filtering**" to activate rule.

Local IP Address: Enter the IP address you would like to restrict.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Destination IP Filtering:**



Destination IP Filtering

Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.

☑ Enable Destination IP Filtering

Destination IP Address:

Comment:

IP Address	Comment	Select	Edit
192.168.1.30		□	Edit

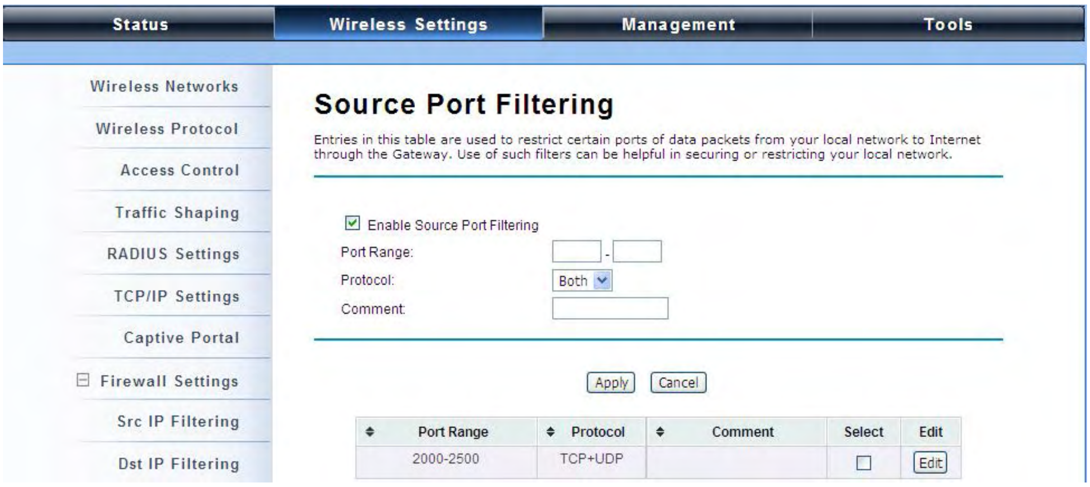
You may create and activate a rule that filters a packet based on the destination IP address to restrict the local computers from accessing certain websites. Check "**Enable Destination IP Filtering**" to activate rule.

<u>Destination IP Address</u>: Enter the IP address to be restricted.

<u>Comment</u>: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated destination IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Source Port Filtering:**



Source Port Filtering

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable Source Port Filtering

Port Range: -

Protocol: Both

Comment:

Port Range	Protocol	Comment	Select	Edit
2000-2500	TCP+UDP		□	Edit

You may create and activate a rule that filters a packet based on the source port from your local network to Internet. Check "**Enable Source Port Filtering**" to activate rule.

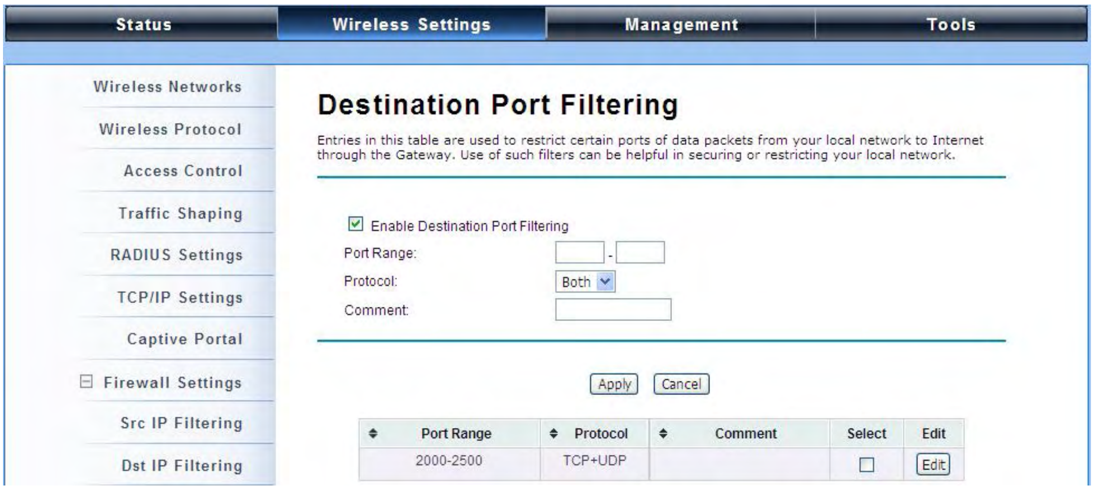
<u>Port Range</u>: Enter the port range you would like to restrict.

<u>Protocol</u>: Select port protocol: **Both**, **TCP**, **UDP**.

<u>Comment</u>: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the restricted source ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Destination Port Filtering:**



Destination Port Filtering

Entries in this table are used to restrict certain ports of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable Destination Port Filtering

Port Range: -

Protocol: Both

Comment:

Port Range	Protocol	Comment	Select	Edit
2000-2500	TCP+UDP		□	Edit

You may create and activate a rule that filters a packet based on the destination port from your local network to Internet. Check "**Enable Destination Port Filtering**" to activate rule.

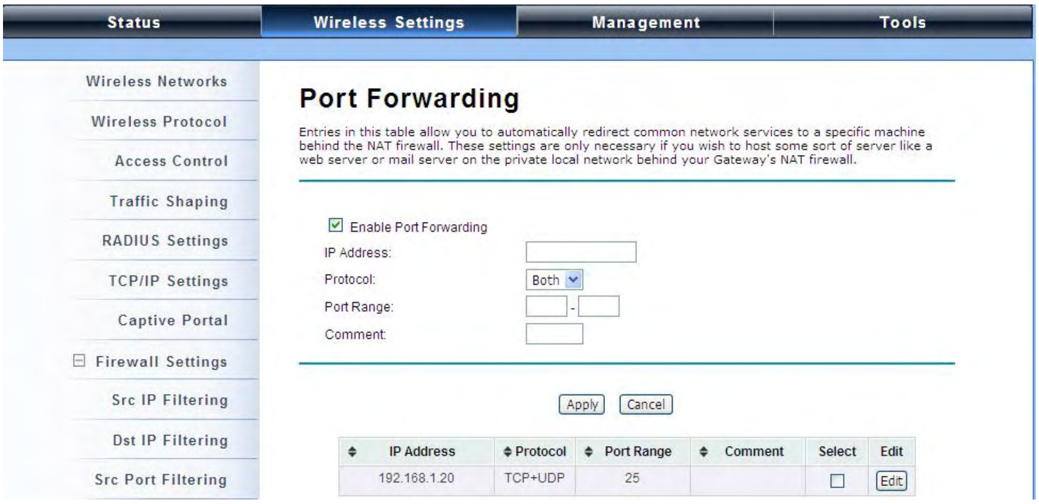
Port Range: Enter the port range you would like to restrict.

Protocol: Select port protocol: **Both**, **TCP**, **UDP**.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the restricted destination ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Port Forwarding:**



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☑ Enable Port Forwarding

IP Address:

Protocol: Both

Port Range: -

Comment:

IP Address	Protocol	Port Range	Comment	Select	Edit
192.168.1.20	TCP+UDP	25		□	Edit

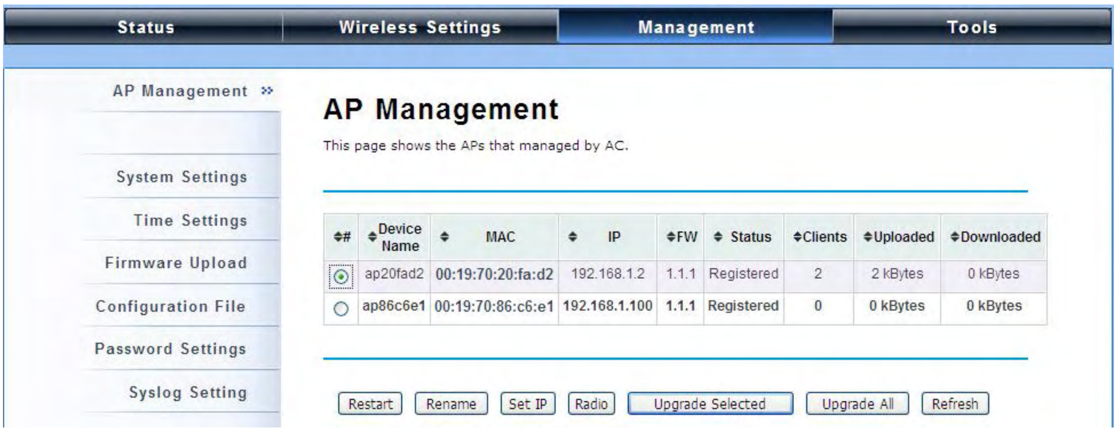
The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind IEEE 802.11n Wireless ZAC Access Point's NAT firewall.

Management

The IEEE 802.11n ZAC Access Points can manage up to 20 ZAC-managed APs. The ZAC Access Point provides thin AP management for editing the ZAC-managed AP settings, upgrading the firmware and monitoring, etc.

AP Management

AP Management allows you to configure and upgrade the ZAC-managed APs. Select the VAP-managed AP you would like to specifically configure.



AP Management

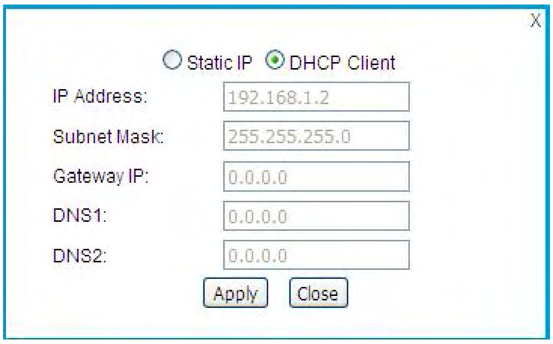
This page shows the APs that managed by AC.

#	Device Name	MAC	IP	FW	Status	Clients	Uploaded	Downloaded
●	ap20fad2	00:19:70:20:fa:d2	192.168.1.2	1.1.1	Registered	2	2 kBytes	0 kBytes
○	ap86c6e1	00:19:70:86:c6:e1	192.168.1.100	1.1.1	Registered	0	0 kBytes	0 kBytes

Restart: Restart the selected ZAC-managed AP.

Rename: Rename for the selected ZAC-managed AP.

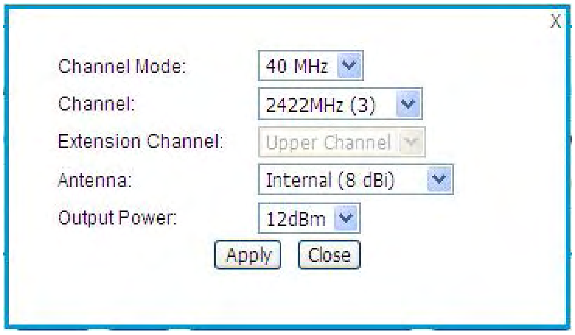
Set IP: Assign a static IP address for the selected ZAC-managed AP or obtain the IP address from ZAC Access Point in AC mode. Default is DHCP client.



○ Static IP ● DHCP Client

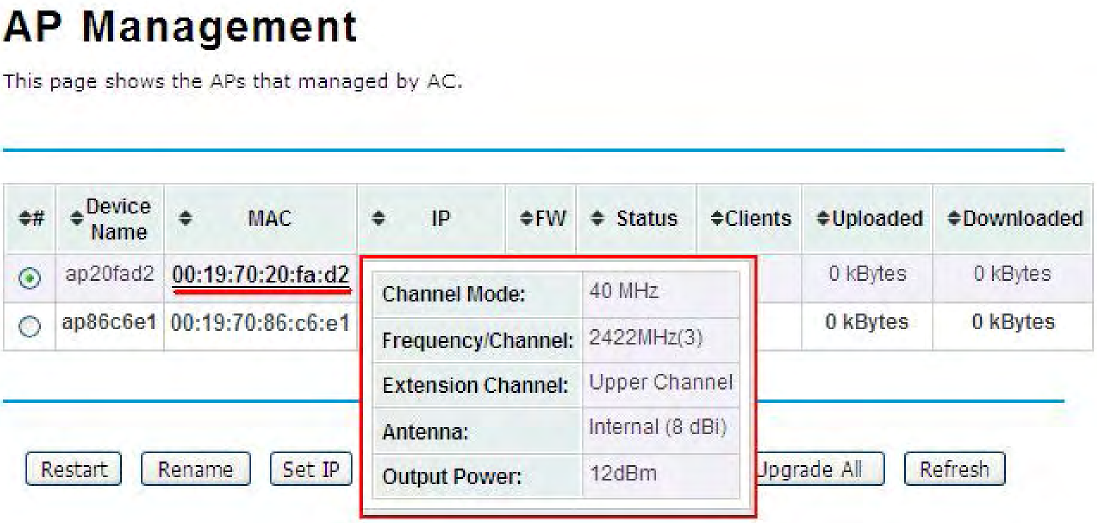
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway IP:	0.0.0.0
DNS1:	0.0.0.0
DNS2:	0.0.0.0

Radio: To display the current radio settings such as channel bandwidth, operating channel, antenna and output power for the selected ZAC-managed Access Point.



Channel Mode:	40 MHz
Channel:	2422MHz (3)
Extension Channel:	Upper Channel
Antenna:	Internal (8 dBi)
Output Power:	12dBm

From the AP Management list, move the mouse cursor to the MAC address of the selected ZAC-managed AP the screen will pop up radio configuration information.



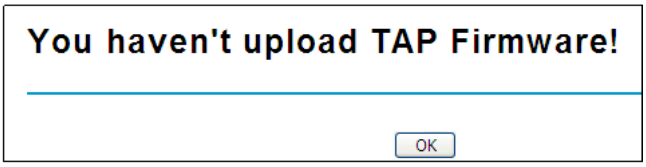
AP Management

This page shows the APs that managed by AC.

#	Device Name	MAC	IP	FW	Status	Clients	Uploaded	Downloaded
●	ap20fad2	00:19:70:20:fa:d2					0 kBytes	0 kBytes
○	ap86c6e1	00:19:70:86:c6:e1					0 kBytes	0 kBytes

Channel Mode:	40 MHz
Frequency/Channel:	2422MHz(3)
Extension Channel:	Upper Channel
Antenna:	Internal (8 dBi)
Output Power:	12dBm

Upgrade Selected: Upgrade firmware for the selected ZAC-managed AP. Note that you need to upload the firmware file into the ZAC Access Point in AC mode prior to firmware upgrade, otherwise a window will pop up saying TAP firmware hasn't been uploaded.



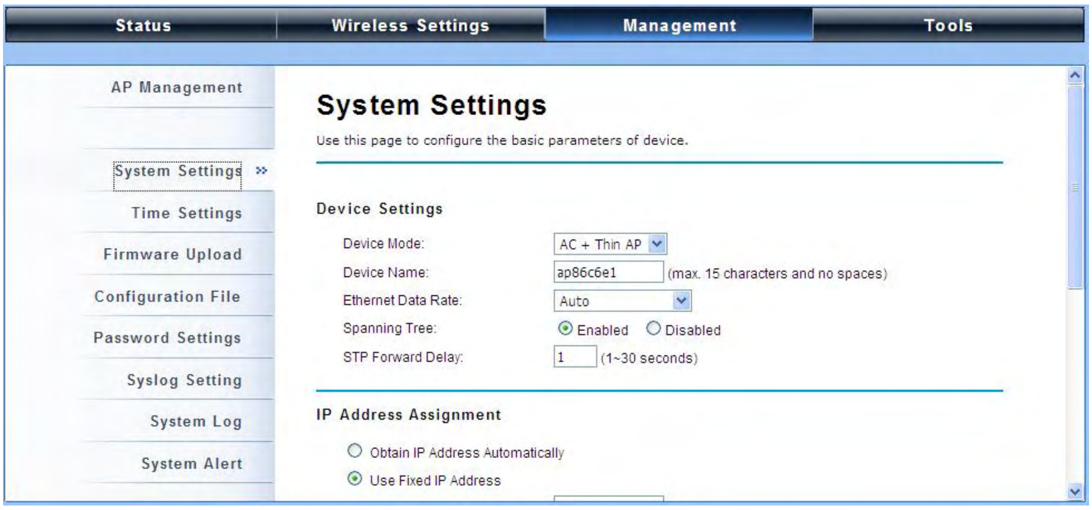
You haven't upload TAP Firmware!

Upgrade All: Click to upgrade all the ZAC-managed APs simultaneously.

Refresh: Refresh the AP management list manually.

System Settings

Allows you to configure device and IP settings for the ZAC Access Point in AC mode.



System Settings

Use this page to configure the basic parameters of device.

Device Settings

Device Mode: AC + Thin AP

Device Name: ap86c6e1 (max. 15 characters and no spaces)

Ethernet Data Rate: Auto

Spanning Tree: ● Enabled ○ Disabled

STP Forward Delay: 1 (1~30 seconds)

IP Address Assignment

○ Obtain IP Address Automatically

● Use Fixed IP Address

- **Device Settings:**

Device Mode: Three modes are provided: **AC+Thin AP**, **Thin AP**, **FAT AP**. Select AC+Thin AP to have the device act as virtual access controller to manage other ZAC-managed APs on your network. Select "Thin AP" to have the ZAC Access Point managed by the ZAC AP in AC mode. Select FAT AP to perform as a standalone AP, neither managing nor managed by other ZAC APs.

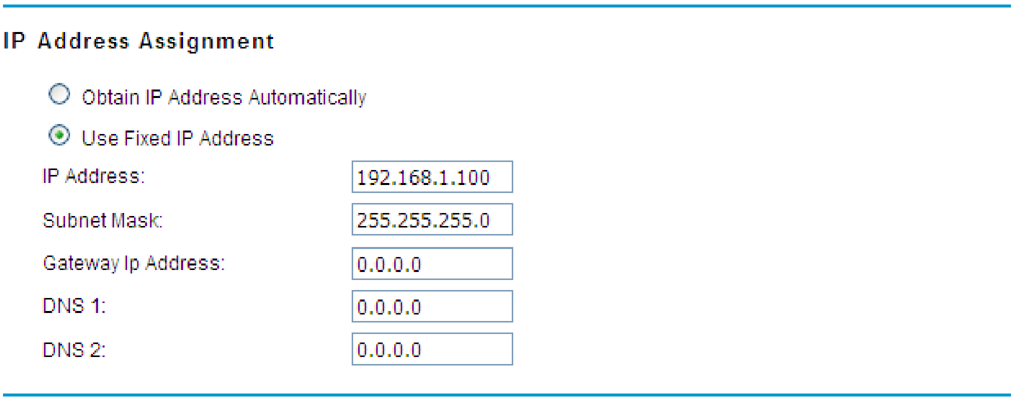
Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Ethernet Data Rate: Specify the transmission rate of data for Ethernet. Default is **Auto**.

Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

STP Forward Delay: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

- **IP Address Assignment:**



IP Address Assignment

○ Obtain IP Address Automatically

● Use Fixed IP Address

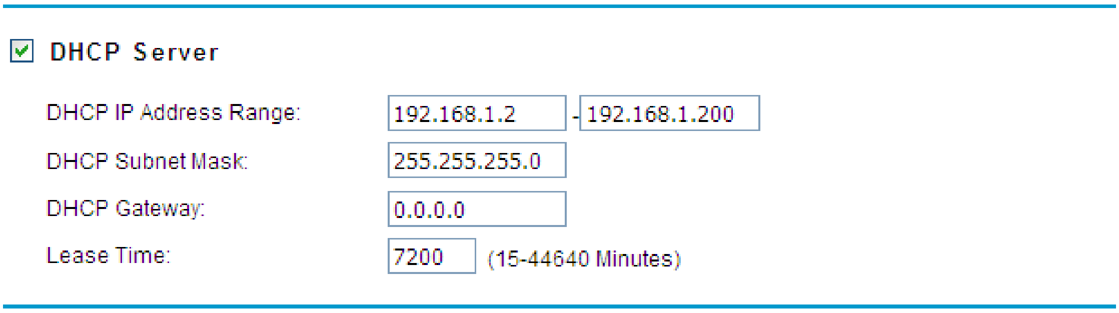
IP Address:	192.168.1.100
Subnet Mask:	255.255.255.0
Gateway Ip Address:	0.0.0.0
DNS 1:	0.0.0.0
DNS 2:	0.0.0.0

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the IEEE 802.11n ZAC Access Pioint is able to obtain IP settings automatically from the DHCP server.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the ZAC Access Point manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

- **DHCP Server**

The ZAC Access Point in AC mode can perform a DHCP server to assign IP address to the ZAC-managed APs. Default is enabled.



☑ DHCP Server

DHCP IP Address Range:	192.168.1.2 - 192.168.1.200
DHCP Subnet Mask:	255.255.255.0
DHCP Gateway:	0.0.0.0
Lease Time:	7200 (15-44640 Minutes)

DHCP IP Address Range: Specify the IP range.

DHCP Subnet Mask: Specify the DHCP Subnet Mask.

DHCP Gateway: Specify the gateway address.

Lease Time: Specify the DHCP lease time.