

# **IEEE 802.11 b/g/n Outdoor Wireless CPE/ IEEE 802.11 a/n Outdoor 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

Copyright © 2014 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

## 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:

---

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

---



### Warning:

---

λ 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 keep 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。

此產品為 HiNA 設備

## 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 ARISING 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.**

DO NOT dispose any component of product package, if you need any serves please contacting with our service centers or local retailer. You can decrease environmental impact by right methods and procedures. If you like to dispose the product or any accessory, please contact your nearest disposal manufacturers/recycle company. If you have any maintenance inquiry, please contacting with our service centers or local retailer, this will extend the life time of 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

<b>Chapter 1 Introduction</b> .....	<b>10</b>
<b>Introduction</b> .....	<b>10</b>
<b>Key Features</b> .....	<b>10</b>
<b>Hardware Overview</b> .....	<b>11</b>
<b>Front View</b> .....	<b>11</b>
<b>Back View</b> .....	<b>11</b>
<b>Inside the Bottom Cover</b> .....	<b>12</b>
LED Indicators .....	<b>12</b>
<b>Typical Management Scenario</b> .....	<b>13</b>
<b>Hardware Installation</b> .....	<b>14</b>
<b>Preparation before Installation</b> .....	<b>14</b>
<b>Professional Installation Required</b> .....	<b>14</b>
<b>Safety Precautions</b> .....	<b>14</b>
<b>Installation Precautions</b> .....	<b>15</b>
<b>Product Package</b> .....	<b>15</b>
Pole Mounting Ring.....	<b>16</b>
Ferrite Suppression Core .....	<b>16</b>
24VDC Power Cord & PoE Injector .....	<b>16</b>
<b>Hardware Installation</b> .....	<b>17</b>
<b>Connect up</b> .....	<b>17</b>
<b>Using the Grounding Wire</b> .....	<b>18</b>
<b>Mount the AP on a Pole</b> .....	<b>19</b>
<b>Power Up</b> .....	<b>20</b>
<b>Connect to the Access Point</b> .....	<b>21</b>
<b>Connect to the Access Point</b> .....	<b>21</b>
<b>Chapter 2 Quick Setup Tutorial</b> .....	<b>24</b>
<b>Access the Web Configurator</b> .....	<b>24</b>

Configure the AC+Thin AP mode .....	26
<b>Chapter 3 Navigate the Web Configurator .....</b>	<b>40</b>
<b>Virtual AC+Thin AP Mode .....</b>	<b>40</b>
<b>Status .....</b>	<b>40</b>
View Basic Information.....	40
View Managed APs .....	40
View Wireless Users .....	41
View DHCP Client Table.....	41
<b>Wireless Settings.....</b>	<b>42</b>
Wireless Networks (VAP Profiles Settings) .....	42
Wireless Protocols .....	46
Access Control .....	48
Traffic Shaping .....	49
Radius Settings.....	50
TCP/IP Settings .....	51
Captive Portal .....	52
Firewall Settings.....	54
<b>Management .....</b>	<b>57</b>
AP Management .....	57
System Settings .....	59
Time Settings .....	61
Firmware Upgrade .....	61
Backup/ Retrieve Settings .....	62
Restore Factory Default Settings.....	62
Reboot.....	63
Password Settings .....	64
Syslog Setting:.....	64
System Log:.....	65
System Alert:.....	66

<b>Tools</b> .....	<b>66</b>
Ping .....	66
Trace Route .....	67
<b>Thin AP Mode</b> .....	<b>68</b>
<b>Information</b> .....	<b>68</b>
<b>Basic Settings</b> .....	<b>68</b>
<b>FAT AP Mode</b> .....	<b>70</b>
<b>Status</b> .....	<b>70</b>
View Basic Information .....	70
View Association List.....	70
View Network Flow Statistics .....	71
View ARP Table.....	72
View Bridge Table .....	72
View Active DHCP Client Table.....	72
View Network Activities .....	73
<b>System</b> .....	<b>74</b>
Basic System Settings.....	74
TCP/IP Settings .....	75
Time Settings .....	77
RADIUS Settings .....	78
Firewall Settings.....	79
UDP Pass Through .....	82
DMZ:.....	82
<b>Wireless</b> .....	<b>83</b>
VAP Profile Settings .....	85
VLAN .....	89
Advanced Settings .....	89
Access Control .....	92
Traffic Shaping.....	93



Captive Portal .....	94
WDS Settings.....	96
<b>Management .....</b>	<b>97</b>
Password .....	97
Upgrade Firmware .....	97
Backup/ Retrieve Settings .....	98
Restore Factory Default Settings.....	98
Reboot.....	99
Remote Management.....	99
SNMP Management.....	100
Certificate Settings .....	102
<b>Tools.....</b>	<b>103</b>
System Log.....	103
Ping Watch Dog .....	103
<b>Appendix A. ASCII .....</b>	<b>105</b>
<b>Appendix B. Specification .....</b>	<b>107</b>

# 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

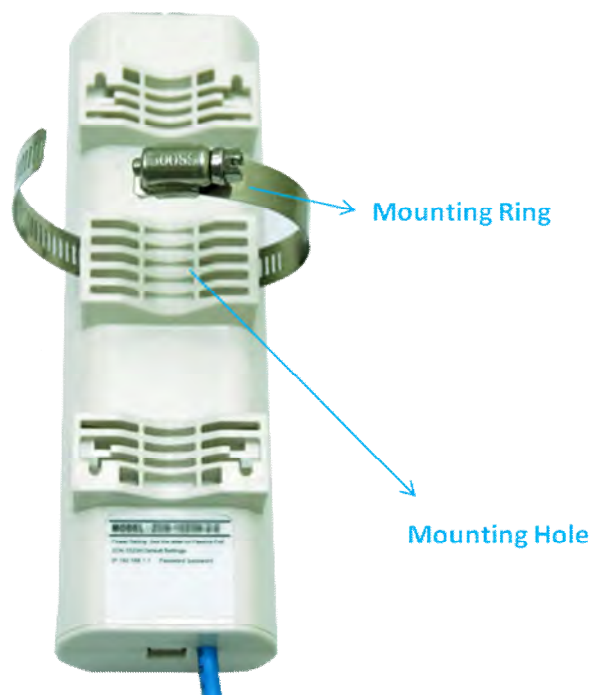
- λ Centralized configuration control for your network
- λ Compliant with IEEE 802.11n standard
- λ Support passive PoE supplied with 24V.
- λ High reliable watertight housing endures almost any harsh environments
- λ Three management modes including AC, AC+Thin AP, Thin AP and Fat AP.
- λ Four wireless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

# Hardware Overview

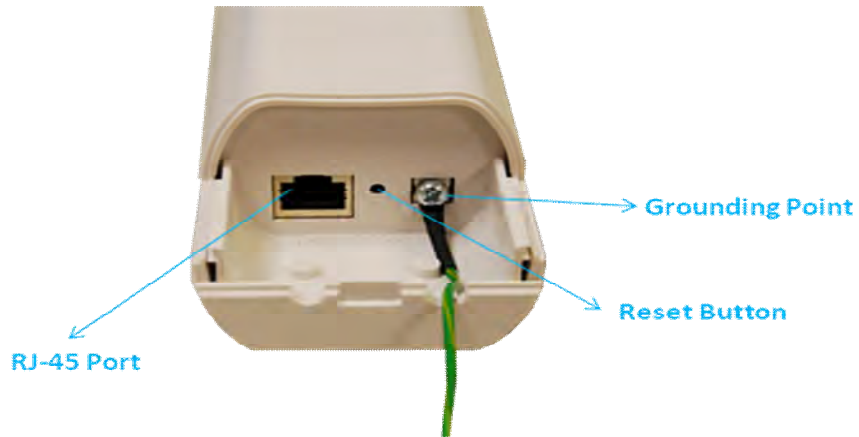
## Front View



## Back View



## Inside the Bottom Cover

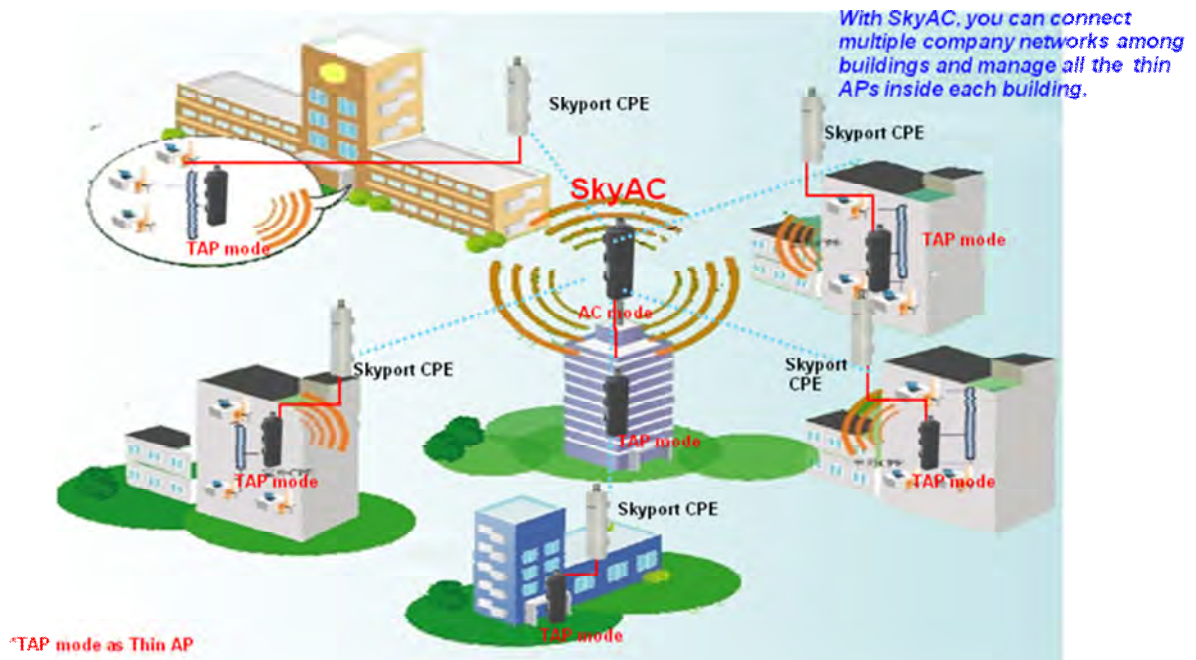


## LED Indicators

LED	COLOR	STATUS	DESCRIPTION
<b>PWR</b>	Green	On	The device is powered on
		Off	The device is not receiving power
<b>LAN</b>	Green	On	The device has the Ethernet connection
		Off	The device has no Ethernet connection
		Blinking	Transmitting/receiving Ethernet packets
<b>WLAN</b>	Green	On	The WLAN is active
		Off	The WLAN is inactive
		Blinking	Transmitting/receiving wireless packets
<b>Signal*3</b>	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 finds 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 WARRANTY.**
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.

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



### Note:

---

λ Product CD contains Quick Installation Guide and User Manual.

---

## Pole Mounting Ring



## Ferrite Suppression Core



## 24VDC Power Cord & PoE Injector



### **Warning:**

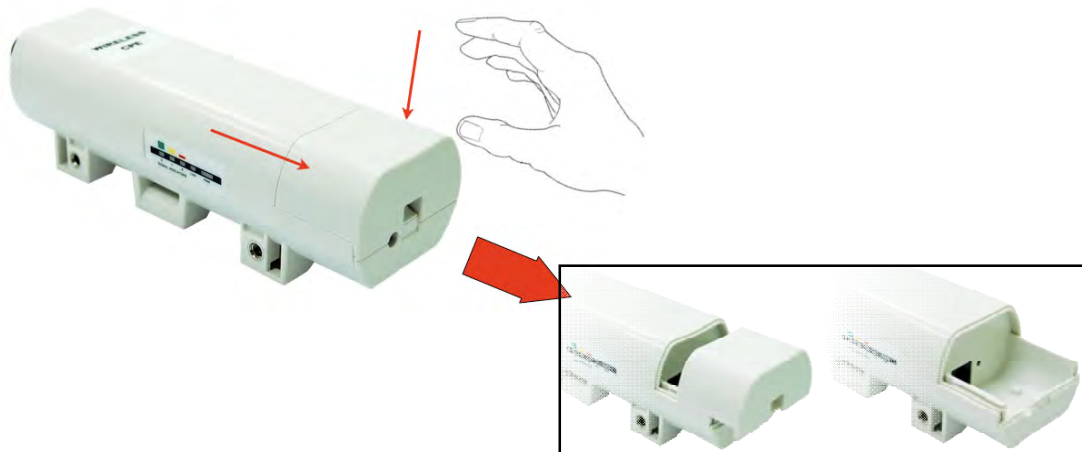
- 
- λ Users MUST use the “Power cord & PoE Injector” shipped in the box with the IEEE 802.11n Wireless Access Point. Use of other options will likely cause damage to the IEEE 802.11n Wireless Access Point..
-



# 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.



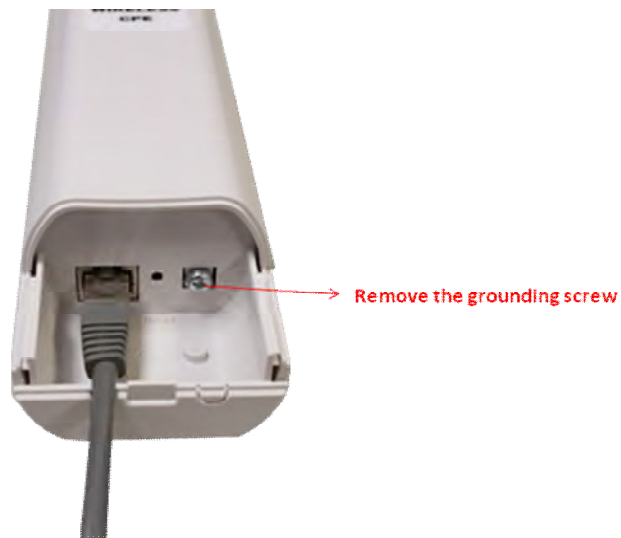
3. Slide the cover back and press down the lock button to seal the bottom of the ZAC Access Point.



## 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.



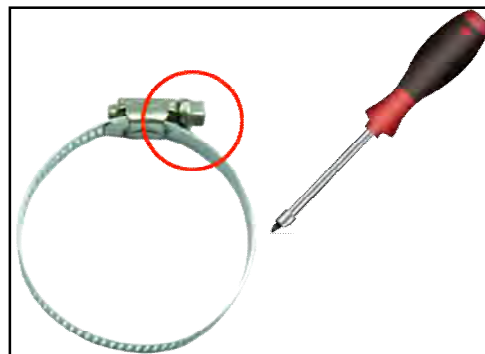
2. Put the grounding wire on the grounding point at the bottom of the ZAC Access Point. Then screw the grounding wire to tighten up.



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:**

---

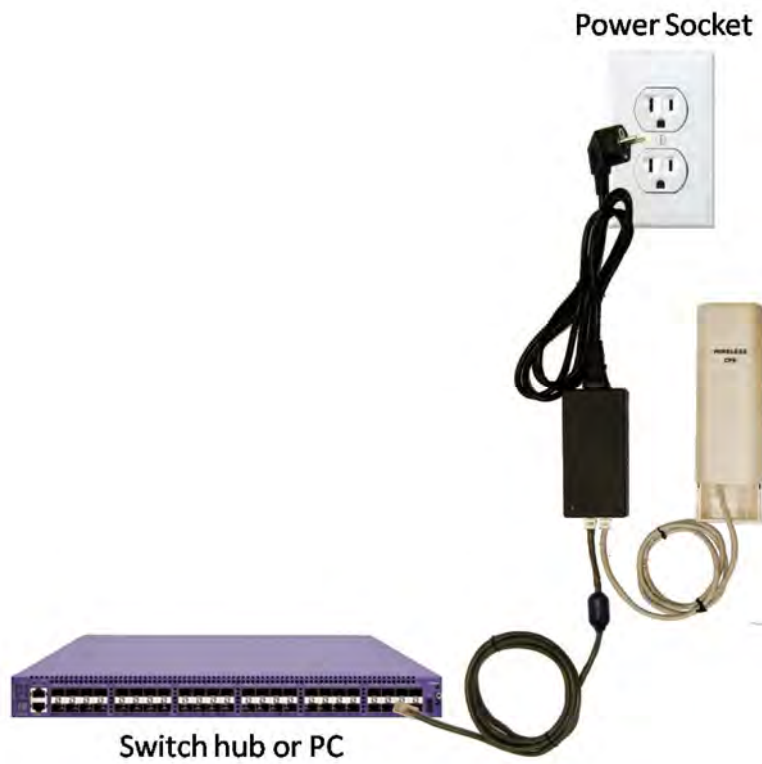
λ The ferrite is professionally installed and a shrink wrap has been put around the ferrite so the users CAN'T take the ferrite off.

---

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.

- λ 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);
- λ 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.



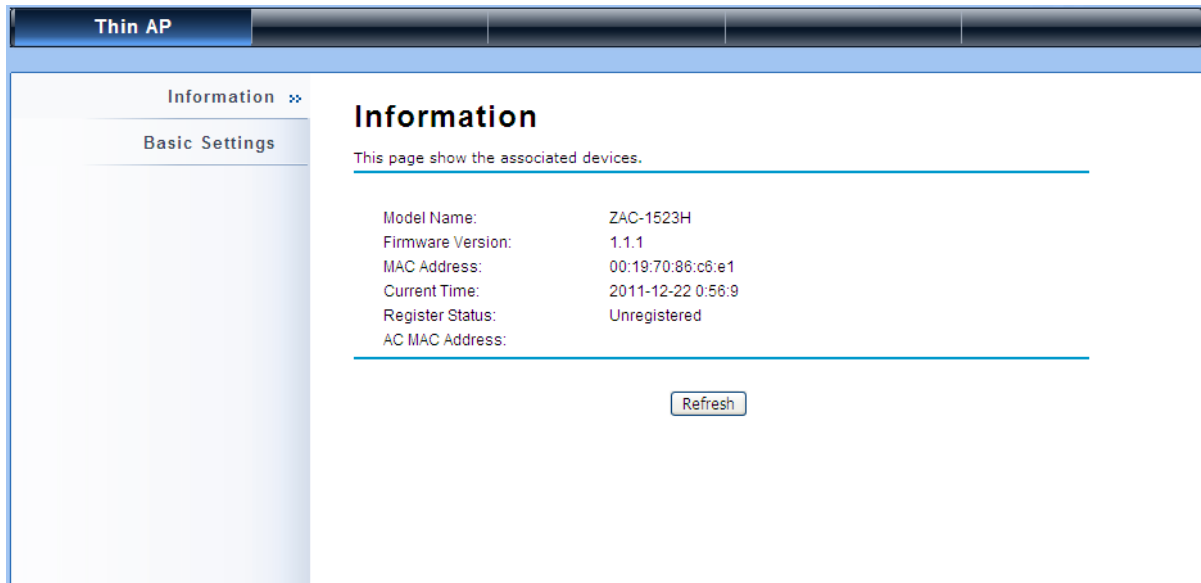
Wireless Broadband Access Point

Name

Password



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



 **Note:**

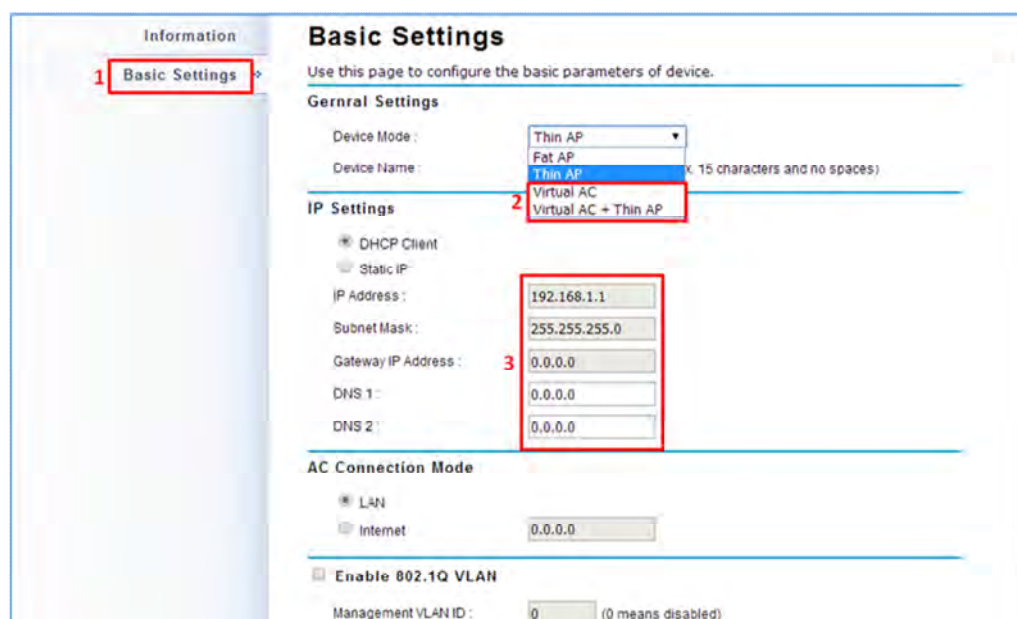
- 
- λ The username and password are case-sensitive, and the password should be no more than 19 characters!
-

# Configure the AC+Thin AP mode

The ZAC Access Point provides 4 operation modes: “Thin AP”, “Virtual AC”, “Virtual 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.



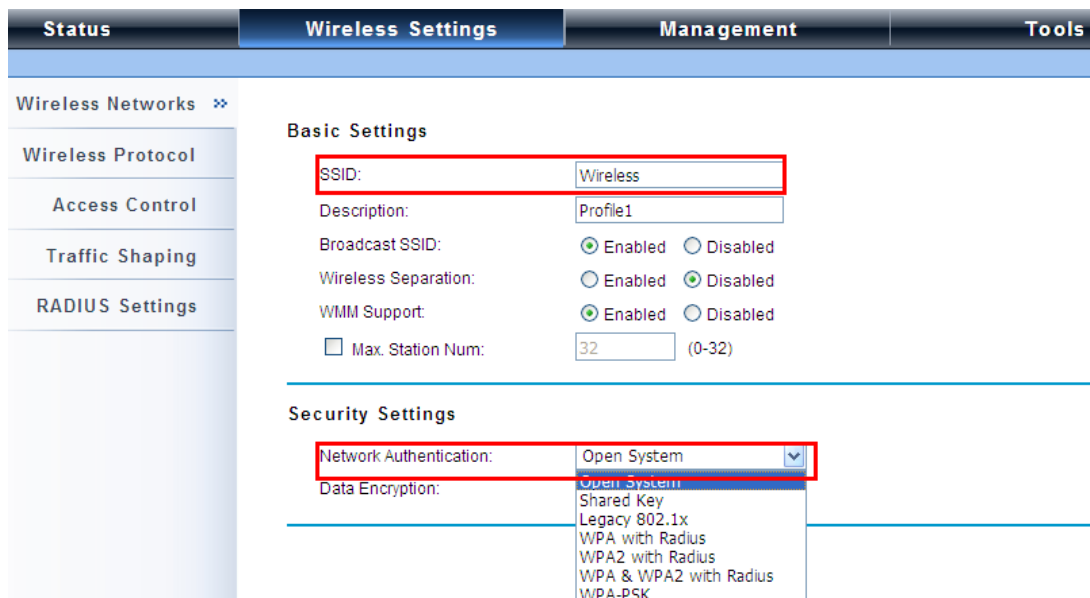
 **Note:**

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

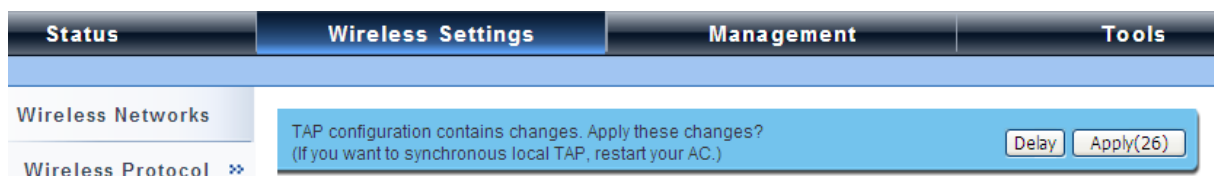
 **Note:**

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

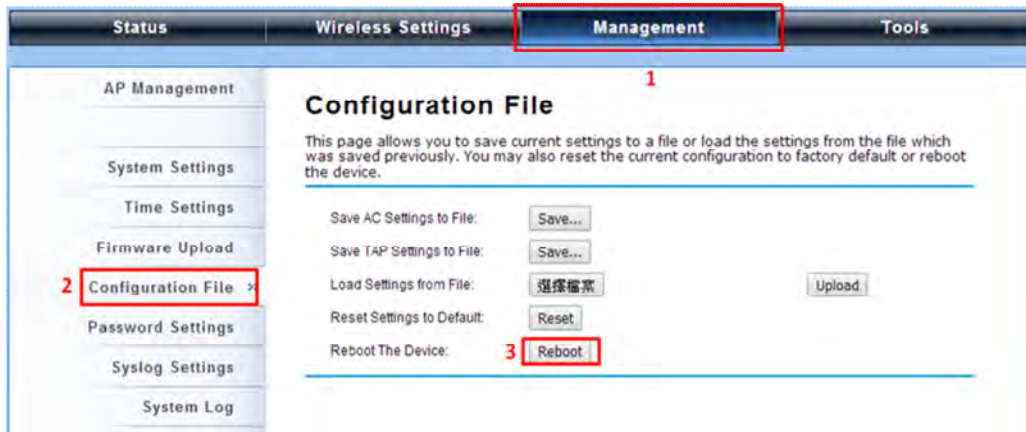
For Virtual Controller + Thin AP mode, if you need to configure the wireless settings for the ZAC Access Point especially SSID and encryption method, go to **Wireless Settings > Wireless Networks** and click on #1 **Wireless** SSID for configuration. After the configuration is made, click **Save** to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



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.



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.



## 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.



## 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.

Management

## 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
○	apeeeeeee	00:60:b3:ee:ee:ee	192.168.1.2	1.1.1	Registered	0	0 kBytes	0 kBytes

Restart Rename Set IP Radio Upgrade Selected Upgrade All Refresh

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	☑	ap01ffdd	00:19:70:b1:f:dd (AC)				0	465.8KB	0.0B

Restart Rename Set IP Radio Refresh

Channel Mode: 20 MHz

Channel: 5745MHz(149)

Extension Channel: None

Antenna: Internal

Output Power: 27dBm

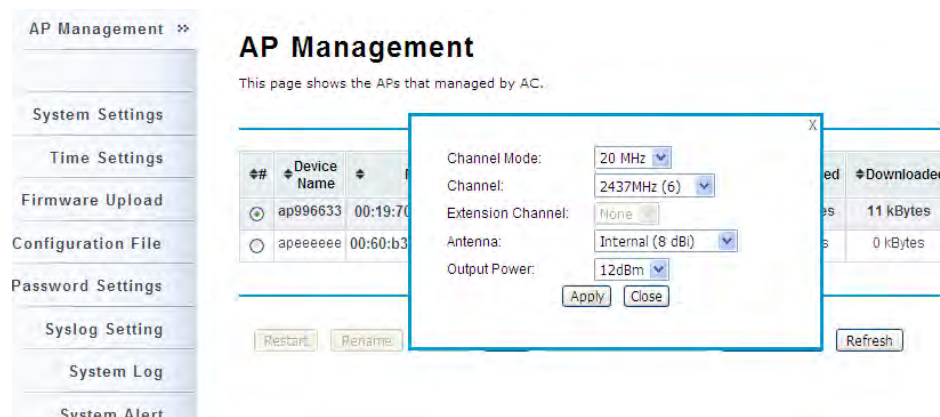
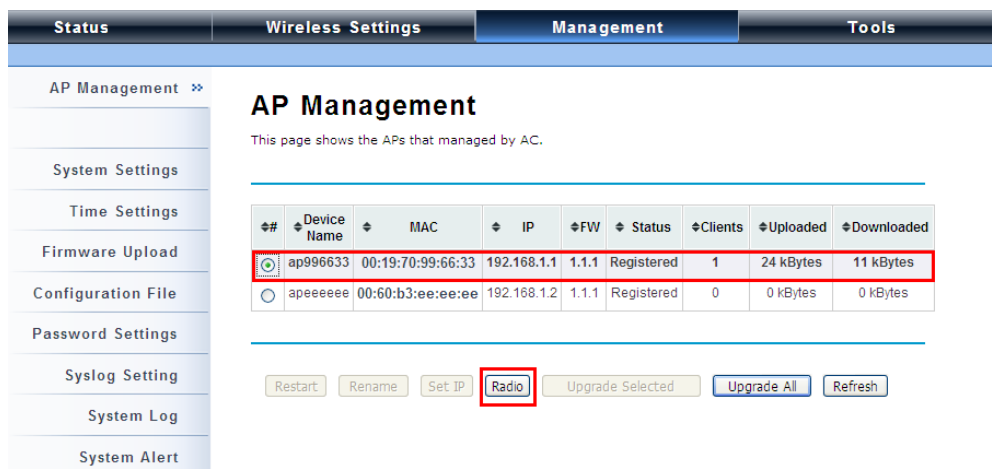
## Manage Thin APs

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.



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**.

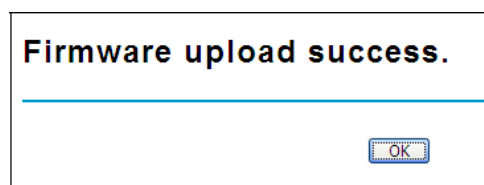


Besides radio setting, you may also reboot the managed AP, change its IP address and perform firmware upgrade for managed AP.

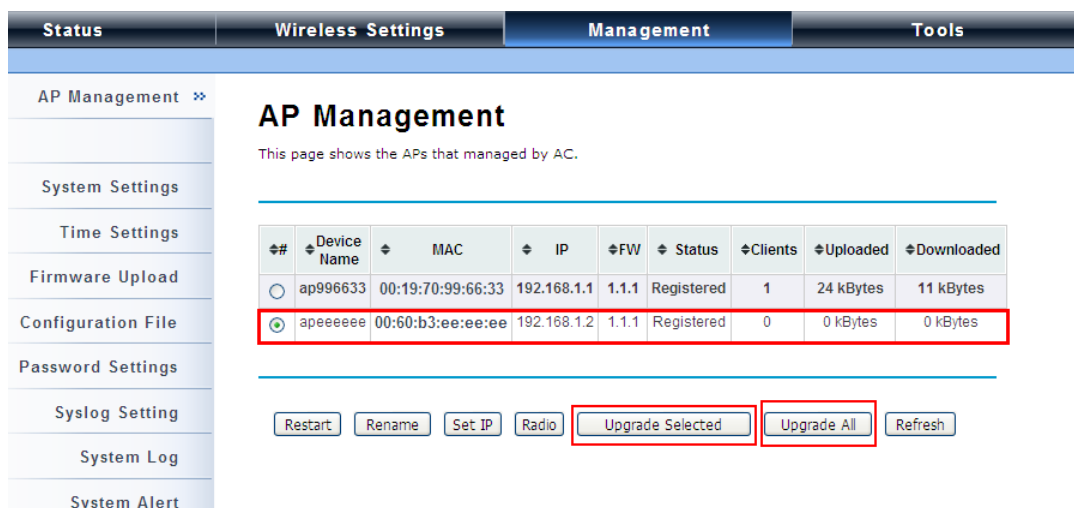
## Firmware Upgrade for Managed Thin APs

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**.



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



## 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.

The screenshot shows the 'Managed APs' page. The top navigation bar includes 'Status', 'Wireless Settings', 'Management', and 'Tools'. The left sidebar has 'Information', 'Managed APs', 'Wireless Users', and 'DHCP Clients'. The main content area is titled 'Managed APs' and includes a sub-header 'This page shows the APs that managed by AC.' Below this is a table with columns: Device Name, MAC, IP, FW, Status, Clients, Uploaded, and Downloaded. The table contains two rows of data. A 'Refresh' button is located at the bottom of the table.

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
apeeeee	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.

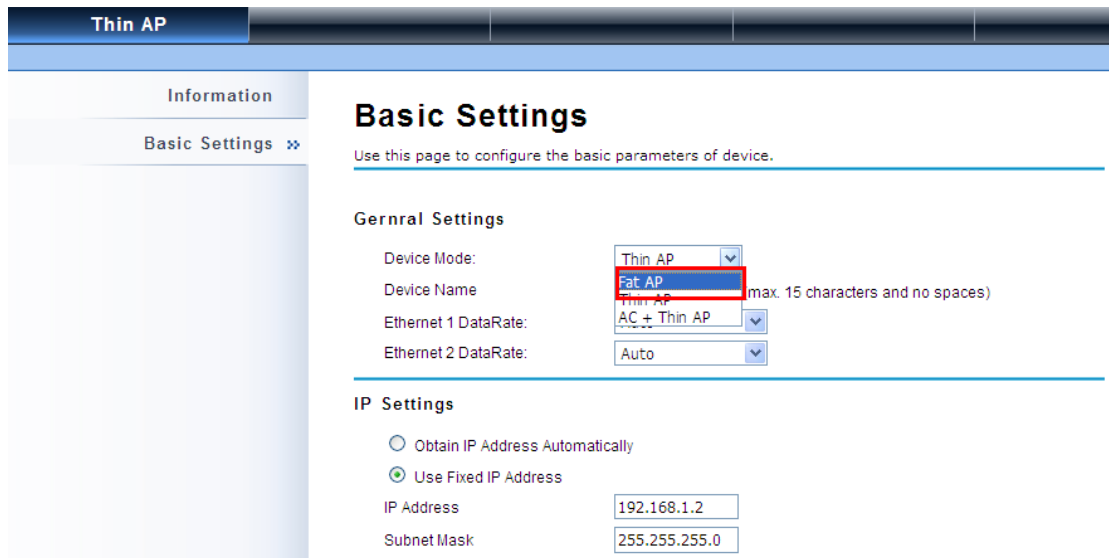
To switch from **Virtual AC** mode to **Fat AP** mode, go to **Management > System Settings**. From the **Device Mode** drop-down list, select "**Fat AP**" and hit **YES** to make the change take effect.

The screenshot shows the 'System Settings' page. The top navigation bar includes 'Status', 'Wireless Settings', 'Management', and 'Tools'. The left sidebar has 'AP Management', 'System Settings', 'Time Settings', 'Firmware Upload', 'Configuration File', 'Password Settings', 'Syslog Settings', and 'System Log'. The main content area is titled 'System Settings' and includes a sub-header 'Use this page to configure the basic parameters of device.' Below this is a 'Device Settings' section with a 'Device Mode' dropdown menu. The dropdown menu is open, showing options: 'Virtual AC + Thin AP', 'Thin AP', 'Virtual AC', and 'Virtual AC + Thin AP'. The 'Fat AP' option is highlighted. Other settings include 'Connect Mode', 'Device Name', 'Spanning Tree', 'STP Forward Delay', 'Enable 802.1Q VLAN', 'Management VLAN ID', and 'IP Address Assignment'.

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.



**Thin AP**

Information

Basic Settings »

## Basic Settings

Use this page to configure the basic parameters of device.

### General Settings

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

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

Ethernet 1 DataRate: Thin AP

Ethernet 2 DataRate: Auto

### IP Settings

Obtain IP Address Automatically

Use Fixed IP Address

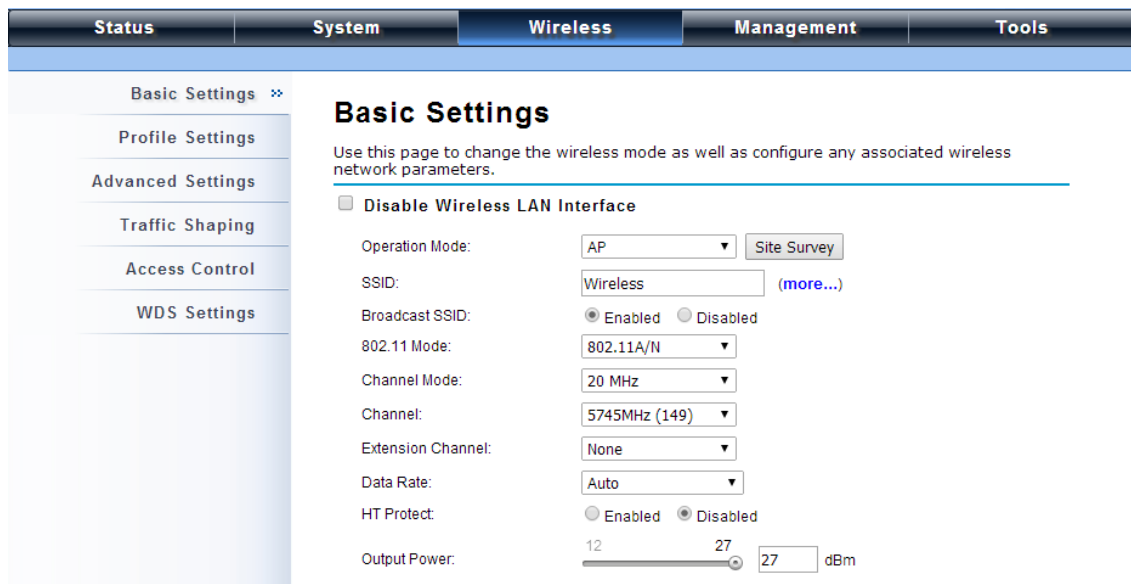
IP Address:

Subnet Mask:

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.



**Status** **System** **Wireless** **Management** **Tools**

Basic Settings »

## 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 Site Survey

SSID:  (more...)

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:    dBm

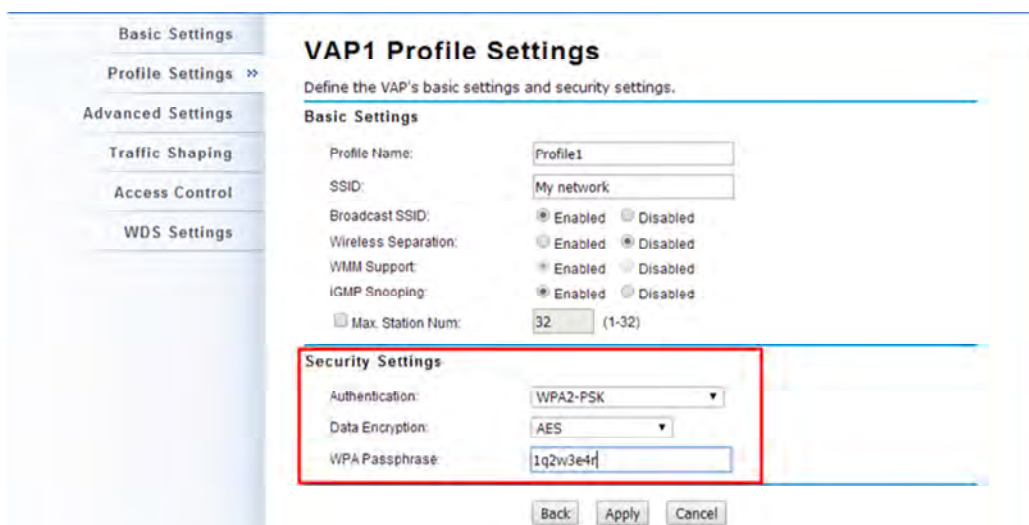
 **Note:**

λ In the example here, we only change the “Wireless Network Name (SSID)” as “Join\_me”.

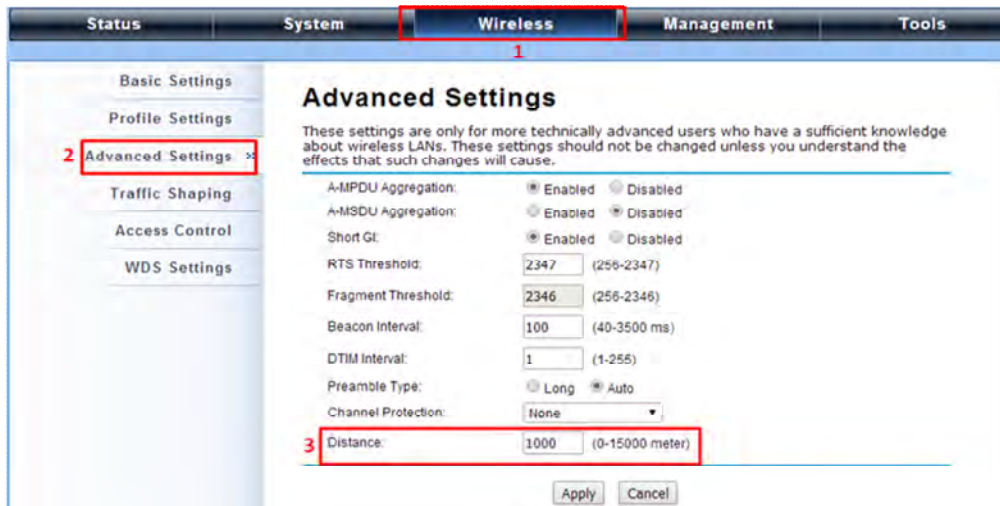
- If security is required, open **Wireless > Profile Setting** and click on “**Profile 1 Settings**” as below.



- 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.



- 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.



## 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.



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:

Locked AP MAC:

802.11 Mode: 802.11B/G/N

Data Rate: Auto

Antenna Gain:  dBi

Output Power:   dBm

Enable MAC Clone

Auto MAC Clone

Manual MAC Clone:

### Wireless Site Survey

This page provides a tool to scan the wireless network.

Selected	SSID	Channel	MAC Address	802.11 Mode	Signal Strength	Security
<input type="checkbox"/>	W8171-SL	2457MHz (10)	00:50:c5:ac:2a:79	802.11B/G	-92	WEP
<input type="checkbox"/>	2450AP	2437MHz (6)	00:19:70:a2:95:72	802.11B/G	-81	WEP
<input checked="" type="checkbox"/>	Wireless	2412MHz (1)	00:19:70:b5:7a:a9	802.11B/G	-83	NONE
<input type="checkbox"/>	MIS-Guest	2422MHz (3)	00:19:70:40:ff:fb	802.11B/G/N	-84	WPA2
<input type="checkbox"/>	MISVOIP	2412MHz (1)	00:18:e7:eb:7d:da	802.11B/G	-85	WEP

- 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.

**Wireless**

**Security Settings**

Define the wireless security settings.

Authentication: WPA2-PSK

Data Encryption: AES

WPA Passphrase:

- 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.

**Status**

**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.

The screenshot shows the 'Wireless' configuration page. The 'Wireless' tab is highlighted. In the left sidebar, 'Basic Settings' is selected. The main content area is titled 'Basic Settings' and contains the following fields:

- Operation Mode:** Bridge (dropdown menu)
- 802.11 Mode:** 802.11B/G/N (dropdown menu)
- Channel Mode:** 20 MHz (dropdown menu)
- Channel:** 2437MHz (6) (dropdown menu)
- Extension Channel:** None (dropdown menu)
- Data Rate:** Auto (dropdown menu)
- Output Power:** 12 to 17 dBm (slider)

Buttons for 'Apply' and 'Cancel' are at the bottom.

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**”.

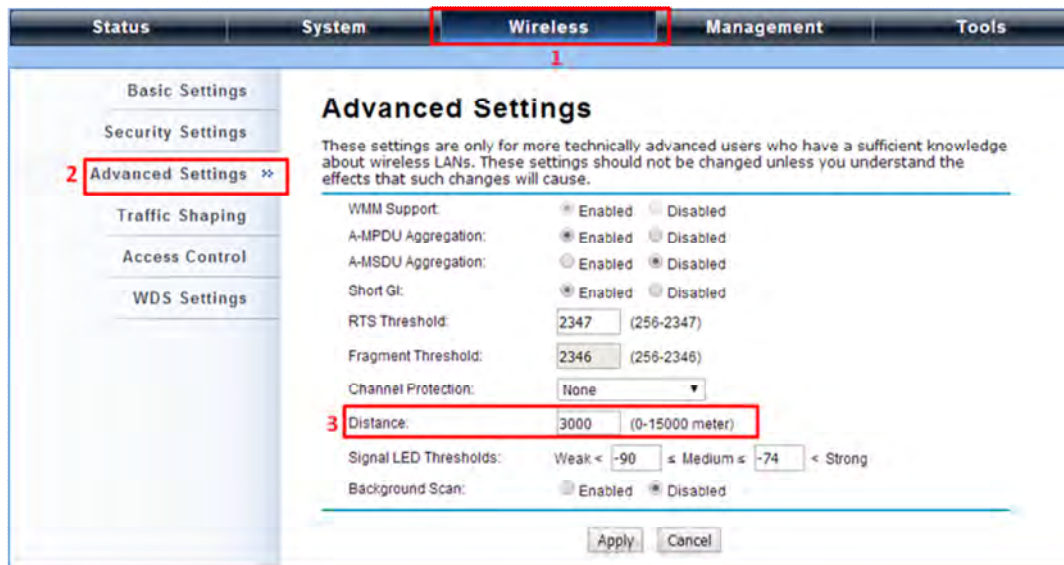
The screenshot shows the 'Wireless' configuration page with the 'WDS Settings' sub-tab selected. The main content area is titled 'WDS Settings' and contains the following fields:

- Local MAC Address:** 00:19:70:00:fc:58
- Remote AP MAC Address 1:** 00:19:70:00:00:01
- Remote AP MAC Address 2:** (empty)
- Remote AP MAC Address 3:** (empty)
- Remote AP MAC Address 4:** (empty)

### Note:

- λ 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.

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



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



## AP Repeater Mode

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

Status	System	Wireless	Management	Tools
--------	--------	----------	------------	-------

Basic Settings »

Profile Settings

Advanced Settings

Access Control

WDS Settings

## 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 Site Survey

Wireless Network Name (SSID): Wireless (more...)

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 antenna): 12 26  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.

The screenshot shows the web configurator interface with the 'Status' tab selected. The 'Information' sub-tab is active, displaying the following details:

- 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:** A table with columns for Index, SSID, Security, Clients, Uploaded, and Downloaded. One network is listed with Index 1, SSID Wireless, Security Open System, 0 Clients, 16KB Uploaded, and 0KB Downloaded.

#### 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.



Status	Wireless Settings	Management	Tools
--------	-------------------	------------	-------

Information

**Managed APs** >>

Wireless Users

DHCP Clients

## 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
apeeeeeee	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.

Status	Wireless Settings	Management	Tools
--------	-------------------	------------	-------

Information

Managed APs

**Wireless Users** >>

DHCP Clients

## 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.

Status	Wireless Settings	Management	Tools
--------	-------------------	------------	-------

Information

Managed APs

Wireless Users

**DHCP Clients** ✖

## 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.

Status	Wireless Settings	Management	Tools
--------	-------------------	------------	-------

Wireless Networks ✖

Wireless Protocol

Access Control

Traffic Shaping

RADIUS Settings

## Wireless Networks

Define each WLAN's attribute.

#	Enable	SSID	Security	VLAN ID	Description
1	<input checked="" type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile1
2	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile2
3	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile3
4	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile4
5	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile5
6	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile6
7	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile7
8	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile8
9	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile9
10	<input type="checkbox"/>	Wireless	Open System	<input type="text" value="0"/>	Profile10

The screenshot shows the 'VAP Profile1 Settings' page. The top navigation bar includes 'Status', 'Wireless Settings', 'Management', and 'Tools'. The left sidebar shows 'Wireless Networks' with sub-items: 'Wireless Protocol', 'Access Control', 'Traffic Shaping', and 'RADIUS Settings'. The main content area is titled 'VAP Profile1 Settings' and contains the following 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

λ **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.

λ **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.

λ **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:**

---

λ 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.

λ **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:**

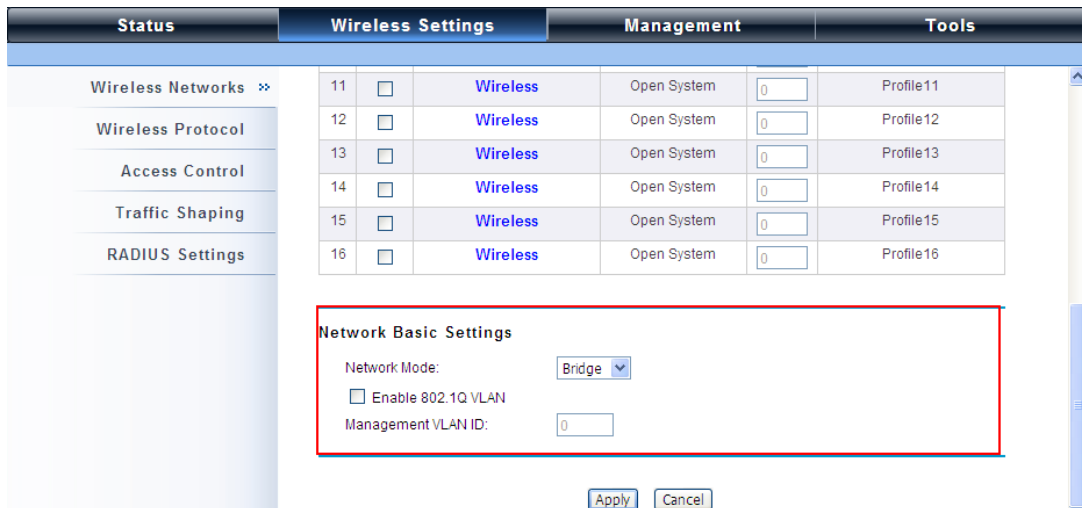
---

λ We strongly recommend you enable wireless security on your network!

λ Only the same Authentication, Data Encryption and Key among the IEEE 802.11n ZAC Access Point and wireless clients can the communication be established!

---

λ **Network Basic Setting:**

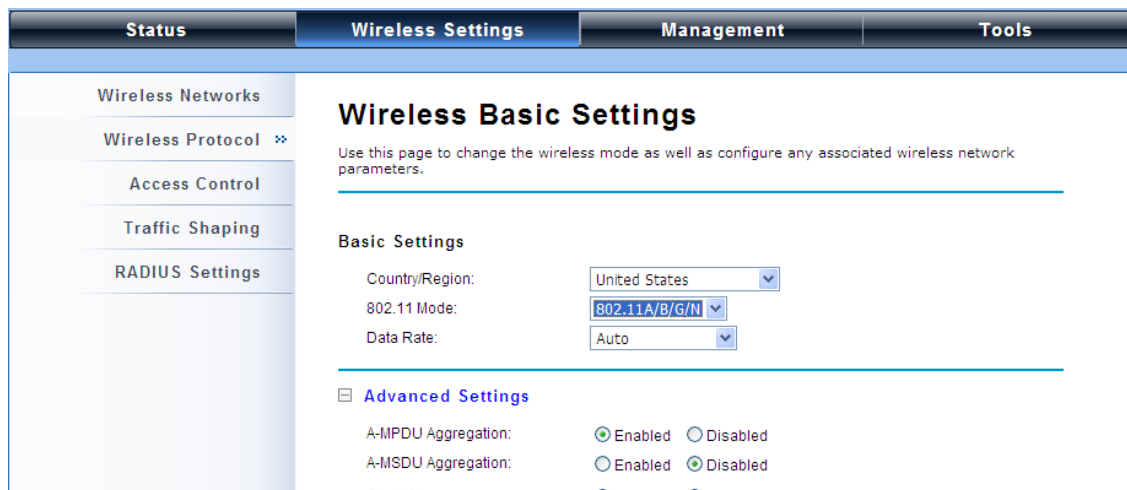


**Network Mode:** Specify the network mode. It includes **Bridge** and **Router**. When switch to Router mode, the LAN IP address for web page access will become 192.168.0.99.

## 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.



λ **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.

λ **Advanced Settings**

Status	Wireless Settings	Management	Tools
Wireless Networks	Country/Region: United States		
Wireless Protocol	802.11 Mode: 802.11A/B/G/N		
Access Control	Data Rate: Auto		
Traffic Shaping	<b>Advanced Settings</b>		
RADIUS Settings	A-MPDU Aggregation: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
	A-MSDU Aggregation: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
	Short GI: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
	IGMP Snooping: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
	RIFS: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
	HT Protect: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
	Preamble Type: <input type="radio"/> Long <input checked="" type="radio"/> 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: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
	TDM Coordination: <input type="radio"/> Enabled <input checked="" type="radio"/> 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:

Apply Cancel

#	MAC Address	Select	Edit
1	00:19:70:86:c6:e3	<input checked="" type="checkbox"/>	Edit

Delete Selected Delete All Refresh

λ **Wireless Network:** Select the VAP network you would like to enable access control.

λ **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.

λ **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.

λ **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.

Status	Wireless Settings	Management	Tools
<div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <p>Wireless Networks</p> <p>Wireless Protocol</p> <p>Access Control</p> <p><b>Traffic Shaping</b> ✖</p> <p>RADIUS Settings</p> </div> <div style="width: 80%; padding-left: 10px;"> <h2 style="margin: 0;">Traffic Shaping</h2> <p style="font-size: small; margin: 0;">Traffic shaping is the control of network traffic in order to optimize or guarantee performance, improve latency.</p> <hr/> <div style="margin-bottom: 5px;">Interface Selection: <input type="text" value="VAP1"/></div> <div style="margin-bottom: 5px;"><input type="checkbox"/> Enable Traffic Shaping</div> <div style="margin-bottom: 5px;">Outgoing Traffic Rate: <input type="text" value="1024000"/> Kbits/s</div> <div style="margin-bottom: 5px;">Outgoing Traffic Burst: <input type="text" value="20"/> KBytes</div> <hr/> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </div> </div> </div>			

λ **Enable Traffic Shaping**

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

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

λ **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.

Status	Wireless Settings	Management	Tools
<div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <ul style="list-style-type: none"> <li>Wireless Networks</li> <li>Wireless Protocol</li> <li>Access Control</li> <li>Traffic Shaping</li> <li style="background-color: #e0e0e0;">RADIUS Settings ✕</li> </ul> </div> <div style="width: 80%; padding-left: 10px;"> <h2 style="margin: 0;">RADIUS Settings</h2> <p style="font-size: small; margin: 0;">Use this page to set the radius server settings.</p> <hr/> <h3 style="margin: 0;">Authentication RADIUS Server</h3> <p>IP Address: <input type="text" value="0.0.0.0"/></p> <p>Port: <input type="text" value="1812"/></p> <p>Shared Secret: <input type="text"/></p> <hr/> <p><input type="checkbox"/> Global-Key Update</p> <p>every <input type="text" value="3600"/> Seconds</p> <hr/> <p style="text-align: right;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div> </div>			

λ **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.

λ **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.

Status	Wireless Settings	Management	Tools												
<div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <ul style="list-style-type: none"> <li>Wireless Networks</li> <li>Wireless Protocol</li> <li>Access Control</li> <li>Traffic Shaping</li> <li>RADIUS Settings</li> <li style="border: 1px dashed #ccc; padding: 2px;">TCP/IP Settings <span style="font-size: 0.8em;">↔</span></li> <li>Captive Portal</li> <li>Firewall Settings</li> </ul> </div> <div style="width: 80%; padding-left: 10px;"> <h2 style="margin: 0;">TCP/IP Settings</h2> <p style="font-size: 0.8em; margin: 0;">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.</p> <hr/> <p><b>LAN Settings :</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">IP Address :</td> <td><input type="text" value="192.168.0.99"/></td> </tr> <tr> <td>Subnet Mask :</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>DHCP Server :</td> <td><input type="text" value="Enabled"/></td> </tr> <tr> <td>DHCP IP Address Range :</td> <td><input type="text" value="192.168.0.1"/> - <input type="text" value="192.168.0.200"/></td> </tr> <tr> <td>DHCP Subnet Mask :</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>Lease Time :</td> <td><input type="text" value="7200"/> (15-44640 Minutes)</td> </tr> </table> </div> </div>				IP Address :	<input type="text" value="192.168.0.99"/>	Subnet Mask :	<input type="text" value="255.255.255.0"/>	DHCP Server :	<input type="text" value="Enabled"/>	DHCP IP Address Range :	<input type="text" value="192.168.0.1"/> - <input type="text" value="192.168.0.200"/>	DHCP Subnet Mask :	<input type="text" value="255.255.255.0"/>	Lease Time :	<input type="text" value="7200"/> (15-44640 Minutes)
IP Address :	<input type="text" value="192.168.0.99"/>														
Subnet Mask :	<input type="text" value="255.255.255.0"/>														
DHCP Server :	<input type="text" value="Enabled"/>														
DHCP IP Address Range :	<input type="text" value="192.168.0.1"/> - <input type="text" value="192.168.0.200"/>														
DHCP Subnet Mask :	<input type="text" value="255.255.255.0"/>														
Lease Time :	<input type="text" value="7200"/> (15-44640 Minutes)														

λ **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:**

---

λ 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.

Status	Wireless Settings	Management	Tools
Wireless Networks	<b>Captive Portal</b>		
Wireless Protocol	Use this page to set basic Captive Portal settings. Captive Portal is implemented by CoovaChilli.		
Access Control	<input checked="" type="checkbox"/> Captive Portal Wireless Network: <input type="text" value="VAP1 - Wireless"/>		
Traffic Shaping	<b>RADIUS Settings</b>		
RADIUS Settings	Primary RADIUS Server: <input type="text" value="radius1.coova.net"/> Secondary RADIUS Server: <input type="text" value="radius2.coova.net"/> RADIUS Auth Port: <input type="text" value="1812"/> RADIUS Acct Port: <input type="text" value="1813"/> RADIUS Shared Secret: <input type="text" value="....."/> RADIUS NASID: <input type="text" value="your-radius-nasid"/>		
TCP/IP Settings	<b>Captive Portal</b>		
Captive Portal >>	UAM Portal URL: <input type="text" value="https://www.coova.n"/> UAM Secret: <input type="text" value="....."/>		
Firewall Settings			

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

λ **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

λ **Radius Administrative-User:**

**Radius Admin Username:** Enter the username of the Radius Administrator

**Radius Admin Password:** Enter the password of the Radius Administrator

λ **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**.

### λ **Source IP Filtering:**

The screenshot shows a web interface for configuring Source IP Filtering. The top navigation bar includes 'Status', 'Wireless Settings' (selected), 'Management', and 'Tools'. A left sidebar lists various settings: 'Wireless Networks', 'Wireless Protocol', 'Access Control', 'Traffic Shaping', 'RADIUS Settings', 'TCP/IP Settings', 'Captive Portal', 'Firewall Settings', 'Src IP Filtering' (selected), and 'Dst IP Filtering'. The main content area is titled 'Source IP Filtering' and contains the following elements:

- A description: "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."
- A checkbox labeled 'Enable Source IP Filtering' which is checked.
- Input fields for 'Local IP Address:' and 'Comment:'.
- 'Apply' and 'Cancel' buttons.
- A table with the following structure:

IP Address	Comment	Select	Edit
192.168.1.3		<input type="checkbox"/>	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**.

λ **Destination IP Filtering:**



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.

**Destination IP Address:** Enter the IP address to be restricted.

**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 destination IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

λ **Source Port Filtering:**



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.

**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 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**.

λ **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:

Comment:

Port Range	Protocol	Comment	Select	Edit
2000-2500	TCP+UDP		<input type="checkbox"/>	<input type="button" value="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**.



## λ Port Forwarding:

The screenshot shows the 'Port Forwarding' configuration page. The left sidebar contains a menu with options: Wireless Networks, Wireless Protocol, Access Control, Traffic Shaping, RADIUS Settings, TCP/IP Settings, Captive Portal, Firewall Settings (expanded), Src IP Filtering, Dst IP Filtering, and Src Port Filtering. The main content area is titled 'Port Forwarding' and includes a sub-header: '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.'

Configuration options include:

- Enable Port Forwarding
- IP Address:
- Protocol:
- Port Range:  -
- Comment:

Buttons for 'Apply' and 'Cancel' are located below the form. Below the form is a table with the following data:

IP Address	Protocol	Port Range	Comment	Select	Edit
192.168.1.20	TCP+UDP	25		<input type="checkbox"/>	<input type="button" value="Edit"/>

The port forwarding allows 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 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.

The screenshot shows the 'AP Management' page. The left sidebar contains a menu with options: AP Management (selected), System Settings, Time Settings, Firmware Upload, Configuration File, Password Settings, and Syslog Setting. The main content area is titled 'AP Management' and includes a sub-header: 'This page shows the APs that managed by AC.'

Below the sub-header is a table with the following data:

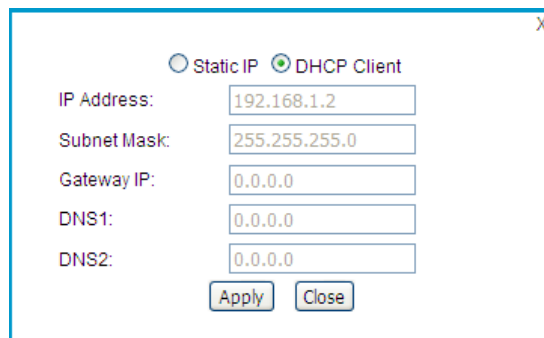
#	Device Name	MAC	IP	FW	Status	Clients	Uploaded	Downloaded
<input checked="" type="radio"/>	ap20fad2	00:19:70:20:fa:d2	192.168.1.2	1.1.1	Registered	2	2 kBytes	0 kBytes
<input type="radio"/>	ap86c6e1	00:19:70:86:c6:e1	192.168.1.100	1.1.1	Registered	0	0 kBytes	0 kBytes

Buttons for 'Restart', 'Rename', 'Set IP', 'Radio', 'Upgrade Selected', 'Upgrade All', and 'Refresh' are located below the table.

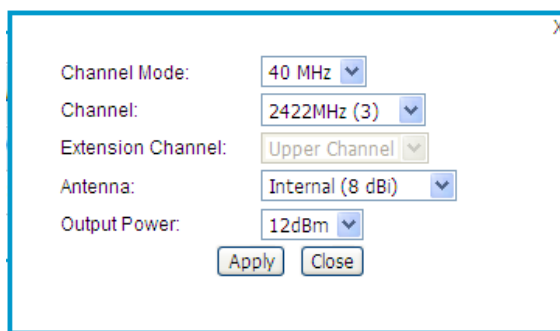
**Restart:** Restart the selected ZAC-managed AP.

**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.



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



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
1	ap20fad2	<u>00:19:70:20:fa:d2</u>					0 kBytes	0 kBytes
2	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

Restart   Rename   Set IP   Upgrade All   Refresh

**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.

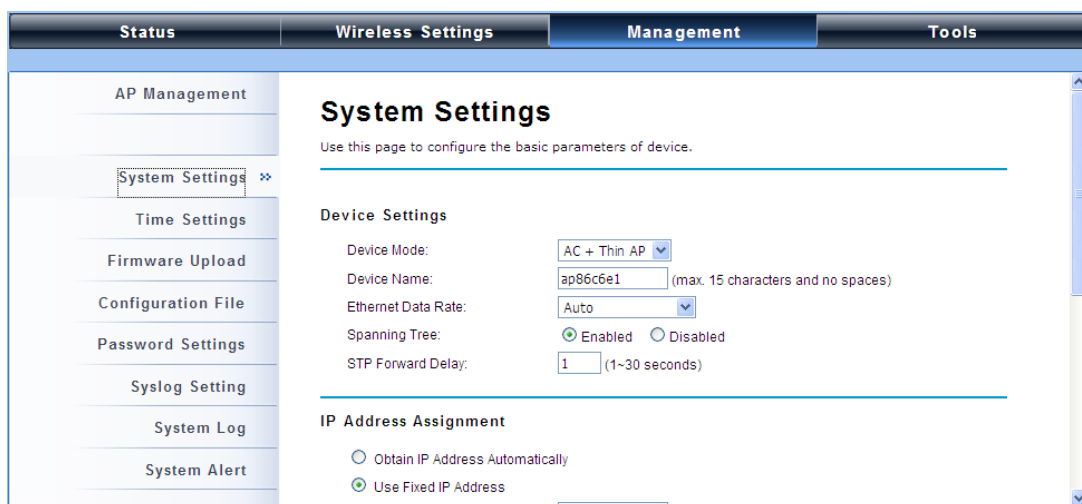


**Upgrade All:** Click to upgrade all the ZAC-managed APs simultaneously.

**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.



### λ 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.

λ **IP Address Assignment:**

---

**IP Address Assignment**

Obtain IP Address Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway Ip Address:

DNS 1:

DNS 2:

---

**Obtain IP Address Automatically:** If a DHCP server exists in your network, you can check this option, thus the IEEE 802.11n ZAC Access Point 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.

λ **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:  -

DHCP Subnet Mask:

DHCP Gateway:

Lease Time:  (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.

## Time Settings

Compliant with NTP, the IEEE 802.11n ZAC Access Point is capable of keeping its time in complete accord with the Internet time. To use this feature, check **“Enable NTP Client Update”** in advance.

The screenshot shows a web interface with a navigation bar at the top containing 'Status', 'Wireless Settings', 'Management', and 'Tools'. On the left, a sidebar lists 'AP Management', 'System Settings', 'Time Settings' (highlighted with a double arrow), 'Firmware Upload', 'Configuration File', 'Password Settings', and 'Syslog Setting'. The main content area is titled 'Time Settings' and includes the following fields: 'Current Time' (Yr: 2011, Mon: 12, Day: 22, Hr: 1, Mn: 55, Sec: 57), 'Time Zone Select' (dropdown menu showing '(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'), 'Enable NTP Client Update' (checked checkbox), 'NTP server' (dropdown menu showing '192.5.41.41 - North America'), and 'Manual IP' (input field with '0.0.0.0'). At the bottom are 'Apply' and 'Cancel' buttons.

### λ Current Time

Display the present time in Yr, Mon, Day, Hr, Min and Sec.

### λ Time Zone Select

Select the time zone from the dropdown list.

### λ NTP Server

Select the time server from the **“NTP Server”** dropdown list. or manually input the IP address of available time server into **“Manual IP”**.

## Firmware Upgrade

Besides upgrading firmware for the ZAC Access Point in AC mode, it also provides firmware update for the ZAC-managed APs.

The screenshot shows a web interface with a navigation bar at the top containing 'Status', 'Wireless Settings', 'Management', and 'Tools'. On the left, a sidebar lists 'AP Management', 'System Settings', 'Time Settings', and 'Firmware Upload' (highlighted with a double arrow). The main content area is titled 'Upgrade Firmware' and includes the following fields: 'Upload AC Firmware' (input field with a file upload icon and an 'Upload' button) and 'Upload TAP Firmware' (input field with a file upload icon and an 'Upload' button'). A warning message at the top states: '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.'

λ **Upload AC Firmware:** Allows the network administrator to upgrade firmware for the ZAC Access Point in AC mode.

λ **Upload TAP Firmware:** Before updating the firmware for the ZAC-managed APs, you need to upload the firmware into the ZAC Access Point in AC mode that allows the virtual controller AP to do

the firmware upgrade for ZAC-managed APs.

 **Note:**

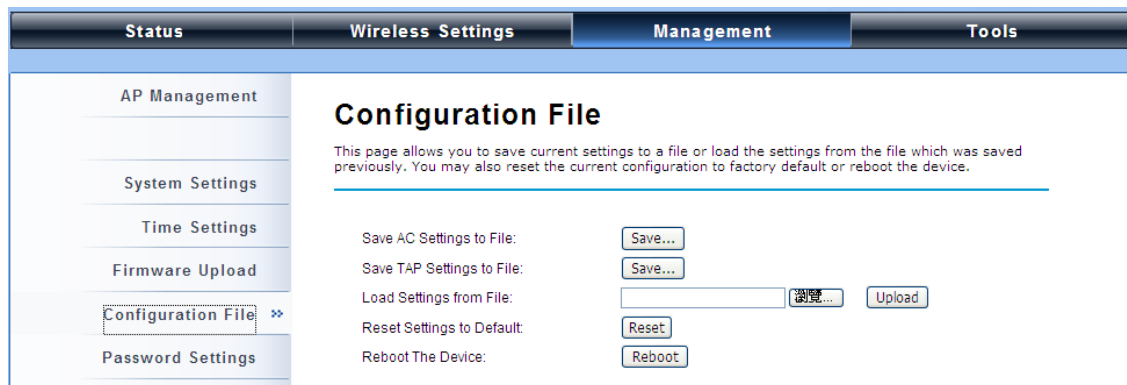
---

λ Do NOT cut the power off during upgrade, otherwise the system may crash!

---

## Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.



λ **Save AC Settings to File**

Click **Save** to export the configuration file of ZAC Access Point in AC mode. Then the configuration file **ac.cfg** will be generated and saved to the specified location.

λ **Save TAP Settings to File**

Click **Save** to export the configuration file of ZAC-managed AP. Then the configuration file **tap.cfg** will be generated and saved to the specified location.

λ **Load Settings from File**

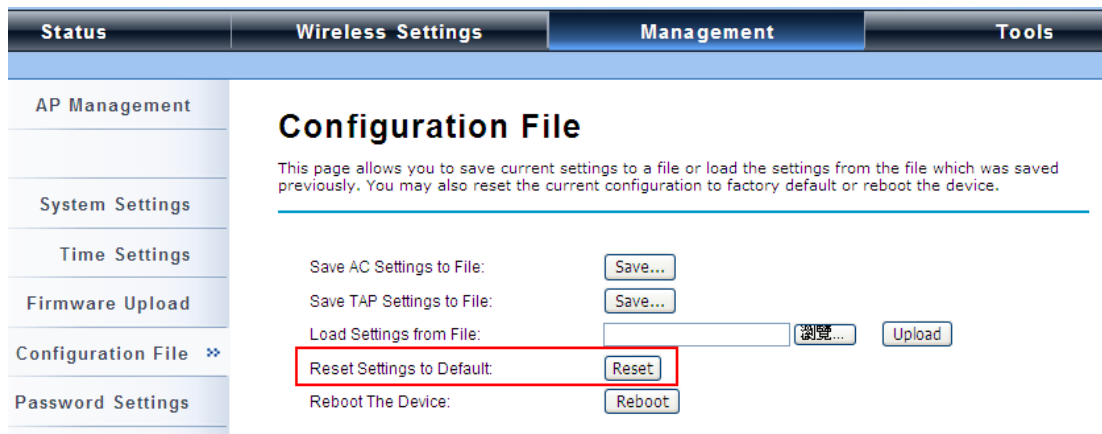
Import **ac.cfg** load into the ZAC Access Point in AC mode.

## Restore Factory Default Settings

The IEEE 802.11n ZAC Access Point provides two ways to restore the factory default settings:

λ **Restore factory default settings via Web**

From **Configuration File** in **Management**, click **Reset** restore factory default settings.

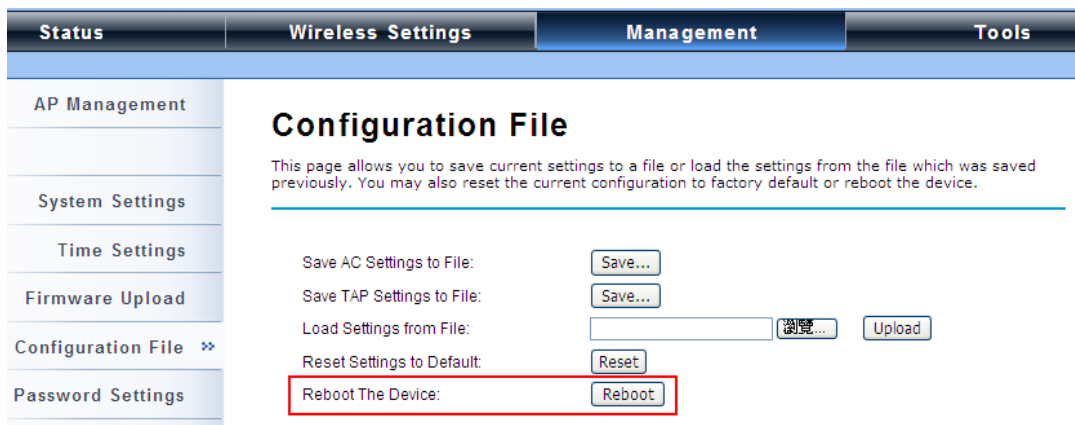


λ **Restore factory default settings via Reset Button**

If software in ZAC Access Point is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink. The hardware reset will take about 2 minutes to complete.

**Reboot**

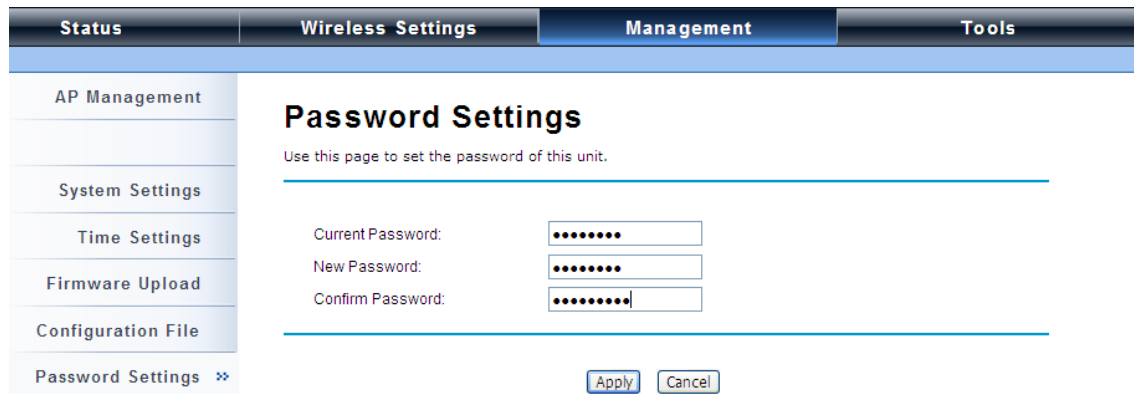
You can software reboot your ZAC Access Point from **Configuration File** in **Management** as below:



Click **“Reboot”** and hit **“Yes”** upon the appeared prompt to start reboot process. This takes a few minutes.

## Password Settings

You can change the password for your IEEE 802.11n ZAC Access Point.



The screenshot shows the 'Management' tab of the device's configuration interface. The left sidebar contains a menu with 'Password Settings' selected. The main content area is titled 'Password Settings' and includes the instruction: 'Use this page to set the password of this unit.' Below this, there are three input fields: 'Current Password:', 'New Password:', and 'Confirm Password:'. Each field contains a series of dots representing masked characters. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

λ **Current Password:** Enter the current password.

λ **New Password:** Enter the new password.

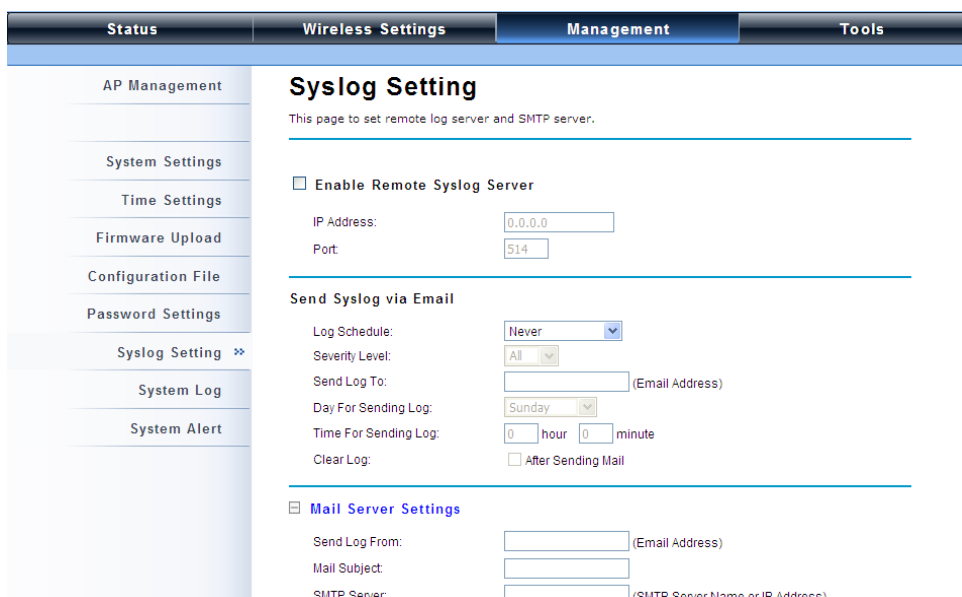
λ **Confirm Password:** Enter the new password again for confirmation.

### Note:

λ The password is case-sensitive and its length cannot exceed 19 characters!

## Syslog Setting:

The ZAC Access Point provides remote syslog management by sending logs to an external syslog server. The log can be also sent through Email.



The screenshot shows the 'Management' tab of the device's configuration interface. The left sidebar contains a menu with 'Syslog Setting' selected. The main content area is titled 'Syslog Setting' and includes the instruction: 'This page to set remote log server and SMTP server.' Below this, there are several sections: 1. 'Enable Remote Syslog Server' with a checkbox and input fields for 'IP Address' (0.0.0.0) and 'Port' (514). 2. 'Send Syslog via Email' with a dropdown for 'Log Schedule' (Never), a dropdown for 'Severity Level' (All), an input field for 'Send Log To' (Email Address), a dropdown for 'Day For Sending Log' (Sunday), and input fields for 'Time For Sending Log' (0 hour, 0 minute). There is also a checkbox for 'Clear Log' (After Sending Mail). 3. 'Mail Server Settings' with input fields for 'Send Log From' (Email Address), 'Mail Subject', and 'SMTP Server' (SMTP Server Name or IP Address).

λ **Remote Syslog Server**

**Enable Remote Syslog:** Enable to send log to remote syslog server.



**IP Address:** Specify the IP address of the remote server.

**Port:** Specify the port number of the remote server.

λ **Send Syslog via Email**

**Log Schedule:** Configure the frequency of logs being sent. 5 scheduling options are provided:

**Never, Hourly, Daily, Weekly, and When log is full.**

**Severity Level:** Choose **All** to send all the logs or **Alert** to send only the alert messages.

**Send Log to:** Specify the email address where you would like to send the log.

**Day for Sending Log:** When Weekly scheduling is selected, you may specify which week day to send the log.

**Time for Sending Log:** Specify the time of the day to send the log.

**Clear Log:** To clear log after sending logs via email, check the **After Sending Mail** checkbox.

λ **Mail Server Setting**

**Send Log From:** Enter the email address of the mail server.

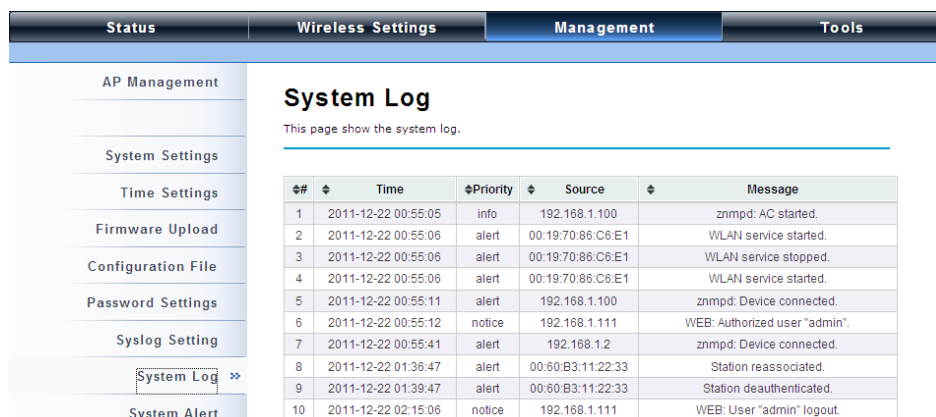
**Mail Subject:** Type a title to be presented in the subject line of the log email message.

**SMTP Server:** Enter the IP address of the SMTP sever.

**SMTP Authentication:** If you want to use SMTP authentication, check **SMTP Authentication** checkbox and enter the user account and password.

## System Log:

System log record and display all logs and alert message in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted. You may click **Clear** to delete logs manually as well.



The screenshot shows a web interface with a navigation menu on the left and a main content area. The navigation menu includes: AP Management, System Settings, Time Settings, Firmware Upload, Configuration File, Password Settings, Syslog Setting, System Log (selected), and System Alert. The main content area is titled "System Log" and contains a table of log entries. Below the title, it says "This page show the system log." The table has columns for #, Time, Priority, Source, and Message.

#	Time	Priority	Source	Message
1	2011-12-22 00:55:05	info	192.168.1.100	znmpd: AC started.
2	2011-12-22 00:55:06	alert	00:19:70:86:C6:E1	WLAN service started.
3	2011-12-22 00:55:06	alert	00:19:70:86:C6:E1	WLAN service stopped.
4	2011-12-22 00:55:06	alert	00:19:70:86:C6:E1	WLAN service started.
5	2011-12-22 00:55:11	alert	192.168.1.100	znmpd: Device connected.
6	2011-12-22 00:55:12	notice	192.168.1.111	WEB: Authorized user "admin".
7	2011-12-22 00:55:41	alert	192.168.1.2	znmpd: Device connected.
8	2011-12-22 01:36:47	alert	00:60:B3:11:22:33	Station reassociated.
9	2011-12-22 01:39:47	alert	00:60:B3:11:22:33	Station deauthenticated.
10	2011-12-22 02:15:06	notice	192.168.1.111	WEB: User "admin" logout.

## System Alert:

System alert record and events occurred on both ZAC Access Point in AC mode and ZAC-managed AP in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted. You may click **Clear** to delete logs manually as well.

The screenshot shows a management interface with a top navigation bar containing 'Status', 'Wireless Settings', 'Management', and 'Tools'. A left sidebar lists various settings: 'AP Management', 'System Settings', 'Time Settings', 'Firmware Upload', 'Configuration File', 'Password Settings', 'Syslog Setting', and 'System Log'. The 'System Alert' option is selected and highlighted. The main content area is titled 'System Alert' and includes the text 'This page show the system alert.' Below this is a table with the following data:

#	Time	Source	Message
1	2011-12-22 00:55:06	00:19:70:86:C6:E1	WLAN service started.
2	2011-12-22 00:55:06	00:19:70:86:C6:E1	WLAN service stopped.
3	2011-12-22 00:55:06	00:19:70:86:C6:E1	WLAN service started.
4	2011-12-22 00:55:11	192.168.1.100	znmpd: Device connected.
5	2011-12-22 00:55:41	192.168.1.2	znmpd: Device connected.
6	2011-12-22 01:36:47	00:60:B3:11:22:33	Station reassociated.
7	2011-12-22 01:39:47	00:60:B3:11:22:33	Station deauthenticated.

At the bottom of the table area, there are 'Refresh' and 'Clear' buttons.

## Tools

The IEEE 802.11n ZAC Access Points provide two tools to test the link status with other ZAC-managed Access Points or anyone on the network.

### Ping

The screenshot shows the 'Tools' section of the management interface. The 'Ping' tool is selected. The page is titled 'Ping' and includes the text 'Use this page to test the ping.' Below this are input fields for 'Ping Address' (containing '192.168.1.2'), 'Ping Count' (containing '5'), and 'Package Size' (containing '40'). At the bottom of the input area, there are 'Start', 'Stop', and 'Clear' buttons. The output area shows the following text:

```
PING 192.168.1.2 (192.168.1.2): 40 data bytes
68 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.7 ms
68 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.5 ms
68 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.6 ms
68 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.7 ms
```

λ **Ping Address**

Enter IP address of the remote destination.

λ **Ping Count:**

Enter the number of pings.

λ **Packet Size:**

Specify ping packet size.

## Trace Route

This tool is used to discover the routes that packets take when traveling to the destination destination.

Status	Wireless Settings	Management	Tools
Ping	<b>Trace Route</b> Use this page to test the path from one station to another.		
Trace Route ✕	Destination IP Address : <input type="text" value="192.168.1.2"/>		
	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Clear"/>		
	1 192.168.1.2 (192.168.1.2) 4.623 ms 0.565 ms 0.5 ms		

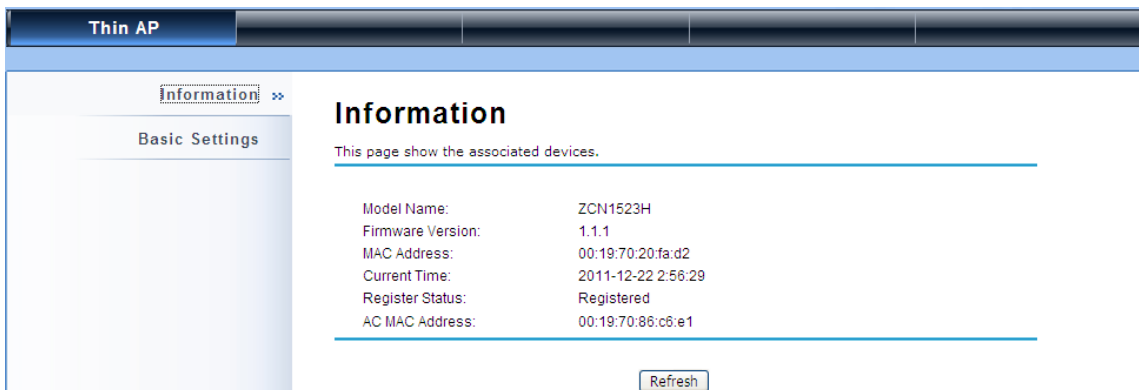
λ **Destination IP Address**

Enter IP address of the remote destination and click **Start** to start.

# Thin AP Mode

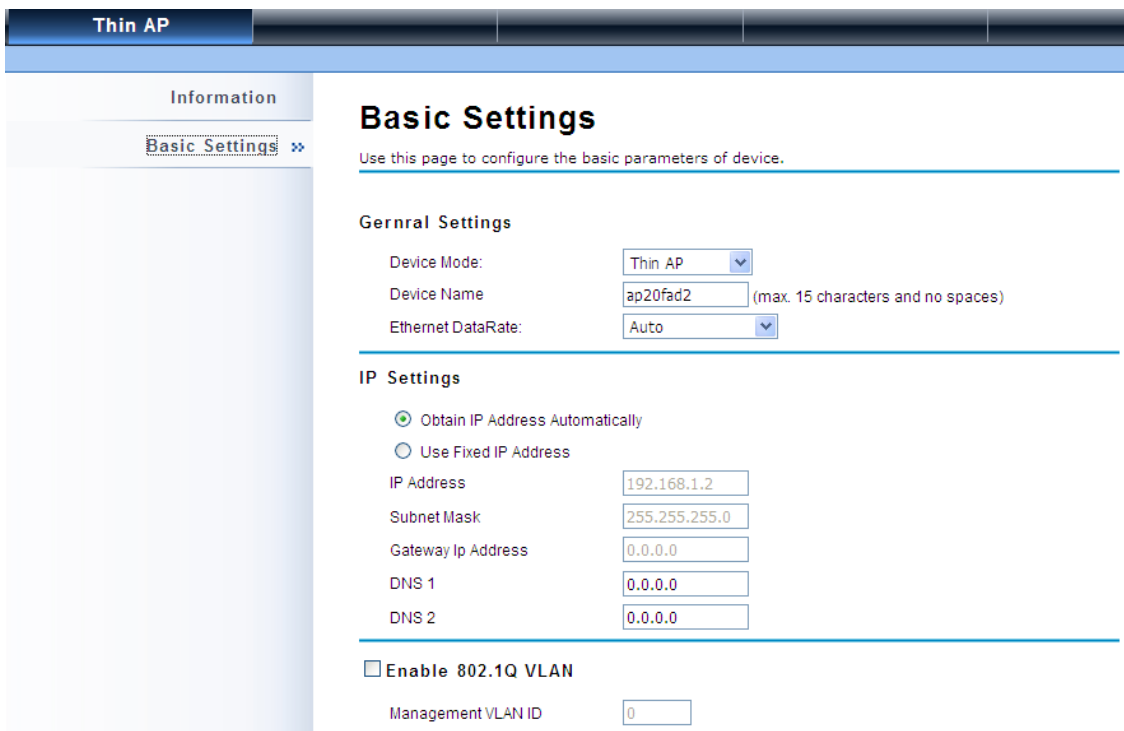
## Information

You may see some ZAC-managed AP's basic information such as model name, firmware version, MAC address, current up time, registration status as well as MAC address.



## Basic Settings

Allows you to configure device and IP settings for the ZAC-managed AP.



λ **General 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**.

λ **IP Address Assignment:**

**Obtain IP Address Automatically:** If a DHCP server exists in your network, you can check this option, thus the IEEE 802.11n ZAC Access Point 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.

λ **Enable 802.1Q VLAN**

To be able to access the web page of the ZAC-managed AP in the VLAN network, you need to assign the VLAN management ID for the ZAC-managed AP. Note that the ID on the switch must be identical of the AP's VLAN ID. Check **Enable 802.1Q VLAN** checkbox to activate it.

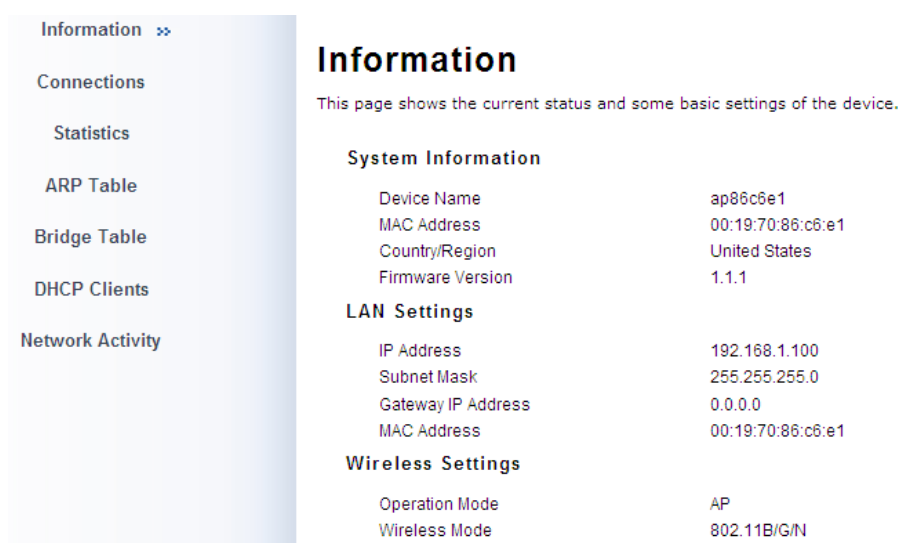
**Management VLAN ID:** Enter the VLAN ID.

# FAT 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, LAN settings, wireless setting and interface status. 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**

Device Name	ap86c6e1
MAC Address	00:19:70:86:c6:e1
Country/Region	United States
Firmware Version	1.1.1

**LAN Settings**

IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:19:70:86:c6:e1

**Wireless Settings**

Operation Mode	AP
Wireless Mode	802.11B/G/N

### View Association List

Open “**Connections**” in “**Status**” to check the information of associated wireless devices such as MAC address, signal strength, connection time, IP address, etc. All is read only. Click “**Refresh**” at the bottom to update the current association list.



**Association List**

This table shows the MAC Address, IP Address and RSSI for each associated wireless client.

VAP Index	MAC Address	Signal Strength	Connection Time	Last IP	Action
1	00:19:70:00:fb:c5	-48	2011-1-24 18:09:20	0.0.0.0	---

Refresh

By clicking on the MAC address of the selected device on the web you may see more details including

device name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, current TX/RX packets.

## Association Node Details

The details information of association node:

MAC Address	00:13:02:71:35:ba	Negotiated Rate	Last Signal
Device Name		6M	-86 dBm
Connect time	2011-1-24 17:59:33	24M	-87 dBm
Signal Strength	-85 dBm	36M	-85 dBm
Noise Floor	-117 dBm		
ACK Timeout	27		
Link Quality	0%		
Last IP	169.254.17.206		
TX/RX Rate	0/24 MBs		
TX/RX Packets	2/115		
Bytes Transmitted	119		
Bytes Received	10002		

## View Network Flow Statistics

Open “**Statistics**” in “**Status**” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “**Refresh**” to view current statistics.

**Status**    **System**    **Wireless**    **Management**    **Tools**

Information  
Connections  
**Statistics** >>  
ARP Table  
Bridge Table  
DHCP Clients  
Network Activities

### Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Poll Interval :  (0-65534) sec       

Wireless		
	Received	Transmitted
Unicast Packets	676	1
Broadcast Packets	400	421
Multicast Packets	19	299
Total Packets	1095	721
Total Bytes	54543	63429

Ethernet 1		
	Received	Transmitted
Total Packets	595	1419
Total Bytes	73818	519993

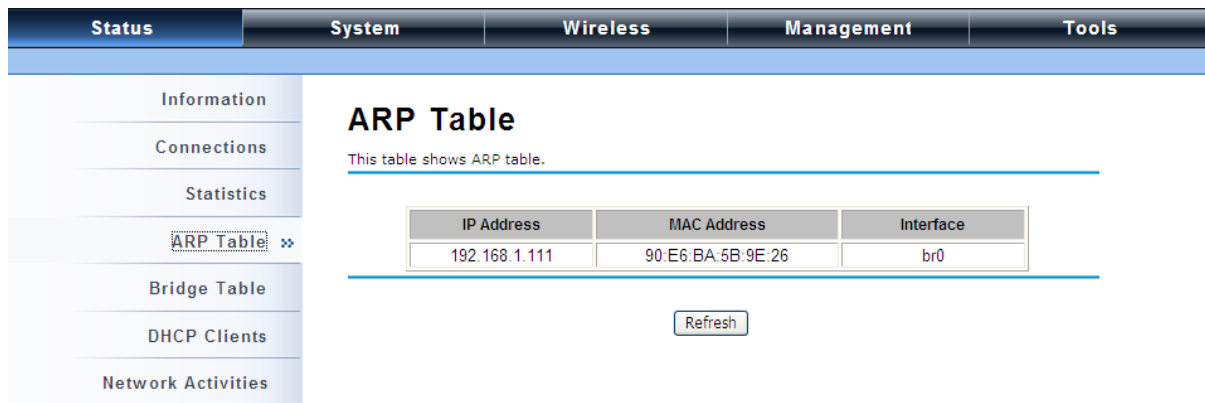
Ethernet 2

### λ Poll Interval

Specify the refresh time interval in the box beside “**Poll Interval**” and click “**Set Interval**” to save settings. “**Stop**” helps to stop the auto refresh of network flow statistics.

## View ARP Table

Open “ARP Table” in “Status” as below. Click “Refresh” to view current table.

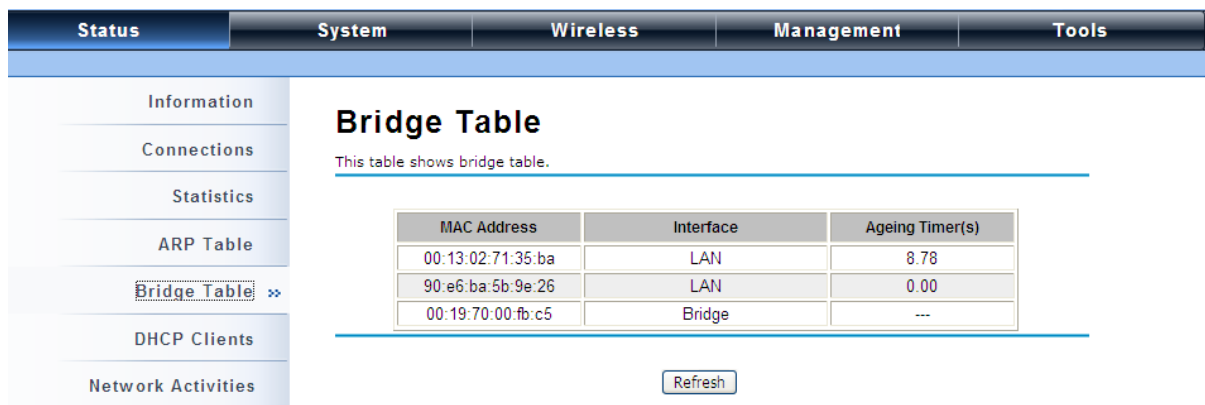


The screenshot shows a network management interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'Status' menu is expanded on the left, showing options like 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The 'ARP Table' option is selected. The main content area displays the title 'ARP Table' and a sub-header 'This table shows ARP table.' Below this is a table with three columns: 'IP Address', 'MAC Address', and 'Interface'. The table contains one entry: IP Address 192.168.1.111, MAC Address 90:E6:BA:5B:9E:26, and Interface br0. A 'Refresh' button is located below the table.

IP Address	MAC Address	Interface
192.168.1.111	90:E6:BA:5B:9E:26	br0

## View Bridge Table

Open “Bridge Table” in “Status” as below. Click “Refresh” to view current connected status..



The screenshot shows the same network management interface as above. The 'Status' menu is expanded, and the 'Bridge Table' option is selected. The main content area displays the title 'Bridge Table' and a sub-header 'This table shows bridge table.' Below this is a table with three columns: 'MAC Address', 'Interface', and 'Ageing Timer(s)'. The table contains three entries: MAC Address 00:13:02:71:35:ba on LAN interface with an ageing timer of 8.78; MAC Address 90:e6:ba:5b:9e:26 on LAN interface with an ageing timer of 0.00; and MAC Address 00:19:70:00:fb:c5 on Bridge interface with an ageing timer of ---. A 'Refresh' button is located below the table.

MAC Address	Interface	Ageing Timer(s)
00:13:02:71:35:ba	LAN	8.78
90:e6:ba:5b:9e:26	LAN	0.00
00:19:70:00:fb:c5	Bridge	---

## View Active DHCP Client Table

Open “DHCP Clients” in “Status” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “Refresh” to view current table.



Status	System	Wireless	Management	Tools
--------	--------	----------	------------	-------

- Information
- Connections
- Statistics
- ARP Table
- Bridge Table
- DHCP Clients >>
- Network Activities

## 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)
192.168.1.100	00:19:70:00:fb:c5	1799913

## View Network Activities

The network activities allows you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Web of the Skyport. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. Throughput statistics can be updated manually using the “Refresh” button.

Status	System	Wireless	Management	Tools
--------	--------	----------	------------	-------

- Information
- Connections
- Statistics
- ARP Table
- Bridge Table
- DHCP Clients
- Network Activities >>

## Network Activities

This page shows Throughput information of LAN and WLAN.

Wireless

Ethernet 1

# System

## Basic System Settings

### λ 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 (-).

**Network Mode:** Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to **TCP/IP Settings**”.

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

**Country Region:** For FCC domain, the default country is United States only.

**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.

### λ GPS Coordinate Settings

The GPS Coordinate Setting helps you mark the latitude and longitude of the ZAC Access Point. Just enter the coordinates and click the **Apply** button.

## TCP/IP Settings

Open “TCP/IP Settings” in “System” as below to configure the parameters for LAN which connects to the LAN port of the ZAC Access Point. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

The screenshot shows the web management interface for the ZAC Access Point. The top navigation bar includes tabs for Status, System (selected), Wireless, Management, and Tools. On the left, a sidebar menu lists Basic Settings, TCP/IP Settings (highlighted with a double arrow), Time Settings, RADIUS Settings, and Firewall Settings. The main content area is titled "TCP/IP Settings" and contains a descriptive paragraph: "Use this page to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..". Below this is the "IP Address Assignment" section, which has two radio button options: "Obtain IP Address Automatically" (unselected) and "Use Fixed IP Address" (selected). Under the "Use Fixed IP Address" option, there are five input fields: 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), and 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 Point is able to obtain IP settings automatically from that DHCP server.



### Note:

---

λ When the IP address of the ZAC Access Point is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the client computer by running the “nbtstat -r” command before using the device name of the ZAC Access Point to access its Web Management page.

λ In case the IEEE 802.11n ZAC Access Point is unable to obtain an IP address from a valid DHCP server, it will fall back to default static IP address.

---

**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.

If the IEEE 802.11n ZAC Access Point is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

**WAN Settings:** Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

**LAN Settings:** When DHCP Server is disabled, users can specify IP address and subnet mask for the ZAC ACCESS POINT manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes). A DHCP relay agents is used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. To enable the DHCP relay agent, check the “Enable DHCP Relay” checkbox and enter the IP address of the DHCP server.

 **Warning:**

- 
- λ In AP mode, the IEEE 802.11n ZAC Access Point must establish connection with another wireless device before it is set to Router mode. To access the unit in Router mode via wired port, please type the WAN IP address to enter the web page for WAN
-

---

is on wired port and LAN is on wireless port. Or, you can access device through the wireless device connected with the ZAC AP.

- λ In wireless client mode, users can access the ZAC Access Point via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to Router mode.
  - λ Bridge mode and AP Repeater mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect the ZAC Access Point with another wireless device before it is set to Router mode and access the ZAC Access Point via the connected wireless device.
- 

## Time Settings

Compliant with NTP, the IEEE 802.11n ZAC Access Point is capable of keeping its time in accord with the Internet time. To use this feature, check **Enable NTP Client Update** in advance.

Status	System	Wireless	Management	Tools
Basic Settings	Time Settings			
TCP/IP Settings				
RADIUS Settings				
Firewall Settings				

### Time Settings

You can synchronize System Log's time stamp with a public time server over the Internet.

Current Time : Yr  Mon  Day  Hr  Mn  Sec

Time Zone Select :

Enable NTP client update

NTP server :

Manual IP :

- λ **Current Time**

Display the present time in Yr, Mon, Day, Hr, Min and Sec.

- λ **Time Zone Select**

Select the time zone from the dropdown list.

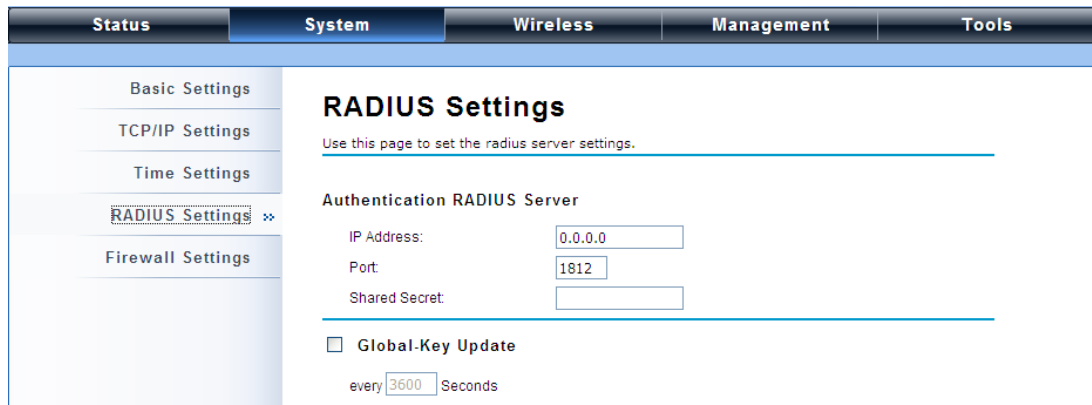
- λ **NTP Server**

Select the time server from the “NTP Server” dropdown list. or manually input the IP address of available time server into “Manual IP”.

## 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.

Open “**RADIUS Settings**” in “**System**” to make RADIUS configuration.



The screenshot shows a web-based configuration interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is active. On the left, a sidebar lists 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings' (highlighted with a double arrow), and 'Firewall Settings'. The main content area is titled 'RADIUS Settings' and includes the instruction 'Use this page to set the radius server settings.' Below this, the 'Authentication RADIUS Server' section contains three input fields: 'IP Address' with the value '0.0.0.0', 'Port' with the value '1812', and 'Shared Secret' which is empty. A checkbox labeled 'Global-Key Update' is unchecked, and below it is a text input field with the value '3600' followed by the text 'Seconds'.

### λ **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.

### λ **Global-Key Update**

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

## 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**.

### λ Source IP Filtering:

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering' (highlighted with a double arrow), 'Dst IP Filtering', 'Src Port Filtering', and 'Dst Port Filtering'. The main content area is titled 'Source IP Filtering' and includes a description: '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.' Below this is a checkbox for 'Enable Source IP Filtering'. There are two input fields: 'Local IP Address:' and 'Comment:'. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table with four columns: 'Local IP Address', 'Comment', 'Select', and '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**.

### λ Destination IP Filtering:

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering' (highlighted with a double arrow), and 'Src Port Filtering'. The main content area is titled 'Destination IP Filtering' and includes a description: 'Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.' Below this is a checkbox for 'Enable Destination IP Filtering'. There are two input fields: 'Destination IP Address:' and 'Comment:'. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table with four columns: 'Destination IP Address', 'Comment', 'Select', and '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.

**Destination IP Address:** Enter the IP address to be restricted.

**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 destination IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

λ **Source Port Filtering:**

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes tabs for Status, System, Wireless, Management, and Tools. The left sidebar contains a list of settings categories: Basic Settings, TCP/IP Settings, Time Settings, RADIUS Settings, Firewall Settings, Src IP Filtering, Dst IP Filtering, Src Port Filtering (highlighted with a double arrow), and Dst Port Filtering. The main content area is titled "Source Port Filtering" and contains the following elements:

- A descriptive paragraph: "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."
- An unchecked checkbox labeled "Enable Source Port Filtering".
- Input fields for "Port Range" (two boxes separated by a hyphen) and "Protocol" (a dropdown menu currently set to "Both").
- A text input field for "Comment".
- "Apply" and "Cancel" buttons.
- A table header with columns: "Source Port Range", "Protocol", "Comment", "Select", and "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.

**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 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**



λ **Destination Port Filtering:**

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**.

λ **Port Forwarding:**

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. Check the **Enable Port Forwarding** checkbox to

activate port forwarding.

**IP Address:** Enter the IP address the local server.

**Protocol:** Select **Both**, **UDP** or **TCP**.

**Port Range:** Specify the port range.

**Comment:** Make comments to record the port forwarding rule.

## UDP Pass Through

The screenshot shows a network management interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings' (highlighted with a red square), 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering', 'Dst Port Filtering', 'Port Forwarding', and 'UDP Pass through >>'. The main content area is titled 'UDP Pass through' and contains the text 'All UDP packets will be passed through the firewall'. Below this is a checkbox labeled 'Enable UDP Pass through' which is currently unchecked. At the bottom of the main area are 'Apply' and 'Cancel' buttons.

By check **Enable UDP Pass through** will allow all the UDPs packets to pass through the firewall.

Note that opening all the UDP ports will be very likely to expose the network to intruders

## DMZ:

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. To activate DMZ, check the **Enable DMZ** checkbox.

The screenshot shows a network management interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings' (highlighted with a red square), and 'Src IP Filtering'. The main content area is titled 'DMZ' and contains the text 'A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers,SMTP (e-mail) servers and DNS servers.' Below this is a checkbox labeled 'Enable DMZ' which is currently unchecked. Underneath is a text input field labeled 'DMZ Host IP Address:' with the value '0.0.0.0'. At the bottom of the main area are 'Apply' and 'Cancel' buttons.

**DMZ Host IP Address:** Enter the local host IP address.

## Wireless

Open “**Basic Settings**” in “**Wireless**” as below to make basic wireless configuration.

The screenshot shows the 'Basic Settings' page for the Wireless interface. The page is divided into a navigation bar at the top with tabs for 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'Wireless' tab is active. On the left side, there is a sidebar with a list of settings: 'Basic Settings' (selected), 'Security Settings', 'Advanced Settings', 'Traffic Shaping', 'Access Control', and 'WDS Settings'. The main content area is titled 'Basic Settings' and contains a checkbox labeled 'Disable Wireless LAN Interface'. Below this checkbox are several configuration fields: 'Operation Mode' (set to 'AP'), 'SSID' (set to 'Wireless'), 'Broadcast SSID' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), '802.11 Mode' (set to '802.11B/G/N'), 'Channel Mode' (set to '20 MHz'), 'Channel' (set to '2437MHz (6)'), 'Extension Channel' (set to 'None'), 'Data Rate' (set to 'Auto'), and 'HT Protect' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected). A 'Site Survey' button is located to the right of the 'Operation Mode' dropdown.

### λ **Disable Wireless LAN Interface**

Check this option to disable WLAN interface, then the wireless module of IEEE 802.11n ZAC Access Point will stop working and no wireless device can connect to it.

### λ **Operation Mode**

Four operating modes are available in IEEE 802.11n ZAC Access Point when acts as a FAT AP.

**AP:** The IEEE 802.11n ZAC Access Point establishes a wireless coverage and receives connectivity from other wireless devices.

**Wireless Client:** The IEEE 802.11n ZAC Access Point is able to connect to the AP and thus join the wireless network around it.

**Bridge:** The IEEE 802.11n ZAC Access Point establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the “**WDS Settings**” for detailed configuration.

**AP Repeater:** The IEEE 802.11n ZAC Access Point servers as AP and Bridge concurrently. In other words, the IEEE 802.11n ZAC Access Point can provide connectivity services for CPEs under Bridge mode.

λ **Wireless Network Name (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 can not exceed 32 characters.

λ **Broadcast SSID**

Under 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 can not scan and find IEEE 802.11n ZAC Access Point, so that malicious attack by some illegal STA could be avoided.

λ **802.11 Mode**

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

λ **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.

λ **Frequency/Channel**

Channel varies much as the available band differs from country to country.

λ **Extension Channel**

Only applicable to AP, AP Repeater, and 40MHz channel width) indicates the use of channel bonding that allows the IEEE 802.11n ZAC Access Point to use two channels at once. Two options are available: Upper Channel and Lower Channel.

λ **Channel Mode**

Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference. **Maximum Output Power (per chain):**

Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. The output power will vary depending on each country's regulation.

λ **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.

λ **Extension 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.

λ **Enable MAC Clone**

Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

λ **Site Survey**

Under wireless client mode, the IEEE 802.11n ZAC Access Point is able to perform site survey, through which, information on the available access points will be detected.

Open **“Basic Settings”** in **“Wireless”**, by clicking the **“Site Survey”** button beside **“Wireless Mode”** option, the wireless site survey window will pop up with a list of available AP in the vicinity.

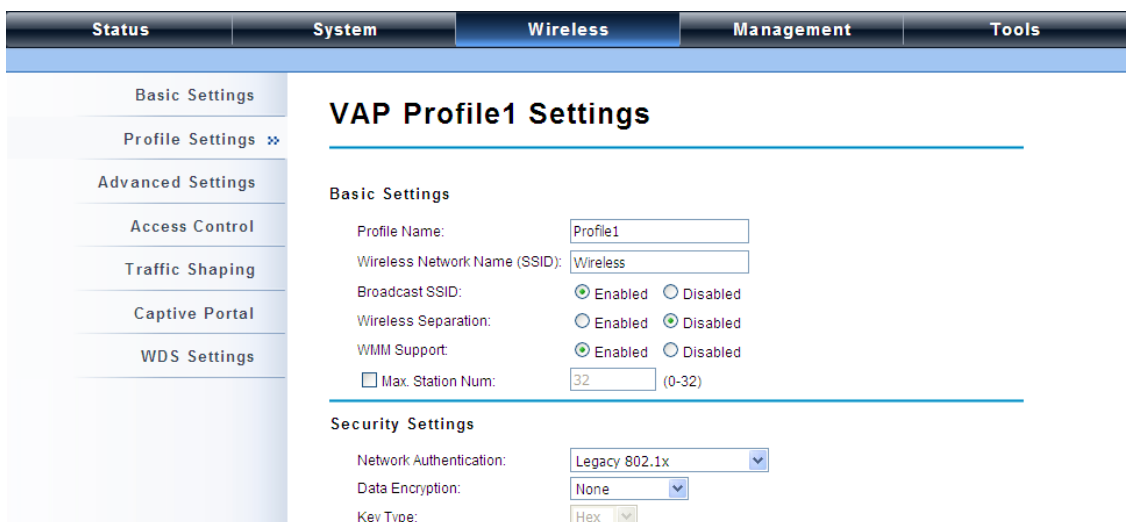
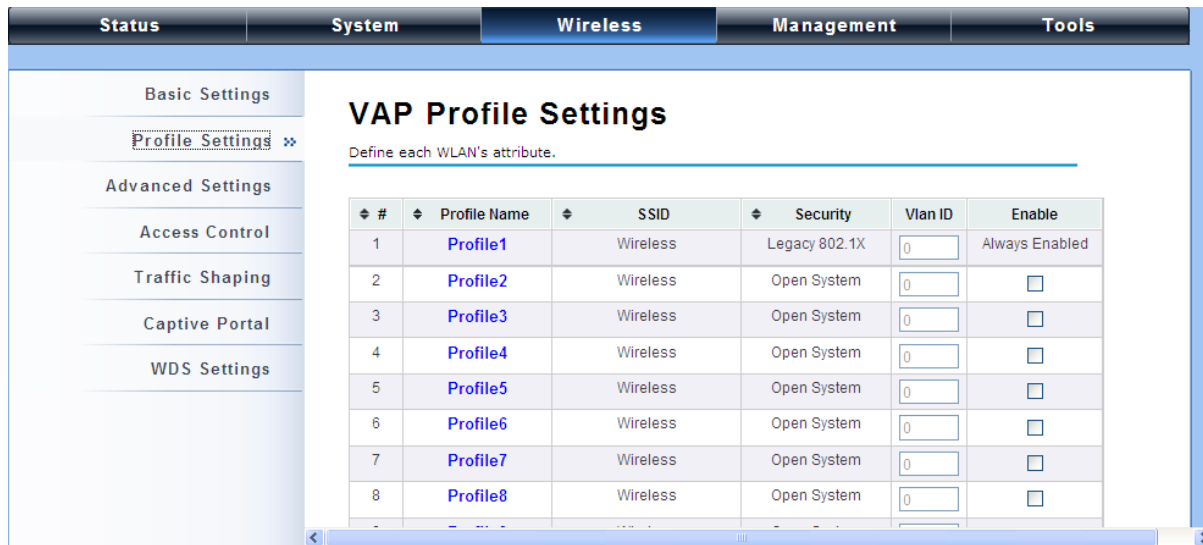
Select the AP you would like to connect and click **“Selected”** to establish connection.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
<input type="radio"/>	aeap17	2412MHz(1)	00:24:01:df:67:8e	802.11B/G	-78	WPA
<input type="radio"/>	aeap18	2412MHz(1)	00:21:91:f6:f7:55	802.11B/G	-77	NONE
<input type="radio"/>	FRITZ!Box Fon WLAN 7270	2412MHz(1)	00:24:fe:46:b9:c8	802.11B/G/N	-75	WPA2
<input type="radio"/>	RT-G32	2437MHz(6)	20:cf:30:d6:5a:d0	802.11B/G	-62	WEP
<input type="radio"/>	MIS-AP2	2437MHz(6)	00:13:f7:8e:8d:d3	802.11B/G/N	-49	WPA2
<input type="radio"/>	HTC	2437MHz(6)	90:21:55:c2:3f:9c	802.11B/G	-81	NONE
<input type="radio"/>	DIR-635	2462MHz(11)	00:24:a5:b4:cf:77	802.11B/G	-64	WPA
<input type="radio"/>	Apple Network 873e69	2417MHz(2)	10:9a:dd:87:3e:69	802.11B/G/N	-75	WPA2
<input type="radio"/>	ASIX_WiFi	2422MHz(3)	00:1e:58:29:28:27	802.11B/G	-65	NONE

**VAP Profile Settings**

Available in AP mode, the IEEE 802.11n ZAC Access Point allows up to 16 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.



λ **Basic Setting**

**Profile Name:** Name of the VAP profile

**Wireless Network Name:** Enter the virtual SSID for the VAP

**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. Under the mode except wireless client mode, enable “**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

**Max. Station Number:** By checking 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. By disabling the checkbox the ZAC Access Point will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

λ **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.

λ **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:**

- 
- λ 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.

λ **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:**

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



## VLAN

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

To allow users on the VLAN to access the WEB page of the IEEE 802.11a/n ZAC Access Point, you need to enable “**Enable 802.1Q VLAN**” and assign a management VLAN ID for your device. Make sure the assigned management VLAN ID is identical to your network VLAN ID to avoid failures of accessing the Web page of the IEEE 802.11n ZAC Access Point.

The screenshot shows the 'Wireless' management page. On the left is a sidebar with navigation options: Basic Settings, Profile Settings, Advanced Settings, Access Control, Traffic Shaping, Captive Portal, and WDS Settings. The main area contains a table with columns: System, Profile, Wireless, Management, and Tools. Below the table is a section for 'Enable 802.1Q VLAN' with a checked checkbox and a 'Management VLAN ID' input field set to '0'. 'Apply' and 'Reset' buttons are at the bottom.

Status	System	Wireless	Management	Tools		
Basic Settings	10	Profile10	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
Profile Settings	11	Profile11	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
Advanced Settings	12	Profile12	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
Access Control	13	Profile13	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
Traffic Shaping	14	Profile14	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
Captive Portal	15	Profile15	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
WDS Settings	16	Profile16	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>

Enable 802.1Q VLAN  
Management VLAN ID:

## Advanced Settings

Open “**Advanced Settings**” in “**Wireless**” to make advanced wireless settings.

The screenshot shows the 'Wireless Advanced Settings' page. The sidebar on the left has 'Advanced Settings' selected. The main area is titled 'Wireless Advanced Settings' and includes a warning: '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.' Below are various settings with radio buttons and input fields.

**Wireless 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:  (1-2347)
- Fragment Threshold:  (256-2346)
- Beacon Interval:  (20-1024 ms)
- DTIM Interval:  (1-255)
- Preamble Type:  Long  Auto
- IGMP Snooping:  Enabled  Disabled
- RIFS:  Enabled  Disabled

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.

λ **Short GI**

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

λ **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.

λ **Fragmentation Length**

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.

λ **Beacon Interval**

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

λ **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.

λ **Preamble Type**

It defines some details on the 802.11 physical layer. “**Long**” and “**Auto**” are available.

λ **IGMP Snooping**

Available in AP/Router mode, 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 or groups.

λ **RIFS**

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

λ **Link Integration**

Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking “**Enabled**”. It can inform the associating wireless clients as soon as the disconnection occurs.

λ **TDM Coordination**

Stands for “Time-Division Multiplexing Technique”, this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in AP/CPE mode. It is highly recommended to enable TDM coordination when there are multiple CPEs needed to connect to the AP in your application.

λ **LAN2LAN CPE**

LAN2LAN CPE mode enables packet forwarding at layer 2 level. It is fully transparent for all the Layer2 protocols.

λ **Space in Meter**

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.

λ **Flow Control**

It allows the administrator to specify the incoming and outgoing traffic limit by checking “**Enable Traffic Shaping**”. This is only available in Router mode.

 **Note:**

---

λ We strongly recommend you leave most advanced settings at their defaults except “Distance in Meters” adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.

---

## **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.



λ **Profile Selection:** Select the VAP network you would like to enable access control.

λ **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.

λ **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.

λ **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.



## λ Overall Traffic Shaping

Check this box to control the overall bandwidth of the ZAC Access Point.

**Incoming Traffic Limit:** To specify maximum incoming bandwidth to a certain rate in kbit/s.

**Incoming Traffic Burst:** To specify the buffer size for incoming 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.

**Outgoing Traffic Limit:** To limit the outbound traffic to a certain rate in kbit/s.

**Outgoing Traffic Burst:** To specify the buffer size for outbound traffic. The suggested value is 20KBytes. You may decrease it to smaller value if the outbound traffic limit is smaller.

## λ VAP Traffic Shaping

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

**Incoming Traffic Limit:** To specify maximum incoming bandwidth to a certain rate in kbit/s.

**Incoming Traffic Burst:** To specify the buffer size for incoming 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.

## 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.

Status	System	Wireless	Management	Tools
<div style="display: flex; justify-content: space-between;"> <div style="width: 20%;"> <ul style="list-style-type: none"> <li>Basic Settings</li> <li>Profile Settings</li> <li>Advanced Settings</li> <li>Access Control</li> <li>Traffic Shaping</li> <li><b>Captive Portal</b> &gt;&gt;</li> <li>WDS Settings</li> </ul> </div> <div style="width: 80%;"> <h2 style="margin: 0;">Captive Portal</h2> <p style="margin: 0;">Use this page to set basic Captive Portal settings.</p> <hr/> <p><input type="checkbox"/> Captive Portal Enable</p> <p>Profile Selection: <input type="text" value="VAP1 - Wireless"/></p> <hr/> <h3>RADIUS Settings</h3> <p>Primary RADIUS Server: <input type="text" value="radius1.coova.net"/></p> <p>Secondary RADIUS Server: <input type="text" value="radius2.coova.net"/></p> <p>RADIUS Auth Port: <input type="text" value="1812"/></p> <p>RADIUS Acct Port: <input type="text" value="1813"/></p> <p>RADIUS Shared Secret: <input type="text" value="*****"/></p> <p>RADIUS NASID: <input type="text" value="your-radius-nasid"/></p> <hr/> <h3>Captive Portal Settings</h3> <p>UAM Portal URL: <input type="text" value="https://www.coova.n"/></p> <p>UAM Secret: <input type="text" value="*****"/></p> </div> </div>				

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

λ **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

λ **Radius Administrative-User:**

**Radius Admin Username:** Enter the username of the Radius Administrator

**Radius Admin Password:** Enter the password of the Radius Administrator

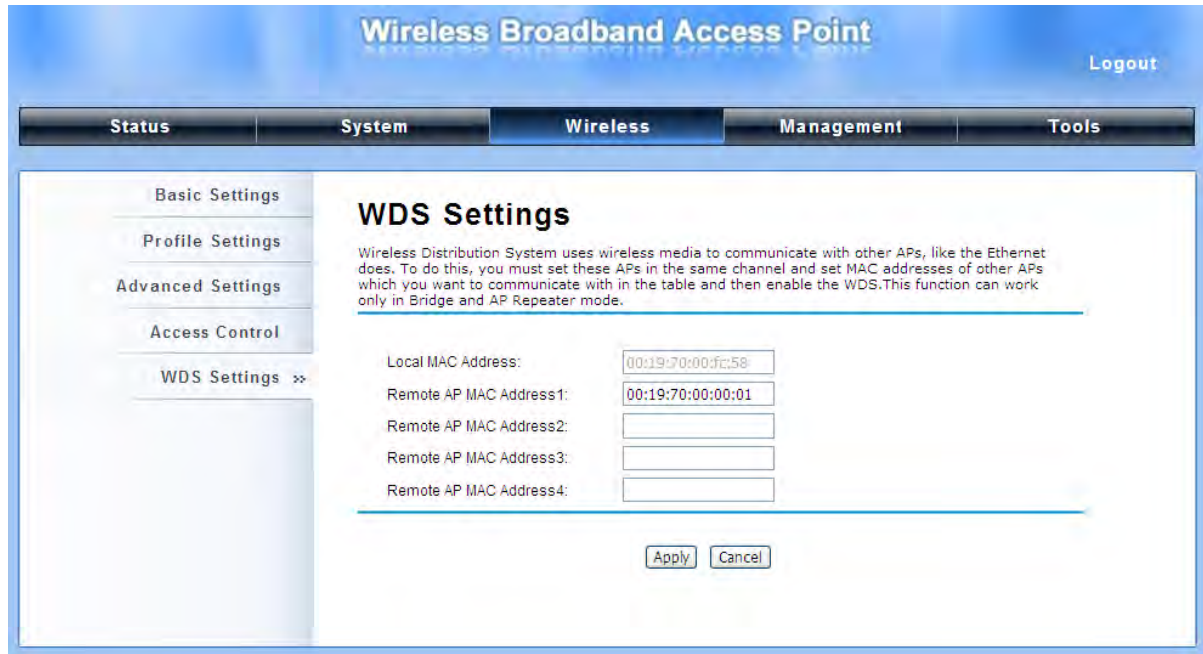
λ **Captive Portal**

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

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

## WDS Settings

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Simply put, you can link the Access Points wirelessly. Open “WDS Settings” in “Wireless” as below:



The screenshot shows the configuration interface for a Wireless Broadband Access Point. The page title is "Wireless Broadband Access Point" with a "Logout" link in the top right. A navigation bar contains tabs for "Status", "System", "Wireless", "Management", and "Tools". The "Wireless" tab is active, and a sidebar on the left lists settings categories: "Basic Settings", "Profile Settings", "Advanced Settings", "Access Control", and "WDS Settings" (which is expanded). The main content area is titled "WDS Settings" and includes a descriptive paragraph: "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." Below this text is a form with five input fields: "Local MAC Address" (pre-filled with 00:19:70:00:fc:58), "Remote AP MAC Address1" (pre-filled with 00:19:70:00:00:01), and four empty fields for "Remote AP MAC Address2" through "Remote AP MAC Address4". "Apply" and "Cancel" buttons are located at the bottom of the form.

Enter the MAC address of another AP you wirelessly want to connect to into the appropriate field and click “**Apply**” to save settings.

 **Note:**

- 
- λ WDS Settings is available only under Bridge and AP Repeater Mode.
  - λ 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.
-



## Management

### Password

From “**Password Settings**” in “**Management**”, you can change the password to manage your IEEE 802.11n ZAC Access Point.

The screenshot shows the web interface with the 'Management' tab selected. On the left, a sidebar contains 'Password Settings' (with a double arrow icon), 'Firmware Upgrade', 'Configuration File', 'User Certificates', 'Remote Services', and 'SNMP Settings'. The main content area is titled 'Password Settings' and includes the instruction: 'Use this page to set the password of this unit.' Below this are three input fields: 'Current Password:', 'New Password:', and 'Confirm Password:'. Each field contains a series of dots representing masked text. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

- λ **Current Password:** Enter the current password.
- λ **New Password:** Enter the new password.
- λ **Confirm Password:** Enter the new password again for confirmation.

#### Note:

- 
- λ The password is case-sensitive and its length cannot exceed 19 characters!
- 

### Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through IEEE 802.11n ZAC Access Point’s Web:

The screenshot shows the web interface with the 'Management' tab selected. On the left, a sidebar contains 'Password Settings', 'Firmware Upgrade' (with a double arrow icon), 'Configuration File', 'User Certificates', 'Remote Services', and 'SNMP Settings'. The main content area is titled 'Firmware Upgrade' and includes the instruction: '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.' Below this is a 'Select File:' label followed by two buttons: '選擇檔案' (Browse) and '未選擇檔案' (No file selected). At the bottom right of the form are 'Upgrade' and 'Cancel' buttons.

- λ Click “**Browse**” to select the firmware file you would like to load;
- λ Click “**Upload**” to start the upload process;
- λ Wait a few minutes, the ZAC Access Point will reboot after successful upgrade.

 **Note:**

---

λ Do NOT cut the power off during upgrade, otherwise the system may crash!

---

## Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open “**Configuration File**” in “**Management**” as below:



λ **Save Setting to File**

By clicking “**Save**”, a dialog box will pop up. Save it, then the configuration file **ap.cfg** will be generated and saved to your local computer.

λ **Load Settings from File**

By clicking “**Browse**”, a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click “**Upload**” to load the file. After automatically rebooting, new settings are applied.

## Restore Factory Default Settings

The IEEE 802.11n ZAC Access Point provides two ways to restore the factory default settings:

λ **Restore factory default settings via Web**

From “**Configuration File**”, clicking “**Reset**” will eliminate all current settings and reboot your device, then default settings are applied.



### λ Restore factory default settings via Reset Button

If software in IEEE 802.11n ZAC Access Point is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

## Reboot

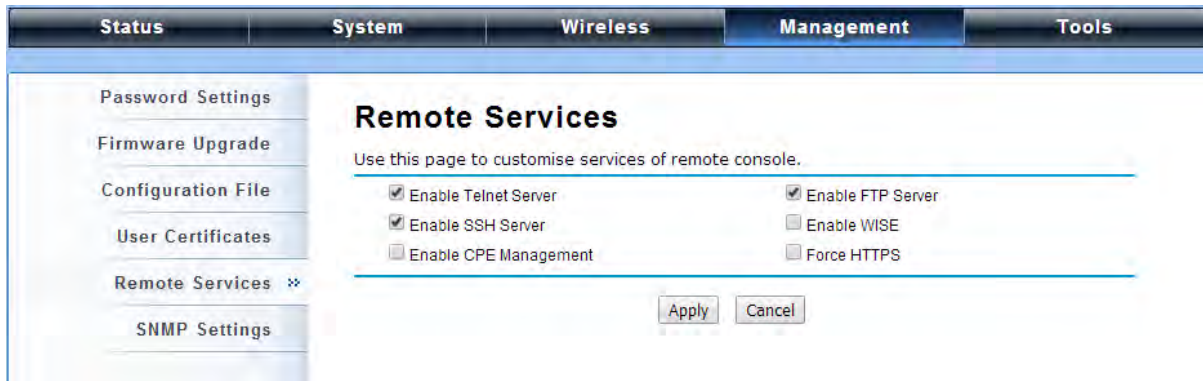
You can reboot your IEEE 802.11n ZAC Access Point from “**Configuration File**” in “**Management**” as below:

Click “**Reboot**” and hit “**Yes**” upon the appeared prompt to start reboot process. This takes a few minutes.



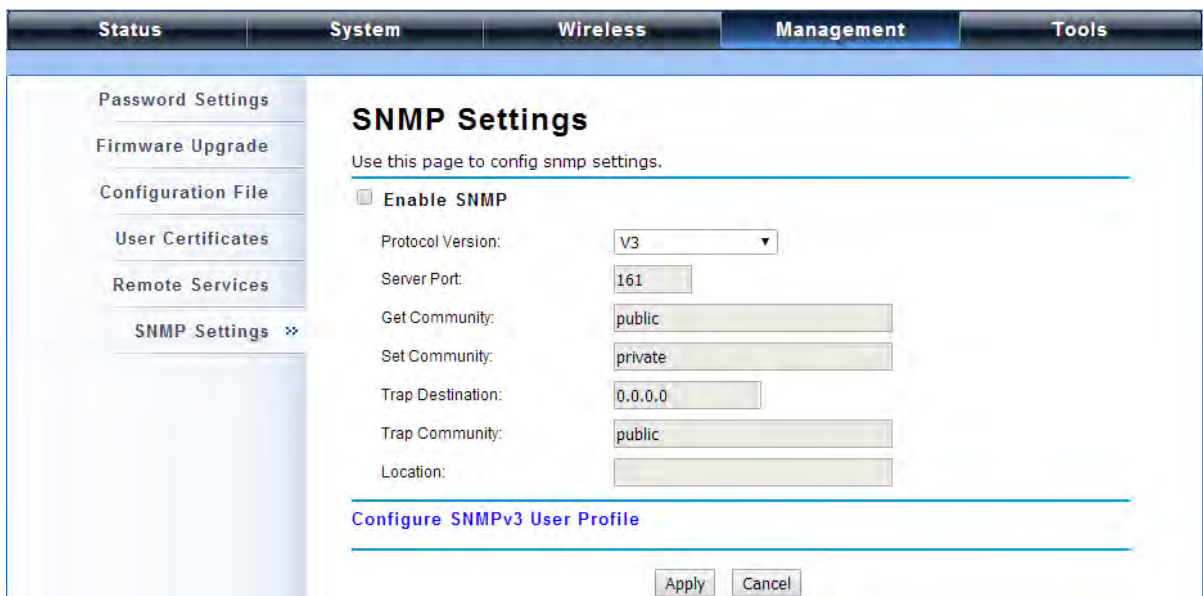
## Remote Management

The IEEE 802.11n ZAC Access Point provides a variety of remotes managements including Telnet, SNMP, FTP, SSH, HTTPS and exclusive WISE tool, making configuration more convenient and secure.



## SNMP Management

The IEEE 802.11n ZAC Access Point supports SNMP for convenient remote management. Open “SNMP Settings” in “Management” shown below. Set the SNMP parameters and obtain MIB file before remote management.



**Protocol Version:** Select the SNMP version, and keep it identical on the IEEE 802.11n ZAC Access Point and the SNMP manager. The IEEE 802.11n ZAC Access Point supports SNMP v2/v3.

**Server Port:** Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

**Get Community:** Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

**Set Community:** Specify the password for the incoming Set requests from the management station. By default, it is set to private.

**Trap Destination**: Specify the IP address of the station to send the SNMP traps to.

**Trap Community**: Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

λ **Configure SNMPv3 User Profile**

For SNMP protocol version 3, you can click “**Configure SNMPv3 User Profile**” in blue to set the details of SNMPv3 user. Check “**Enable SNMPv3 Admin/User**” in advance and make further configuration.

**User Name**: Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the IEEE 802.11n ZAC Access Point.

**Password**: Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the IEEE 802.11n Wireless ZAC Access Point.

**Confirm Password**: Input that password again to make sure it is your desired one.

**Access Type**: Select “**Read Only**” or “**Read and Write**” accordingly.

**Authentication Protocol**: Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

**PriZACy Protocol**: Specify the encryption method for SNMP communication. None and DES are available. **None** means no encryption is applied. **DES** is a Data Encryption Standard that applies a 58-bit key to each 64-bit block of data.

## Certificate Settings

Under Wireless Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The Server can trust all certificates issued by a given CA.

To import a user certificate, from Import User Certificates, click “**Browse**” and specify the location where the user certificate is placed. Click “**Import**”.



The screenshot shows a web interface with a top navigation bar containing tabs for Status, System, Wireless, Management, and Tools. The Management tab is active. On the left is a sidebar menu with options: Password Settings, Firmware Upgrade, Configuration File, User Certificates (selected with a double arrow), Remote Services, and SNMP Settings. The main content area is titled "User Certificates" and includes the instruction "Use this page to upload/delete user certificates." Below this, there are two rows of controls. The first row is for "Import Certificate" and contains a file selection button with "選擇檔案" (Choose File) and "未選擇檔案" (No file selected) text, and an "Import" button. The second row is for "Delete Certificate" and contains a dropdown menu and a "Delete" button.

λ **Delete User Certificate:** Delete the selected user certificate.

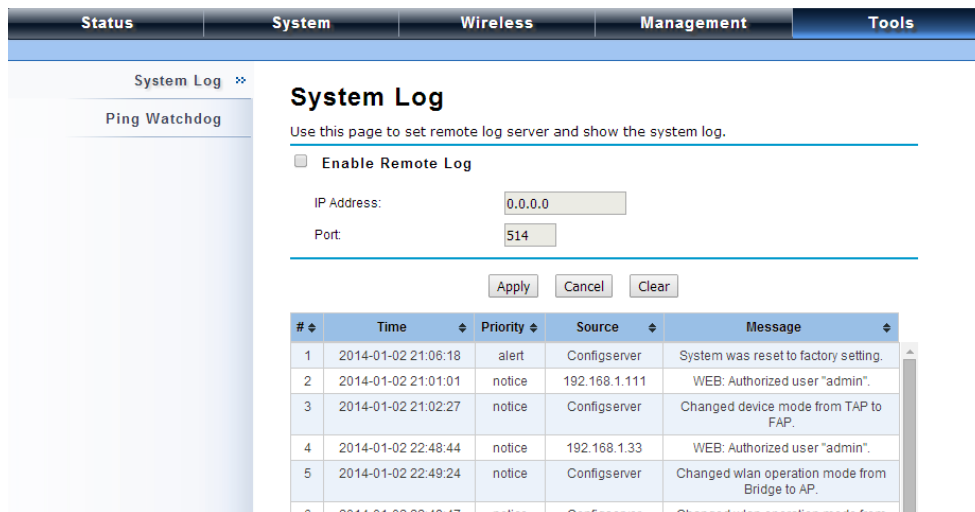
λ **Import User Certificates:** Imported the user certificate

## Tools

### System Log

System log is used for recording events occurred on the IEEE 802.11n ZAC Access Point, including station connection, disconnection, system reboot and etc.

Open “**System Log**” in “**Tools**” as below.



#	Time	Priority	Source	Message
1	2014-01-02 21:06:18	alert	Configserver	System was reset to factory setting.
2	2014-01-02 21:01:01	notice	192.168.1.111	WEB: Authorized user "admin".
3	2014-01-02 21:02:27	notice	Configserver	Changed device mode from TAP to FAP.
4	2014-01-02 22:48:44	notice	192.168.1.33	WEB: Authorized user "admin".
5	2014-01-02 22:49:24	notice	Configserver	Changed wlan operation mode from Bridge to AP.
6	2014-01-02 22:49:47	notice	Configserver	Changed wlan operation mode from

#### λ Remote Syslog Server

**Enable Remote Syslog:** Enable System log to alert remote server.

**IP Address:** Specify the IP address of the remote server.

**Port:** Specify the port number of the remote server.

### Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.

Status	System	Wireless	Management	Tools
System Log				
Ping Watchdog ✖				
<h3>Ping Watchdog</h3> <p>This page provides a tool to configure the Ping Watchdog. If the fail count of the Ping reaches a specified value, the watchdog will reboot the device.</p> <hr/> <input checked="" type="checkbox"/> Enable Ping Watchdog IP Address to Ping: <input type="text" value="192.168.1.111"/> Ping Interval: <input type="text" value="300"/> seconds Startup Delay: <input type="text" value="100"/> seconds(>=100) Failure Count To Reboot: <input type="text" value="300"/> <hr/> <div style="text-align: right;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>				

λ **Ping Watchdog**

**Enable Ping Watchdog:** To activate ping watchdog, check this checkbox.

**IP Address to Ping:** Specify the IP address of the remote unit to ping.

**Ping Interval:** Specify the interval time to ping the remote unit.

**Startup Delay:** Specify the startup delay time to prevent reboot before the IEEE 802.11n ZAC Access Point is fully initialized.

**Failure Count To Reboot:** If the ping timeout packets reached the value, the IEEE 802.11n ZAC Access Point will reboot automatically.



# Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ACSII).

As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

**Table 1 ACSII**

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64		7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		



# Appendix B. Specification

## B-1 ZAC-1023-5-13

Features	Additional Information
Standard Compliance	<ul style="list-style-type: none"> <li>- IEEE802.3u MDI / MDIX 10/100 Fast Ethernet</li> <li>- IEEE802.11a/n wireless LAN interface</li> <li>- IEEE 802.11n wireless LAN standard</li> </ul>
DDRII	64Mbyte
Flash	16Mbyte
Power input requirement	Passive PoE 24V Pin 4,5 VDC+ Pin 7,8 VDC-
Ethernet PHY	10/100 Mbps
Antenna	Internal 11 +/- 2 dBi directional antenna (Vertical, Horizontal)
Antenna Frequency Band	5150-5250 ; 5250-5470 ; 5470-5725 ; 5725-5850 MHz
Vertical Port HPBW	(XY Plane /H-Plane) : 67°; (XZ Plane /E-Plane): 15°
Horizontal Port HPBW	(XY Plane /H-Plane) : 87°; (XZ Plane /E-Plane): 20°
Antenna Configuration	2 * 2 (2 Tx,2 Rx)
LAN port	1port
Reset Button	Reset to factory default
Ground	Ground terminal x1
System Update Capability	<ul style="list-style-type: none"> <li>- Support Web-UI upgrade via Ethernet port or wireless network</li> <li>- Support TFTP upgrade via Ethernet port</li> </ul>
LED Definition	<p><b>Power (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Green On: Power / system on</li> <li>• Green Off: power / system off</li> </ul> <p><b>LAN (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Off: No Ethernet connection detected</li> <li>• Green On: Ethernet connection detected</li> <li>• Green Blinking: Sending / receiving data</li> </ul> <p><b>5G WLAN (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Green Off: WLAN disabled</li> <li>• Green On: WLAN enable</li> <li>• Green Blinking: WLAN data transmit</li> </ul> <p><b>Signal *3 (Single-color LED x3)</b></p> <ul style="list-style-type: none"> <li>• Excellent: 3 LED Green ON</li> <li>• Good: 2 LED Green ON</li> <li>• Weak: 1 LED Green ON</li> </ul>
Data Rate	11a: 54M, 48M, 36M, 24M, 18M, 12M, 9M, 6Mbps auto fallback 11n: HT20 MCS0~15 HT40 MCS0~15

Data modulation type	DSSS/BPSK/QPSK/CCK/DQPSK/DBPSK 802.11a: OFDM 802.11n: OFDM			
RF frequency range <sup>1 2</sup>	FCC: 5.15GHz~5.25GHz ; 5.725GHz~5.85GHz NCC: 5.15GHz~5.25GHz ; 5.725GHz~5.85GHz CE: 5.15GHz~5.35GHz; 5.47GHz~5.725GHz			
Power Consumption (W)	<12W			
Average Output Power @ 25°C (Single Chain) (± 2dBm) <sup>3</sup> <sup>4</sup>	802.11a	Date	5150~5725MHz	5725~5850MHz
		Rate/Frequency		
		6, 9, 12, 18, 24Mbps	23dBm	20 dBm
		36Mbps	22 dBm	20 dBm
		48Mbps	21 dBm	20 dBm
	54Mbps	20 dBm	20 dBm	
	802.11an At HT20	Date	5150~5725	5725~5850
		Rate/Frequency	MHz	MHz
		MCS0, MCS8	23dBm	20 dBm
		MCS1, MCS2, MCS3, MCS9, MCS10, MCS11	23 dBm	20 dBm
		MCS4, MCS12	22 dBm	20 dBm
		MCS5, MCS13	21 dBm	20 dBm
		MCS6, MCS14	20 dBm	20 dBm
		MCS7, MCS15	19 dBm	19 dBm

<sup>1</sup> Disable 5600~5650MHz due to Environment Canada weather satellites operating in the band are protected.

<sup>2</sup> Disable 5250~5350MHz & 5470~5725MHz due to DFS band at FCC domain.

<sup>3</sup> The listed value is the target power calibrated in the card. The actual power will vary depending on each country's regulation. For detailed CTL table settings please contact our sales representative.

<sup>4</sup> The output power been measured from U.FL connector without RF cable loss.

	802.11an At HT40	Date	5150~5725	5725~5850
		Rate/Frequency	MHz	MHz
		MCS0, MCS8	21dBm	20 dBm
		MCS1, MCS2, MCS3, MCS9, MCS10, MCS11	21 dBm	20 dBm
		MCS4, MCS12	21 dBm	20 dBm
		MCS5, MCS13	21 dBm	20 dBm
		MCS6, MCS14	20 dBm	20 dBm
		MCS7, MCS15	19 dBm	19 dBm
Sensitivity (at single chain)	Mode	11a	11n HT20	11n HT40
	6Mbps	$\geq -89$		
	9Mbps	$\geq -88$		
	12Mbps	$\geq -85$		
	18Mbps	$\geq -83$		
	24Mbps	$\geq -80$		
	36Mbps	$\geq -76$		
	48Mbps	$\geq -71$		
	54Mbps	$\geq -70$		
	MCS 0/8		$\geq -83$	$\geq -80$
	MCS 1/9		$\geq -80$	$\geq -77$
	MCS 2/10		$\geq -78$	$\geq -75$
	MCS 3/11		$\geq -75$	$\geq -72$
	MCS 4/12		$\geq -71$	$\geq -68$
	MCS 5/13		$\geq -67$	$\geq -64$
MCS 6/14		$\geq -66$	$\geq -63$	
MCS 7/15		$\geq -65$	$\geq -62$	

Features	Additional Information
Standard Compliance	<ul style="list-style-type: none"> <li>- IEEE802.3u MDI / MDIX 10/100 Fast Ethernet</li> <li>- IEEE802.11b/g wireless LAN interface</li> <li>- IEEE 802.11n wireless LAN standard</li> </ul>
DDRII	64Mbyte
Flash	16Mbyte
Power input requirement	Passive PoE 24V Pin 4,5 VDC+ Pin 7,8 VDC-
Ethernet PHY	10/100 Mbps
Antenna	Internal 9dBi directional antenna (Vertical, Horizontal)
Antenna Frequency band	2.4~2.5GHz
Vertical Port HPBW	(XY Plane /H-Plane) : >80° ; (XZ Plane /E-Plane) : >60°
Horizontal Port HPBW	(XY Plane /E-Plane) : >70° ; (XZ Plane /H-Plane) : >50°
Antenna Configuration	2 * 2 (2 Tx,2 Rx)
LAN port	1port
Reset Button	Reset to factory default
Ground	Ground terminal x1
System Update Capability	<ul style="list-style-type: none"> <li>- Support Web-UI upgrade via Ethernet port or wireless network</li> <li>- Support TFTP upgrade via Ethernet port</li> </ul>
LED Definition	<p><b>Power (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Green On: Power / system on</li> <li>• Green Off: power / system off</li> </ul> <p><b>LAN (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Off: No Ethernet connection detected</li> <li>• Green On: Ethernet connection detected</li> <li>• Green Blinking: Sending / receiving data</li> </ul> <p><b>WLAN (Single-color LED x1)</b></p> <ul style="list-style-type: none"> <li>• Green Off: WLAN disabled</li> <li>• Green On: WLAN enable</li> <li>• Green Blinking: WLAN data transmit</li> </ul> <p><b>Signal *3 (Single-color LED x3)</b></p> <ul style="list-style-type: none"> <li>• Excellent: 3 LED Green ON</li> <li>• Good: 2 LED Green ON</li> <li>• Weak: 1 LED Green ON</li> </ul>
Data Rate	11b: 11M, 5.5M, 2M, 1Mbps 11g: 54M, 48M, 36M, 24M, 18M, 12M, 9M, 6Mbps 11n: HT20 MCS0~15 HT40 MCS0~15
Data modulation type	DSSS/BPSK/QPSK/CCK/DQPSK/DBPSK 802.11b/g/n: OFDM 802.11n: OFDM

RF frequency range	FCC: 2.412 GHz ~ 2.462 GHz NCC: 2.412 GHz ~ 2.462 GHz CE: 2.412 GHz ~ 2.472 GHz				
Power Consumption (W)	<12W				
Average Output Power @ 25°C (Single Chain) (± 2dBm) 5	11b	1,5,11Mbps		27dB	
	11g	6, 9, 12, 18, 24Mbps		25dB	
		36Mbps		24dB	
		48, 54Mbps		23dB	
	11gn(HT20)	MCS0, MCS8		27dB	
		MCS1,MCS2,MCS3, MCS9,MCS10, MCS11		26dB	
		MCS4, MCS12		25dB	
		MCS5, MCS13		24dB	
		MCS6, MCS7, MCS14, MCS15		23dB	
	11gn(HT40)	MCS0, MCS8		26dB	
		MCS1,MCS2,MCS3, MCS9,MCS10, MCS11		25dB	
		MCS4, MCS12		24dB	
		MCS5, MCS13		23dB	
		MCS6, MCS7, MCS14, MCS15		22dB	
	Sensitivity (at single chain)	Mode	11b	11g	11n HT 20
		FER<8%	FER<10%	FER<10 %	FER<10%
11		-85	-	-	-
5.5		-88	-	-	-
2		-89	-	-	-
1		-91	-	-	-
6		-	-89	-	-
9		-	-88	-	-
12		-	-85	-	-
18		-	-83	-	-
24		-	-80	-	-
36		-	-76	-	-
48		-	-71	-	-
54		-	-70	-	-
0/8		-	-	-83	-
1/9		-	-	-80	-
2/10		-	-	-78	-
3/11		-	-	-75	-
4/12		-	-	-71	-
5/13		-	-	-67	-
6/14		-	-	-66	-
7/15		-	-	-65	-
0/8		-	-	-	-80
1/9		-	-	-	-77
2/10		-	-	-	-75
3/11	-	-	-	-72	

The listed value is the target power calibrated in the card. The actual power will vary depending on each country's regulation. For detailed CTL table settings please contact our sales representative.

	4/12	-	-	-	-68
	5/13	-	-	-	-64
	6/14	-	-	-	-63
	7/15	-	-	-	-62