

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

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

ZAC-503 / ZAC-504

ZWA-3090 / ZWA-3100

ZN-7200-2EI-O / ZN-7200-2AEI-O



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 Wireless Access Point and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

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



Note:

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



Warning:

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

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

Federal Communication Commission Interference Statement

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

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

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

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

This transmitter is restricted to indoor use only within the 5.15-5.25GHz and 5.470-5.725GHz bands.

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。

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.

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

Table of Content

Chapter 1 Introduction	12
Introduction.....	12
Appearance	13
Key Features	13
Typical Application.....	14
Chapter 2 Hardware Installation.....	15
Preparation before Installation	15
Professional Installation Required.....	15
Safety Precautions	15
Installation Precautions	16
Product Package	16
Hardware Installation	18
Connect up.....	18
Using the Grounding Wire.....	19
Install External Antennas	19
Mount the AP on a Pole	22
Power Up	23
Connect to the Access Point	24
Chapter 3 Basic Settings.....	27
Factory Default Settings	27
System Requirements.....	28
How to Login the Web-based Interface	28
Basic System Settings.....	30
Network Settings.....	30
Time Settings	33
RADIUS Settings	34
Firewall Filtering	35

Port Forwarding	36
DMZ.....	37
Basic Wireless Settings	38
Site Survey	40
VAP Profile Settings.....	41
Chapter 4 Advanced Settings	44
Advanced Wireless Settings.....	44
Traffic Shaping	45
Wireless Security Settings	46
Access Control.....	48
WDS Settings	49
Chapter 5 Management	51
Password.....	51
Upgrade Firmware.....	51
Backup/ Retrieve Settings	52
Restore Factory Default Settings	53
Reboot	53
User Certificate	54
Remote Management	55
SNMP Management.....	55
Chapter 6 Monitoring Tools.....	58
System Log	58
Ping Watch Dog.....	58
Chapter 7 Status	60
View Basic Information	60
View Association List.....	60
View Network Flow Statistics	61
View ARP Table	62

View Bridge Table	63
View Routing Table	63
View Active DHCP Client Table.....	63
Chapter 8 Troubleshooting	65
Appendix A. ASCII	67

FIGURE

Figure 1 IEEE 802.11n Wireless Access Point.....	13
Figure 2 Typical Application	14
Figure 3 Login Page	28
Figure 4 Main Page	29
Figure 5 Basic System Settings	30
Figure 6 Network Settings.....	31
Figure 7 TCP/IP Settings (Router).....	32
Figure 8 Time Settings.....	34
Figure 9 RADIUS Settings	35
Figure 10 Source IP Filtering	36
Figure 11 Port Forwarding	37
Figure 12 DMZ	37
Figure 13 Basic Wireless Settings.....	38
Figure 14 Site Survey	41
Figure 15 VAP Profile Settings	41
Figure 16 VAP Profile Settings	42
Figure 17 Advanced Wireless Settings.....	44
Figure 18 Traffic Shaping.....	46
Figure 19 Security Settings.....	46
Figure 20 Access Control.....	49
Figure 21 WDS Settings	50
Figure 22 Password Settings	51
Figure 23 Firmware Upgrade	52
Figure 24 Backup/Retrieve Settings.....	52
Figure 25 Restore to Default Settings	53
Figure 26 Reboot.....	54
Figure 27 Reboot.....	54
Figure 28 Remote Management.....	55
Figure 29 SNMP Management.....	55

Figure 30 Syslog	58
Figure 31 Ping Watchdog	59
Figure 32 Basic Information	60
Figure 33 Connection	61
Figure 34 Network Flow Statistics	62
Figure 35 ARP Table.....	62
Figure 36 Bridge Table.....	63
Figure 37 Routing Table.....	63
Figure 38 DHCP Client Table	64
Figure 57 MAC Address.....	65

TABLE

Table 1 IEEE 802.11n Wireless Access Point Factory Default Settings27

Table 2 ACSII.....67

Chapter 1 Introduction

Introduction

Designed for environment application, the IEEE 802.11n Wireless Access Point is a high-performance last-mile broadband solution that provides reliable wireless network coverage. Designed with IEEE 802.11n standard, 2x2 MIMO technology and high output power makes it possible deliver up to 300Mbps high data rate with longer range for applications. ZAC-1023-2 operates at 2.4GHz band while ZAC-1023-5 operates at 5GHz band.

IEEE 802.11n Wireless Access Point can be used as the access point, the customer premises equipment (CPE), the WDS and the AP Repeater. While being as the access point, it can be deployed to provide wireless internet service. In the other way to be as the CPE, it can receive wireless signal over the last mile, helping WISPs deliver internet service to the new residential and the business customer where wired broadband internet service, such as cable and DSL, cannot serve in. In addition, the easy-to-install IEEE 802.11n Wireless Access Point features with outstanding throughput performance and a cost-effective design that allows users to have the reliable wireless connection at the affordable price.

Appearance



Figure 1 IEEE 802.11n Wireless Access Point

Key Features

- Compliant with IEEE 802.11n standard
- Support passive PoE which is supplied with 24V.
- High reliable watertight housing endures almost any harsh environments
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- User-friendly Web and SNMP-based management interface

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing IEEE 802.11n Wireless 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 IEEE 802.11n Wireless 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 IEEE 802.11n Wireless 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 IEEE 802.11n Wireless 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 IEEE 802.11n Wireless Access Point; otherwise, a random lightening could easily cause fatal damage to IEEE 802.11n Wireless 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 IEEE 802.11n Wireless Access Point. Use of other options will likely cause damage to the IEEE 802.11n Wireless Access Point.
3. Users MUST power off the ZAC Access Point first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the unit; otherwise, damage might be caused to the ZAC Access Point itself.
4. This device is for indoor use only.

Product Package

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

● IEEE 802.11n Wireless Access Point	× 1
● Detachable 5dBi Antennas	× 2
● Pole Mounting Ring	× 2
● 24VDC Power Cord & PoE Injector	× 1
● Ferrite Suppression Core	× 1
● Grounding Wire	× 1
● Product CD	× 1

 **Note:** Product CD contains Quick Installation Guide and User Manual.

Pole Mounting Ring



Ferrite Suppression Core



24VDC Power Cord & PoE Injector



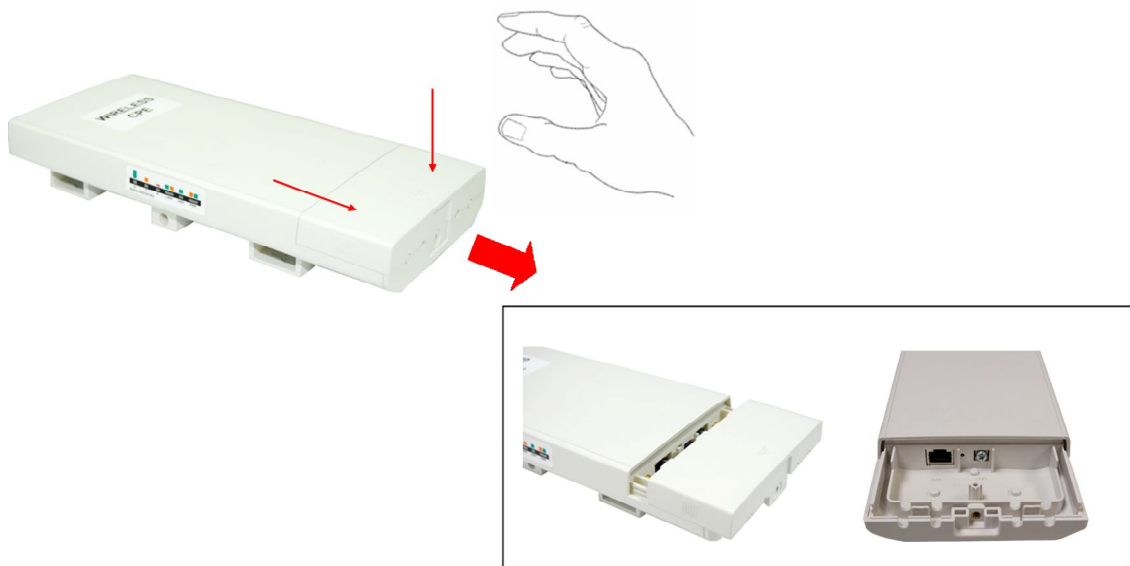
Warning:

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

Hardware Installation

Connect up

1. The bottom of the 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 Access Point.



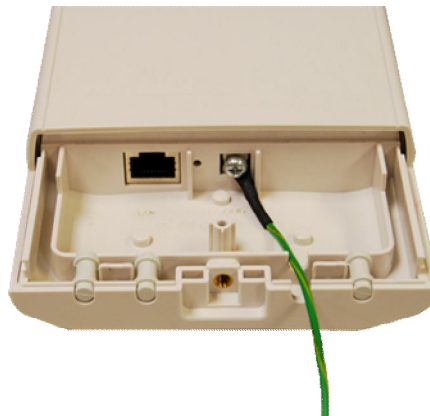
Using the Grounding Wire

The IEEE802.11n Wireless 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 Access Point.



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



Install External Antennas

The Access Point provides two reverse SMA antenna connectors for connecting external antennas.



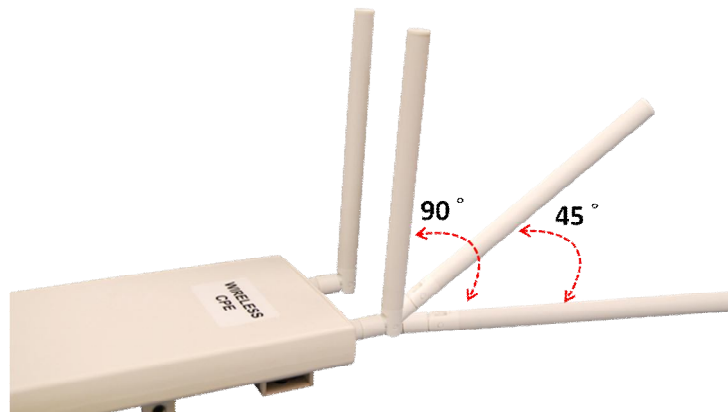
1. Connect external antennas that came with the package to the SMA-type connectors on top of the Access Point.



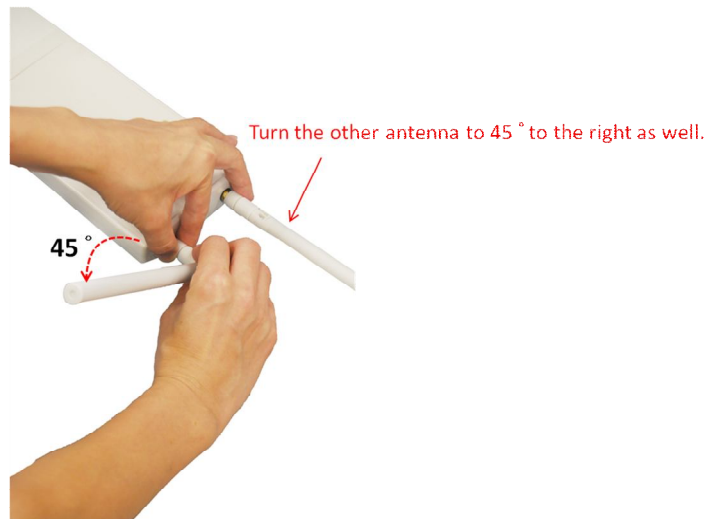
 Warning:

-
- Users MUST power off the Access Point first before connecting the external antenna to it. Do not power on the device for a certain of time without physically attaching the external antenna; otherwise, damage might be caused to the unit itself.
-

2. Bend the antennas to 90 degree or 45 degree.



3. You may turn one antenna 45 degrees to the left and the other 45 degrees to the right. The tilted antennas are a reasonable way to operate and the best way if the antennas are fairly close together since they couple together much less than if they are both pointed in the same direction (parallel).



 Note:

-
- The polarization of antennas should be properly aligned. Maximum signal strength between bridges occurs when both bridges are using identical polarization.
-

4. Tighten up the connector joint clockwise to fix the antennas.



5. To adjust antennas, loose the connector joint counterclockwise first, then adjust antenna to the desired position. **DO NOT** bend or turn the antennas without loosening the connector joint, otherwise, damage might be caused to the antennas.

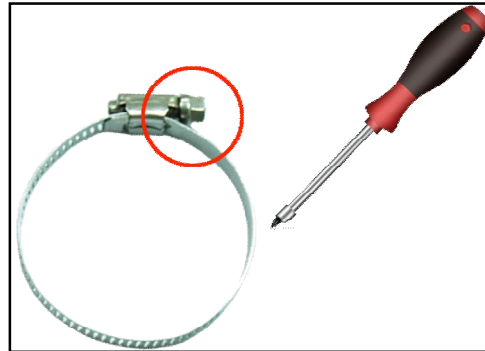


6. Antenna installation is complete.



Mount the AP on a Pole

1. Turn the 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 Access Point steadily to the pole by locking the pole mounting ring tightly.



P.S. This device is for indoor use only.

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:

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



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



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



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



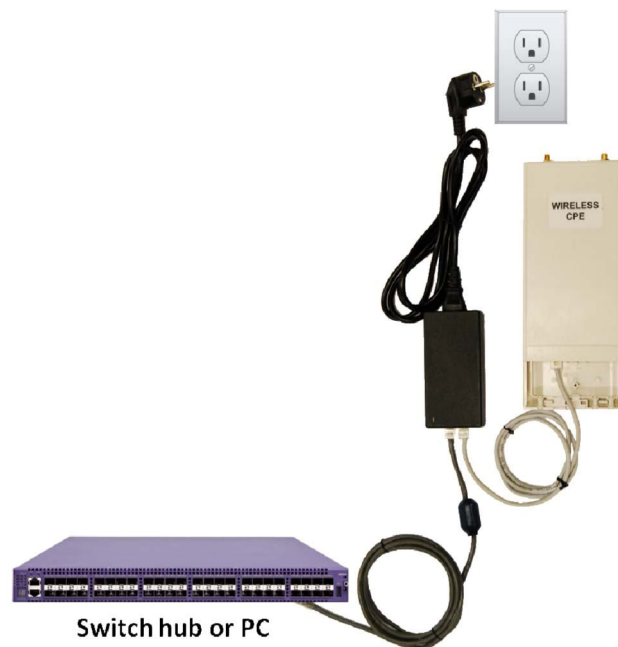
Note:

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

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



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



To configure the Access Point, please refer to **Chapter 3 Basic Settings**.

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the IEEE 802.11n Wireless Access Point factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "[Restore Factory Default Settings](#)".

Table 1 IEEE 802.11n Wireless Access Point Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
Data Rate		Auto
Output Power		Full
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Channel Protection		None
Short GI		Enable
Distance		1000m
Flow Control by AP		Disable
Security		Open System
Encryption		None

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of IEEE 802.11n Wireless Access Point is 192.168.1.1. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape, Firefox or Google Chrome.

How to Login the Web-based Interface

The IEEE 802.11n Wireless Access Point provides you with user-friendly Web-based management tool.

- Open Web browser and enter the IP address (Default: **192.168.1.1**) of IEEE 802.11n Wireless Access Point into the address field. You will see the login page as below.



Wireless Broadband Access Point

Name:

Password:

Language:

Figure 3 Login Page

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click “**Login**” to login the main page of IEEE 802.11n Wireless Access Point. As you can see, this management interface provides five main options in the black bar above, which are Status, System, Wireless, Management and Tools.

Information

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

System Information

MAC Address:	00:19:70:b1:ff:dd
Firmware Version:	1.1.1(ZC)1
System Uptime:	4m:38s
Device Name:	apb1ffdd
Country/Region:	United States

LAN Settings

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

Wireless Settings

Operation Mode:	AP
802.11 Mode:	802.11A/N
SSID:	Wireless
Encryption:	Open System
ACK Timeout:	35 μs

Interface Status

Interface	Status	Channel	Rate
Wireless	Up	5745MHz (149)	Auto
Ethernet	Up	N/A	100M/Full-Duplex

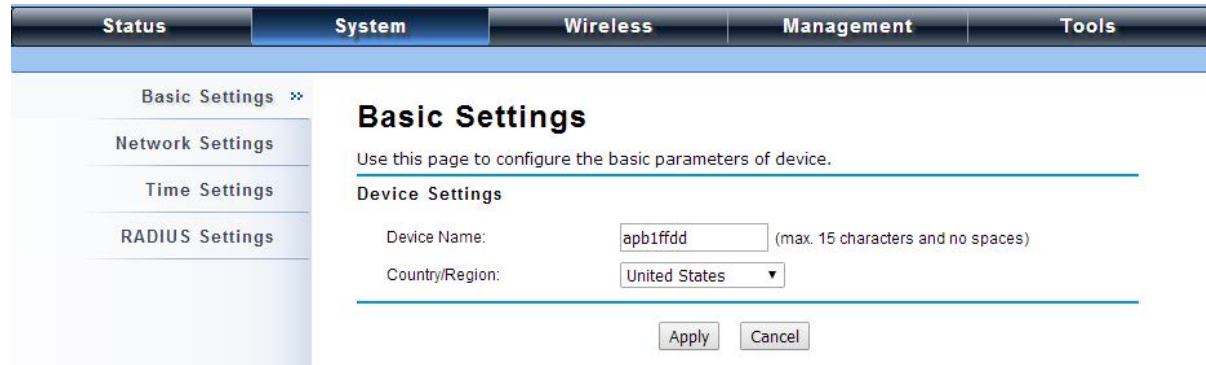
Figure 4 Main Page

Note:

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

Basic System Settings

For users who use the IEEE 802.11n Wireless Access Point for the first time, it is recommended that you begin configuration from “**Basic Settings**” in “**System**” shown below:



The screenshot shows a web interface with a top navigation bar containing tabs: Status, System (selected), Wireless, Management, and Tools. On the left, a sidebar lists settings categories: Basic Settings (selected), Network Settings, Time Settings, and RADIUS Settings. The main content area is titled 'Basic Settings' and includes a subtitle 'Use this page to configure the basic parameters of device.' Below this, the 'Device Settings' section contains two fields: 'Device Name' with the value 'apb1ffdd' and a note '(max. 15 characters and no spaces)', and 'Country/Region' with a dropdown menu showing 'United States'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 5 Basic System Settings

- **Device Name:** Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).
- **Country Region:** For FCC domain, default country is United States only.

Network Settings

The Network Settings allows you to change network, IP address and configure few network parameters like spanning tree and management VLAN ID. Make configuration in “**Network Settings**” from “**System**”.

Figure 6 Network Settings

- **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**”.

- **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.

- **802.1Q VLAN:**

To allow users on the VLAN to access the WEB page of the IEEE 802.11n Wireless 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 Wireless Access Point.

- **IP Address Assignment**

Users may change the settings for IP Address, Subnet Mask, and DHCP Server.

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



Note:

- When the IP address of the 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 Access Point to access its Web Management page.
- In case the IEEE 802.11n Wireless 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 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 Wireless Access Point configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

Figure 7 TCP/IP Settings (Router)

- **WAN Access Type:**

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 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:

-
- In AP mode, the IEEE 802.11n Wireless 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 Access Point.
 - In wireless client mode, users can access the 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.
 - 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 Access Point with another wireless device before it is set to Router mode and access the Access Point via the connected wireless device.
-

Time Settings

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

Figure 8 Time Settings

- **Current Time:**
Display the present time in Yr, Mon, Day, Hr, Min and Sec.
- **Time Zone Select:**
Select the time zone from the dropdown list.
- **NTP Server:**
Select the time server from the “**NTP Server**” dropdown list.
- **Manual IP:** Manually input the IP address of available time server.
Hit “**Apply**” to save settings.

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.

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

Figure 9 RADIUS Settings

- **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 Wireless Access Point and RADIUS during authentication.

- **Global-Key Update:**

Check this option and specify the time interval between two global-key updates.

Firewall Filtering

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. IEEE 802.11n Wireless 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.

To make the **Firewall Filtering** page show up, select Router from **System > Network Settings** and it will appear under **System** menu. Tick **Enable Firewall Filtering** to enable firewall functions.

Firewall Filtering

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

☒ **Enable Firewall Filtering**

Filter Type:

Target:

Protocol:

Direction:

MAC Address:

Comment:

#	Type	Target	Protocol	Direction	Value	Comment
---	---	---	---	---	---	---

Figure 10 Source IP Filtering

◆ **Filter Type:**

MAC Filtering: The MAC filtering gives users the ability to restrict packets from certain devices by entering MAC address.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through IEEE 802.11n Wireless Access Point. Use of such filters can be helpful in securing or restricting your local network.

Destination IP Filtering: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses.

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through IEEE 802.11n Wireless Access Point. Use of such filters can be helpful in securing or restricting your local network.

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through IEEE 802.11n Wireless Access Point. Use of such filters can be helpful in securing or restricting your local network.

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 Access Point's NAT firewall.

The screenshot shows the 'Port Forwarding' configuration page. The left sidebar contains a menu with 'Port Forwarding' selected. The main content area has a title 'Port Forwarding' and a description: '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.' Below the description is a checkbox 'Enable Port Forwarding' which is checked. There are input fields for 'IP Address', 'Protocol' (set to 'TCP'), 'Port' (with a range selector), and 'Comment'. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Clear', and 'Refresh'. Below these buttons is a table with columns: '#', 'IP', 'Protocol', 'Port' (subdivided into 'From' and 'To'), and 'Comment'. The table is currently empty.

Figure 11 Port Forwarding

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 enable it tick the **Enable DMZ** checkbox.

The screenshot shows the 'DMZ' configuration page. The left sidebar contains a menu with 'DMZ' selected. The main content area has a title 'DMZ' and a description: '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 the description is a checkbox 'Enable DMZ' which is unchecked. There is an input field for 'DMZ Host IP Address' with the value '0.0.0.0'. At the bottom, there are buttons for 'Apply' and 'Cancel'.

Figure 12 DMZ

• Enable DMZ:

DMZ Host IP Address: Type the IP address of the device you want to place under DMZ.

Basic Wireless Settings

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

The screenshot shows the 'Basic Settings' page for wireless configuration. The top navigation bar includes 'Status', 'System', 'Wireless' (active), 'Management', and 'Tools'. The left sidebar lists 'Basic Settings' (active), 'Security Settings', 'Advanced Settings', 'Traffic Shaping', 'Access Control', and 'WDS Settings'. The main content area is titled 'Basic Settings' and contains a description: 'Use this page to change the wireless mode as well as configure any associated wireless network parameters.' Below this is a checkbox 'Disable Wireless LAN Interface'. The main configuration section includes: Operation Mode (AP), SSID (Wireless), Broadcast SSID (Enabled), 802.11 Mode (802.11B/G/N), Channel Mode (20 MHz), Channel (2437MHz (6)), Extension Channel (None), Data Rate (Auto), HT Protect (Disabled), Antenna Gain (0 dBi), and Output Power (30 dBm). There are 'Apply' and 'Cancel' buttons at the bottom.

Figure 13 Basic Wireless Settings

- ◆ **Disable Wireless LAN Interface:**

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

- ◆ **Operation Mode:**

Four operating modes are available in IEEE 802.11n Wireless Access Point.

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

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

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

AP Repeater: The IEEE 802.11n Wireless Access Point servers as AP and Bridge concurrently.

In other words, the IEEE 802.11n Wireless Access Point can provide connectivity services for ACCESS POINTs under Bridge mode.

- ◆ **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 cannot exceed 32 characters.

- ◆ **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 Wireless Access Point, so that malicious attack by some illegal STA could be avoided.

- ◆ **802.11 Mode:**

The IEEE 802.11n Wireless Access Point can communicate with wireless devices of 802.11b/g or 802.11b/g/n. (For ZAC-1023-5-13 it's 802.11a or 802.11n)

- ◆ **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

- ◆ **Channel:**

Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- ◆ **Extension Channel:**

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

- ◆ **Data Rate:**

Usually “Auto” is preferred. Under this rate, the IEEE 802.11n Wireless 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.

- ◆ **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.

- **Antenna Gain**

The antenna gain calculates the TX power back off needed to remain in compliance with regulations. You should use the default detachable antenna and adjust the antenna gain settings for the output power.

- **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.

- **Enable MAC Clone**

Available only under wireless client mode, it hides the MAC address of the AP while displays the one of the device connected to the Access Point. Default is **Auto MAC Clone**. User may choose to enter the MAC address to be cloned manually.

Site Survey

Under wireless client mode, the IEEE 802.11n Wireless 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.

Wireless Site Survey - Windows Internet Explorer

http://192.168.1.1/wlsurvey.asp

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

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

Figure 14 Site Survey

VAP Profile Settings

Available in AP mode, the IEEE 802.11n Wireless 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 **Enabled** 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

System

Wireless

Management

Tools

Basic Settings

Profile Settings

Advanced Settings

Traffic Shaping

Access Control

WDS Settings

Profile Settings

Define each VAP's attribute.

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

Figure 15 VAP Profile Settings

Figure 16 VAP Profile Settings

- ◆ **Profile Name:**

Name of the VAP profile

- ◆ **SSID:**

Assign a network name 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 Wireless 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 Access Point will only allow up to 32 wireless clients to

associate with for better bandwidth for each client. By disabling the checkbox the Access Point will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

- **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.

- **Security Setting:**

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE802.11n Wireless Access Point provides you with rock solid security settings. For detailed information please go to **Chapter 4 Wireless Security Setting**.

Chapter 4 Advanced Settings

Advanced Wireless Settings

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

The screenshot shows the 'Wireless Broadband Access Point' configuration interface. At the top, there is a 'Logout' button. Below it is a navigation bar with tabs: 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'Wireless' tab is selected. On the left side, there is a sidebar with a tree view containing 'Basic Settings', 'Profile Settings', 'Advanced Settings' (which is expanded and highlighted with a double arrow), 'Access Control', and 'WDS Settings'. The main content area is titled 'Wireless Advanced Settings'. It contains a warning message: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will take.' Below the warning, there are several settings with radio buttons for 'Enabled' and 'Disabled', and input fields for numerical values. The settings are: A-MPDU aggregation (Enabled), A-MSDU aggregation (Disabled), Short GI (Disabled), RTS Threshold (2346, range 1-2347), Fragment Threshold (2346, range 256-2346), Beacon Interval (100, range 20-1024 ms), DTIM Interval (1, range 1-255), IGMP Snooping (Enabled), RIFS (Enabled), Link Integration (Disabled), and TDM Coordination (Disabled).

Setting	Value	Range
A-MPDU aggregation	Enabled	
A-MSDU aggregation	Disabled	
Short GI	Disabled	
RTS Threshold	2346	(1-2347)
Fragment Threshold	2346	(256-2346)
Beacon Interval	100	(20-1024 ms)
DTIM Interval	1	(1-255)
IGMP Snooping	Enabled	
RIFS	Enabled	
Link Integration	Disabled	
TDM Coordination	Disabled	

Figure 17 Advanced Wireless Settings

◆ 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.

◆ RTS Threshold

The IEEE 802.11n Wireless 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 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.

- ◆ **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.

- ◆ **Preamble Type**

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

- ◆ **Distance:**

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

Traffic Shaping

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

Status	Wireless Settings	Management	Tools
Wireless Networks Wireless Protocol Access Control Traffic Shaping ✕ RADIUS Settings			
Traffic Shaping Traffic shaping is the control of network traffic in order to optimize or guarantee performance, improve latency. Interface Selection: VAP1 ▼ ☐ Enable Traffic Shaping Outgoing Traffic Rate: 1024000 Kbits/s Outgoing Traffic Burst: 20 KBytes Save Cancel			

Figure 18 Traffic Shaping

- **Enable Traffic Shaping**

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

- **Interface Selection:**

Select the VAP network you would like to enable traffic shaping.

- **Outgoing Traffic Rate:**

To specify maximum outgoing bandwidth to a certain rate in kbit/s.

- **Outgoing Traffic Burst:**

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

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11n Wireless Access Point provides you with rock solid security settings.

Open “**Profile Setting**” in “**Wireless**” and enter “**VAP Profile 1 Settings**” as below.

The screenshot displays the 'Wireless' configuration page. On the left is a sidebar with navigation links: 'Basic Settings', 'Profile Settings' (selected), 'Advanced Settings', 'Traffic Shaping', 'Access Control', and 'WDS Settings'. The main content area is titled 'Define the VAP's basic settings and security settings.' and is divided into two sections. The 'Basic Settings' section includes fields for 'Profile Name' (Profile1), 'SSID' (Wireless), 'Broadcast SSID' (radio buttons for Enabled/Disabled), 'Wireless Separation' (a dropdown menu currently showing 'Open System'), 'WMM Support', 'IGMP Snooping', and a checkbox for 'Max. Station Num.'. The 'Security Settings' section includes 'Authentication' (a dropdown menu currently showing 'WPA2-PSK'), 'Data Encryption' (a dropdown menu currently showing 'AES'), and 'WPA Passphrase' (12345678). The 'Wireless Separation' and 'Authentication' dropdown menus are open, showing a list of security protocols including Open System, Shared Key, Legacy 802.1x, WPA with Radius, WPA2 with Radius, WPA & WPA2 with Radius, WPA-PSK, WPA2-PSK (highlighted), WPA-PSK&WPA2-PSK, and WPA2-PSK.

Figure 19 Security Settings

- **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: Available in AP/Wireless Client mode, 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.

 Note:

-
- For first time users, if EAP type “TLS” is selected, you need to import valid user certificate given by CA in prior. To import user certificates, please refer to Chapter 5 Management/Certificate Settings for more details. .
-

WPA with RADIUS: Available in AP/Wireless Client mode, 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: Available in AP/Wireless Client mode, as a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required. It is only available in AP/Wireless Client mode.

WPA&WPA2 with RADIUS: Available in AP mode, 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.

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

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

WPA-PSK&WPA2-PSK: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES)

encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

• **Data Encryption**

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

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

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

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

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

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

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

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



Note:

-
- We strongly recommend you enable wireless security on your network!
 - Only setting the same Authentication, Data Encryption and Key in the IEEE 802.11n Wireless Access Point and other associated wireless devices, can the communication be established!
-

Access Control

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

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

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

Basic Settings
Profile Settings
Advanced Settings
Traffic Shaping
Access Control ✕
WDS Settings

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.

Profile Selection: VAP1 - Wireless
Access Control Mode: Allow Listed
MAC Address: 00:60:b3:aa:bb:11
Apply

MAC Address	Selected	Edit
00:60:b3:aa:bb:11	☐	Edit

Delete
Clear
Refresh

Figure 20 Access Control

Profile Selection

Select the VAP profile you would like to enable Access Control

Access Control Mode

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

MAC Address

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

Delete/Clear

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

WDS Settings

Bridge mode extends 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. To enable Bridge mode, please go to **Wireless > Basic Settings** and choose “Bridge” in **Operation Mode**. Then go to “**WDS Settings**” in “**Wireless**” as below:

Status	System	Wireless	Management	Tools										
Basic Settings Security Settings Advanced Settings Traffic Shaping Access Control WDS Settings														
WDS Settings A Wireless Distribution System allows interconnection of access points in an IEEE 802.11 network. To do this, you must set all interconnected APs in the same channel, input the MAC addresses of the other APs which you want to communicate with in the table below and enable the WDS Separation function. This function will only work in Bridge and AP Repeater modes. <table> <tr> <td>Local MAC Address:</td> <td> 00:19:70:a2:91:0b </td> </tr> <tr> <td>WDS MAC Address 1:</td> <td> 00:19:70:b1:ff:de </td> </tr> <tr> <td>WDS MAC Address 2:</td> <td> </td> </tr> <tr> <td>WDS MAC Address 3:</td> <td> </td> </tr> <tr> <td>WDS MAC Address 4:</td> <td> </td> </tr> </table> Apply Cancel					Local MAC Address:	00:19:70:a2:91:0b	WDS MAC Address 1:	00:19:70:b1:ff:de	WDS MAC Address 2:		WDS MAC Address 3:		WDS MAC Address 4:	
Local MAC Address:	00:19:70:a2:91:0b													
WDS MAC Address 1:	00:19:70:b1:ff:de													
WDS MAC Address 2:														
WDS MAC Address 3:														
WDS MAC Address 4:														

Figure 21 WDS Settings

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

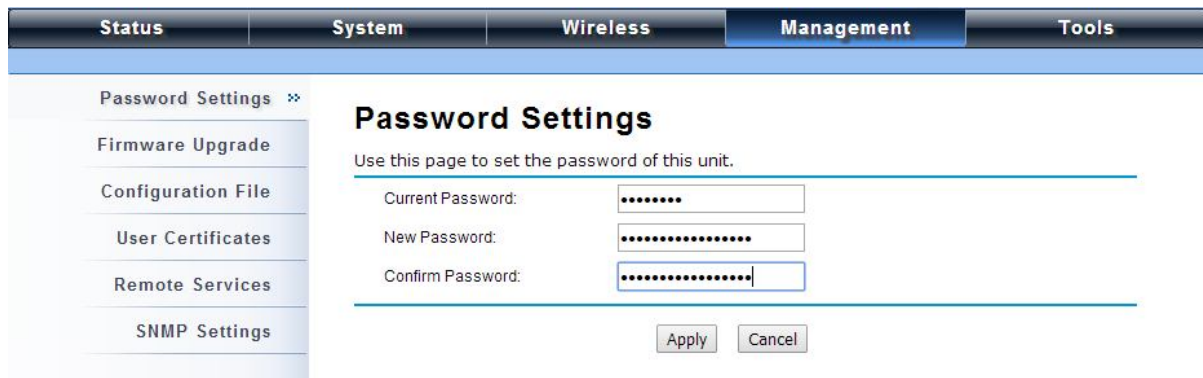
Note:

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

Chapter 5 Management

Password

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



The screenshot shows a web interface with a top navigation bar containing tabs: Status, System, Wireless, Management (selected), and Tools. On the left, a sidebar lists: Password Settings (selected), 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:" (filled with 7 dots), "New Password:" (filled with 12 dots), and "Confirm Password:" (filled with 12 dots). At the bottom right of the form are "Apply" and "Cancel" buttons.

Figure 22 Password Settings

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

 Note:

- ◆ 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 VAC Access Point’s Web:

Status	System	Wireless	Management	Tools
Password Settings Firmware Upgrade ✕ Configuration File User Certificates Remote Services SNMP Settings Firmware Upgrade 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. Select File: 選擇檔案 未選擇檔案 Upgrade Cancel				

Figure 23 Firmware Upgrade

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

Note:

- 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:

Status	System	Wireless	Management	Tools
Password Settings Firmware Upgrade Configuration File ✕ User Certificates Remote Services SNMP Settings Configuration File This page allows you to save current settings to a file or load the settings from the file which was saved previously. You may also reset the current configuration to factory default or reboot the device. Save Settings to File: Save... Load Settings from File: 選擇檔案 未選擇檔案 Upload Reset Settings to Default: Reset Reboot The Device: Reboot				

Figure 24 Backup/Retrieve Settings

- 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.

- ◆ **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 VAC Access Point provides two ways to restore the factory default settings:

- ◆ **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.



The screenshot shows the web interface of the IEEE 802.11n VAC Access Point. The top navigation bar includes tabs for Status, System, Wireless, Management, and Tools. The left sidebar lists various settings: Password Settings, Firmware Upgrade, Configuration File (selected), User Certificates, Remote Services, and SNMP Settings. The main content area is titled 'Configuration File' and contains a description: 'This page allows you to save current settings to a file or load the settings from the file which was saved previously. You may also reset the current configuration to factory default or reboot the device.' Below this, there are four rows of controls: 'Save Settings to File:' with a 'Save...' button; 'Load Settings from File:' with buttons for '選擇檔案' (Select File) and '未選擇檔案' (No File Selected), and an 'Upload' button; 'Reset Settings to Default:' with a 'Reset' button (highlighted by a red box); and 'Reboot The Device:' with a 'Reboot' button.

Figure 25 Restore to Default Settings

- ◆ **Restore factory default settings via Reset Button**

If software in IEEE 802.11n VAC 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 VAC 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.



Figure 26 Reboot

User Certificate

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**”.



Figure 27 Reboot

- **Delete User Certificate:**

Delete the selected user certificate.

- **Import User Certificates:**

Imported the user certificate

Remote Management

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

The screenshot shows the 'Remote Services' configuration page. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management' (selected), and 'Tools'. The left sidebar lists 'Password Settings', 'Firmware Upgrade', 'Configuration File', 'User Certificates', 'Remote Services' (selected with a double arrow), and 'SNMP Settings'. The main content area is titled 'Remote Services' and contains the instruction 'Use this page to customise services of remote console.' Below this, there are two columns of checkboxes: 'Enable Telnet Server' (checked), 'Enable SSH Server' (checked), 'Enable CPE Management' (unchecked), 'Enable FTP Server' (checked), 'Enable WISE' (unchecked), and 'Force HTTPS' (unchecked). At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 28 Remote Management

SNMP Management

The IEEE 802.11n VAC 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.

The screenshot shows the 'SNMP Settings' configuration page. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management' (selected), and 'Tools'. The left sidebar lists 'Password Settings', 'Firmware Upgrade', 'Configuration File', 'User Certificates', 'Remote Services', and 'SNMP Settings' (selected with a double arrow). The main content area is titled 'SNMP Settings' and contains the instruction 'Use this page to config snmp settings.' Below this, there is a checkbox for 'Enable SNMP' which is unchecked. To the right of this checkbox are several input fields: 'Protocol Version' (a dropdown menu set to 'V3'), 'Server Port' (a text box with '161'), 'Get Community' (a text box with 'public'), 'Set Community' (a text box with 'private'), 'Trap Destination' (a text box with '0.0.0.0'), 'Trap Community' (a text box with 'public'), and 'Location' (an empty text box). Below these fields, there is a link 'Configure SNMPv3 User Profile'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 29 SNMP Management

- ◆ **Protocol Version:**

Select the SNMP version, and keep it identical on the IEEE 802.11n VAC Access Point and the SNMP manager. The IEEE 802.11n VAC 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.

- ◆ **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 VAC 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 VAC 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.

Privacy 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.

Chapter 6 Monitoring Tools

System Log

System log is used for recording events occurred on the IEEE 802.11n VAC 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

Figure 30 Syslog

• Remote Syslog Server

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 ✕				
Ping Watchdog 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. ☒ Enable Ping Watchdog IP Address to Ping: 192.168.1.111 Ping Interval: 300 seconds Startup Delay: 100 seconds(>=100) Failure Count To Reboot: 300 Apply Cancel				

Figure 31 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 VAC Access Point is fully initialized.

- **Failure Count To Reboot:**

If the ping timeout packets reached the value, the IEEE 802.11n VAC Access Point will reboot automatically.

Chapter 7 Status

View Basic Information

Open “**Information**” in “**Status**” to check the basic information of the 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.

StatusSystemWirelessManagementTools

Information ↗

Connections

Statistics

ARP Table

Bridge Table

ARP Table

Bridge Table

Information

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

System Information

MAC Address:	00:19:70:b1:ff:dd
Firmware Version:	1.1.1(ZC)1
System Uptime:	4m:38s
Device Name:	apb1ffdd
Country/Region:	United States

LAN Settings

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

Wireless Settings

Operation Mode:	AP
802.11 Mode:	802.11A/N
SSID:	Wireless
Encryption:	Open System
ACK Timeout:	35 μs

Interface Status

Interface	Status	Channel	Rate
Wireless	Up	5745MHz (149)	Auto
Ethernet	Up	N/A	100M/Full-Duplex

Figure 32 Basic Information

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.

Status	System	Wireless	Management	Tools
Information				
Connections »				
Statistics				
ARP Table				
Bridge Table				

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:b3:ff:85	802.11A/N	-73 dBm	15s

Refresh

Figure 33 Connection

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.

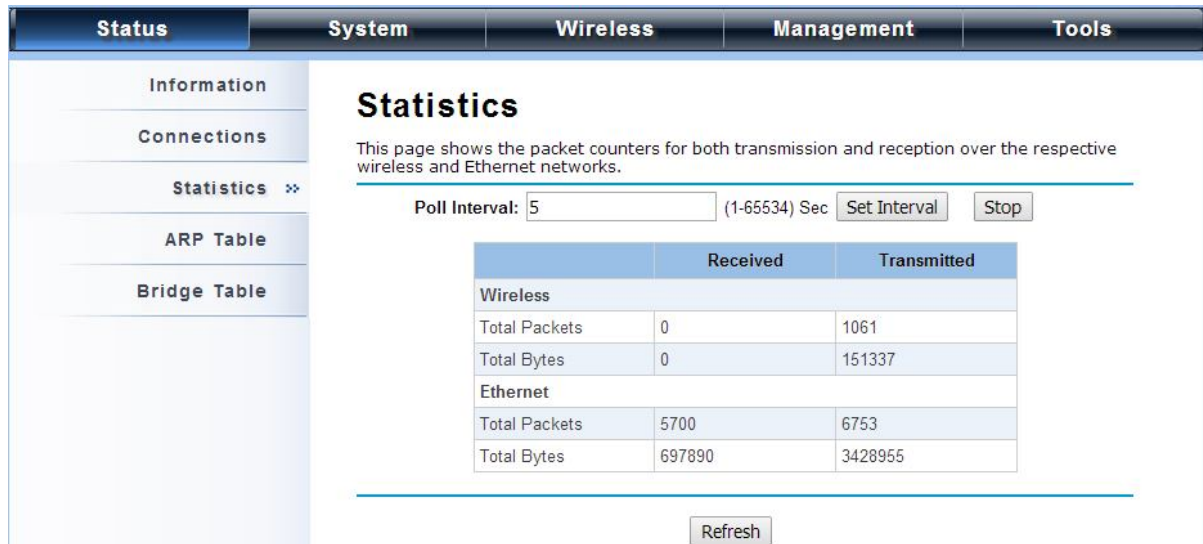


Figure 34 Network Flow Statistics

• 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.

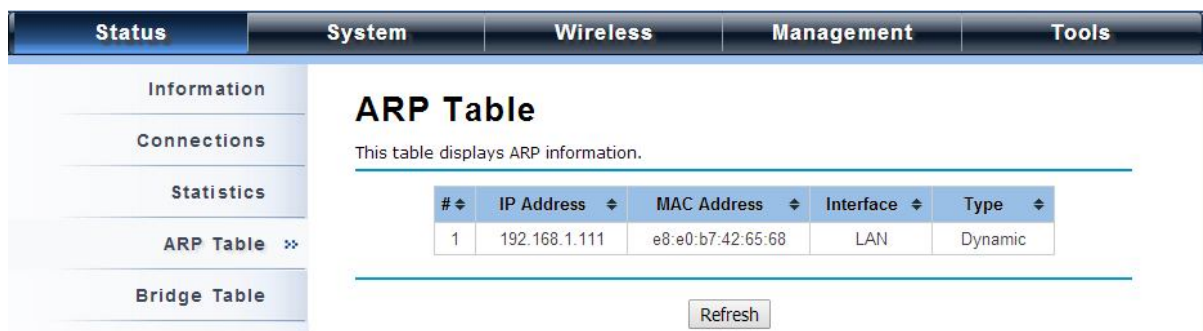


Figure 35 ARP Table

View Bridge Table

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

Status	System	Wireless	Management	Tools
Information				
Connections				
Statistics				
ARP Table				
Bridge Table ✕				

Bridge Table

This table displays bridge information.

#	MAC Address	Interface	Ageing Time(s)
1	e8:e0:b7:42:65:68	Ethernet	0.04
2	00:19:70:a2:91:0b	Bridge	---

Refresh

Figure 36 Bridge Table

View Routing Table

Available in Router mode, the routing table shows the current route information.

Status	System	Wireless	Management	Tools
Information				
Connections				
Statistics				
ARP Table				
Bridge Table				
Routing Table ✕				
DHCP Clients				

Routing Table

The routing table contains data packet transmission path of the network topology information.

Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	LAN
192.168.0.0	255.255.255.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.0.254	WAN

Refresh

Figure 37 Routing Table

View Active DHCP Client Table

Available in Router mode, the DHCP allows to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “**Refresh**” to view current table.

Wireless Broadband Access Point

Logout

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

Refresh

Figure 38 DHCP Client Table

Chapter 8 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the IEEE 802.11n Wireless Access Point. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of IEEE 802.11n Wireless Access Point?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

- Each device has a label posted with the MAC address. Please refer below.

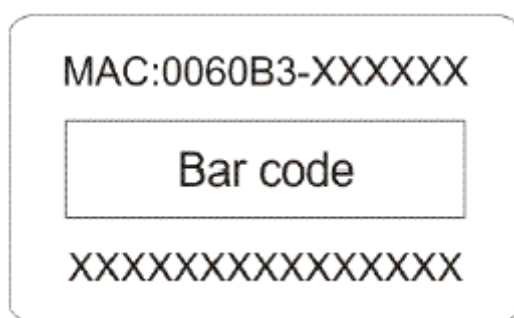


Figure 39 MAC Address

- On the IEEE 802.11n Wireless Access Point Web-based management interface, you can view the MAC Address from [“View Basic Information”](#).

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in **“Configuration File”** from **“Management”**.

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in **“Configuration File”** from **“Management”**.

Q 4. What if I can not access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);

- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the IEEE 802.11n Wireless Access Point comes with a built-in directional antenna, it is recommended make the IEEE 802.11n Wireless Access Point face to the direction where the AP is to get the best connection quality.
- In addition, you can start **“Site Survey”** in **“Wireless Basic Settings”** to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.

Appendix A. ASCII

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

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

Table 2 ASCII

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		