

User Manual

WA211 Series

Industrial Wireless 802.11an AP/Client/Bridge

Nov.21.2018 V1.1



WoMaster

WA211 Series Industrial Wireless 802.11an AP/Client/Bridge Series

User Manual

Copyright Notice

© WoMaster. All rights reserved.

About This Manual

This user manual is intended to guide a professional installer to install and to configure the WA211 Series. It includes procedures to assist you in avoiding unforeseen problems.



NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this switch.

Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

WoMaster Online Technical Services

At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

TABLE OF CONTENTS

1. INTRODUCTION	1
1.1 DESCRIPTION	1
1.2 PRODUCT FEATURES	1
1.3 PACKAGE CHECKLIST	2
1.3.2 FERRITE SUPPRESSION CORE	2
1.3.3 24VDC POWER CORD & POE INJECTOR	3
1.4 HARDWARE OVERVIEW	4
1.4.1 DIMENSION	4
1.4.2 FRONT VIEW	5
1.4.3 INSIDE THE BOTTOM COVER	6
1.4.4 LED INDICATORS	6
1.5 HARDWARE INSTALLATION	7
1.5.1 PREPARATION BEFORE INSTALLATION	7
1.5.1.1 PROFESSIONAL INSTALLATION REQUIRED	7
1.5.1.2 SAFETY PRECAUTIONS	7
1.5.1.3 INSTALLATION PRECAUTIONS	7
1.5.2 CONNECT UP	7
1.5.3 USING THE GROUNDING WIRE	8
1.5.4 THE AP ON A POLE	9
1.5.5 POWER UP	10
1.5.6 CONNECT TO THE ACCESS POINT	10
2. QUICK SETUP TUTORIAL	13
2.1 ACCESS THE WEB INTERFACE	13
2.2 CONFIGURE FAT AP	14
3. NAVIGATE THE WEB CONFIGURATOR	22
3.1 FAT AP MODE	22
3.1.1 STATUS	22
3.1.1.1 VIEW BASIC INFORMATION	22

3.1.1.2 VIEW ASSOCIATION LIST	22
3.1.1.3 VIEW NETWORK FLOW STATISTICS	23
3.1.1.4 VIEW ARP TABLE	24
3.1.1.5 VIEW BRIDGE TABLE	24
3.1.1.6 VIEW ACTIVE DHCP CLIENT TABLE	24
3.1.1.7 VIEW NETWORK ACTIVITIES	25
3.1.2 SYSTEM	25
3.1.2.1 BASIC SYSTEM SETTINGS	25
3.1.2.2 TCP/IP SETTINGS	26
3.1.2.3 TIME SETTINGS	28
3.1.2.4 RADIUS SETTINGS	28
3.1.2.5 FIREWALL SETTINGS	29
3.1.2.6 UDP PASS THROUGH	31
3.1.2.7 DMZ	32
3.1.3 WIRELESS	32
3.1.3.1 VAP PROFILE SETTINGS	34
3.1.3.2 VLAN	37
3.1.3.3 ADVANCED SETTINGS	37
3.1.3.4 ACCESS CONTROL	39
3.1.3.5 TRAFFIC SHAPING	39
3.1.3.6 CAPTIVE PORTAL	40
3.1.3.7 WDS SETTINGS	41
3.1.4 MANAGEMENT	42
3.1.4.1 PASSWORD	42
3.1.4.2 UPGRADE FIRMWARE	42
3.1.4.3 BACKUP/ RETRIEVE SETTINGS	43
3.1.4.4 RESTORE FACTORY DEFAULT SETTINGS	43
3.1.4.5 REBOOT	44
3.1.4.6 REMOTE MANAGEMENT	44
3.1.4.7 SNMP MANAGEMENT	45
3.1.4.8 CERTIFICATE SETTINGS	46
3.1.5 TOOLS	46
3.1.5.1 SYSTEM LOG	46
3.1.5.2 PING WATCH DOG	47

1. INTRODUCTION

1.1 DESCRIPTION

The WA211 Series Access Point is the high performance IEEE 802.11a/n compliant waterproof outdoor (IP55) wireless bridges with 2T2R MIMO data rate up to 300Mbps and wireless coverage up to 2km. WA211 is equipped with external antenna, whilst WA211B has internal directional high power, high gain antenna. For congestion control, 5G + auto channel selection was implemented. A web-based utility provides with an easy and secure management and firmware upgrade. Both WA211 and WA211B operate 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. WA211series is an ideal cost-effective high speed wireless communication solution with multiple operation modes for outdoor surveillance applications.

1.2 PRODUCT FEATURES

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

1.3 PACKAGE CHECKLIST

MODELS Package Checklists	WA211-EU/US (Items)	WA211B-EU/US (Items)
IEEE 802.11n Wireless Access Point	1	1
Detachable 5dBi antennas	2	-
Pole Mounting Ring	2	1
24VDC Power cord & PoE Injector	1	1
Ferrite Suppression Core	1	1
Grounding Wire	1	1

NOTE: Product CD contains Quick Installation Guide and User Manual.

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 AP.

1.3.1 POLE MOUNTING RING



1.3.2 FERRITE SUPPRESSION CORE



1.3.3 24VDC POWER CORD & POE INJECTOR

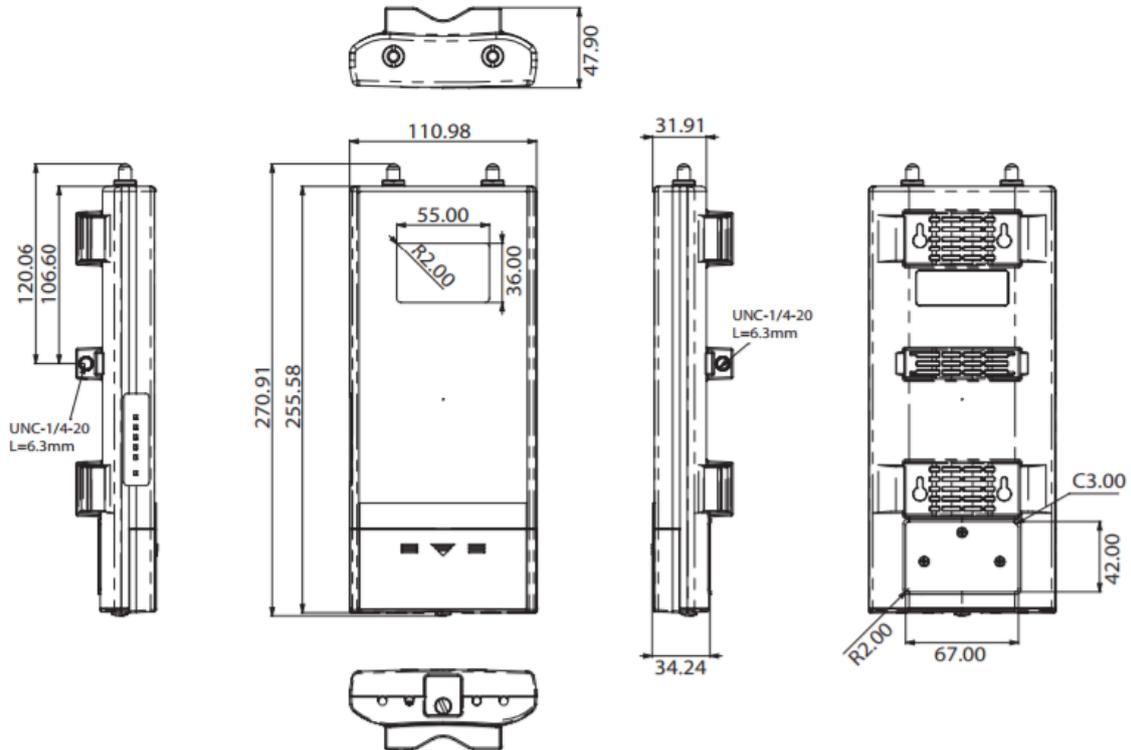


WARNING: Users MUST use the “Power cord & PoE Injector” shipped in the box with the IEEE 802.11n Wireless Access Point. Use of other options will likely cause damage to the AP.

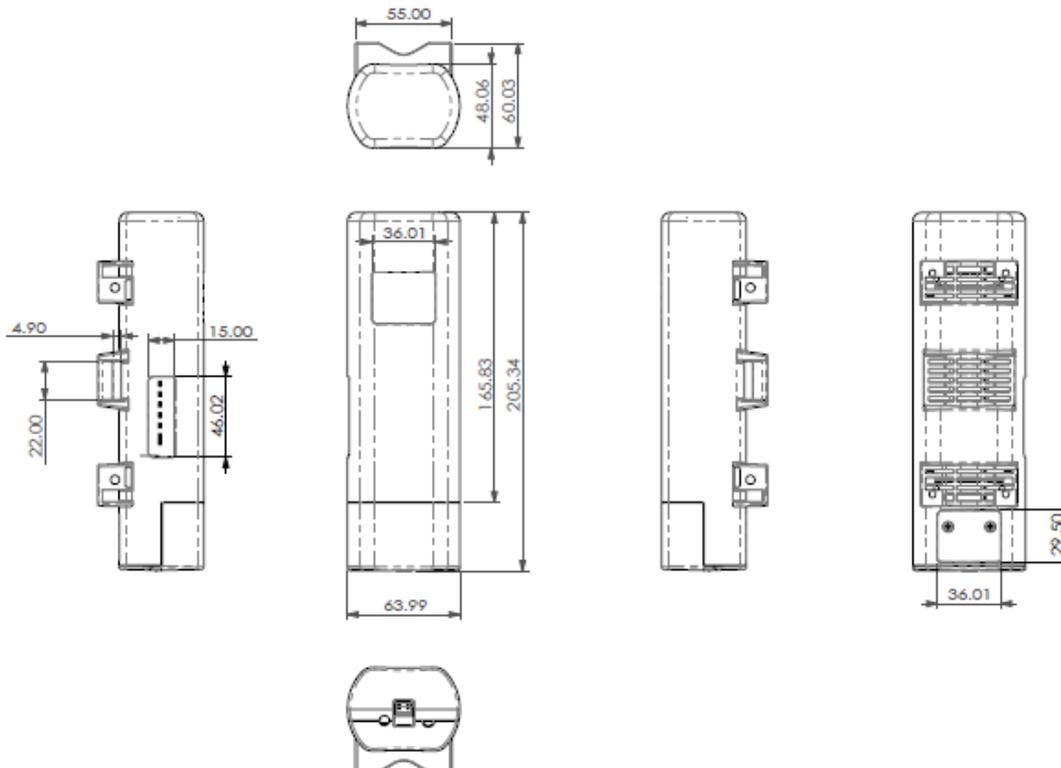
1.4 HARDWARE OVERVIEW

1.4.1 DIMENSION

The WA211 dimension (H x W x D) is **47.65mm x 255.6mm x 110.98 mm**.

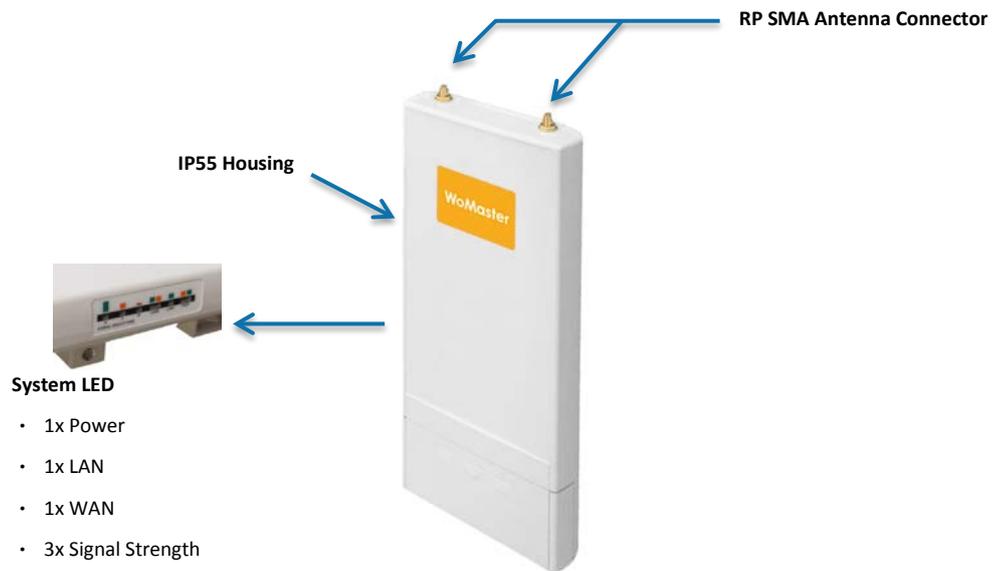


The WA211B dimension (H x W x D) is **64mm x 205mm x 61 mm**.



1.4.2 FRONT VIEW

WA211

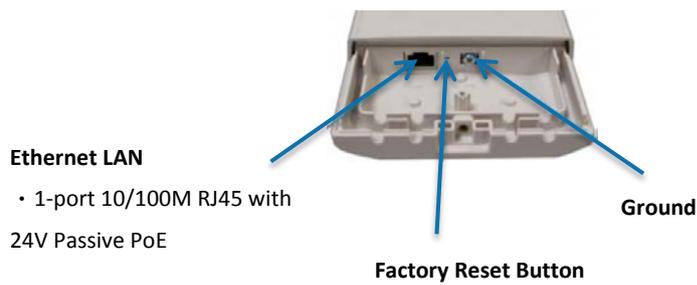


WA211B

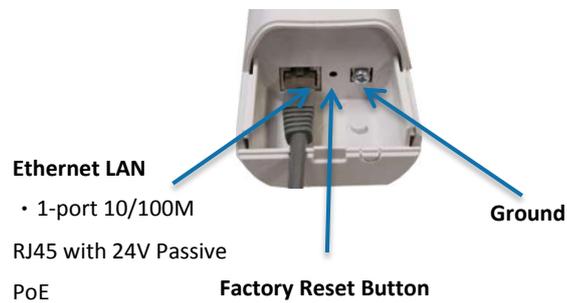


1.4.3 INSIDE THE BOTTOM COVER

WA211



WA211B



1.4.4 LED INDICATORS

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

1.5 HARDWARE INSTALLATION

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

1.5.1 PREPARATION BEFORE INSTALLATION

1.5.1.1 PROFESSIONAL INSTALLATION REQUIRED

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

1.5.1.2 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 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 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.

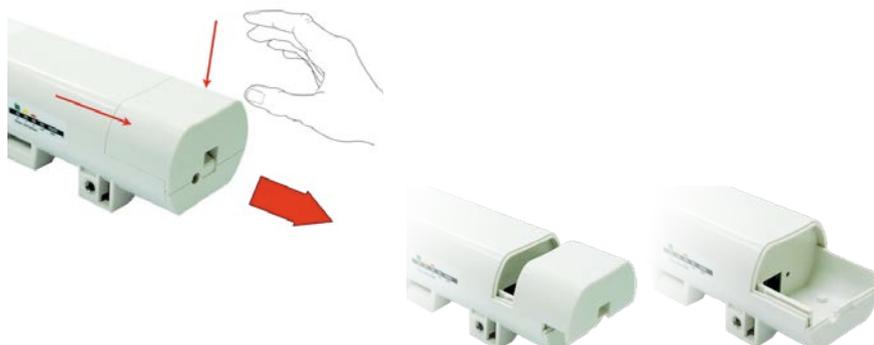
1.5.1.3 INSTALLATION PRECAUTIONS

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

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

1.5.2 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.



1.5.3 USING THE GROUNDING WIRE

The Womaster 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.



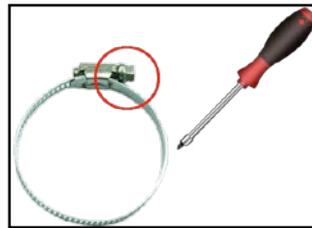
- Put the grounding wire at the grounding point at the bottom of the Access Point. Then screw the grounding wire to tighten up.



- Connect the grounding wire to earth ground.

1.5.4 THE AP ON A POLE

- Turn the Access Point over. Put the pole mounting ring through the middle hole in it. Note that you should unlock the pole mounting ring with a screwdriver before putting it through the device as the following right picture shows.



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



1.5.5 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.

1.5.6 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.



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.



2. QUICK SETUP TUTORIAL

2.1 ACCESS THE WEB INTERFACE

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

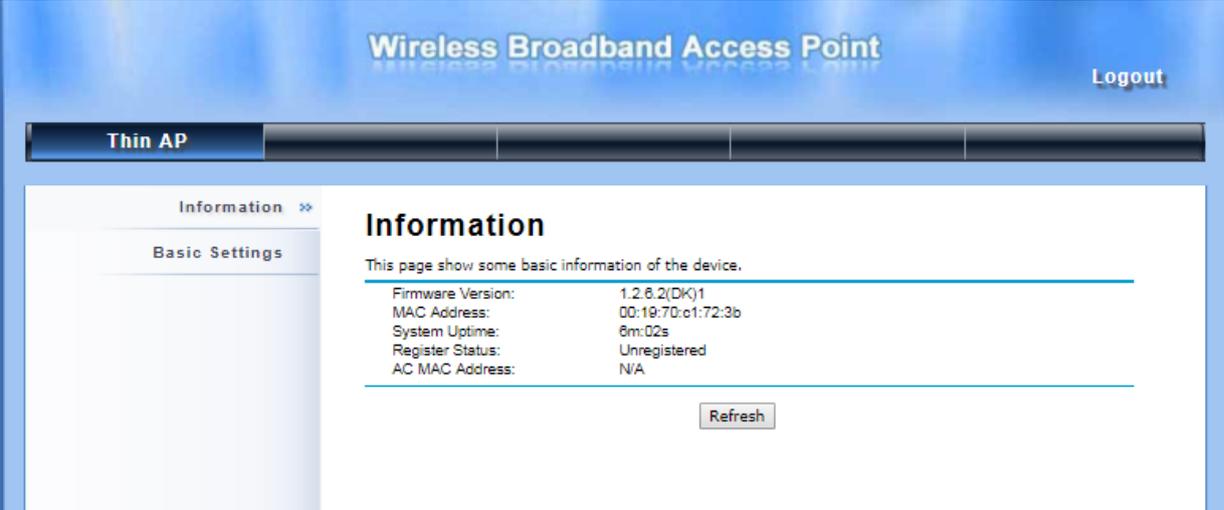
Configure the computer with a static IP address of 192.168.1.x, as the default IP address of the Access Point is 192.168.1.1 (X cannot be 0, 1, nor 255);

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



The screenshot shows the login page for the Wireless Broadband Access Point. The page has a blue header with the title "Wireless Broadband Access Point". Below the header, there are three input fields: "Name:" with the value "admin", "Password:" with masked characters "*****", and "Language:" with a dropdown menu set to "English". At the bottom of the form, there are two buttons: "Login" and "Reset".

Enter the username (Default: **admin**) and password (Default: **password**) respectively, and click "**Login**" to login to the main page of the Access Point. And user can select the language setting for **English** or **Chinese** language. After clicking Login, user will see the interface below.



The screenshot shows the main interface of the Wireless Broadband Access Point. The page has a blue header with the title "Wireless Broadband Access Point" and a "Logout" button in the top right corner. Below the header, there is a navigation bar with "Thin AP" selected. The main content area is titled "Information" and contains a table of device information. A "Refresh" button is located at the bottom of the table.

Information	
This page show some basic information of the device.	
Firmware Version:	1.2.6.2(DK)1
MAC Address:	00:19:7D:c1:72:3b
System Uptime:	0m:02s
Register Status:	Unregistered
AC MAC Address:	N/A

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

2.2 CONFIGURE FAT AP

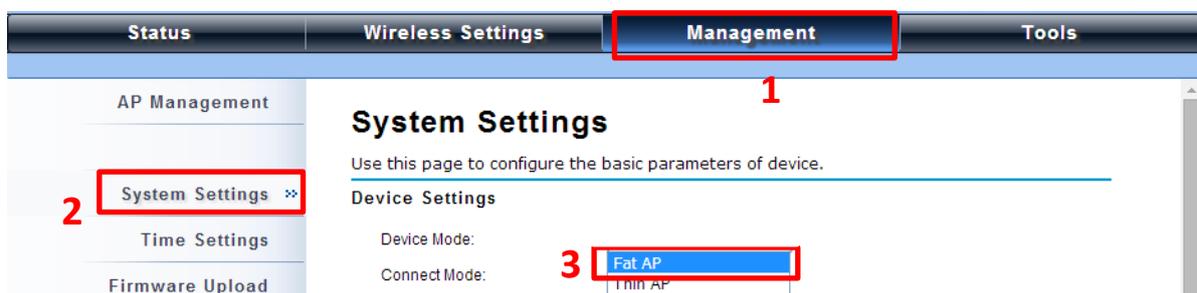
The Access Point provides “**FAT AP**” as the default mode. You need to switch one of the Access Points to virtual controller mode first. To change the mode, please do the following.

NOTE:

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

Configure the Fat AP mode

Fat AP mode operates as standalone AP that cannot be managed by the Access Point. To change the operation 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 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 parameters such as SSID, operating channel, transmit output power, etc. After the configuration is made, click **Apply** to save the parameters.

NOTE: In the example here, we only change the “Wireless Network Name (SSID)” as “Join_me”.

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

#	Enabled	Profile Name	SSID	Security	VLAN ID
1	<input checked="" type="checkbox"/>	Profile1	Wireless	Open System	0
2	<input type="checkbox"/>	Profile2	Wireless	Open System	0
3	<input type="checkbox"/>	Profile3	Wireless	Open System	0
4	<input type="checkbox"/>	Profile4	Wireless	Open System	0
5	<input type="checkbox"/>	Profile5	Wireless	Open System	0
6	<input type="checkbox"/>	Profile6	Wireless	Open System	0
7	<input type="checkbox"/>	Profile7	Wireless	Open System	0
8	<input type="checkbox"/>	Profile8	Wireless	Open System	0

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

VAP1 Profile Settings
Define the VAP's basic settings and security settings.

Basic Settings

Profile Name:

SSID:

Broadcast SSID: Enabled Disabled

Wireless Separation: Enabled Disabled

WMM Support: Enabled Disabled

IGMP Snooping: Enabled Disabled

Max. Station Num: (1-32)

Security Settings

Authentication:

Data Encryption:

WPA Passphrase:

- To decrease the chances of data retransmission at long distance, the Access Point can automatically adjust the proper ACK timeout value by specifying the 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.

The screenshot shows the 'Wireless' configuration page. The 'Wireless' tab is selected at the top. In the left sidebar, 'Advanced Settings' is highlighted. The main content area is titled 'Advanced Settings' and contains various configuration options. The 'Distance' field is highlighted with a red box and the number 3, showing a value of 1000. Other fields include A-MPDU Aggregation, A-MSDU Aggregation, Short GI, RTS Threshold, Fragment Threshold, Beacon Interval, DTIM Interval, Preamble Type, and Channel Protection. The 'Apply' and 'Cancel' buttons are at the bottom.

Wireless Client Mode

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

The screenshot shows the 'Wireless' configuration page. The 'Wireless' tab is selected at the top. In the left sidebar, 'Basic Settings' is highlighted. The main content area is titled 'Basic Settings' and contains various configuration options. The 'Operation Mode' dropdown is highlighted with a red box and the number 3, showing 'Wireless Client'. The 'SSID' field is also highlighted with a red box and the number 3, showing 'Wireless1'. Other fields include Locked AP MAC, 802.11 Mode, Data Rate, Output Power, and MAC Clone options. The 'Apply' and 'Cancel' buttons are at the bottom.

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 the 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="radio"/>	W8171-SL	2457MHz (10)	00:50:c6:ac:2a:79	802.11B/G	-92	WEP
<input type="radio"/>	2450AP	2437MHz (6)	00:19:70:a2:95:72	802.11B/G	-81	WEP
<input checked="" type="radio"/>	Wireless	2412MHz (1)	00:19:70:b5:7a:a9	802.11B/G	-83	NONE
<input type="radio"/>	MIS-Guest	2422MHz (3)	00:19:70:40:ff:fb	802.11B/G/N	-84	WPA2
<input type="radio"/>	MISVOIP	2412MHz (1)	00:18:e7:eb:7d:da	802.11B/G	-85	WEP

2

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

Status System **Wireless** Management Tools

Basic Settings

2 Profile Settings

Advanced Settings

Traffic Shaping

Access Control

WDS Settings

Security Settings

Define the wireless security settings.

3 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.

The screenshot shows the 'Status' page with the 'Connections' menu item selected. The 'Association List' table displays the following data:

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

Bridge Mode

- Go to **Wireless > Basic Settings**. Choose "Bridge" from Wireless Mode, choose a clean channel and click **Apply** to save configuration.

The screenshot shows the 'Wireless' page with 'Basic Settings' selected. The 'Operation Mode' is set to 'Bridge', '802.11 Mode' is '802.11B/G/N', 'Channel Mode' is '20 MHz', and 'Channel' is '2437MHz (6)'. The 'Output Power' is set to 17 dBm.

- 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' page with 'WDS Settings' selected. The 'Remote AP MAC Address 1' field is populated with '00:19:70:00:00:01'.

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

- Repeat the above procedures to configure the remote bridge.
- Enter the actual distance in the Distance field. For example, if the distance between the two bridges is 3 kilometers, enter 3000 in the field. Click **Apply** to save configuration.

Advanced Settings

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

WMM Support: Enabled Disabled

A-MPDU Aggregation: Enabled Disabled

A-MSDU Aggregation: Enabled Disabled

Short GI: Enabled Disabled

RTS Threshold: (256-2347)

Fragment Threshold: (256-2346)

Channel Protection:

Distance: (0-15000 meter)

Signal LED Thresholds: Weak < ≤ Medium ≤ < Strong

Background Scan: Enabled Disabled

Apply Cancel

- 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.

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

Refresh

AP Repeater Mode

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

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

Basic Settings ✕	<h3>Wireless Basic Settings</h3> <p>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.</p> <p><input type="checkbox"/> Disable Wireless LAN Interface</p> <p>Wireless Mode: AP Repeater Site Survey</p> <p>Wireless Network Name (SSID): <input type="text" value="Wireless"/> (more...)</p> <p>Broadcast SSID: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p>802.11 Mode: 802.11B/G/N</p> <p>HT protect: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>Frequency/Channel: 2437MHz (6)</p> <p>Extension Channel: None</p> <p>Channel Mode: 20 MHz</p> <p>Maximum Output Power (per antenna): <input type="text" value="12"/> <small>12 26</small> dBm</p>
Profile Settings	
Advanced Settings	
Access Control	
WDS Settings	

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.

3. NAVIGATE THE WEB CONFIGURATOR

3.1 FAT AP MODE

FAT Mode is the default mode operation, when user first time accesses the switch.

3.1.1 STATUS

3.1.1.1 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.

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

3.1.1.2 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	---

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		

3.1.1.3 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		

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.

3.1 1.4 VIEW ARP TABLE

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

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. On the left, a sidebar menu lists 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The 'ARP Table' menu item is highlighted. The main content area is titled 'ARP Table' and includes 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 row with the values '192.168.1.111', '90:E6:BA:5B:9E:26', and '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

3.1.1.5 VIEW BRIDGE TABLE

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

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. On the left, a sidebar menu lists 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The 'Bridge Table' menu item is highlighted. The main content area is titled 'Bridge Table' and includes 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 rows with the following data: (00:13:02:71:35:ba, LAN, 8.78), (90:e6:ba:5b:9e:26, LAN, 0.00), and (00:19:70:00:fb:c5, Bridge, ---). 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	---

3.1.1.6 VIEW ACTIVE DHCP CLIENT TABLE

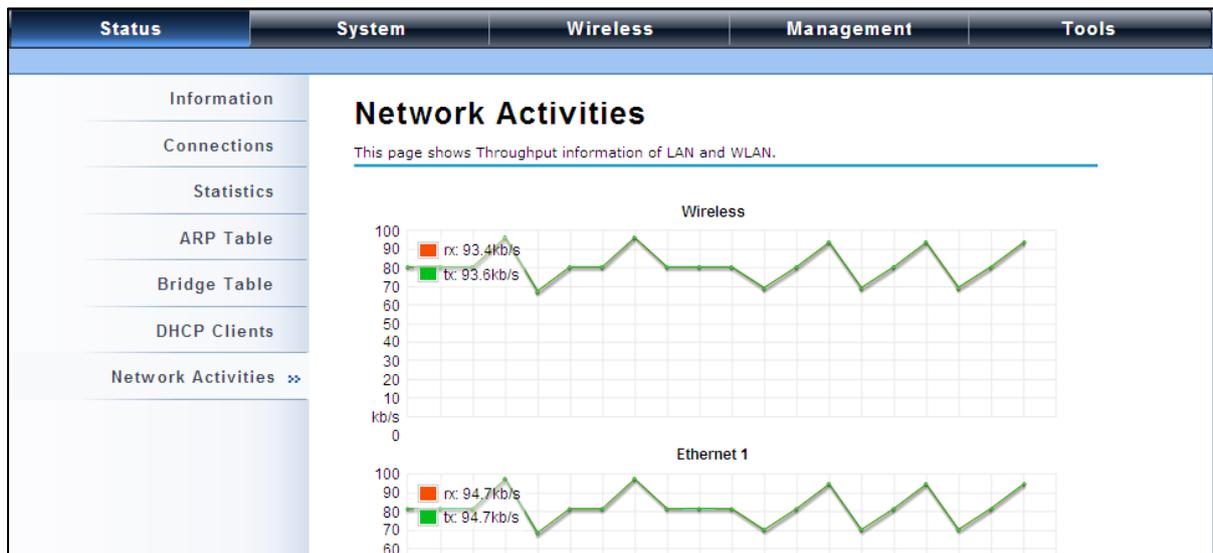
Open “DHCP Clients” in “Status” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “Refresh” to view current table.

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. On the left, a sidebar menu lists 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The 'DHCP Clients' menu item is highlighted. The main content area is titled 'DHCP Clients' and includes a sub-header 'This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.' Below this is a table with three columns: 'IP Address', 'MAC Address', and 'Time Expired(s)'. The table contains one row with the values '192.168.1.100', '00:19:70:00:fb:c5', and '1799913'. A 'Refresh' button is located below the table.

IP Address	MAC Address	Time Expired(s)
192.168.1.100	00:19:70:00:fb:c5	1799913

3.1.1.7 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.



3.1.2 SYSTEM

3.1.2.1 BASIC SYSTEM SETTINGS

The screenshot shows the 'Basic Settings' page. The left sidebar has 'Basic Settings' selected. The main content area is titled 'Basic Settings' and includes a subtitle: 'Use this page to configure the basic parameters of device.' Below this are two sections: 'Device Settings' and 'GPS Coordinate Settings'. The 'Device Settings' section includes: Device Mode (Fat AP), Device Name (ap86c6e1), Network Mode (Router), Ethernet DataRate (Auto), Country/Region (United States), Spanning Tree (Enabled), and STP Forward Delay (1). The 'GPS Coordinate Settings' section includes Latitude (N 0 0 0) and Longitude (E 0 0 0).

Device Settings

Device Mode: **FAT AP** as the default mode. Select FAT AP to perform as a standalone AP, neither managing nor managed by other 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: The availability of some specific channels and/or operational frequency bands is country dependent.

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.

GPS Coordinate Settings

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

3.1.2.2 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 Access Point. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

The screenshot shows a web management interface with a navigation bar at the top containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is selected. On the left, a sidebar 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 includes a subtitle: '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..'. Under the heading 'IP Address Assignment', there are two radio button options: 'Obtain IP Address Automatically' (unselected) and 'Use Fixed IP Address' (selected). Below these are input fields for '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 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 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 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 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 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 AP.
- 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.

3.1.2.3 TIME SETTINGS

Compliant with NTP, the IEEE 802.11n 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.

The screenshot shows the 'Time Settings' page in the configuration interface. The page has a navigation bar with 'Status', 'System', 'Wireless', 'Management', and 'Tools'. Under 'System', there is a sidebar with 'Basic Settings', 'TCP/IP Settings', 'Time Settings' (selected), 'RADIUS Settings', and 'Firewall Settings'. The main content area is titled 'Time Settings' and includes a sub-header: 'You can synchronize System Log's time stamp with a public time server over the Internet.' Below this, there are fields for 'Current Time' (Yr: 2010, Mon: 8, Day: 19, Hr: 21, Mn: 44, Sec: 21), 'Time Zone Select' (dropdown menu showing '(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'), an unchecked checkbox for 'Enable NTP client update', a radio button for 'NTP server' (selected) with a dropdown menu showing '192.5.41.41 - North America', and a radio button for 'Manual IP' with a text input field containing '0.0.0.0'.

- **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. or manually input the IP address of available time server into “Manual IP”.

3.1.2.4 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 the 'RADIUS Settings' page in the configuration interface. The page has a navigation bar with 'Status', 'System', 'Wireless', 'Management', and 'Tools'. Under 'System', there is a sidebar with 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings' (selected), and 'Firewall Settings'. The main content area is titled 'RADIUS Settings' and includes a sub-header: 'Use this page to set the radius server settings.' Below this, there is a section for 'Authentication RADIUS Server' with fields for 'IP Address' (0.0.0.0), 'Port' (1812), and 'Shared Secret'. There is also an unchecked checkbox for 'Global-Key Update' and a text input field for 'every 3600 Seconds'.

Authentication RADIUS Server

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

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

Port: Enter the port number of the Radius Server;

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

Global-Key Update

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

3.1.2.5 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 Access Point has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under **Router Mode**.

Source IP Filtering:

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. On the left, a sidebar lists settings categories: '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 descriptive paragraph: '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, there are 'Apply' and 'Cancel' buttons, and a table with columns for '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**.

Destination IP Filtering:

The screenshot shows a web interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. On the left, a sidebar lists settings categories: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering' (highlighted with a double arrow), 'Src Port Filtering', and 'Dst Port Filtering'. The main content area is titled 'Destination IP Filtering' and includes a descriptive paragraph: '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, there are 'Apply' and 'Cancel' buttons, and a table with columns for '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**.

Source Port Filtering:

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering' (which is 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".
- A "Port Range" field consisting of two input boxes separated by a hyphen.
- A "Protocol" dropdown menu currently set to "Both".
- A "Comment" text input field.
- "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**

Destination Port Filtering:

The screenshot shows a web-based configuration interface for a network device, similar to the one above. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering', and 'Dst Port Filtering' (which is highlighted with a double arrow). The main content area is titled 'Destination 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 Destination Port Filtering".
- A "Port Range" field consisting of two input boxes separated by a hyphen.
- A "Protocol" dropdown menu currently set to "Both".
- A "Comment" text input field.
- "Apply" and "Cancel" buttons.
- A table header with columns: "Dest Port Range", "Protocol", "Comment", "Select", and "Edit".

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

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

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

Comment: Make comments to record your filtering rule.

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

Port Forwarding:

The screenshot shows a web-based configuration interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings categories: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering', 'Dst Port Filtering', and 'Port Forwarding'. The 'Port Forwarding' section is active, displaying the title 'Port Forwarding' and a descriptive paragraph: '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 text is a form with a checkbox for 'Enable Port Forwarding', an 'IP Address' input field, a 'Protocol' dropdown menu set to 'Both', a 'Port Range' input field, and a 'Comment' input field. At the bottom of the form are 'Apply' and 'Cancel' buttons. A table at the very bottom of the page has columns for 'Local IP Address', 'Protocol', 'Port Range', 'Comment', 'Select', and 'Edit', but it is currently empty.

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 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.

3.1.2.6 UDP PASS THROUGH

The screenshot shows a web-based configuration interface with a top navigation bar containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar lists various settings categories: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering', 'Dst Port Filtering', 'Port Forwarding', and 'UDP Pass through'. The 'UDP Pass through' section is active, displaying the title 'UDP Pass through' and a descriptive paragraph: 'All UDP packets will be passed through the firewall'. Below the text is a form with a checkbox for 'Enable UDP Pass through'. At the bottom of the form 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

3.1.2.7 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.



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

3.1.3 WIRELESS

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



Disable Wireless LAN Interface

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

Operation Mode

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

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

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

Bridge: The IEEE 802.11n 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 Access Point servers as AP and Bridge concurrently. In other words, the IEEE 802.11n Access Point can provide connectivity services for CPEs 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 cannot scan and find IEEE 802.11n Access Point, so that malicious attack by some illegal STA could be avoided.

802.11 Mode

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

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.

Frequency/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 Access Point to use two channels at once. Two options are available: Upper Channel and Lower Channel.

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.

Data Rate

Usually "Auto" is preferred. Under this rate, the IEEE 802.11n 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.

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.

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.

Site Survey

Under wireless client mode, the 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
<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

3.1.3.1 VAP PROFILE SETTINGS

Available in AP mode, the IEEE 802.11n 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.

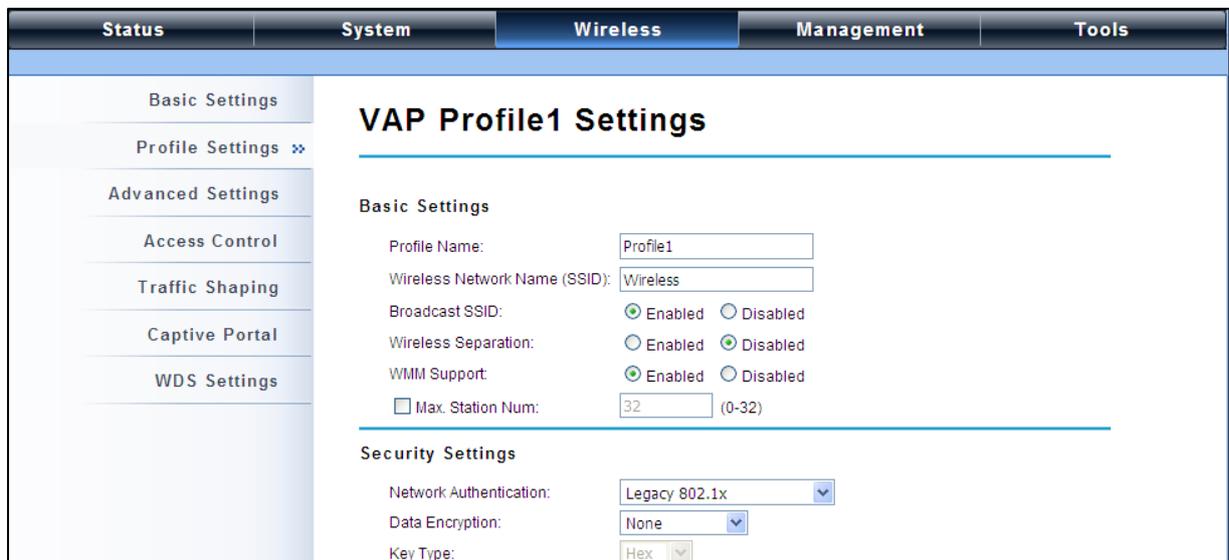
Status System **Wireless** Management Tools

Basic Settings
Profile Settings »
 Advanced Settings
 Access Control
 Traffic Shaping
 Captive Portal
 WDS Settings

VAP Profile Settings

Define each WLAN's attribute.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	Profile1	Wireless	Legacy 802.1X	<input type="text" value="0"/>	Always Enabled
2	Profile2	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
3	Profile3	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
4	Profile4	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
5	Profile5	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
6	Profile6	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
7	Profile7	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
8	Profile8	Wireless	Open System	<input type="text" value="0"/>	<input type="checkbox"/>



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 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.

Security Setting:

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11a/n Access Point provides you with rock solid 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: It provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

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

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

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

NOTE: If Radius relevant authentication type is selected, please go to [Wireless → Radius Settings](#) for further radius server configuration.

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

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

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

Data Encryption

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

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

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

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

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

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

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

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

NOTE:

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

3.1.3.2 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 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 Access Point.

The screenshot shows the 'Wireless' management page. On the left is a sidebar with navigation options: Basic Settings, Profile Settings (selected), Advanced Settings, Access Control, Traffic Shaping, Captive Portal, and WDS Settings. The main area contains a table with 7 columns: Profile ID, Profile Name, Mode, Authentication, Security, and a checkbox. Below the table is a red-bordered box containing the 'Enable 802.1Q VLAN' checkbox (checked), a 'Management VLAN ID' input field with the value '0', and 'Apply' and 'Reset' buttons.

Profile ID	Profile Name	Mode	Authentication	Security	
10	Profile10	Wireless	Open System		<input type="checkbox"/>
11	Profile11	Wireless	Open System		<input type="checkbox"/>
12	Profile12	Wireless	Open System		<input type="checkbox"/>
13	Profile13	Wireless	Open System		<input type="checkbox"/>
14	Profile14	Wireless	Open System		<input type="checkbox"/>
15	Profile15	Wireless	Open System		<input type="checkbox"/>
16	Profile16	Wireless	Open System		<input type="checkbox"/>

Enable 802.1Q VLAN
Management VLAN ID:

3.1.3.3 ADVANCED SETTINGS

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

The screenshot shows the 'Wireless Advanced Settings' page. The sidebar is the same as in the previous screenshot, but 'Advanced Settings' is selected. The main area has a title 'Wireless Advanced Settings' and 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 this are several settings:

- 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

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.

RTS Threshold

The IEEE 802.11n 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.

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.

RIFS

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

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.

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.

LAN2LAN CPE

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

Space in Meter

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

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: 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.

3.1.3.4 ACCESS CONTROL

The Access Control appoints the authority to wireless client on accessing IEEE 802.11n 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.



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

Access Control Mode

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

MAC Address

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

Delete Selected/All

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

3.1.3.5 TRAFFIC SHAPING

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



Overall Traffic Shaping

Check this box to control the overall bandwidth of the 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.

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.

3.1.3.6 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 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.

The screenshot shows a web interface for configuring the Captive Portal. The interface has a top navigation bar with tabs: Status, System, Wireless (selected), Management, and Tools. On the left, there is a sidebar menu with options: Basic Settings, Profile Settings, Advanced Settings, Access Control, Traffic Shaping, Captive Portal (selected and highlighted with a double arrow), and WDS Settings. The main content area is titled 'Captive Portal' and contains the following settings:

- Basic Settings:** A checkbox for 'Captive Portal Enable' is currently unchecked. Below it, 'Profile Selection:' is set to 'VAP1 - Wireless' via a dropdown menu.
- RADIUS Settings:** This section includes several input fields: 'Primary RADIUS Server:' (radius1.coova.net), 'Secondary RADIUS Server:' (radius2.coova.net), 'RADIUS Auth Port:' (1812), 'RADIUS Acct Port:' (1813), 'RADIUS Shared Secret:' (masked with dots), and 'RADIUS NASID:' (your-radius-nasid).
- Captive Portal Settings:** This section includes 'UAM Portal URL:' (https://www.coova.net) and 'UAM Secret:' (masked with dots).

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

Radius Settings

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

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

Radius Auth Port: Enter the port number for authentication

Radius Acct Port: Enter the port number for billing

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

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

Radius Administrative-User:

Radius Admin Username: Enter the username of the Radius Administrator

Radius Admin Password: Enter the password of the Radius Administrator

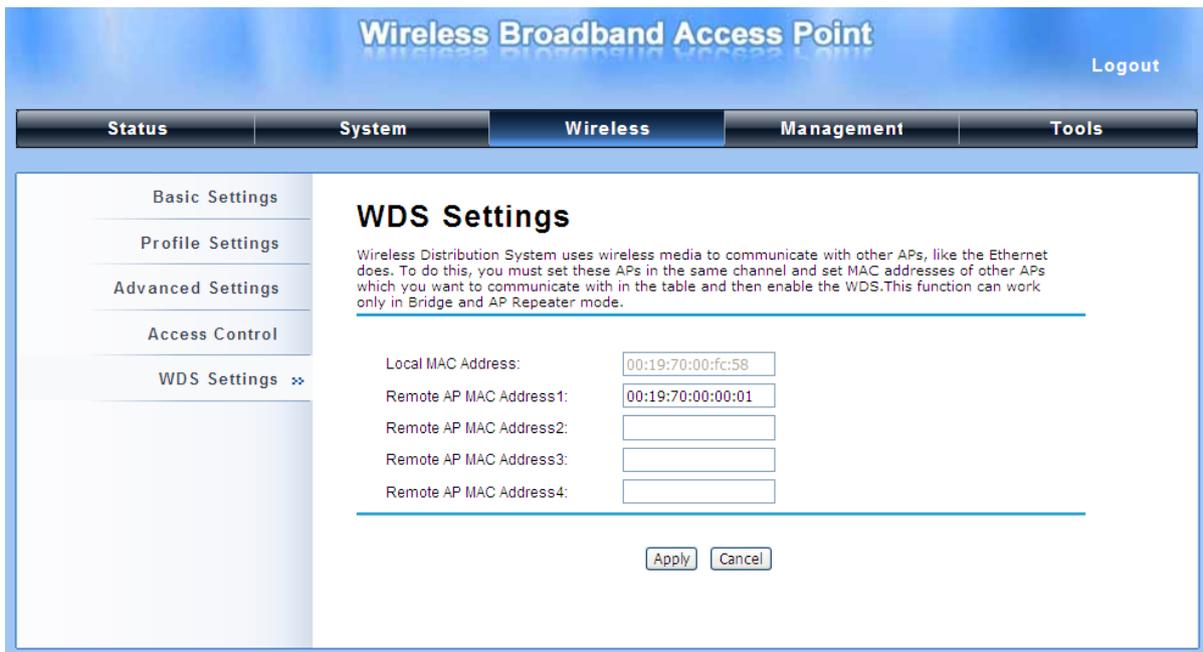
Captive Portal

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

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

3.1.3.7 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:



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

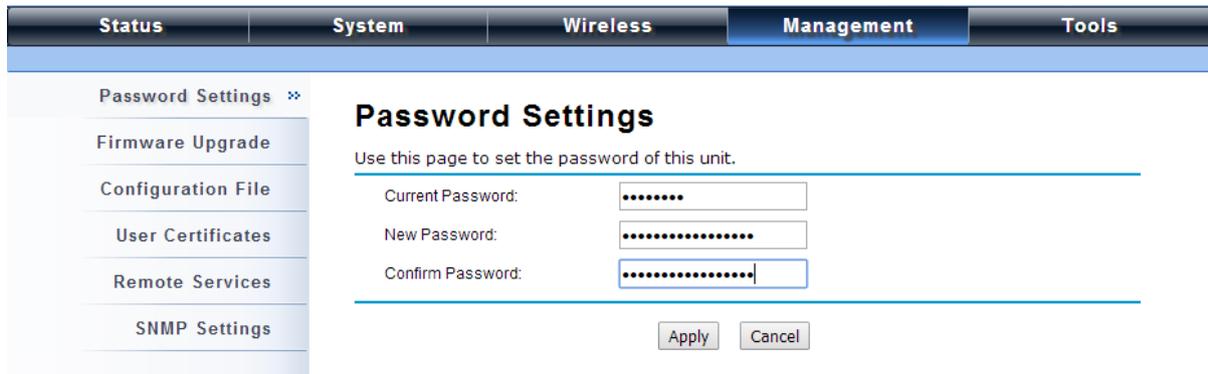
NOTE:

- 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.

3.1.4 MANAGEMENT

3.1.4.1 PASSWORD

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



The screenshot shows the web interface for the IEEE 802.11n Access Point. The top navigation bar includes tabs for Status, System, Wireless, Management (selected), and Tools. On the left, a sidebar menu lists Password Settings (selected), Firmware Upgrade, Configuration File, User Certificates, Remote Services, and SNMP Settings. The main content area is titled "Password Settings" and contains 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 with a masked password field. At the bottom right, there are "Apply" and "Cancel" buttons.

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!

3.1.4.2 UPGRADE FIRMWARE

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



The screenshot shows the web interface for the IEEE 802.11n Access Point. The top navigation bar includes tabs for Status, System, Wireless, Management (selected), and Tools. On the left, a sidebar menu lists Password Settings, Firmware Upgrade (selected), Configuration File, User Certificates, Remote Services, and SNMP Settings. The main content area is titled "Firmware Upgrade" and contains 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 a file selection button labeled "選擇檔案" and "未選擇檔案". At the bottom right, there are "Upgrade" and "Cancel" buttons.

Click “**Browse**” to select the firmware file you would like to load;

Click “**Upload**” to start the upload process;

Wait a few minutes, the Access Point will reboot after successful upgrade.

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

3.1.4.3 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:



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.

3.1.4.4 RESTORE FACTORY DEFAULT SETTINGS

The IEEE 802.11n 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.



Restore factory default settings via Reset Button

If software in IEEE 802.11n 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.

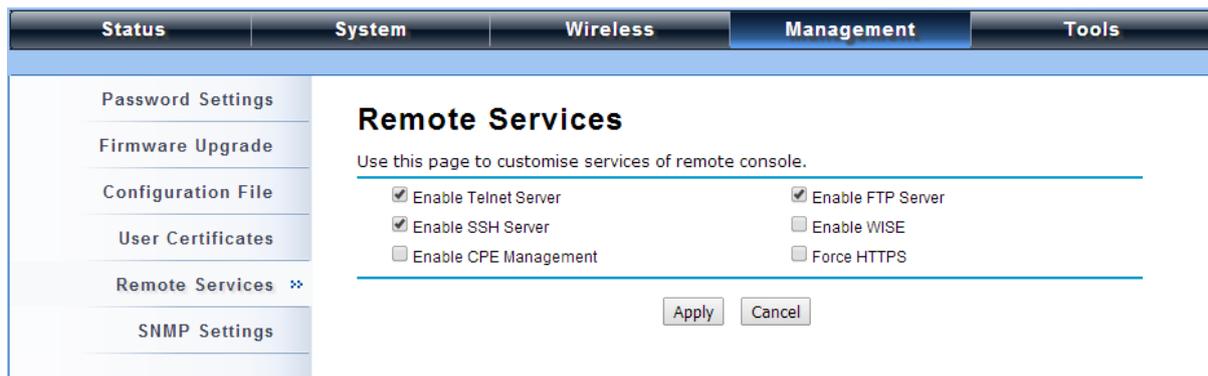
3.1.4.5 REBOOT

You can reboot your IEEE 802.11n 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.



3.1.4.6 REMOTE MANAGEMENT

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



3.1.4.7 SNMP MANAGEMENT

The IEEE 802.11n 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 interface includes a top navigation bar with tabs for 'Status', 'System', 'Wireless', 'Management', and 'Tools'. A left sidebar contains a menu with items: 'Password Settings', 'Firmware Upgrade', 'Configuration File', 'User Certificates', 'Remote Services', and 'SNMP Settings' (which is expanded). The main content area is titled 'SNMP Settings' and contains the following fields and options:

- Enable SNMP
- Protocol Version: V3 (dropdown menu)
- Server Port: 161 (text input)
- Get Community: public (text input)
- Set Community: private (text input)
- Trap Destination: 0.0.0.0 (text input)
- Trap Community: public (text input)
- Location: (empty text input)

At the bottom of the configuration area, there is a blue link labeled 'Configure SNMPv3 User Profile' and two buttons: 'Apply' and 'Cancel'.

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

Priy 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.

3.1.4.8 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 the 'User Certificates' page under the 'Management' tab. The left sidebar contains a menu with 'User Certificates' selected. The main content area has the title 'User Certificates' and a subtitle 'Use this page to upload/delete user certificates.' Below this, there are two sections: 'Import Certificate:' with a file selection button (showing '選擇檔案 未選擇檔案') and an 'Import' button; and 'Delete Certificate:' with a dropdown menu and a 'Delete' button.

Delete User Certificate: Delete the selected user certificate.

Import User Certificates: Imported the user certificate

3.1.5 TOOLS

3.1.5.1 SYSTEM LOG

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

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

The screenshot shows the 'System Log' page under the 'Tools' tab. The left sidebar has 'System Log' selected. The main content area has the title 'System Log' and a subtitle 'Use this page to set remote log server and show the system log.' Below this, there is a checkbox for 'Enable Remote Log'. Underneath, there are input fields for 'IP Address' (set to '0.0.0.0') and 'Port' (set to '514'). At the bottom of the configuration section are 'Apply', 'Cancel', and 'Clear' buttons. Below the configuration is a table showing system log entries.

#	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

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.

3.1.5.2 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.



The screenshot shows a web interface with a navigation bar at the top containing 'Status', 'System', 'Wireless', 'Management', and 'Tools'. Below the navigation bar, there is a sidebar with 'System Log' and 'Ping Watchdog' (indicated with a double arrow). The main content area is titled 'Ping Watchdog' and contains the following text: '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.' Below this text, there is a checkbox labeled 'Enable Ping Watchdog' which is checked. There are four input fields: 'IP Address to Ping' with the value '192.168.1.111', 'Ping Interval' with the value '300' and the unit 'seconds', 'Startup Delay' with the value '100' and the unit 'seconds(>=100)', and 'Failure Count To Reboot' with the value '300'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

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 Access Point is fully initialized.

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

4. 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 1 ASCII

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		

