# WAP3xDC FAT Web Manual

## Manual Version: v2.0

# Content

# Chapter 1 Introduction

## *1.1 Overview*

This manual covers the complete line of Amer “Acuity” access points.
This includes the WAP33DC, WAP38DC, WAP42DC and the WAP43DC.

Managing the access point configurations are done through a web browser.

## *1.2 Login Web Management*

The default Web login information:

User name: **admin**

Password: **admin**

IP address: **192.168.1.10**

How to access the device:

Connect your PC to the PoE port on the WAP3xDC using an ethernet cable
Configure your TCP/IP settings with a static IP address of 192.168.1.100

Launch a web browser and input 192.168.1.10 into the address bar. By default the username and password is **admin**

Fig 1-2 Web network management login page

## *1.3 Logging out of the Web Management*

Click the “log off” button on the upper right corner on the Web management page to quit.

## *1.4 Introduction to Page Layout of Web Management*

Fig 1-4 Initial page of Web management


**Navigation bar:** Used to explore the settings of the device.

**Configuration Section:** Change the desired settings.

**Help Section**: Help section provides basic user information. Click on more for a more detailed explanation.

## *1.5 Introduction to Web Management Function*

Listed below are the available functions within the Network Management Interface. Table 1-1:

| | | |
|---|---|---|
| Basic Settings | | Show the AP address (IP address and MAC address), version (firmware version) and device information. The admin password, serial ports configuration and system settings can be configured. |
| Status | Interfaces | Show the real-time wired and wireless configuration of the APs. |
| | Transmit/Receive | Show the transmission of packets with the associated AP. |
| | Client Association | Show the current status of the connected APs |
| Advanced Configuration | | Configure the wireless parameters for the Access point. |
| | Ethernet Settings | Configure the related wired settings of an AP. This includes Host name, Management VLAN, Untagged VLAN, DHCP, Static IP and DNS server. |
| | Wireless Settings | Configure the related wireless settings of an AP. This includes country code, radio interface, physical mode and channel. |
| | Radio | Configure the RF parameters. This includes radio interface, physical mode, channel, channel bandwidth, primary channel, supporting short protection interval or not, STBC mode, protection, beacon frame interval, DTIM interval, fragment threshold, RTS threshold, maximum stations, transmission power. |
| | VAP (Virtual AP) | Configure the authentication mode of a virtual AP and the related configuration. |
| | WDS | Configure the WDS settings. |
| | AP Mode | Configure the mode and IP address of an AP. |
| System Maintenance | | Reset the unit, back up the config, update the firmware. |
| | Configuration | Restart an AP. Restore an AP to factory defaults. Import and export files. |
| | Upgrade | Update the firmware of an AP. |

## *1.6 Introduction to Common Controls of Web Page*

1. <Update>

Click < Update > button to submit changes.

2. <Refresh>

Click <Refresh> button to refresh the information on the current page.

## *1.7 Usage Restriction of Web Network Management*

(1) The operating systems supported by Web network management include: Windows XP, Windows 2000, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Vista, Windows 7, Linux and MAC OS.

(2) The browsers supported by Web network management include: Microsoft Internet Explorer 6.0 SP2 or higher, Mozilla Firefox 3.0 or higher, Google Chrome and Safari.

(3) Web network management does not support the “previous”, “next” and “refresh” buttons from the browser.

(4) The Windows Operating System Firewall will limit the number of connected users and an error may occur where the page does not load due to a high amount of users. To avoid this error, temporarily disable the Windows Firewall.

(5) After a software version change, we suggest clearing the cache data of the browser before logging into the web network management.

# Chapter 2 Basic Settings

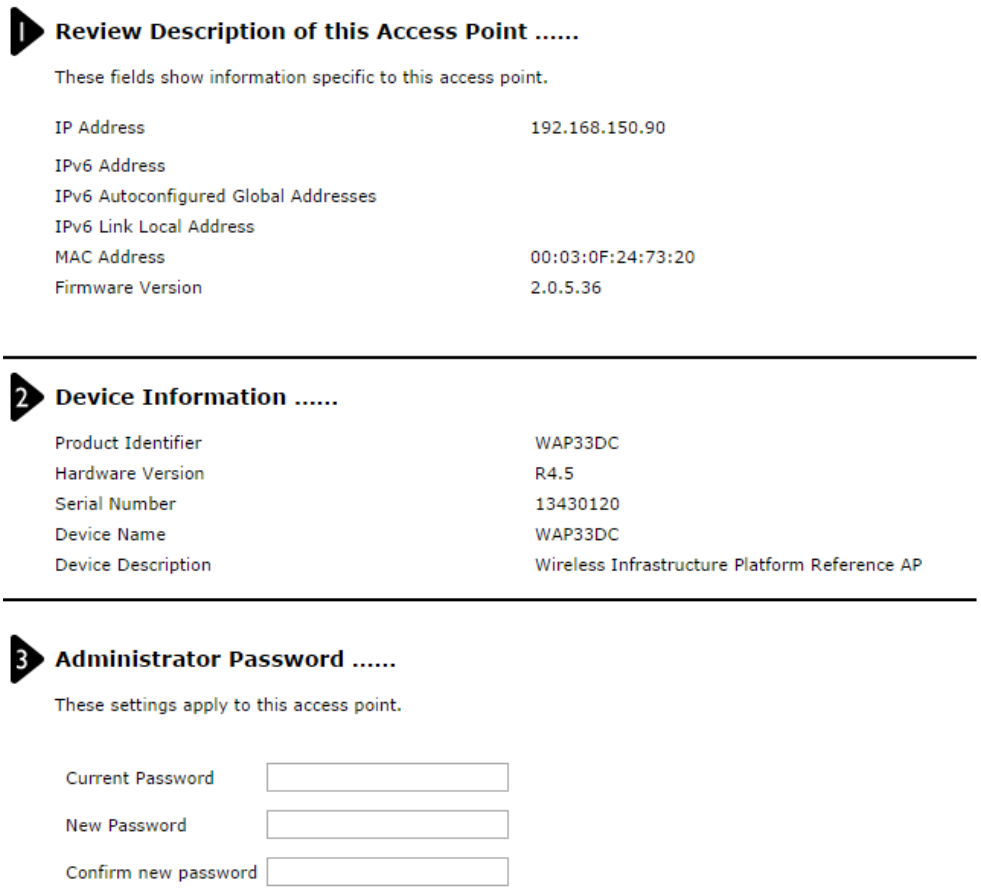
This section shows basic information about the AP, which include;
Description of this access point

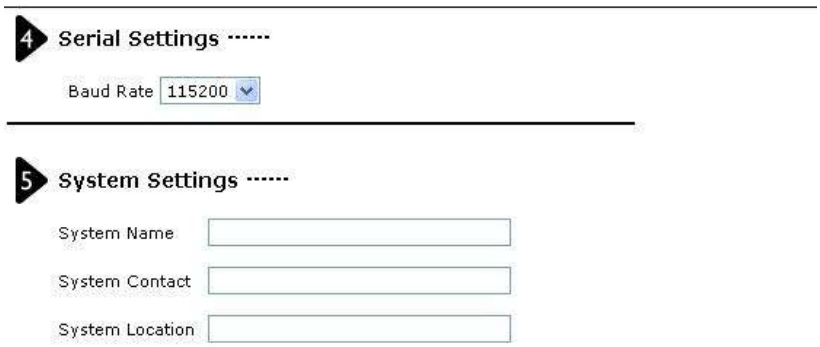
Device information;

Administrator password;

Serial settings;

System settings.






## *2.1 Detailed Explanation of Settings*

### 2.1.1 Description of Access Point

| | |
|---|---|
| IP address | IP address of the access point. |
| MAC address | MAC address of the accesses point. |
| Firmware version | Current firmware version of the access Point. |

### 2.1.2 Device Information

| | |
|---|---|
| Product identifier | Model name of the access point. . |
| Hardware version | Hardware version of the access point. |
| Serial number | Serial number of the access point. |
| Device name | Device name of the access point. |
| Device description | Description of the access point. |

### 2.1.3 Administrator Password

| | |
|---|---|
| Current password | Enter the current administrator password. |
| New password | Input the new password. |
| Confirm new password | Verify new password. |

Click on the update button to apply the new password to the access point.

### 2.1.4 Serial Settings

| | |
|---|---|
| Baud Rate | Configure the baud rate of the serial port. |

### 2.1.5 System Settings

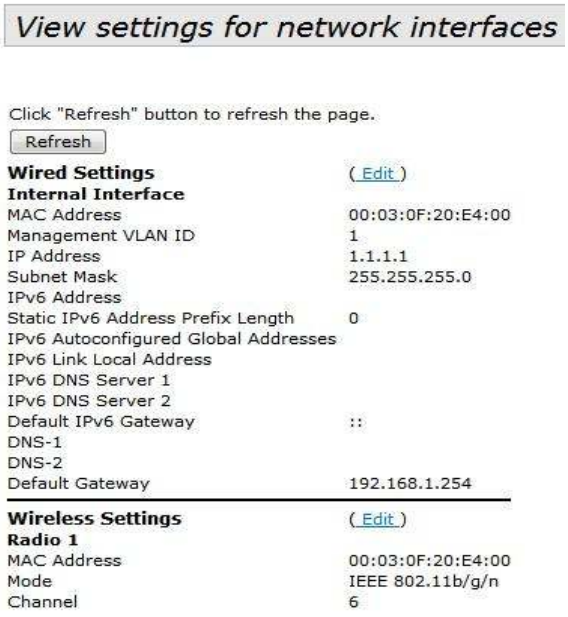
| | |
|---|---|
| System name | Configure the system name. |
| System contact | Configure the system contact. |
| System location | Configure the device location. |

These settings are used in the CLI to identify the access point you are connecting to.

# Chapter 3 Status

The current status includes network information, transmission statistics and the client association.

## *3.1 Network Information*




### 3.1.1 Wired Settings

| | |
|---|---|
| MAC address | MAC address of the AP / Radio 1. |
| Management VLAN ID | The current VLAN id of the management interface/ |
| IP address | IP address of the AP web gui. |
| Subnet mask | Subnet Mask of the AP |
| IPv6 Admin Mode | Show if the AP supports the IPv6 management on-off. |
| IPv6 Auto Config Admin Mode | Show if the AP supports to get the IPv6 address dynamically. |

| | |
|---|---|
| Static IPv6 Address | Shows the static IPv6 address of AP. |
| Static IPv6 Address Prefix Length | Shows the prefix length of static IPv6 address. |
| IPv6 Auto-configured Global Addresses | Shows the IPv6 address list that the AP gets dynamically. |
| IPv6 Link Local Address | Shows the IPv6 link local address of AP. |
| Default IPv6 Gateway | Shows the default IPv6 gateway of AP. |
| IPv6 DNS Server 1 | Shows the IPv6 DNS server 1 of AP. |
| IPv6 DNS Server 2 | Shows the IPv6 DNS server 2 of AP. |
| DNS-1 | Shows the IP address of DNS-1 server of the AP. |
| DNS-2 | Shows the IP address of DNS-2 server of the AP. |
| Default gateway | Shows the default gateway of the AP. |

### 3.1.2 Wireless Settings

| | |
|---|---|
| MAC address | MAC address information of Radio 1 or 2. |
| Mode | Wireless mode configured for Radio 1 or 2. |
| Channel | Show the channel information of Radio1 or 2. |

### 3.1.3 Explanation

Click the “edit” link on the right hand side of the wired and wireless configuration to link to those pages directly.

## *3.2 Statistics for Transmitting and Receiving IP Traffic*

### 3.2.1 Device Information Status

Show all the physical ports and the status of virtual AP.

| | |
|---|---|
| Interface | The name of the Ethernet, VAP or WDS interface. |
| Status | Shows whether the interface is up or down. |
| MAC Address | MAC address for the specified interface. The UAP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios. |
| Name (SSID) | Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP or WDS tab. |

### 3.2.2 Transmit/Receive Packets

| | |
|---|---|
| Total Packets | Indicates total packets sent (in Transmit table) or received (in Received table) by this AP. |
| Total Bytes | Indicates total bytes sent (in Transmit table) or received (in Received table) by this AP. |
| Total Dropped Packets | Indicates total number of packets sent (in Transmit table) or received (in Received table) by this AP that were dropped. |
| Total Dropped Bytes | Indicates total number of bytes sent (in Transmit table) or received (in Received table) by this AP that were dropped. |
| Errors | Indicates total errors related to sending and receiving data on this AP. |

## *3.3 Client Association*

Client association showing:

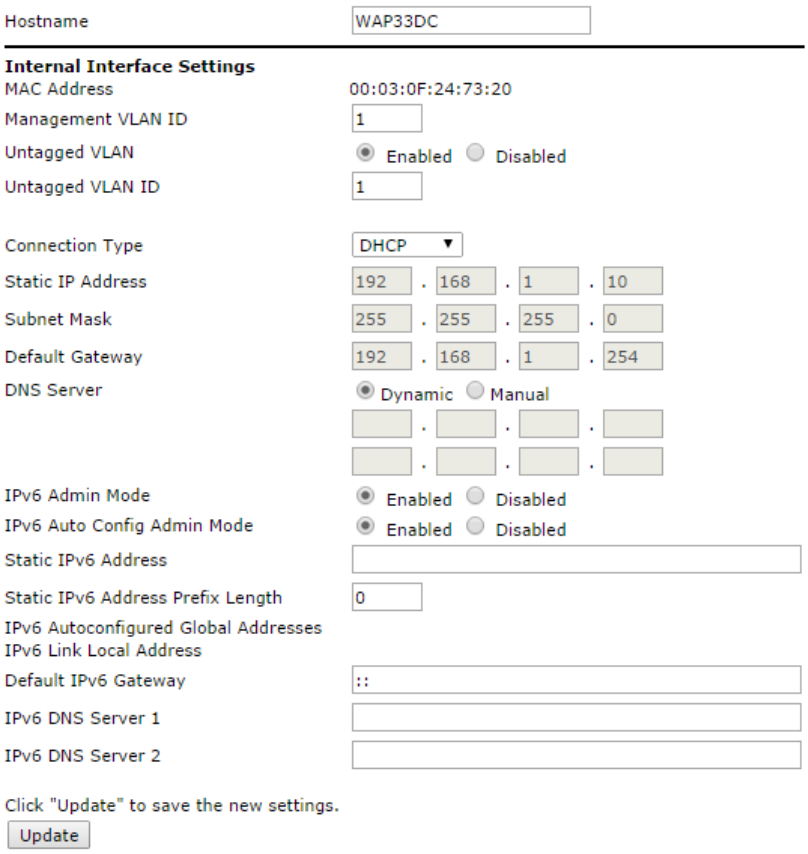
| Network | Station | Status | | From Station | | | | To Station | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Authenticated | Associated | Packets | Bytes | Drop Packets | Drop Bytes | Packets | Bytes | Drop Packets | Drop Bytes |
| test | 00:0d:a3:13:31:6d | Yes | Yes | 151 | 18021 | 0 | 0 | 53 | 4910 | 0 | 0 |

| | |
|---|---|
| Network | Shows which VAP the client is associated with. For example, an entry of wlan0vap2 means the client is associated with Radio 1, VAP 2.<br>An entry of wlan0 means the client is associated with VAP 0 on Radio 1. An entry of wlan1 means the client is associated with VAP 0 on Radio 2. |
| Station | Shows the MAC address of the associated wireless client. |
| Status | The Authenticated and Associated Status shows the underlying IEEE 802.11 authentication and association status, which is present no matter which type of security the client uses to connect to the AP. This status does not show IEEE 802.1X authentication or association status.<br><br>Some points to keep in mind with regard to this field are:<br><br>* If the AP security mode is None or Static WEP, the authentication and association status of clients showing on the Client Associations tab will be in line with what is expected; that is, if a client shows as authenticated to the AP, it will be able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.)<br><br>* If the AP uses IEEE 802.1X or WPA security, however, it is possible for a client association to show on this tab as authenticated (via the IEEE 802.11 security) but actually not be authenticated to the AP via the second layer of security. |
| From Station | From Station<br>Shows the number of packets and bytes received from the wireless client and the number of packets and bytes that were dropped after being received. |
| To Station | Shows the number of packets and bytes transmitted from the AP to the wireless client and the number of packets and bytes that were dropped upon transmission. |

# Chapter 4 Advance Configuration

The Manage tab includes Ethernet settings, Wireless settings, RF parameters, and Virtual AP and AP modes.

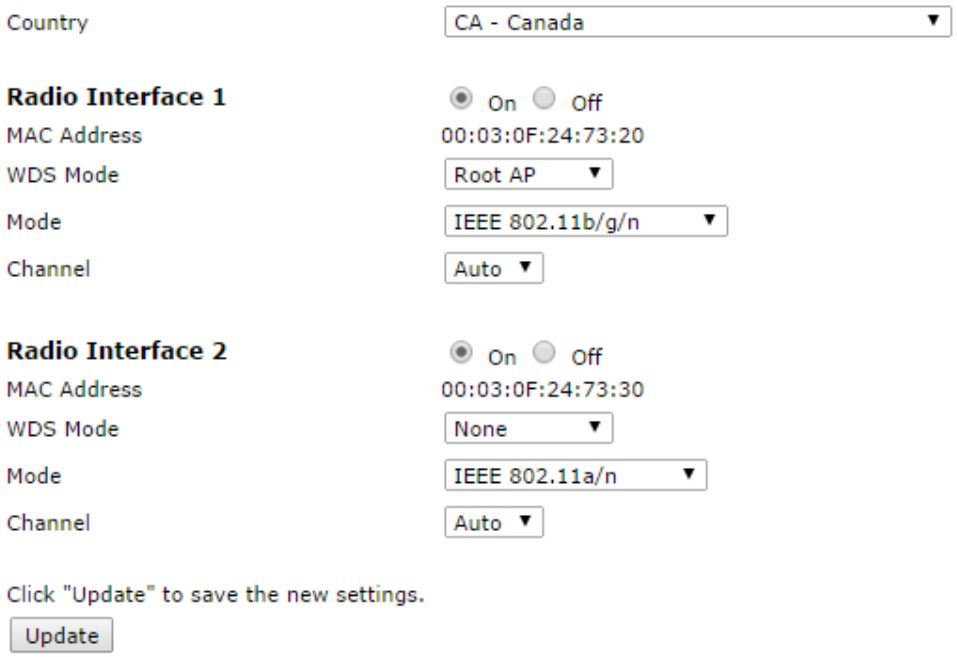
## *4.1 Ethernet Settings*




| | |
|---|---|
| Hostname | Enter a hostname for the AP. The hostname appears in the CLI prompt.<br>The hostname has the following requirements:<br>* The length must be between 1-63 characters.<br>* Upper and lower case characters, numbers, and hyphens are accepted.<br>* The first character must be a letter (a-z or A-Z), and the last character cannot be a hyphen. |
| MAC Address | Shows the MAC address for the LAN interface for the Ethernet port on this AP. This is a read-only field that you cannot change. |

| | |
|---|---|
| Management VLAN ID | The management VLAN is the VLAN associated with the IP address you use to access the AP. The default management VLAN ID is 1.<br>Provide a number between 1 and 4094 for the management VLAN ID. |
| Untagged VLAN | If you disable the untagged VLAN, all traffic is tagged with a VLAN ID.<br>By default all traffic on the UAP uses VLAN 1, which is the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS. |
| Untagged VLAN ID | Provide a number between 1 and 4094 for the untagged VLAN ID. Traffic on the VLAN that you specify in this field will not be tagged with a VLAN ID. |
| Connection Type | If you select DHCP, the UAP acquires its IP address, subnet mask, DNS, and gateway information from a DHCP server.<br>If you select Static IP, you must enter information in the Static IP Address, Subnet Mask, and Default Gateway fields. |
| Static IP Address | Enter the static IP address in the text boxes. This field is disabled if you use DHCP as the connection type. |
| Subnet Mask | Enter the Subnet Mask in the text boxes. |
| Default Gateway | Enter the Default Gateway in the text boxes. |
| DNS Name servers | Select the mode for the DNS. This field only works in FIT mode.<br>In Dynamic mode, the IP addresses for the DNS servers are assigned automatically via DHCP. This option is only available if you specified DHCP for the Connection Type.<br>In Manual mode, you must assign static IP addresses to resolve domain names. |
| IPv6 Admin Mode | Enable or disable IPv6 management access to the AP. |
| IPv6 Auto Config Admin Mode | Enable or disable IPv6 auto address configuration on the AP.<br>When IPv6 Auto Config Mode is enabled, automatic IPv6 address configuration and gateway configuration is allowed by processing the Router Advertisements received on the LAN port. The AP can have multiple auto configured IPv6 addresses. |
| Static IPv6 Address | Enter a static IPv6 address. The AP can have a static IPv6 address even if addresses have already been configured automatically. |
| Static IPv6 Address Prefix Length | Enter the static IPv6 prefix length, which is an integer in the range of 0-128. |
| IPv6 Auto configured Global Addresses | If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed. |
| IPv6 Link Local Address | Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process. |
| Default IPv6 Gateway | Enter the default IPv6 gateway. |
| IPv6 DNS Server 1 | Enter the first static IPv6 address for DNS Servers. |
| IPv6 DNS Server 2 | Enter the second static IPv6 address for DNS Servers. |

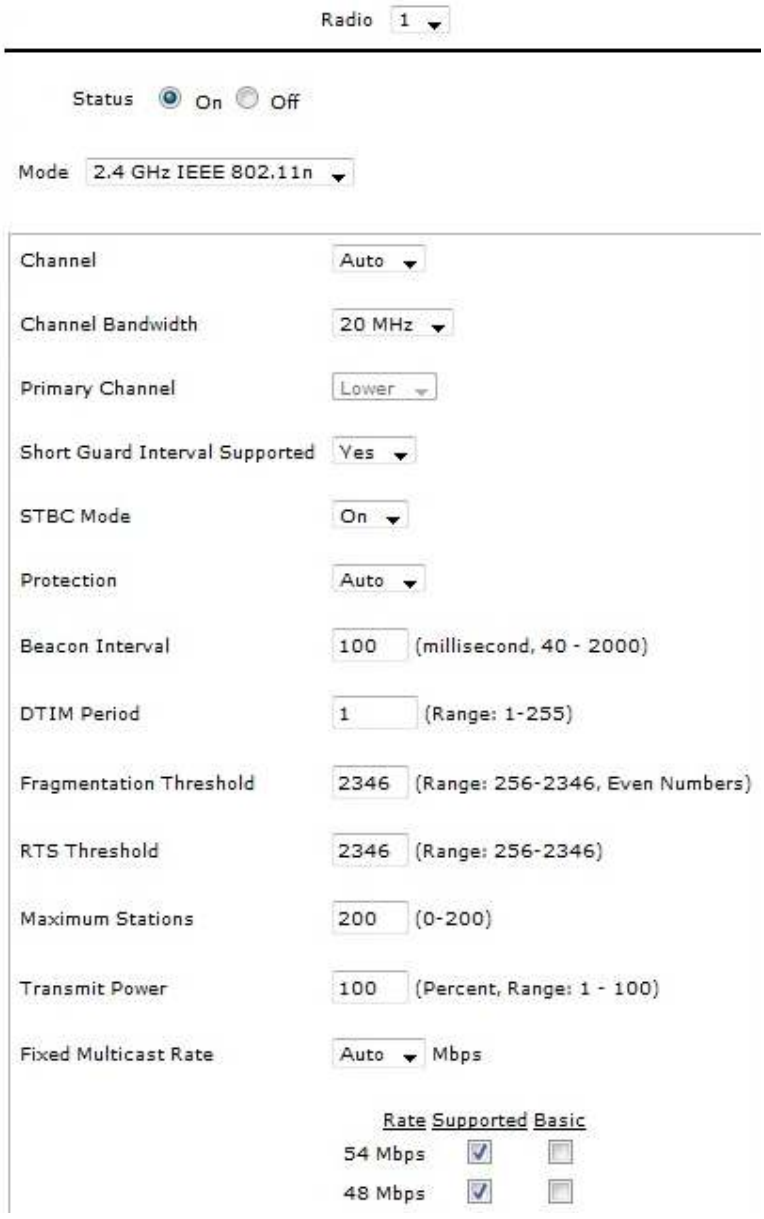
## 4.2 Wireless Settings




| | |
|---|---|
| Country | Select the country in which the AP is operating.<br>Wireless regulations vary from country to country. Make sure you select the correct country code so that the AP complies with the regulations in your country. The country code selection affects the radio modes the AP can support as well as the list of channels and transmission power of the radio. |
| Radio Interface | Specify whether you want the radio interface on or off. |
| MAC Address | Indicates the Media Access Control (MAC) addresses for the interface.<br>This page shows the MAC addresses for Radio Interface One and Radio Interface Two.<br>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. |
| WDS Mode | The wds mode of the current radio interface.<br>Select one of the following modes for each radio interface:<br><br>None-The radio interface working in this mode cannot provide wds functions.<br>Root AP-The access point working in this mode provides wds functions.<br>Satellite AP-The access point working in this mode can bridge wireless traffic with Root AP.<br>Note: We cannot configure wireless mode or channel using the AP in Satellite mode |

| | |
|---|---|
| Mode | The Mode defines the Physical Layer (PHY) standard the radio uses<br>Note: The modes available depend on the country code setting.<br>Select one of the following modes for each radio interface:<br>IEEE 802.11a - Only 802.11a clients can connect to the AP.<br>IEEE 802.11b/g - 802.11b and 802.11g clients can connect to the AP.<br>IEEE 802.11a/n - 802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP.<br>IEEE 802.11b/g/n (default) - 802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.<br>5 GHz IEEE 802.11n - Only 802.11n clients operating in the 5-GHz frequency can connect to the AP.<br>2.4 GHz IEEE 802.11n - Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP. |
| Channel | Select the Channel.<br>The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected.<br>The Channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).<br>When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel field. This allows the automatic channel feature to set the channels for the radios in the cluster |

## *4.3 Radio*


Radio 1
Status On Off
Mode 2.4 GHz IEEE 802.11n
Channel Auto
Channel Bandwidth 20 MHz
Primary Channel Lower
Short Guard Interval Supported Yes
STBC Mode On
Protection Auto
Beacon Interval 100 (millisecond, 40 - 2000)
DTIM Period 1 (Range: 1-255)
Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)
RTS Threshold 2346 (Range: 256-2346)
Maximum Stations 200 (0-200)
Transmit Power 100 (Percent, Range: 1 - 100)
Fixed Multicast Rate Auto Mbps
Rate Supported Basic
54 Mbps
48 Mbps

| | |
|---|---|
| Radio | Select Radio 1or Radio 2 to specify which radio to configure. The rest of the settings on this tab apply to the radio you select in this field. Be sure to configure settings for both radios. |
| Status (On/Off) | Specify whether you want the radio on or off by clicking On or Off.<br>If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs. |
| Mode | The Mode defines the Physical Layer (PHY) standard the radio uses<br>Note: The modes available depend on the country code setting.<br>Select one of the following modes for each radio interface:<br>IEEE 802.11a-Only 802.11a clients can connect to the AP.<br>IEEE 802.11b/g-802.11b and 802.11g clients can connect to the AP.<br>IEEE 802.11a/n-802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP.<br>IEEE 802.11b/g/n (default)-802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.<br>5 GHz IEEE 802.11n-Only 802.11n clients operating in the 5-GHz frequency can connect to the AP.<br>2.4 GHz IEEE 802.11n-Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP. |
| Channel | Select the Channel.<br>The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected.<br>The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).<br>Note: When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel field. This allows the automatic channel feature to set the channels for the radios in the cluster. |
| Channel Bandwidth (802.11n modes only) | The 802.11n specification allows a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices.<br>Set the field to 20-MHz to restrict the use of the channel bandwidth to a 20-MHz channel. |
| Primary Channel (802.11n modes only) | This setting can be changed only when the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients.<br>Select one of the following options:<br>Upper-Set the Primary Channel as the upper 20-MHz channel in the 40-MHz band.<br>Lower-Set the Primary Channel as the lower 20-MHz channel in the 40-MHz band. |

| | |
|---|---|
| Short Guard Interval Supported | This field is available only if the selected radio mode includes 802.11n.<br>The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput.<br>Select one of the following options:<br>Yes-The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the short guard interval.<br>No-The AP transmits data using an 800 ns guard interval. |
| STBC Mode | This field is available only if the selected radio mode includes 802.11n.<br>Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams.<br>Select one of the following options:<br>On-The AP transmits the same data stream on multiple antennas at the same time.<br>Off-The AP does not transmit the same data on multiple antennas. |
| Protection | The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP.<br>You can disable (Off) these protection mechanisms; however, when protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions.<br>Note: This setting does not affect the ability of the client to associate with the AP. |
| Beacon Interval | Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). Enter a value from 40 to 2000 milliseconds. |
| DTIM Period | Specify a DTIM period from 1 to 255 beacons.<br>The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the AP awaiting pick-up.<br>The DTIM period you specify indicates how often the clients served by this AP should check for buffered data still on the AP awaiting pickup. The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon. |
| Fragmentation Threshold | Specify a number between 256 and 2,346 to set the frame size in bytes.<br>The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold you set, the fragmentation function is activated and the packet is sent as multiple 802.11 frames.<br>If the packet being transmitted is equal to or less than the threshold, fragmentation is not used.<br>Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation plays no role when Aggregation is enabled. |

| | |
|---|---|
| | Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) might help with some interference problems; for example, with microwave ovens.<br>By default, fragmentation is off. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput. |
| RTS Threshold | Specify a Request to Send (RTS) Threshold value between 256 and 2346.<br>The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.<br>Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference. |
| Maximum Stations | Specify the maximum number of stations allowed to access this AP at any one time.<br>You can enter a value between 0 and 200. |
| Transmit Power | Enter a percentage value for the transmit power level for this AP.<br>The default value, which is 100%, can be more cost-efficient than a lower percentage since it gives the AP a maximum broadcast range and reduces the number of APs needed.<br>To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This helps reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network. |
| Fixed Multicast Rate | Select the multicast traffic transmission rate you want the AP to support. |
| Rate Sets | Check the transmission rate sets you want the AP to support and the basic rate sets you want the AP to advertise:<br>Rates are expressed in megabits per second.<br>Supported Rate Sets indicate rates that the AP supports. You can check multiple rates (click a check box to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP.<br>Basic Rate Sets indicate rates that the AP will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets. |

## *4.4 Virtual AP*

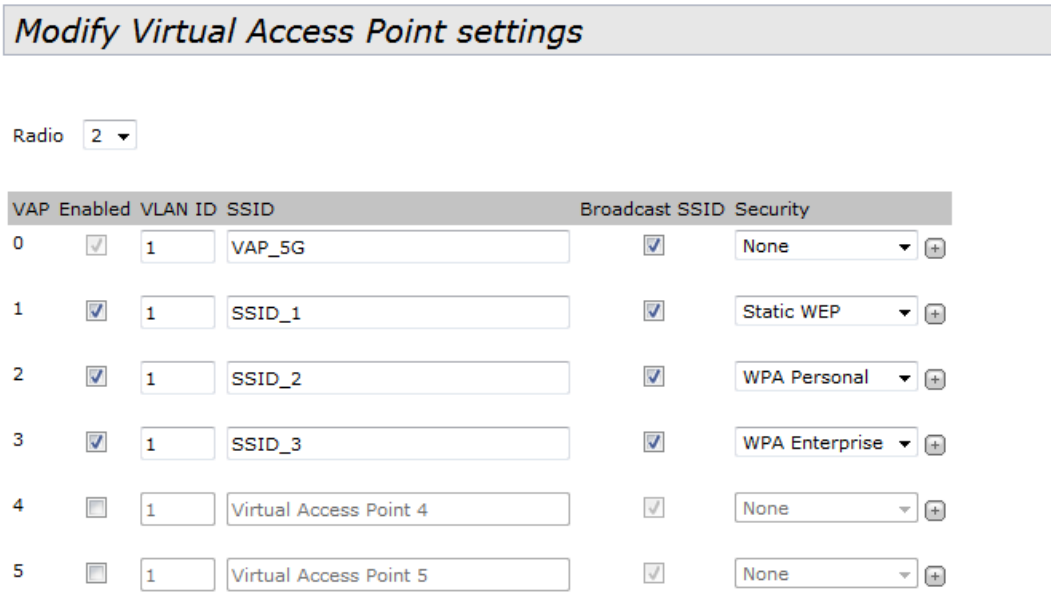
VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple APs in one physical AP. Each radio supports up to 16 VAPs.

For each VAP, you can customize the security mode to control the wireless client access. Each VAP can also have a unique SSID. Multiple SSIDs make a single AP look like two or more APs to other systems on the network. By configuring VAPs, you can maintain better control over broadcast and multicast traffic, which affects the network performance.

You can configure each VAP to use a different VLAN, or you can configure multiple VAPs to use the same VLAN, whether the VLAN is on the same radio or on a different radio, whether the VLAN is on the same radio or on a different radio. VAP0, which is always enabled on both radios, is assigned to the default VLAN 1.

The AP adds VLAN ID tags to wireless client traffic based on the VLAN ID you configure on the VAP page or by using the RADIUS server assignment. If you use an external RADIUS server, you can configure multiple VLANs on each VAP. The external RADIUS server assigns wireless clients to the VLAN when the clients associate and authenticate.

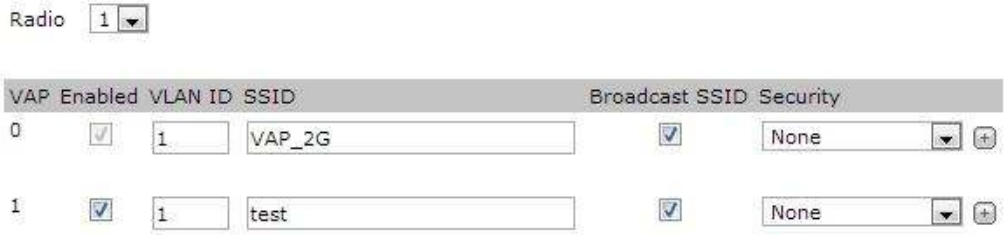
If wireless clients use a security mode that does not communicate with the RAIDUS server, or if the RADIUS server does not provide the VLAN information, you can assign a VLAN ID to each VAP. The AP assigns the VLAN to all wireless clients that connect to the AP through that VAP.



| | |
|---|---|
| Radio | Select the radio to configure, Radio 1 or Radio 2. VAPs are configured independently on each radio. |
| VAP | You can configure up to 16 VAPs for each radio. VAP0 is the physical radio interface, so to disable VAP0, you must disable the radio. |
| Enabled | You can enable or disable a configured network.<br>To enable the specified network, select the Enabled option beside the appropriate VAP.<br>To disable the specified network, clear the Enabled option beside the appropriate VAP.<br>If you disable the specified network, you will lose the VLAN ID you entered. |
| VLAN ID | When a wireless client connects to the AP by using this VAP, the AP tags all traffic from the wireless client with the VLAN ID you enter in this field unless you enter the untagged VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is 1-4094. |
| SSID | Enter a name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. You can use the same SSID for multiple VAPs, or you can choose a unique SSID for each VAP.<br>Note: If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting. |
| Broadcast SSID | Specify whether to allow the AP to broadcast the Service Set Identifier (SSID) in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect.<br>To enable the SSID broadcast, select the Broadcast SSID check box.<br>To prohibit the SSID broadcast, clear the Broadcast SSID check box.<br>Note: Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available. |
| Security | Select one of the following Security modes for this VAP:<br>None<br>Static WEP<br>WPA Personal<br>WPA Enterprise<br>If you select a security mode other than None, additional fields appear. These fields are explained below.<br>Note: The Security mode you set here is specifically for this VAP. |

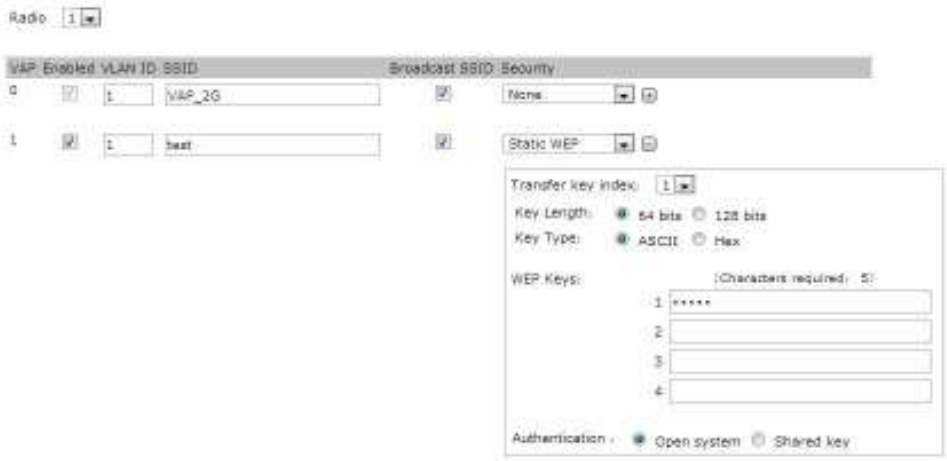
### 4.4.1 No Security Configuration

Choose the security configuration as none, the security configuration will not be used with clients association; it can be associated with the virtual AP directly.




### 4.4.2 Static WEP Security Configuration

Choose the security configuration as Static WEP and show the detailed configuration information of static WEP security configuration. The WEP key should be used with the client to authentication and to decrypt the packet.




| | |
|---|---|
| Transfer Key Index | Select a key index from the drop-down menu. Key indexes 1 through 4 are available. The default is 1.<br>The Transfer Key Index indicates which WEP key the AP will use to encrypt the data it transmits. |
| Key Length | Specify the length of the key by clicking one of the radio buttons: 40 bits or 104 bits. |
| Key Type | Select the key type by clicking one of the radio buttons: ASCII or Hex. |

| | |
|---|---|
| WEP Keys | You can specify up to four WEP keys. In each text box, enter a string of characters for each key. The keys you enter depend on the key type selected:<br>ASCII-Includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.<br>Hex-Includes digits 0 to 9 and the letters A to F.<br>Use the same number of characters for each key as specified in the Characters Required field. These are the RC4 WEP keys shared with the stations using the AP.<br>Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP.<br>Characters Required: The number of characters you enter into the WEP Key fields is determined by the Key length and Key type you select. For example, if you use 104-bit ASCII keys, you must enter 13 characters in the WEP key; if you use 104-bit Hex keys, you must enter 26 characters in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type. |
| Authentication | The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an AP when static WEP is the security mode.<br>Specify the authentication algorithm you want to use by choosing one of the following options:<br>Open System authentication allows any client station to associate with the AP whether that client station has the correct WEP key or not. This algorithm is also used in plaintext, IEEE 802.1X, and WPA modes. When the authentication algorithm is set to Open System, any client can associate with the AP.<br>Shared Key authentication requires the client station to have the correct WEP key in order to associate with the AP. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key will not be able to associate with the AP. |

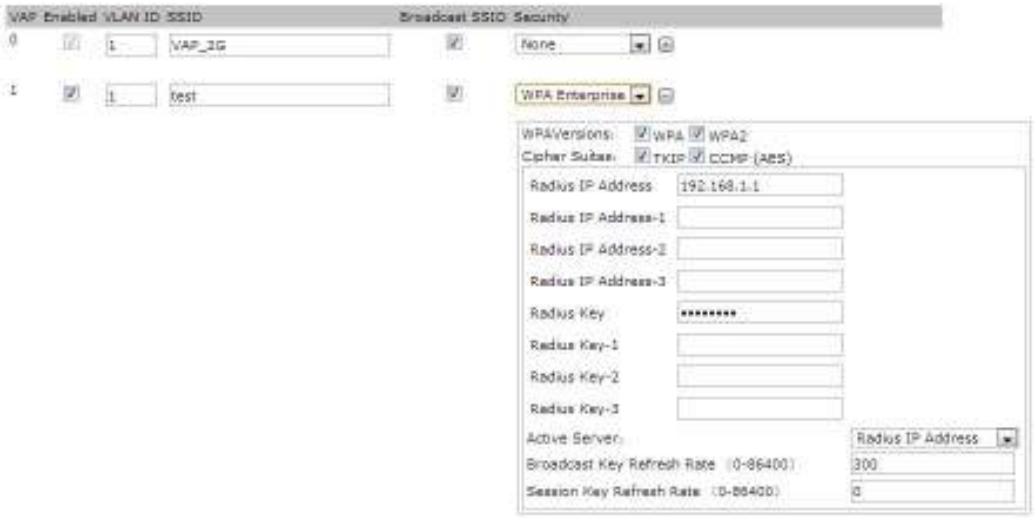
### 4.4.3 WPA Personal Security Configuration

Choose the security configuration as WPA Personal and show the detailed configuration information of WPA Personal security configuration. The WPA key should be used on the client to authentication and to decrypt the packet.


| | |
|---|---|
| WPA Versions | Select the types of client stations you want to support:<br>WPA. If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA.<br>WPA2. If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.<br>WPA and WPA2. If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security. |
| Cipher Suites | Select the cipher suite you want to use:<br>TKIP, CCMP(AES) or TKIP and CCMP (AES)<br>Both TKIP and AES clients can associate with the AP. WPA clients must have one of the following to be able to associate with the AP:<br>A valid TKIP key<br>A valid AES-CCMP key<br>Clients not configured to use a WPA Personal will not be able to associate with the AP. |
| Key | The Pre-shared Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. |
| Broadcast Key Refresh Rate | Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 300). The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed. |

### 4.4.4 WPA Enterprise Security Configuration

Choose the security configuration as WPA Enterprise and show the detailed configuration information of WPA Enterprise security configuration. The direct user name and password from the radius server should be used in the client to pass authentication.




| | |
|---|---|
| WPA Versions | Select the types of client stations you want to support:<br>WPA. If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA.<br>WPA2. If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.<br>WPA and WPA2. If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both WPA and WPA2. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security. |
| Cipher Suites | Select the cipher suite you want to use:<br>TKIP, CCMP(AES) or TKIP and CCMP (AES)<br>By default both TKIP and CCMP are selected. When both TKIP and CCMP are selected, client stations configured to use WPA with RADIUS must have one of the following:<br>A valid TKIP RADIUS IP address and RADIUS Key<br>A valid CCMP (AES) IP address and RADIUS Key |
| RADIUS IP Address Type | Specify the IP version that the RADIUS server uses.<br>You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the AP contacts only the RADIUS server or servers for the address type you select in this field. |
| RADIUS IP Address<br>RADIUS IPv6 Address | Enter the IPv4 or IPv6 address for the primary RADIUS server for this VAP.<br>If the IPv4 RADIUS IP Address Type option is selected in the previous field, enter the IP address of the RADIUS server that all |

| | |
|---|---|
| | VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd. |
| RADIUS IP or IPv6 Address 1-3 | Enter up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP. The field label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected.<br>If authentication fails with the primary server, each configured backup server is tried in sequence. |
| RADIUS Key | Enter the RADIUS key in the text box.<br>The RADIUS Key is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. |
| RADIUS Key 1-3 | Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on. |
| Enable RADIUS Accounting | Select this option to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on.<br>If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers. |
| Active Server | Select a radius server from the drop-down menu. Radius IP Address and Radius IP Address 1-3 are available. The default is Radius IP Address. The Active Server indicates which RADIUS server the AP will use. |
| Broadcast Key Refresh Rate | Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 300). The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed. |
| Session Key Refresh Rate | Enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0 or 30-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed. |

## *4.5 WDS mode*

The Wireless Distribution System (WDS) allows you to connect multiple APs. With WDS, APs communicate with one another without any wires connecting them. WDS can extend the reach of your network into areas where cabling might be too difficult. This allows the network to extend over an area too large for one access point to cover. It can also simplify the network infrastructure by reducing the amount of cabling required.

To enable WDS mode, select it from Advanced Configuration > Wireless Settings, in section 4.2 of this manual.

The 2 options are Root or satellite mode for the WDS function.

Root AP-The main access point which will initiate the connection.

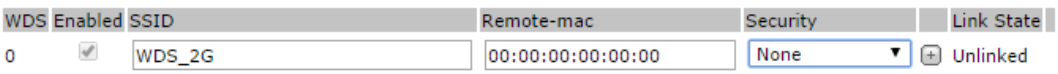
Satellite AP-The connecting access point in this mode can bridge wireless traffic with Root AP.

Note: We cannot configure wireless mode and channel in the Satellite AP mode.

| | |
|---|---|
| WDS | You can configure up to 16 WDS links for each radio. The wds link with the number 0 is enabled by default. |
| Enabled | You can enable or disable a configured wds link.<br>*To enable the specified wds link, select the Enabled option.<br>*To disable the specified wds link, clear the Enabled option. |
| SSID | Enter a name for the wireless network used by the wds link. The SSID is an alphanumeric string of up to 32 characters. You can use the same SSID for multiple wds links, or you can choose a unique SSID for each wds link. |
| Remote-mac | Specify the MAC address of the destination AP; that is, the AP on the other end of the WDS link to which data will be sent or handed-off and from which data will be received. It must be a valid unicast MAC address with the format of "**-**-**-**-**-**". Acceptable characters include upper and lower case alphabetic letters and the numeric digits. |
| Security | Select one of the following Security modes for this VAP:<br>*None<br>*WPA Personal<br>If you select WPA Personal as the security mode, additional fields appear. These fields are explained below.<br>Note: The Security mode you set here is specifically for this wds link. |
| Link State | The status of this wds link: Linked or Unlinked. |

## 4.5.1 None (Plain-text)

If you select None as your security mode, no further options are configurable on the AP. This mode means that any data transferred to and from the AP is not encrypted. This security method can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.



### 4.5.2 WPA Personal

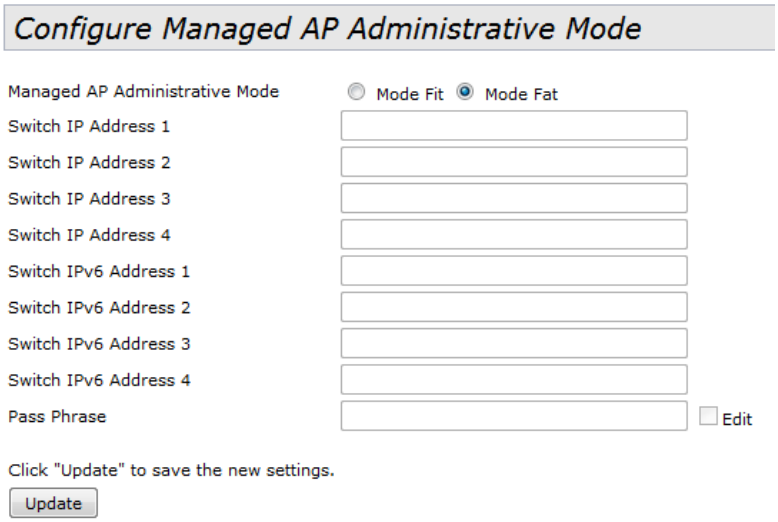
WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP mechanisms. The Personal version of WPA employs a pre-shared key (instead of using IEEE 802.1X and EAP as is used in the Enterprise WPA security mode). The PSK is used for an initial check of credentials only.

This security mode is backwards-compatible for wireless clients that support the original WPA.


| | |
|---|---|
| Key | The Pre-shared Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. |
| Broadcast Key Refresh Rate | Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 300). The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed. |

## *4.6 AP Modes*

The AP modes can be switched on this page. Configure the address of the AC and the password of an AP.

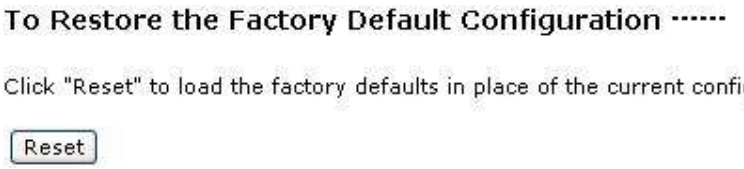



| | |
|---|---|
| Managed AP Administrative Mode | Click Mode Fit to allow the AP and switch to discover each other. If the AP successfully authenticates itself with a wireless switch, you will not be able to access the Administrator UI.<br>Click Mode Fat to prevent the AP from contacting wireless switches. |
| Switch IP address | Enter the IP address of up to four wireless switches that can manage the AP. You can enter the IP address in dotted format or as an DNS name.<br>You can view a list of wireless switches on your network that were configured by using a DHCP server.<br>The AP attempts to contact Switch IP Address 1 first. |
| Switch IPv6 address | Enter the IPv6 address of up to four wireless switches that can manage the AP.<br>You can view a list of wireless switches on your network that were configured by using a DHCP server.<br>The AP attempts to contact Switch IPv6 Address 1 first. |
| Pass Phrase | Select the Edit option and enter a passphrase to allow the AP to authenticate itself with the wireless switch. The passphrase must be between 8 and 63 characters.<br>To remove the password, select Edit, delete the existing password, and then click Update.<br>You must configure the same passphrase on the switch. |

# Chapter 5 Maintenance

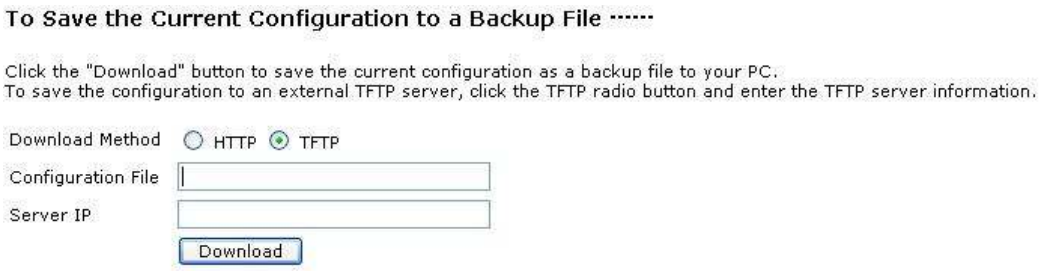
The system maintenance includes management configuration and firmware upgrading.

## *5.1 Configuration Management*



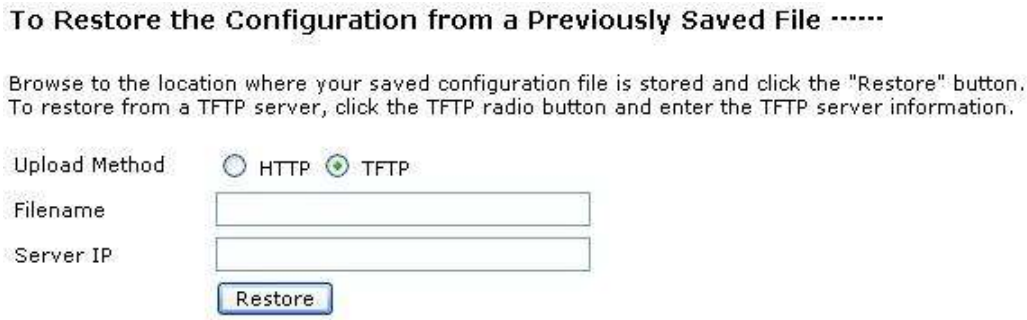

Click the “reset” button to restore the AP to the default configuration. The default working mode of an AP is fit AP mode.


Choose the download method as HTTP mode, click the “download” button and confirm, the current configuration files of the AP will be downloaded through HTTP directly.

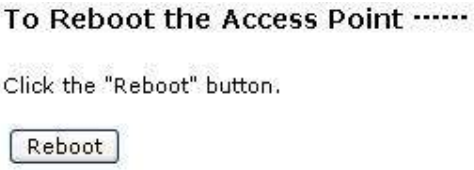



Choose the download method as TFTP mode, input the file name of the configuration file (the format is *.xml) and the IP address of the TFTP server. Then click “download” button and confirm. The configuration file will be downloaded using the TFTP server.


When the upload method is selected as HTTP mode, click the “browse” button to choose the configuration file (the format is *.xml) which needs to be uploaded. Confirm it and click the “restore” button. The current configuration of the AP will be restored to the configuration in the uploaded configuration file.

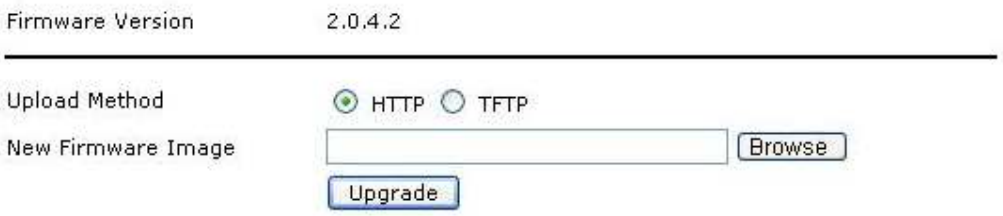



When the upload method is selected as TFTP mode, input the file name of the configuration file (the format is *.xml) and the IP address of the TFTP server. Click the “restore” button and confirm it. The current configuration of the AP will be restored to the configuration in the uploaded configuration file.




Click “reboot” button and confirm it. The AP will restart

## *5.2 Upgrade*




| | |
|---|---|
| Platform Version of firmware | Show the version firmware of the current AP. |

Complete the firmware upgrading of the AP by using HTTP through the following steps:

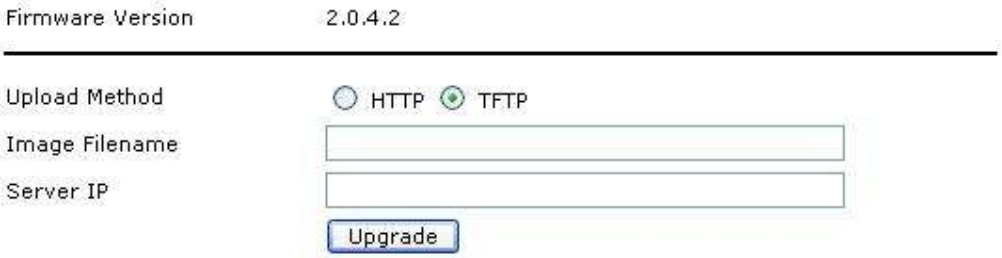
1. Choose HTTP as the upgrading method.
2. Browse for the firmware file.

   The firmware file should have the extension ".tar".
3. Click the “Firmware Upgrading” button to apply the new firmware file.

   The controller will display the next steps.
4. Click the “Confirm” button to start the upgrading process.

The upgrading process may take a few minutes. During this time, the AP cannot be accessed. Do not unplug the AP or restart it. After upgrading, the AP will restart. Upon competition, the AP will automatically configure to its previous settings.

5. Check the firmware version within the firmware management page (or the basic configuration label). If the upgrading was successful, the new version will be displayed.



Complete the firmware upgrading of the AP by using TFTP through the following steps:

1. Choose TFTP as the uploading method.

2. Input the name of the mirror file in the text box (1 to 256 characters). The name includes the integral path of the mirror file.

For example, if the file of "ap_upgrade.tar" in the content of /share/builds/ap needs to be uploaded, input “/share/builds/ap/ap_upgrade.tar” in the text box.

The upgrading file of firmware must be a “tar” file. Please do not try to use the bin file or any other kinds of files to upgrade; these files would not work.

3. Input the IP address of the TFTP server.

4. Click the “firmware upgrading” button.

After clicked the “firmware upgrading” button, there will be a window which describes the upgrading process.

5. Click the “confirm” button to confirm to upgrade and start the upgrading process. Notice: click the “firmware upgrading” button and confirm it in the window. The Upgrading process will start.

The upgrading process will take a few minutes. During this period, the AP cannot be accessed. Please do not turn off the AP's power during the upgrade. After upgrading, the AP will restart. After the restart, the AP will use the new configuration

6. To check if the firmware upgrade worked, please check the firmware version in the firmware management page (or the basic configuration page).

# Chapter 6 Configuration Examples

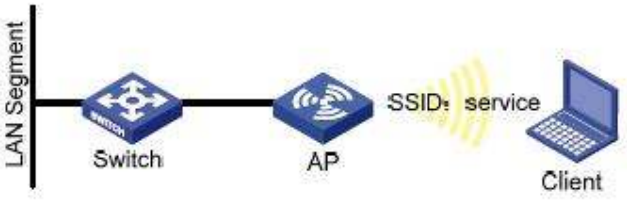
## *6.1 Wireless Access Laws*

### 6.1.1 Networking Requirements

An effective network must be able to give users access to the internal network resources anytime. The device administrator can configure the wireless access laws. The required steps are listed below.

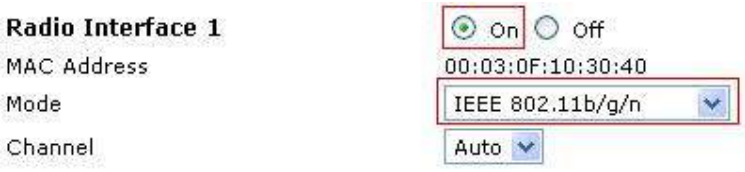
- AP provides the wireless access service with an SSID as the method of “service”.
- For meeting the high bandwidth demands of wireless users, select the 802.11n (2.4GHz) RF mode.

Fig 1-11 wireless access method




### 6.1.2 Configuration Steps

1. Login into the AP and enter the wireless configuration page.




- Choose “enable” for Radio Interface 1.
- Choose IEEE 802.11b/g/n for the wireless mode.
- Choose the default configuration for the channel.
- Click “submit”.

2. Enter into the virtual AP configuration page.


- Choose the virtual AP enabled box (the virtual AP "0" is enabled as default.

- Configure the VLAN ID according to the actual situation.
- Configure SSID as “service”.
- Use the default configuration for “broadcast SSID”.
- Choose “None” for the security configuration.
- Click “submit” button.

### 6.1.3 Test the Configuration Results

- Enter into the client association page to view the successful on-line clients.

## *6.2 Cipher Wireless Access of Static-WEP (Open-System)*

### 6.2.1 Networking Requirements

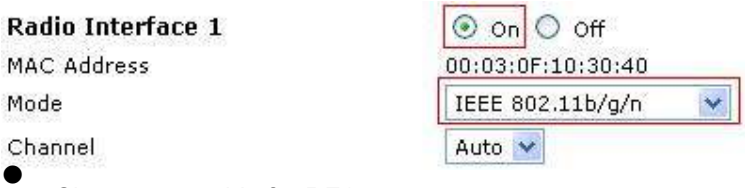
In a small office, the device administrator can complete the WEP (Open-System) cipher configuration through the web page. The detailed commands are listed below:

- AP provides the WEP (Open-System) cipher wireless access service with an SSID as “wep”.
- For meeting the high bandwidth demands of wireless users, select the 802.11n (2.4GHz) RF mode.

Fig 1-14 WEP（Open-System）cipher wireless access


### 6.2.2 Configuration Steps

1. Login the AP configuration page and enter into the wireless configuration page.




- Choose to enable for RF1.

- Choose IEEE 802.11b/g/n for the wireless mode.
- Use the default configuration for the channel.
- Click “submit” button.

2. Enter into the virtual AP configuration page.


- Choose the virtual AP enabled box (the virtual AP 0 is enabled as default.)
- Configure the VLAN ID according to the actual situation.
- Configure SSID as “WEP”.
- Use the default configuration for “broadcast SSID”.
- Choose “Static WEP” for the security configuration.
- Configure the key index as 1.
- Configure the length of key as 64bits.
- Configure the key type as ASC II.
- Configure the WEP key 1 as 12345.
- Configure the authentication method as “open system”
- Click “submit” button.

### 6.2.3 Test the Configuration Results

- Enable the wireless client and refresh the network list. Find the configured network service in the list of “choose wireless network” (it is PSK in this example). Click “connect” and input the WEP key as 12345 in the dialog box (the input WEP key must be the same as the configured WEP key on the device). After associated with the AP successfully, user can access the wireless network.
- Enter into the client association page and the successful online clients can be viewed.

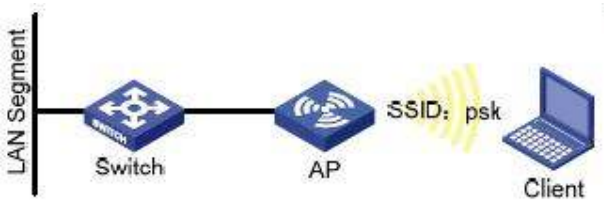
## *6.3 WPA2-PSK Wireless Access*

### 6.3.1 Networking Requirements

In a small office, the device administrator can complete the WPA2-PSK wireless access configuration through the web page. The detailed commands are listed below:

- AP provides the WPA2-PSK wireless access service with SSID as “psk”.
- For meeting the high bandwidth demands of wireless users, select the 802.11n (2.4GHz) RF mode.

Fig 1-18 WPA2-PSK wireless access




## 6.3.2 Configuration Steps

1. Login into the AP configuration page and enter into the wireless configuration page.


- Choose to enable for RF1.
- Choose IEEE 802.11b/g/n for the wireless mode.
- Use the default configuration for the channel.
- Click “submit” button.

2. Enter into the virtual AP configuration page.


- Choose the virtual AP enabled box (the virtual AP 0 is enabled as default.)
- Configure the VLAN ID according to the actual situation.
- Configure SSID as “psk”.
- Use the default configuration for “broadcast SSID”.
- Choose “WPA Personal” for the security configuration.
- Click to choose WPA2 for the WPA version according to the requirement and cancel the WPA.
- Use the default configuration for the cipher suites.
- Configure the Key 1 as 12345678.
- Use the default configuration for the broadcast key refresh rate.
- Click “submit” button.

### 6.3.3 Test the Configuration Results

- Enable the wireless client and refresh the network list. Find the configured network service in the list of “choose wireless network” (it is PSK in this example). Click “connect” and input the pre-shared key as 12345678 in the dialog box (the input pre-shared key must be the same as the configured pre-shared key on the device). After associated with the AP successfully, users can access the wireless network.
- Enter into the client association page and the successful online clients can be viewed.

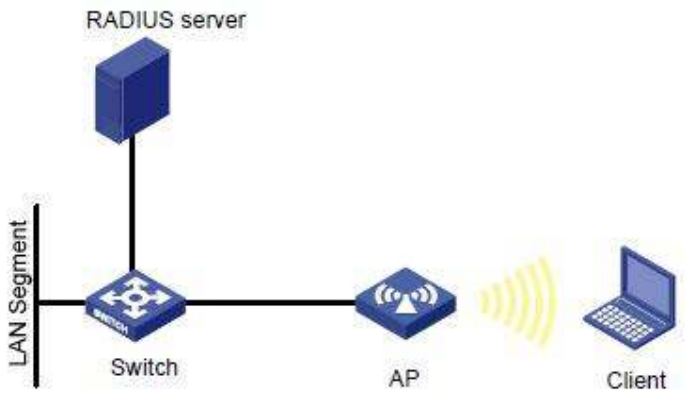
## *6.4 WPA2-Enterprise Wireless Access*

### 6.4.1 Networking Requirements

In an office environment, the staff needs to have constant access to the wireless network; while other foreign devices should be denied access. The administrator can configure the WPA2-Enterprise through the web function. The detailed features are listed below:

- AP provides the WPA2-Enterprise wireless access service with SSID as “WPA-Enterprise”.
- For meeting the high bandwidth demands of wireless users, select the 802.11n (2.4GHz) RF mode.

Fig 1-19 WPA2-Enterprise wireless access

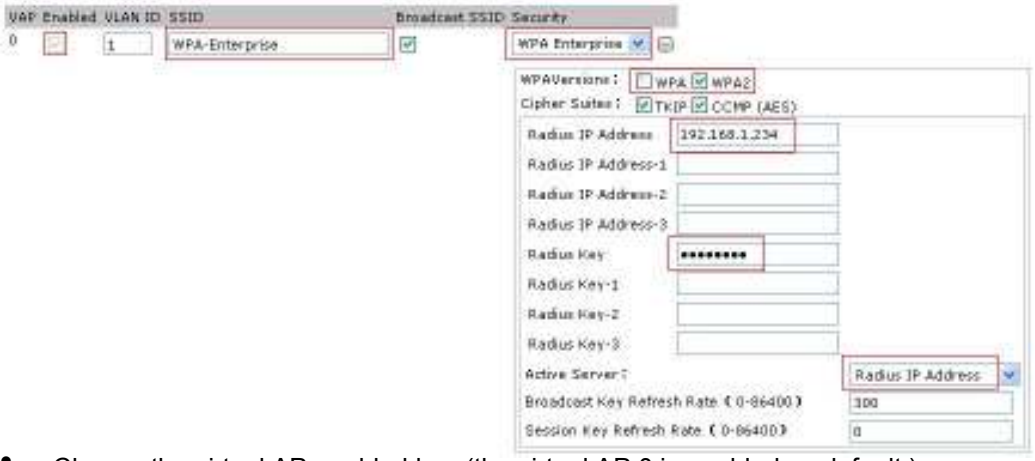



### 6.4.2 Configuration Steps

1. Login into the AP configuration page and enter into the wireless configuration page.


- Choose to enable for RF1.
- Choose IEEE 802.11b/g/n for the wireless mode.
- Use the default configuration for the channel.
- Click “submit” button.

2. Enter into the virtual AP configuration page.




- Choose the virtual AP enabled box (the virtual AP 0 is enabled as default.)
- Configure the VLAN ID according to the actual situation.
- Configure SSID as “WPA-Enterprise”.
- Use the default configuration for “Broadcast SSID”.
- Choose “WPA Enterprise” for the security configuration.
- Click to choose WPA2 for the WPA version according to the requirement and cancel the WPA.
- Use the default configuration for the cipher suites.
- Configure the Radius IP address according to the actual requirements; it is configured as “192.168.1.234” in this example.
- Configure the Radius key according to the actual requirements; it is configured as “test”.
- Choose the server and configure it as Radius IP address.
- Use the default configuration for the broadcast key refresh rate.
- Use the default configuration for the unicast key refresh rate.
- Click “submit” button.

### 6.4.3 Test the Configuration Results

Enable the wireless client and click “modify the advanced configuration”; choose the wireless network configuration in the window. Choose the windows to Configure my wireless network configuration and click the “add” button; input “WPA-Enterprise” in the window for the SSID. Choose WPA2 for the network authentication in the key and choose AES for the data cipher; and then confirm it. Choose the first choice of the network and click “property“; and then click “authenticate”. Choose the “protected EAP (PEAP)” for the EAP types and confirm that ”authenticate as computer when the computer information is useful”, click “property”; and then cancel “authentication server”. Choose the “EAP-MSCHAP v2” for the authentication and click “property”; and then cancel using the login name and password (and the domain if it exists) automatically and click to confirm it. Enable the wireless client again and refresh the network list. Find the configured network service in the list of “choose wireless network” (it is WPA-Enterprise in this example). Click “connect” and input the user name and password existed in Radius server in the dialog box. After associated with the AP successfully, user can access the wireless network.

Enter into the client association page and the successful online clients can be viewed.