Content

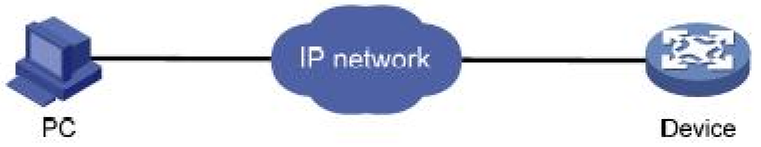
Chapter 1 Introduction

1.1 Overview

For the network administrator to configure and maintain to devices, this device provides the WEB network management function. The administrator can use WEB interface to manage and maintain the network devices visually.

The running environment of Web network management is shown as fig 1-1.

Fig 1-1 Web The running environment of Web network management



1.2 Login Web Network Management

The default Web login information has been configured after made. User can use this default information directly to login the web interface of the device.

The default Web login information includes:

User name: admin

Password: admin

IP address of the device: 192.168.1.10

The steps of web login:

(1) Connect the device to PC

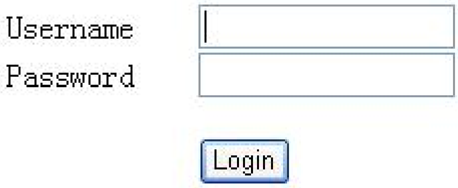
Use the cable to connect PC to the Ethernet interface of the device.

(2) Configure the IP address for PC and ensure that it can communicate with the device. For example: modify the IP address to 192.168.1.0/24.

(3) Launch the browser and input the login information

Launch the browser on PC, and input “http://192.168.1.10” in the address bar and then enter it. Enter into the web login page as shown as fig 1-2. Input the user name of admin and password of admin, click “login” to login.

Fig 1-2 Web network management login page



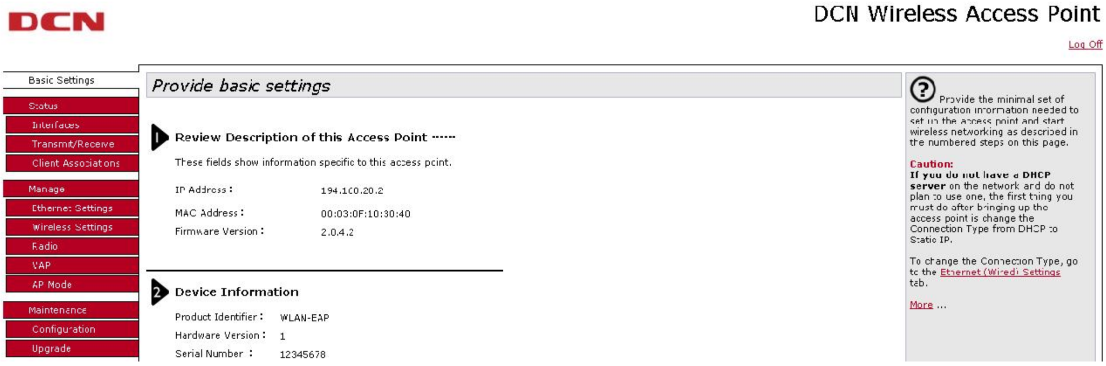
1.3 Quit Web Network Management

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

1.4 Introduction to Page Layout of Web Network Management

Web network management page includes: navigation bar, configuration area and help area shown as fig 1-4.

Fig 1-4 initial page of Web network management



DCN Wireless Access Point

Provide basic settings

1 Review Description of this Access Point ------

These fields show information specific to this access point.

IP Address： 194.100.20.2

MAC Address： 00:03:0F:10:30:40

Firmware Version： 2.0.4.2

2 Device Information

Product Identifier： WLAN-EAP

Hardware Version： 1

Serial Number ： 12345678

Provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

Caution:
If you do not have a DHCP server on the network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

Navigation bar: organize the Web network management menu by using the navigation tree. User can choose the function menu in the navigation bar and the result will be shown in the configuration area.

Configuration area: User can configure and check.

Help area: It provides the basic help information. The “more” button can check more help information. And it provides the “log off” button to quit.

1.5 Introduction to Web Network Management Function

The Web network management function explanation is as table 1-1:

Table 1-1 Web network management function explanation

Menu/label		Function explanation
Basic settings		Show the AP address (IP address and MAC address), version (firmware version) and device information. The administrator password, serial ports configuration and system settings can be configured.
Status	Network interface	Show the real-time wired and wireless configuration of AP.
	Transmit/Receive	Show the virtual AP enabling situation and the statistic of transmitting and receiving packets of AP.
	Client association	Show the information of transmitting and receiving packets of the client which has been associated with AP.
Manage	Ethernet settings	Configure the related wired configuration of AP including host name, management vlan, untagged vlan, DHCP, static ip and dns server.
	Wireless settings	Configure the related wireless configuration of AP including country code, radio interface, physical mode and channel.
	RF parameters	Configure the detailed RF parameters including 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, multicast rate and supported rate.
	Virtual AP	Configure the authentication mode of virtual AP and the related configuration.
	Modes of AP	Configure the modes and IP address of AP.
System maintenance	Configuration management	Configure to restart AP and restore it to be the factory configuration. Import and export the files.
	Firmware upgrading	Configure the firmware upgrading of AP.

1.6 Introduction to Common Controls of Web Page

1. <Update> button

Click < Update > button to submit the input information.

2. <Refresh> button

Click <Refresh> button to refresh the information of 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 and the versions above, Mozilla Firefox3.0 and the versions above, Google chrome and Safari.

(3) Web network management does not support the “previous”, “next” and “refresh” buttons from the browser. Using these buttons may cause the unusual page showing.

(4) Because the firewall of the Windows operating system will limit the number of connected TCP, there will be the situation that the page cannot be opened when using web network management occasionally. For avoiding this situation, we suggest to close the firewall of the Windows.

(5) After the software version of the device has changed, we suggest to clear the cache data of the browser first when login the device through web network management. Otherwise, the content of web network management may not be shown normally.

Chapter 2 Basic Configuration

Show the basic configuration of the device and it includes the following content:

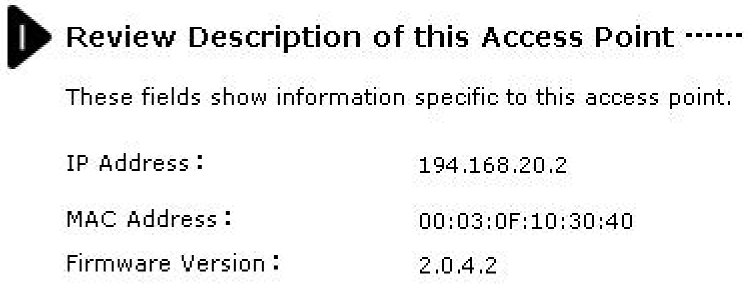
Review description of this access point

Device information;

Administrator password;

Serial settings;

System settings.



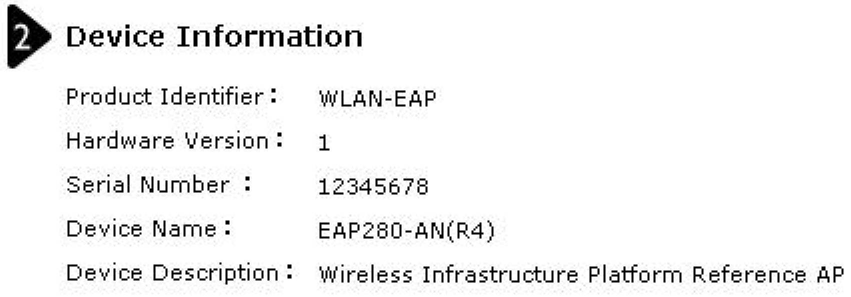
1 Review Description of this Access Point ······

These fields show information specific to this access point.

IP Address : 194.168.20.2

MAC Address : 00:03:0F:10:30:40

Firmware Version : 2.0.4.2



2 Device Information

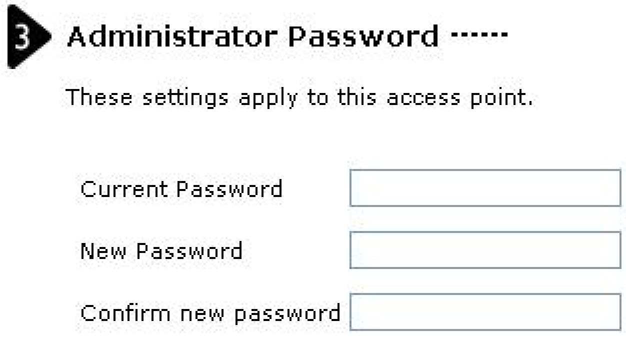
Product Identifier : WLAN-EAP

Hardware Version : 1

Serial Number : 12345678

Device Name : EAP280-AN(R4)

Device Description : Wireless Infrastructure Platform Reference AP



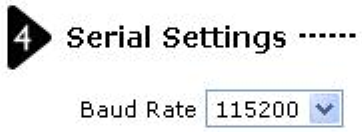
3 Administrator Password ······

These settings apply to this access point.

Current Password

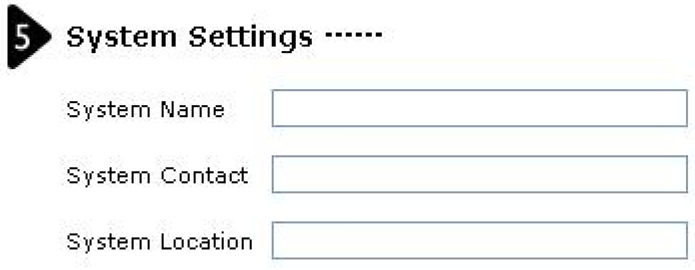
New Password

Confirm new password



4 Serial Settings ······

Baud Rate 115200



5 System Settings ······

System Name

System Contact

System Location

2.1 Detailed Explanation of settings

2.1.1 Description of this Access Point

IP address	Show the IP address of the current device.
MAC address	Show the MAC address of the current device.
Firmware version	Show the firmware version of the current device.

2.1.2 Device Information

Product identifier	Show the product ID of the current device.
Hardware version	Show the hardware version of the current device.
Serial number	Show the serial number of the current device.
Device name	Show the device name of the current device.
Device description	Show the device description of the current device.

2.1.3 Administrator Password

Current password	Input the current administrator password.
New password	Input the new password.
Confirm new password	Input the new password again and it must be same as the above new password.

2.1.4 Serial Settings

Baud Rate	Configure the baud rate of the serial ports.

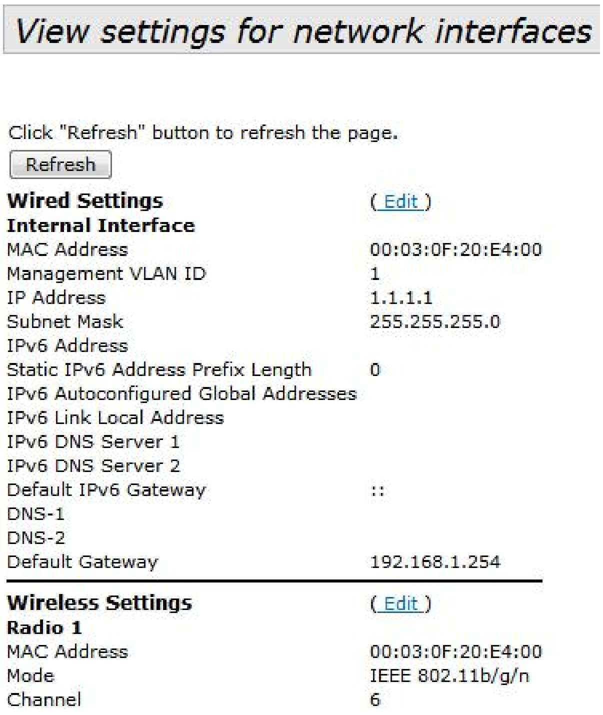
2.1.5 System Settings

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

Chapter 3 Current Status

The current status includes network information, statistic of transmitting and receiving packets and the client association.

3.1 Network Information



View settings for network interfaces

Click "Refresh" button to refresh the page.

Wired Settings	(Edit)
Internal Interface	
MAC Address	00:03:0F:20:E4:00
Management VLAN ID	1
IP Address	1.1.1.1
Subnet Mask	255.255.255.0
IPv6 Address	
Static IPv6 Address Prefix Length	0
IPv6 Autoconfigured Global Addresses	
IPv6 Link Local Address	
IPv6 DNS Server 1	
IPv6 DNS Server 2	
Default IPv6 Gateway	::
DNS-1	
DNS-2	
Default Gateway	192.168.1.254
Wireless Settings	(Edit)
Radio 1	
MAC Address	00:03:0F:20:E4:00
Mode	IEEE 802.11b/g/n
Channel	6

3.1.1 Wired Settings

MAC address	Show the MAC address of the current device.
Management VLAN ID	Show the vlan ID of the current device.
IP address	Show the IP address of the current device.
Subnet mask	Show the subnet mask of the current device.
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	Show the static IPv6 address of AP.
Static IPv6 Address Prefix Length	Show the prefix length of static IPv6 address.
IPv6 Autoconfigured Global Addresses	Show the IPv6 address list that the AP gets dynamically.
IPv6 Link Local Address	Show the IPv6 link local address of AP.
Default IPv6 Gateway	Show the default IPv6 gateway of AP.
IPv6 DNS Server 1	Show the IPv6 DNS server 1 of AP.
IPv6 DNS Server 2	Show the IPv6 DNS server 2 of AP.
DNS-1	Show the ip address of dns-1 server of the current device.
DNS-2	Show the ip address of dns-2 server of the current device.
Default gateway	Show the default gateway of the current device.

3.1.2 Wireless Settings

MAC address	Show the MAC address information of RF1 or 2.
Mode	Show the wireless mode information of RF1 or 2.
Channel	Show the channel information of RF1 or 2.

3.1.3 Explanation

Click the “edit” link behind the wired and wireless configuration to link to the wired and wireless configuration page directly.

3.2 Statistic 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 Ethernet interface or VAP

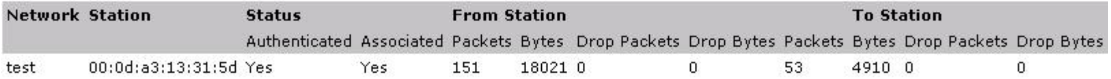
	interface
Status	Mark the interface is up or down.
MAC address	MAC address of the specific interface. Every interface of AP has the unparalleled MAC address. Each interface of each RF of the two RF has a different MAC address.
Vlan ID	VLAN ID You can use VLAN to create multiple internal and customer networks on the same AP. VLAN ID is configured in VAP label.
Network name (ssid)	Wireless network name. it is also named as SSID which is used to mark the WLAN. SSID is configured in VAP label.

3.2.2 Transmit/Receive Packets

Interface	The name of Ethernet interface or VAP interface
Packets number	Show the number of the packets that the AP sent (in the transmitting packet table) or received (in the receiving packet table).
Bytes number of packets	Show the number of the bytes that the AP sent (in the transmitting packet table) or received (in the receiving packet table).
Dropped packets number	Show the number of the sent (in the transmitting packet table) or received (in the receiving packet table) packets that the AP dropped.
Bytes number of dropped packets	Show the number of the sent (in the transmitting packet table) or received (in the receiving packet table) bytes that the AP dropped.
Error statistics	Show the total error number of AP transmitting and receiving data.

3.3 Client Association

Client association showing:



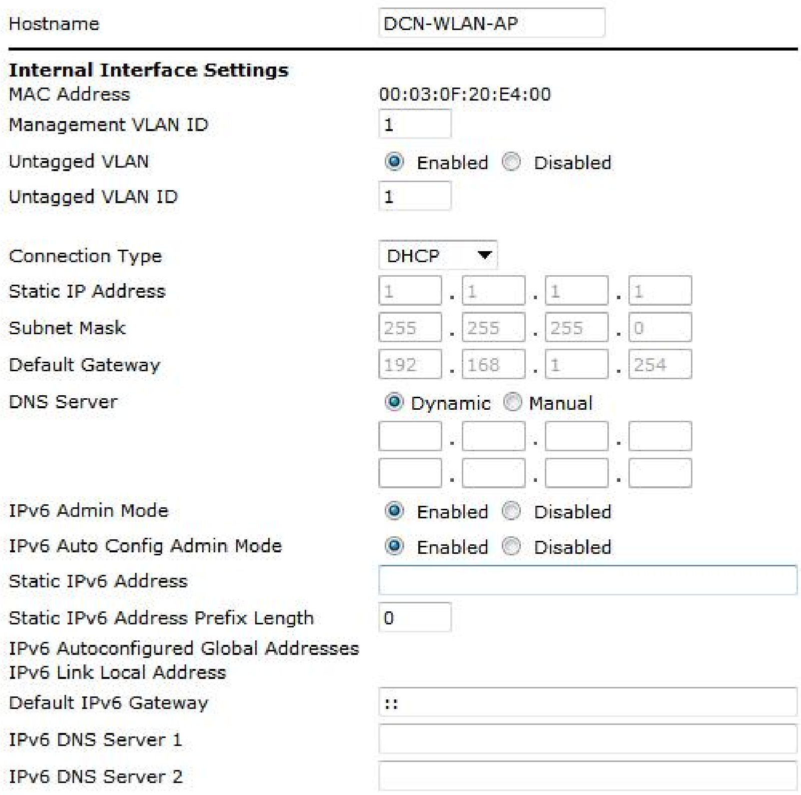
Network	Station	Status		From Station				To Station			
		Authenticated	Associated	Packets	Bytes	Drop Packets	Drop Bytes	Packets	Bytes	Drop Packets	Drop Bytes
test	00:0d:a3:13:31:5d	Yes	Yes	151	18021	0	0	53	4910	0	0

Network		The SSID of the client associated network.
Station		The MAC address of the associated client.
Status	Authenticated	The status of authenticated means the IEEE 802.11 authentication status.
	Associated	The status of associated means the IEEE 802.11 association status.
From station	Packets Bytes Dropped packets Dropped bytes	It means that the number of packets and bytes received from the client and the number of dropped packets and bytes after received.
To station	Packets Bytes Dropped packets Dropped bytes	It means that the number of packets and bytes client received and the number of dropped packets and bytes in transmission.

Chapter 4 Mange

The “manage” includes Ethernet settings, wireless settings, RF parameters, virtual AP and AP modes.

4.1 Ethernet Settings

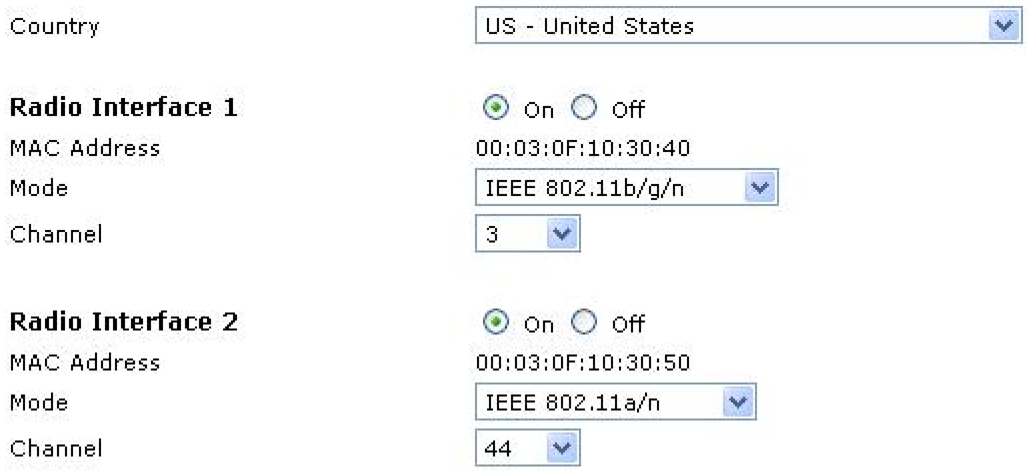


Hostname	DCN-WLAN-AP
Internal Interface Settings	
MAC Address	00:03:0F:20:E4:00
Management VLAN ID	1
Untagged VLAN	● Enabled ○ Disabled
Untagged VLAN ID	1
Connection Type	DHCP
Static IP Address	1 . 1 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 254
DNS Server	● Dynamic ○ Manual
	. . .
	. . .
IPv6 Admin Mode	● Enabled ○ Disabled
IPv6 Auto Config Admin Mode	● Enabled ○ Disabled
Static IPv6 Address	
Static IPv6 Address Prefix Length	0
IPv6 Autoconfigured Global Addresses	
IPv6 Link Local Address	
Default IPv6 Gateway	::
IPv6 DNS Server 1	
IPv6 DNS Server 2	

Host name	The host name of AP.
MAC address	The MAC address of the Ethernet interface of AP.
Management VLAN ID	The management VLAN is used to access the VLAN which is associated with the IP address of AP.
Untagged VLAN	If the untagged VLAN was disabled, all the packets will be marked with the same VLAN number.
Untagged VLAN ID	The packet transmitted in this VLAN has no tagged VLAN number.

Connection type	Configure the IP address obtaining of AP.
Static IP address	Configure the static IP address. If the IP obtaining is DHCP, this property cannot be used.
Subnet mask	Configure the subnet mask. If the IP obtaining is DHCP, this property cannot be used.
Default gateway	Configure the default gateway. If the IP obtaining is DHCP, this property cannot be used.
DNS nameservers	Configure the DNS mode. Under the manual appointed mode, the DNS address can be configured to analyze the domain name.
IPv6 Admin Mode	IPv6 management on-off. If it is enabled, AP and AC can be managed through the IPv6 address; if the IPv4 and IPv6 are both enabled, IPv4 is preferential.
IPv6 Auto Config Admin Mode	IPv6 automatic address. If it is enabled, AP supports to get the address automatically.
Static IPv6 Address	Show the static IPv6 address of AP.
Static IPv6 Address Prefix Length	Show the prefix length of static IPv6 address.
IPv6 Autoconfigured Global Addresses	Show the IPv6 address that the AP gets dynamically. If there are multiple addresses, they can be shown in the list.
IPv6 Link Local Address	Show the IPv6 link local address of AP.
Default IPv6 Gateway	Show the default IPv6 gateway of AP.
IPv6 DNS Server 1	Show the IPv6 DNS server 1 of AP.
IPv6 DNS Server 2	Show the IPv6 DNS server 2 of AP.

4.2 Wireless Settings



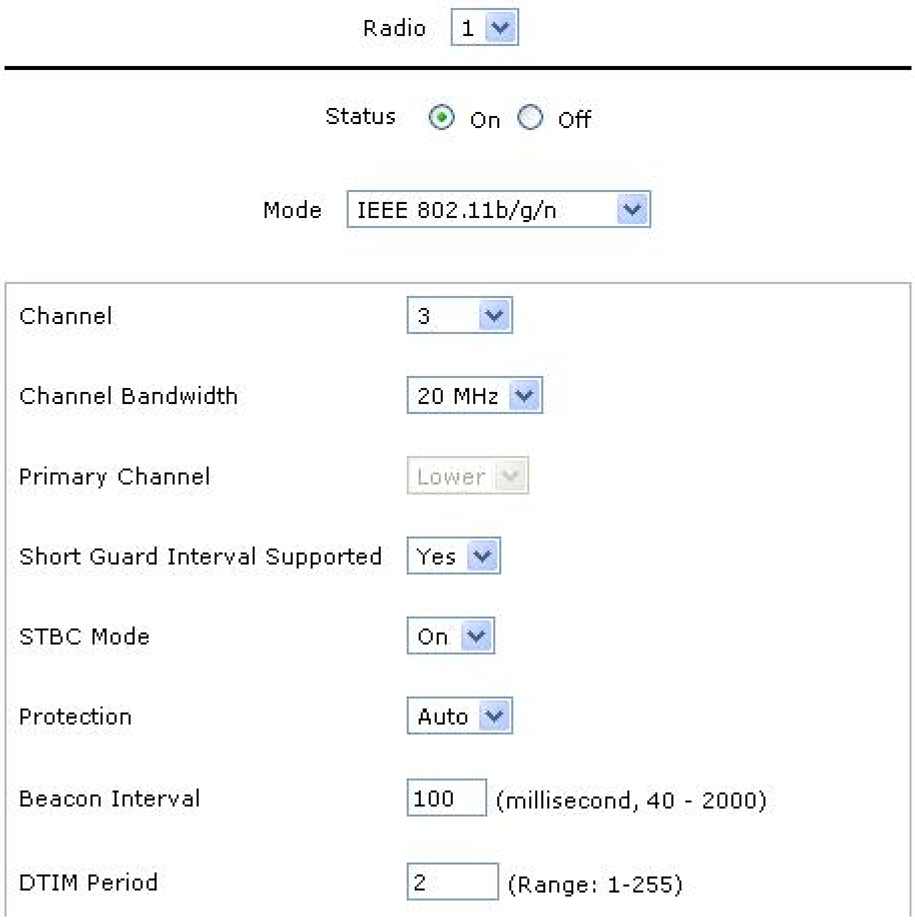
Country: US - United States

Radio Interface 1 ● On ○ Off
MAC Address: 00:03:0F:10:30:40
Mode: IEEE 802.11b/g/n
Channel: 3

Radio Interface 2 ● On ○ Off
MAC Address: 00:03:0F:10:30:50
Mode: IEEE 802.11a/n
Channel: 44

Country	Choose the country of AP.
Radio interface 1/Radio interface 2	Appoint the RF device is enabled or disabled.
MAC address	The MAC address of the RF interface.
Mode	The Physical Layer standard the radio uses.
Channel	Choose the channel.

4.3 RF Parameters

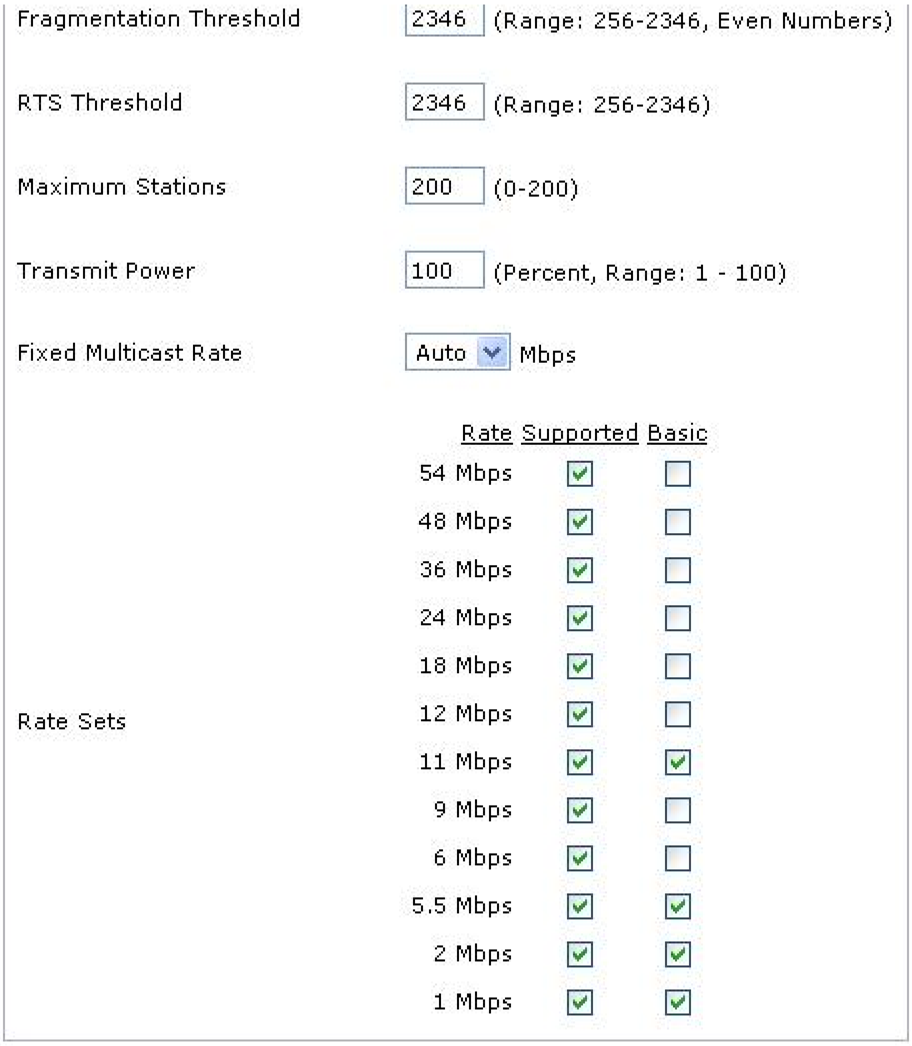


Radio: 1

Status: ● On ○ Off

Mode: IEEE 802.11b/g/n

Channel	3
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	2 (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

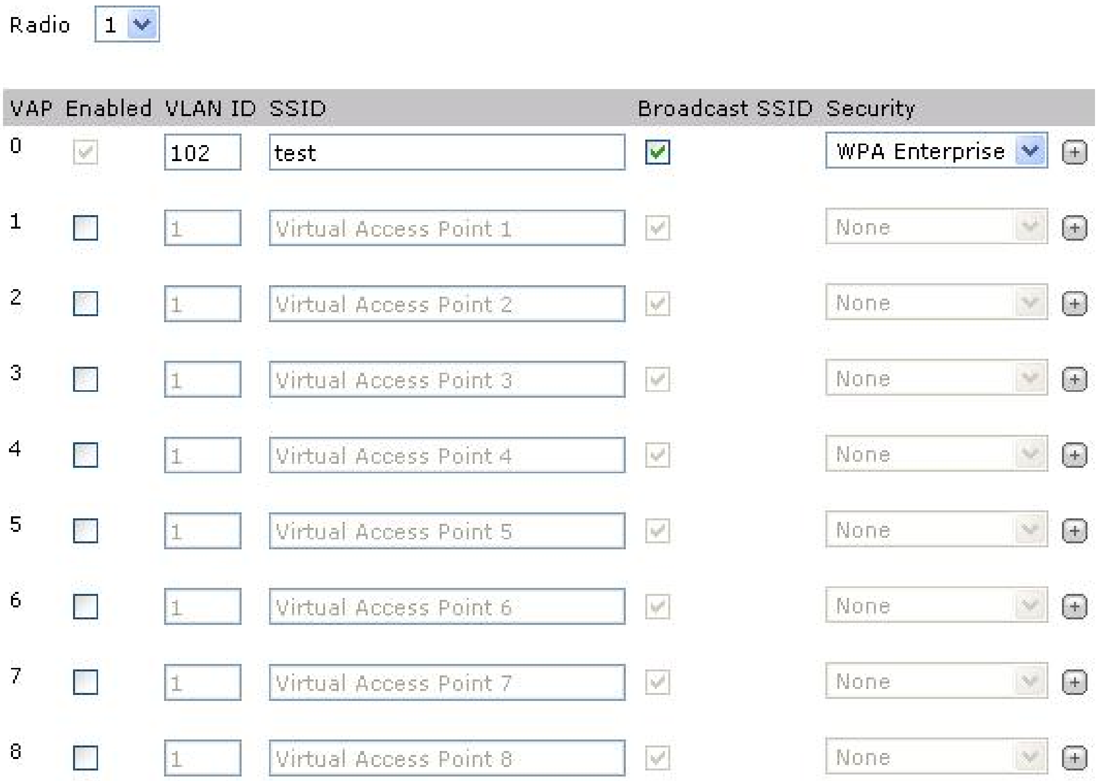
Rate Sets

Rate	Supported	Basic
54 Mbps	☑	□
48 Mbps	☑	□
36 Mbps	☑	□
24 Mbps	☑	□
18 Mbps	☑	□
12 Mbps	☑	□
11 Mbps	☑	☑
9 Mbps	☑	□
6 Mbps	☑	□
5.5 Mbps	☑	☑
2 Mbps	☑	☑
1 Mbps	☑	☑

Radio	Choose the configured RF.
Status	Enable/disable the RF.
Mode	The PHY standard used by RF.
Channel	Choose the channel.
Channel bandwidth	The channel bandwidth of 802.11n mode.
Primary channel	The mode of the primary channel (only the 802.11n mode is supported)
Short guard interval supported	Configure the short guard. (only the 802.11n mode is supported)
STBC mode	Configure the STBC mode. (only the 802.11n mode is supported)
Protection	Configure the protection function.
Beacon interval	Configure the Beacon interval.
DTIM interval	Configure the DTIM interval.
Fragment threshold	Configure the fragment threshold.

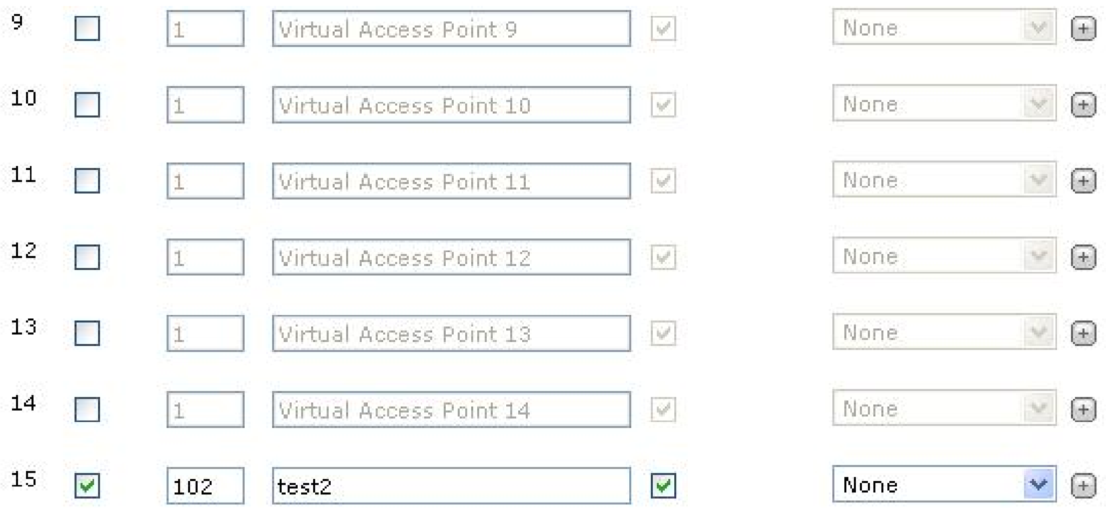
RTS threshold	Configure the RTS threshold.
Maximum stations	Configure the maximum number of associated stations.
Transmit power	Configure the percentage of the RF transmission power.
Fixed multicast rate	Configure the supported multicast rate.
Rate sets	Configure the transmission rate set and the basic broadcast rate set that supported by RF.

4.4 Virtual AP



Radio 1

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	102	test	☑	WPA Enterprise
1	□	1	Virtual Access Point 1	☑	None
2	□	1	Virtual Access Point 2	☑	None
3	□	1	Virtual Access Point 3	☑	None
4	□	1	Virtual Access Point 4	☑	None
5	□	1	Virtual Access Point 5	☑	None
6	□	1	Virtual Access Point 6	☑	None
7	□	1	Virtual Access Point 7	☑	None
8	□	1	Virtual Access Point 8	☑	None

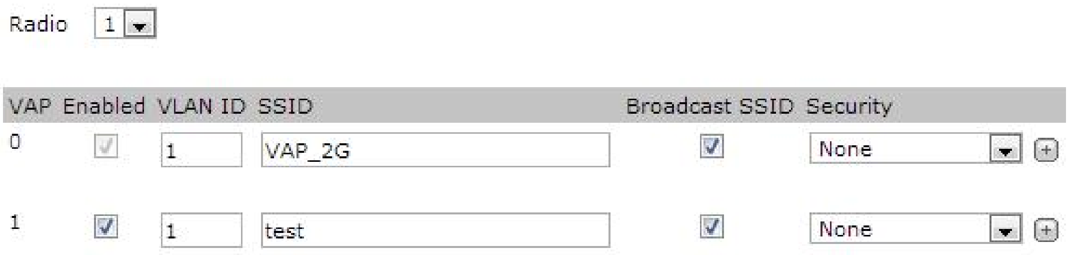


9	□	1	Virtual Access Point 9	☑	None
10	□	1	Virtual Access Point 10	☑	None
11	□	1	Virtual Access Point 11	☑	None
12	□	1	Virtual Access Point 12	☑	None
13	□	1	Virtual Access Point 13	☑	None
14	□	1	Virtual Access Point 14	☑	None
15	☑	102	test2	☑	None

Radio	Choose the configured RF.
VAP	Show the ID number of the virtual AP.
Enabled	Configure the status of the virtual AP.
VLAN ID	Configure the VLAN that the client associated with the virtual AP belongs to.
SSID	Configure the name of wireless network.
Broadcast SSID	Configure if broadcast the SSID.
Security	Configure the security mode.

4.4.1 None Security Configuration

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

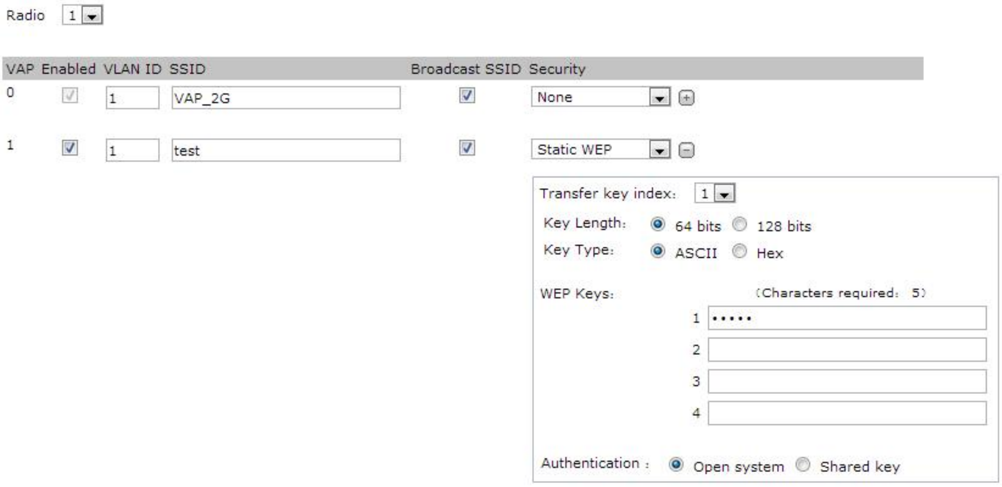


Radio 1

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	VAP_2G	☑	None
1	☑	1	test	☑	None

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 direct key should be input in client to pass the authentication or the decryption packet.



Radio 1

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	VAP_2G	☑	None ⊕
1	☑	1	test	☑	Static WEP ⊖

Transfer key index: 1

Key Length: ● 64 bits ○ 128 bits

Key Type: ● ASCII ○ Hex

WEP Keys: （Characters required: 5）

1 •••••

2

3

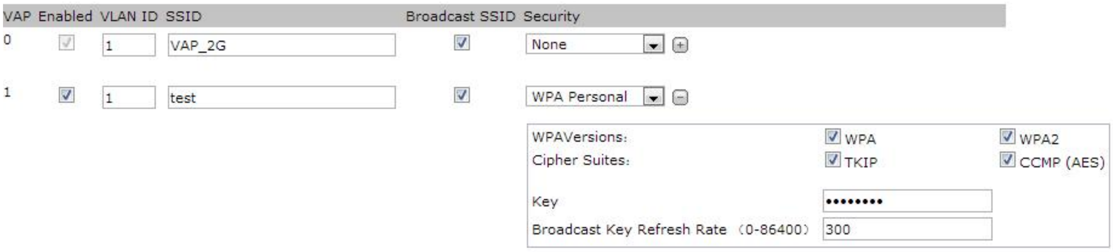
4

Authentication : ● Open system ○ Shared key

Transfer key index	Configure the key index.
Key length	Configure the length of key.
Key type	Configure the type of key.
Wep keys	Configure the key of 1-4.
Authentication	Configure the authentication mode.

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 direct key should be input in client to pass the authentication.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	VAP_2G	☑	None ⊕
1	☑	1	test	☑	WPA Personal ⊖

WPAVersions: ☑ WPA ☑ WPA2

Cipher Suites: ☑ TKIP ☑ CCMP (AES)

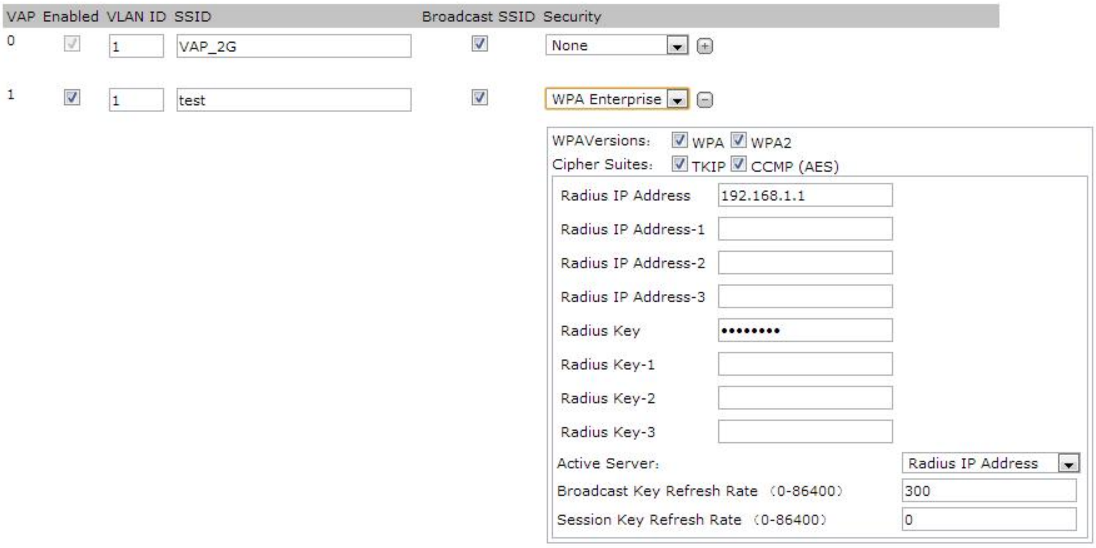
Key ••••••••

Broadcast Key Refresh Rate （0-86400） 300

WPA versions	Configure the WPA version.
Cipher suites	Configure the cipher suites.
Key	Configure the key.
Broadcast key refresh key	Configure the interval of broadcast key updating.

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 existed in radius server should be input in client to pass the authentication.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	VAP_2G	☑	None
1	☑	1	test	☑	WPA Enterprise

WPAVersions: ☑ WPA ☑ WPA2

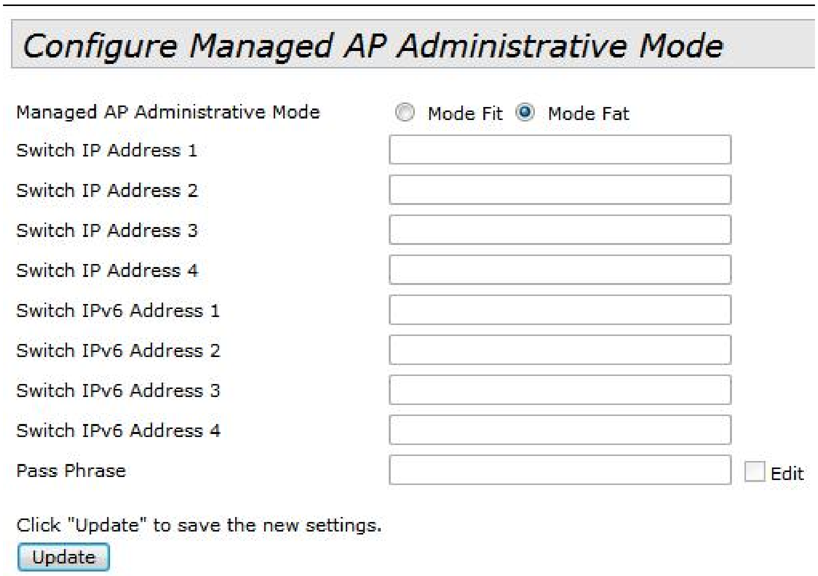
Cipher Suites: ☑ TKIP ☑ CCMP (AES)

Radius IP Address	192.168.1.1
Radius IP Address-1	
Radius IP Address-2	
Radius IP Address-3	
Radius Key	••••••••
Radius Key-1	
Radius Key-2	
Radius Key-3	
Active Server:	Radius IP Address
Broadcast Key Refresh Rate （0-86400）	300
Session Key Refresh Rate （0-86400）	0

WPA version	Configure the WPA version.
Cipher suites	Configure the cipher suites.
Radius IP address	Configure the IP address of radius server.
Radius IP address of 1-3	Configure the IP address of the backup radius server.
Radius key	Configure the radius server key.
Radius key of 1-3	Configure the key of the backup radius server.
Active server	Choose the radius server.
Broadcast key refresh rate (0-86400)	Configure the interval of broadcast key updating.
Session key refresh rate (0-86400)	Configure the interval of unicast key updating.

4.5 AP Modes

The AP modes can be switched on this page. Configure the address of AC and the password of AP authentication under the thin AP mode.



Configure Managed AP Administrative Mode

Managed AP Administrative Mode	○ Mode Fit ● Mode Fat
Switch IP Address 1	
Switch IP Address 2	
Switch IP Address 3	
Switch IP Address 4	
Switch IPv6 Address 1	
Switch IPv6 Address 2	
Switch IPv6 Address 3	
Switch IPv6 Address 4	
Pass Phrase	□ Edit

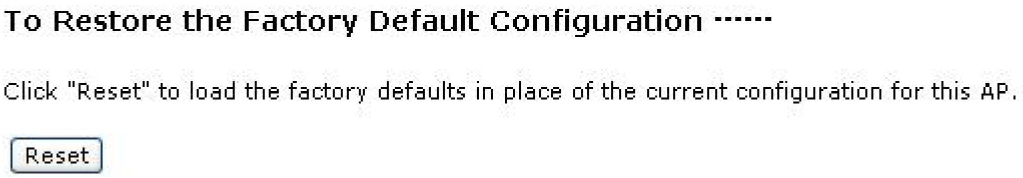
Click "Update" to save the new settings.

Management AP administrative mode	Configure the AP modes.
Switch IP address of 1-4	Configure the IP address of AC under the fit AP mode.
Switch IPv6 address of 1-4	Configure the IPv6 address of AC under the fit AP mode.
Pass phrase	Configure the password of the associated authentication between AP and AC under the fit AP mode.

Chapter 5 System Maintenance

The system maintenance includes configuration management and firmware upgrading.

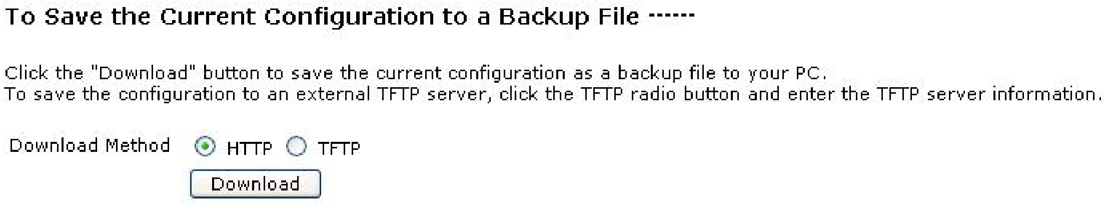
5.1 Configuration Management



To Restore the Factory Default Configuration ······

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

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

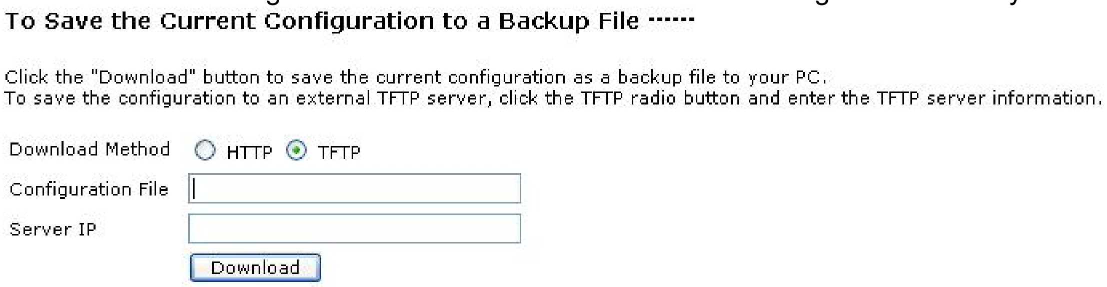


To Save the Current Configuration to a Backup File ······

Click the "Download" button to save the current configuration as a backup file to your PC.
To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method ● HTTP ○ TFTP

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



To Save the Current Configuration to a Backup File ······

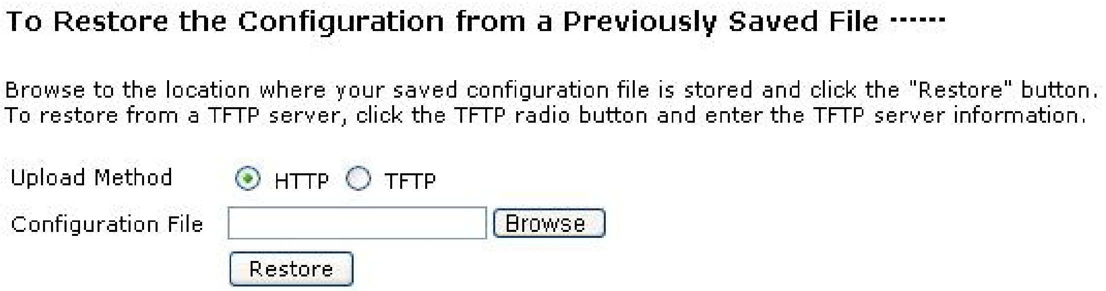
Click the "Download" button to save the current configuration as a backup file to your PC.
To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method ○ HTTP ● TFTP

Configuration File

Server IP

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



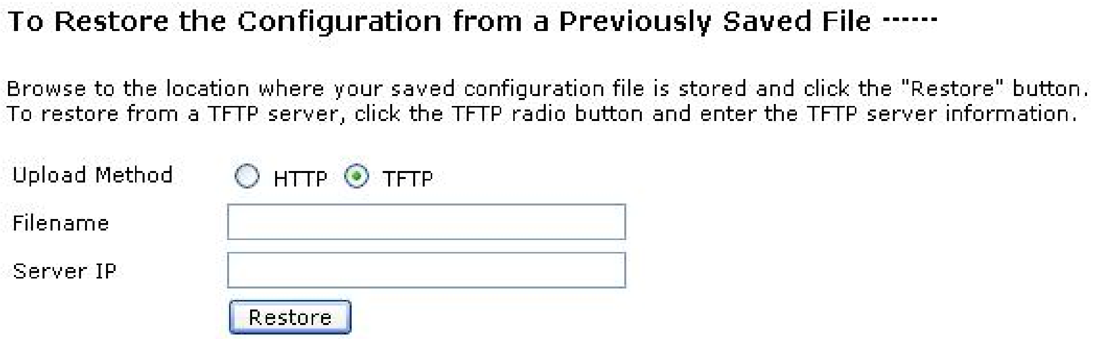
To Restore the Configuration from a Previously Saved File ······

Browse to the location where your saved configuration file is stored and click the "Restore" button.
To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method ● HTTP ○ TFTP

Configuration File

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



To Restore the Configuration from a Previously Saved File ······

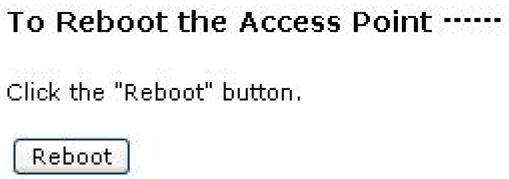
Browse to the location where your saved configuration file is stored and click the "Restore" button.
To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method ○ HTTP ● TFTP

Filename

Server IP

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

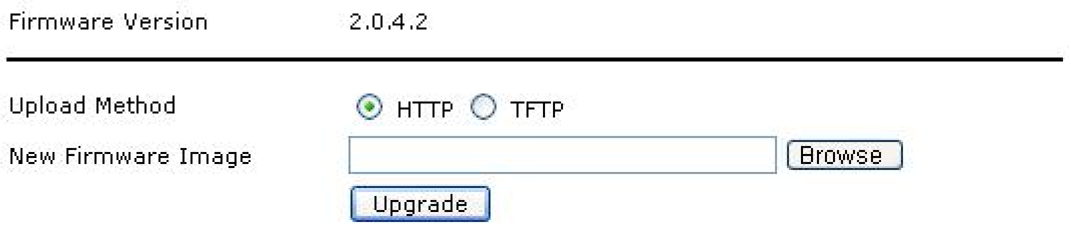


To Reboot the Access Point ······

Click the "Reboot" button.

Click “reboot” button and confirm it. Then the AP will be restarted.

5.2 Firmware Upgrading



Firmware Version 2.0.4.2

Upload Method ● HTTP ○ TFTP

New Firmware Image

Platform	

Version of firmware	Show the version of firmware of the current AP.

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

1. Choose the HTTP as the upgrading method.

2. If you knew the path of the new firmware file, input this path in the text box. Otherwise, click the “browse” button to locate the upgrading file of firmware.

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

3. Click the “firmware upgrading” button to apply the new firmware file.

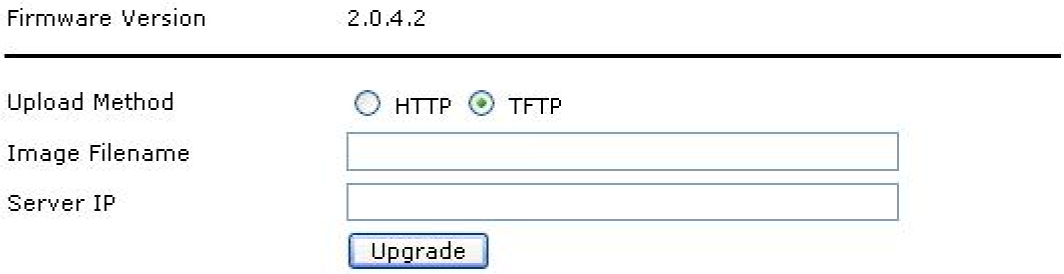
After clicked the “firmware upgrading” button, there will be a window which describes the upgrading process.

4. 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 be continued for a few minutes. During this period, AP cannot be accessed. Please do not turn off the AP power in upgrading. After upgrading, AP will restart. After restarted, AP will use the configuration before upgrading still.

5. If wants to known whether the firmware upgrading was successful, please check the firmware version in the firmware management page (or the basic configuration label). If the upgrading was successful, the version after upgrading will be shown.



Firmware Version 2.0.4.2

Upload Method ○ HTTP ● TFTP

Image Filename

Server IP

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

1. Choose the 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 the tar file. Please do not try to use the bin file or other kinds of files to upgrade; these files would not run.

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 be continued for a few minutes. During this period, AP cannot be accessed. Please do not turn off the AP power in upgrading. After upgrading, AP will restart. After restarted, AP will use the configuration before upgrading still.

6. If wants to known whether the firmware upgrading was successful, please check the firmware version in the firmware management page (or the basic configuration label). If the upgrading was successful, the version after upgrading will be shown.

Chapter 6 Configuration Examples

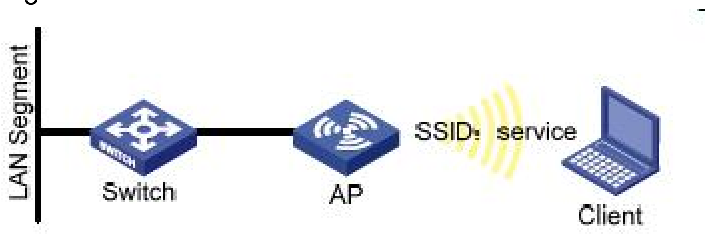
6.1 Laws Wireless Access

6.1.1 Networking Requirements

A department needs to achieve the mobile office through deploying AP for that the staffs can visit the internal network resources anytime and anywhere. The device administrator can configure the laws wireless access and the detailed demand is as below:

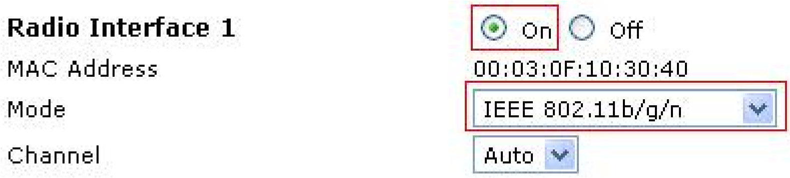
- AP provides the wireless access service with SSID as the laws method of “service”.
- For meeting the high bandwidth demands and the compatible 802.11g wireless network, adopt the 802.11n (2.4GHz) RF mode.

Fig 1-11 laws wireless access



6.1.2 Configuration Steps

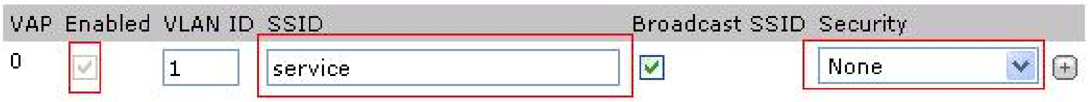
1. Login the AP configuration page and enter into the wireless configuration page.



Radio Interface 1	● On ○ Off
MAC Address	00:03:0F:10:30:40
Mode	IEEE 802.11b/g/n
Channel	Auto

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

2. Enter into the virtual AP configuration page.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	service	☑	None

- 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.

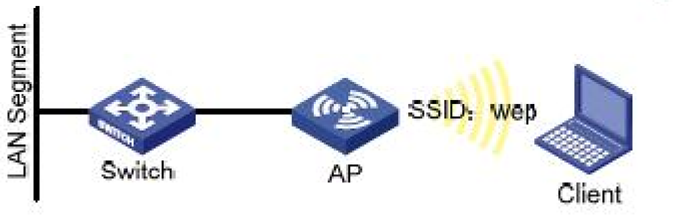
6.2 Cipher Wireless Access of Static-WEP (Open-System)

6.2.1 Networking Requipments

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

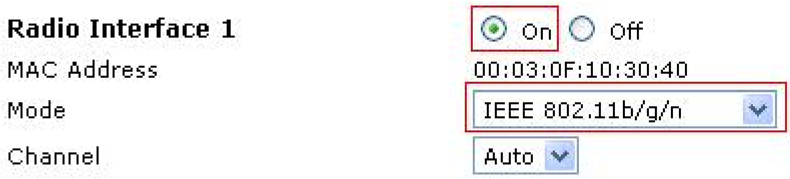
- AP provides the WEP (Open-System) cipher wireless access service with SSID as “wep”.
- For meeting the high bandwidth requirements and the compatible 802.11g wireless network, adopt the 802.11n (2.4GHz) RF mode.

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.

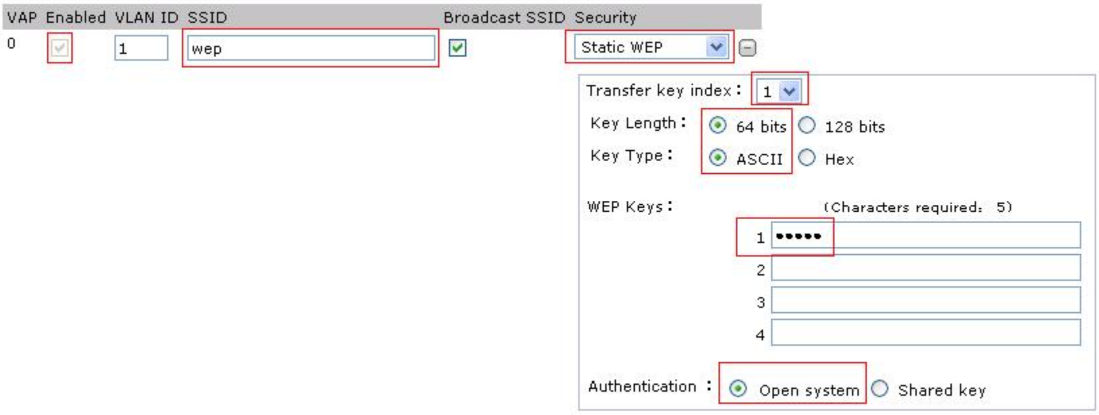


Radio Interface 1	● On ○ Off
MAC Address	00:03:0F:10:30:40
Mode	IEEE 802.11b/g/n
Channel	Auto

- 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.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	wep	☑	Static WEP

Transfer key index: 1

Key Length: ● 64 bits ○ 128 bits

Key Type: ● ASCII ○ Hex

WEP Keys: (Characters required: 5)

1 •••••
2
3
4

Authentication: ● Open system ○ Shared key

- 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.

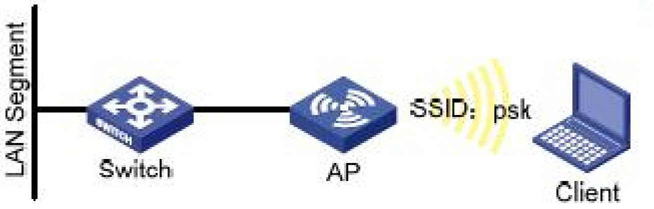
6.3 WPA2-PSK Wireless Access

6.3.1 Networking Requipments

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

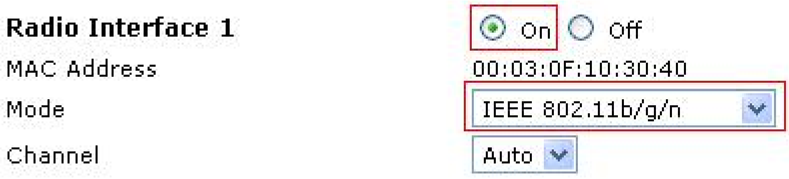
- AP provides the WPA2-PSK wireless access service with SSID as "psk".
- For meeting the high bandwidth requirements and the compatible 802.11g wireless network, adopt the 802.11n (2.4GHz) RF mode.

Fig 1-18 WPA2-PSK wireless access



6.3.2 Configuration Steps

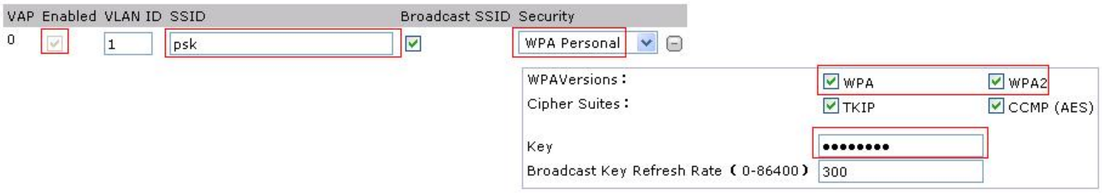
1. Login the AP configuration page and enter into the wireless configuration page.



Radio Interface 1	● On ○ Off
MAC Address	00:03:0F:10:30:40
Mode	IEEE 802.11b/g/n
Channel	Auto

- 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.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	psk	☑	WPA Personal

WPAVersions：	☑ WPA	☑ WPA2
Cipher Suites：	☑ TKIP	☑ CCMP (AES)
Key	••••••••	
Broadcast Key Refresh Rate（0-86400）	300	

- 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, user can access the wireless network.
- Enter into the client association page and the successful online clients can be viewed.

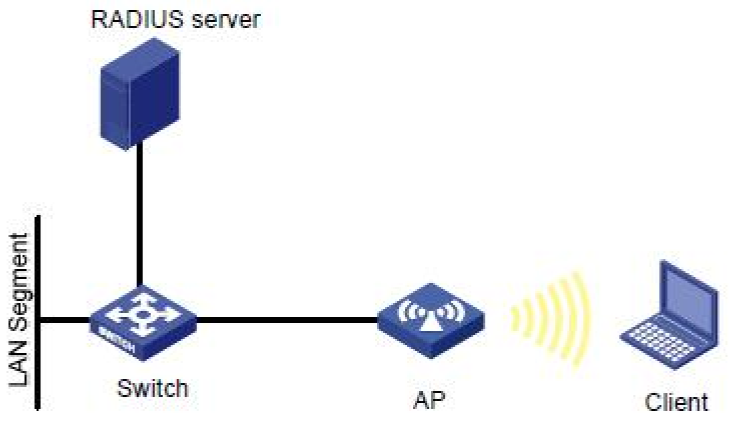
6.4 WPA2-Enterprise Wireless Access

6.4.1 Networking Requipments

In an office building of a company, the staffs need to access the office environment through the wireless network; the other mobile devices that do not belong to the staffs cannot be accessed. The administrator can configure the WPA2-Enterprise through the web page. The detailed demand is as below:

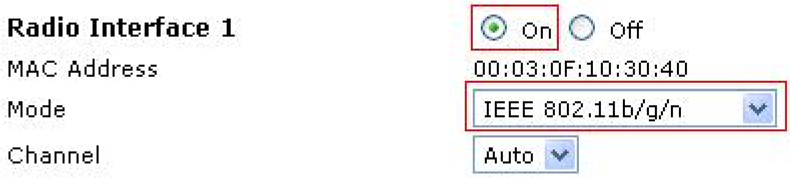
- AP provides the WPA2-Enterprise wireless access service with SSID as “WPA-Enterprise”.
- For meeting the high bandwidth requirements and the compatible 802.11g wireless network, adopt the 802.11n (2.4GHz) RF mode.

Fig 1-19 WPA2-Enterprise wireless access



6.4.2 Configuration Steps

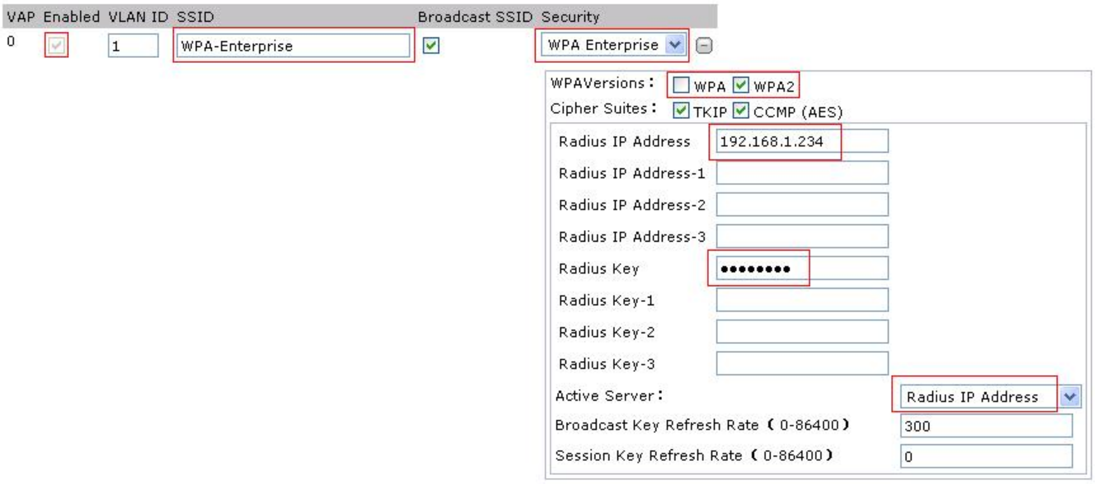
1. Login the AP configuration page and enter into the wireless configuration page.



Radio Interface 1: ● On ○ Off
MAC Address: 00:03:0F:10:30:40
Mode: IEEE 802.11b/g/n
Channel: Auto

- 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.



VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security
0	☑	1	WPA-Enterprise	☑	WPA Enterprise

WPAVersions : □ WPA ☑ WPA2
Cipher Suites : ☑ TKIP ☑ CCMP (AES)
Radius IP Address: 192.168.1.234
Radius IP Address-1:
Radius IP Address-2:
Radius IP Address-3:
Radius Key: ••••••••
Radius Key-1:
Radius Key-2:
Radius Key-3:
Active Server : Radius IP Address
Broadcast Key Refresh Rate (0-86400): 300
Session Key Refresh Rate (0-86400): 0

- 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 the “modify the advanced configuration”; choose the wireless network configuration in the window. Choose to use the windows to configure my wireless network configuration and click “add” button; input “WPA-Enterprise” in the window of SSID. Choose WPA2 for the network authentication in the key and choose AES for the data cipher; and then click to confirm it. Choose the added first choice of network and click “property“; and then click “authenticate”. Choose the “protected EAP (PEAP)” for the EAP types and cancel 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.