3Com AP9152 and AP9552 Access Points

Quick Configuration Guide

Manual Version: 6W101
www.3com.com

3C Number：
3CRWE955275(Fat Mode)
3CRWE915275(Fat Mode)

3Com Corporation

350 Campus Drive, Marlborough, MA, USA 01752 3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labeled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

About This Manual

Organization

3Com AP9152 and AP9552 Access Points Quick Configuration Guide is organized as follows:

Chapter	Contents
1 Logging In to the Web Interface	Describes how to logging in to the web interface.
2 Setting IP Address	Describes how to setting IP address.
3 WLAN Service Configuration	Describes the detailed configuration procedures for wireless service configuration, access service based VLAN configuration, PSK （WPA or WPA2）authentication, local MAC authentication, remote MAC authentication, remote 802.1X authentication and 802.11n configuration.
4 WDS Configuration	Describes the detailed configuration procedures for WDS and WDS point-to-multipoint.
5 Repeater Mode Configuration	Describes the detailed configuration procedures for repeater mode.
6 Workgroup Bridge Mode Configuration	Describes the detailed configuration procedures for workgroup bridge mode.
7 Save Configuration over reboot	Describes how to save configuration.

Conventions

The manual uses the following conventions:

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
⚠ **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
📝 **Note**	Means a complementary description.

Related Documentation

In addition to this manual, each 3Com AP9152 and AP9552 Access Points documentation set includes the following:

Manual	Description
3Com AP9552 Dual Band 802.11n PoE Access Point Quick Installation Guide	Introduces the hardware configuration, installation preparations, and installation of the 3Com AP9552 indoor WLAN access point.
3Com AP9152 Single-Band 802.11n PoE Access Point Quick Installation Guide	Introduces the hardware configuration, installation preparations, and installation of the 3Com AP9152 indoor WLAN access point.
3Com AP9152 and AP9552 Access Points Web-Based Configuration Manual	This manual guides you to configure 3Com AP9152 and AP9552 Access Points through the Web interface. For how to quickly set up your device, see *3Com AP9152 and AP9552 Access Points Quick Configuration Guide.* For how to log in to the Web management interface, see *Web Overview.* For how to configure a software feature through the Web interface, and corresponding configuration examples, see the specific configuration document for the feature.
3Com AP9152 and AP9552 Access Points User Manual	This manual guides you to configure 3Com AP9152 and AP9552 Access Points at the command line interface. For manual organization and feature overview, see *Documentation Guide*. For specific software feature overview, detailed configuration procedures, and configuration examples, see *Operation Manual*. For a complete description of all command lines and the command index, see *Command Manual*.

Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

Table of Contents

1 Logging In to the Web Interface 1-1

Logging In to the Web Interface 1-1

2 Setting IP Address 2-1

Setting IP Address 2-1

3 WLAN Access Configuration 3-

Wireless Service Configuration Example 3-1

Access Service Based VLAN Configuration Example 3-3

PSK Authentication Configuration Example 3-5

Local MAC Authentication Configuration Example 3-7

Remote MAC Authentication Configuration Example 3-10

Remote 802.1X Authentication Configuration Example 3-18

802.11n Configuration Example 3-26

4 WDS Configuration 4-1

WDS Configuration Example 4-

WDS Point-to-Multipoint Configuration Example 4-4

5 Repeater Mode Configuration 5-

Repeater Mode Configuration Example 5-1

6 Workgroup Bridge Mode Configuration 6-1

Workgroup Bridge Mode Configuration Example 6-1

7 Save Configuration over reboot 7-1

Save Configuration to File 7-

Note

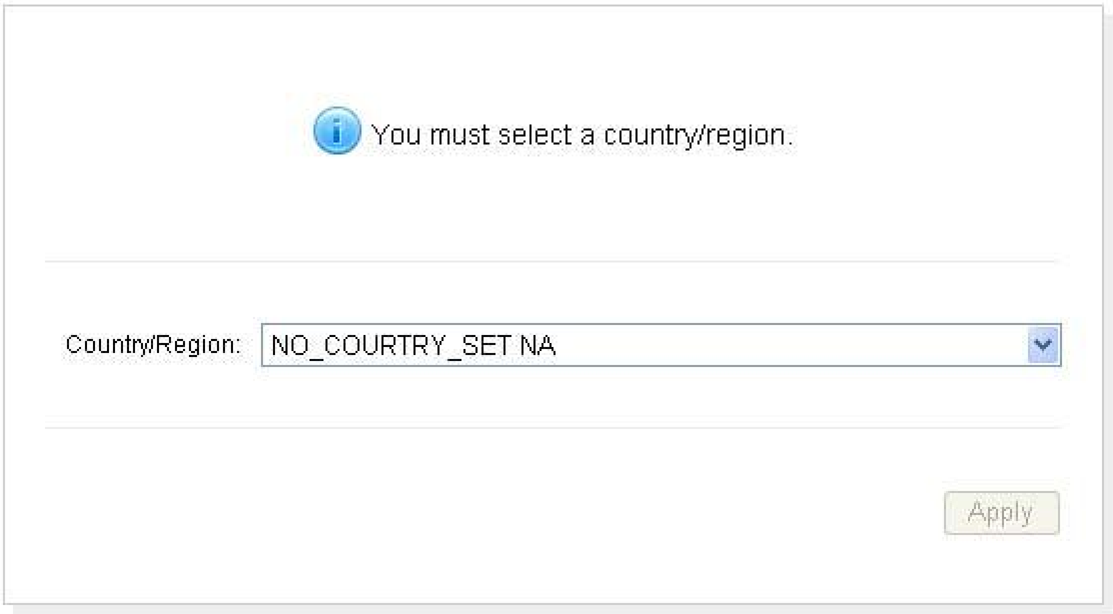
- The displayed web pages may vary depending on your device model.
- If a function or parameter is grayed out, it is either not supported or cannot be modified.
- The Console default setting is 9600, 8, N, 1.

1 Logging In to the Web Interface

Logging In to the Web Interface

To enter the web configuration page when the device starts with the null configuration, you need to select the country/region code after login, and then click Apply, as shown in Figure 1-1.

Figure 1-1 Select a country/region



You must select a country/region.

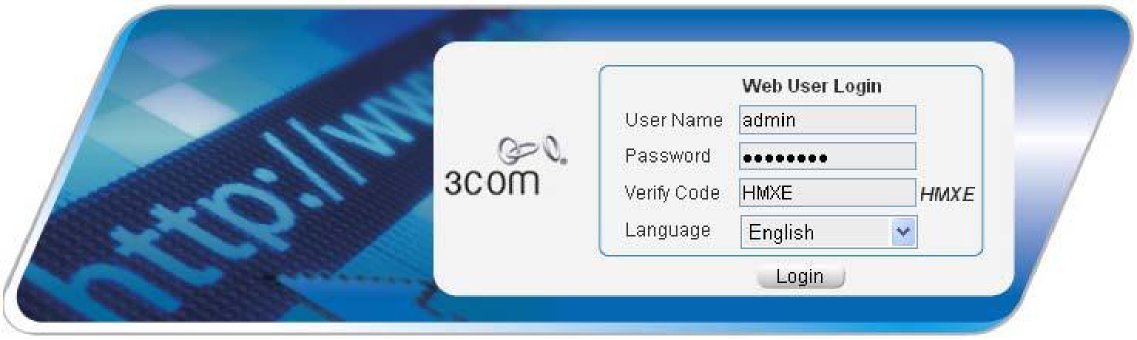
Country/Region: NO_COURTRY_SET NA

The device is provided with the default Web login information. You can use the default information to log in to the Web interface. The default Web login information is:

- Username: admin
- Password: password
- IP address of the device: 192.168.0.50.

On the PC, open the browser, type the IP address http://192.168.0.50 in the address bar, press **Enter** and you can enter the login page of the Web interface, as shown in Figure 1-2. Input the username **admin**, password **password**, and the verification code, select the language, and click **Login**.

Figure 1-2 Login page of the Web interface



Web User Login

User Name: admin

Password: ••••••••

Verify Code: HMXE HMXE

Language: English

⚠ **Caution**

- The PC where you configure the device is not necessarily the Web-based network management terminal. A Web-based network management terminal is a PC (or another terminal) used to log in to the Web interface and is required to be reachable to the device.
- After logging in to the Web interface, you can create a new user and configure the IP address of the interface connecting the user and the device.
- If you click the verification code displayed on the Web login page, you can get a new verification code.
- Up to five users can concurrently log in to the device through the Web interface.

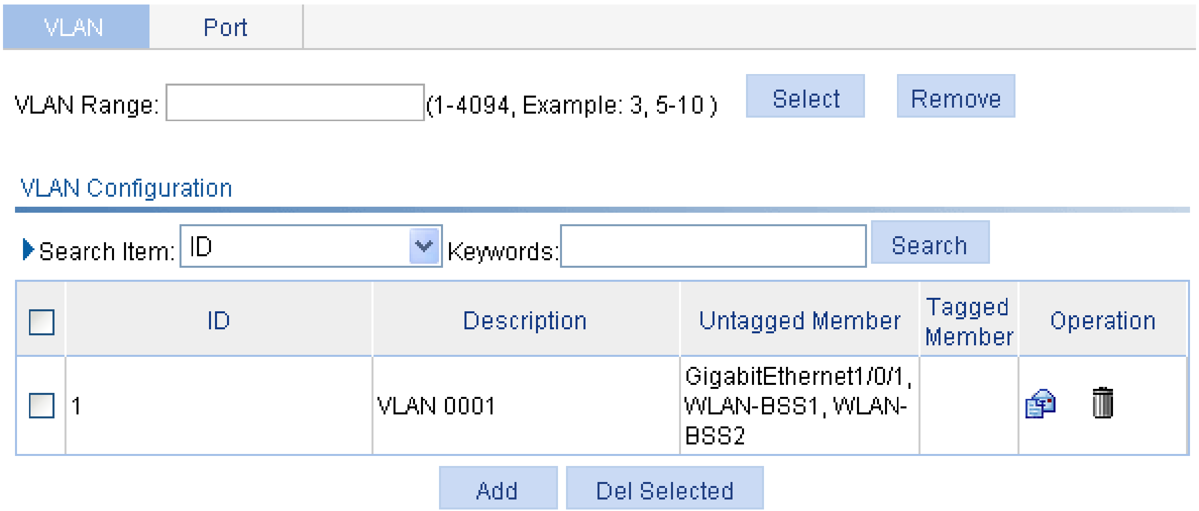
2 Setting IP Address

Setting IP Address

Creating a VLAN

Select **Network** > **VLAN** in the navigation tree. The system automatically selects the **VLAN** tab and enters the page as shown in Figure 2-1.

Figure 2-1 VLAN configuration page



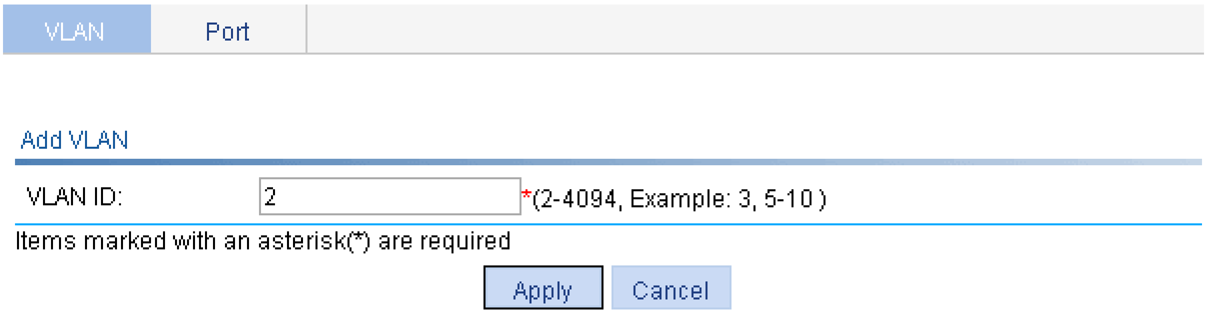
VLAN Range: (1-4094, Example: 3, 5-10)

Search Item: ID Keywords:

□	ID	Description	Untagged Member	Tagged Member	Operation
□	1	VLAN 0001	GigabitEthernet1/0/1, WLAN-BSS1, WLAN-BSS2		

Click **Add** to enter the page for creating a VLAN, as shown in Figure 2-2.

Figure 2-2 Create a VLAN



VLAN ID: 2 *(2-4094, Example: 3, 5-10)

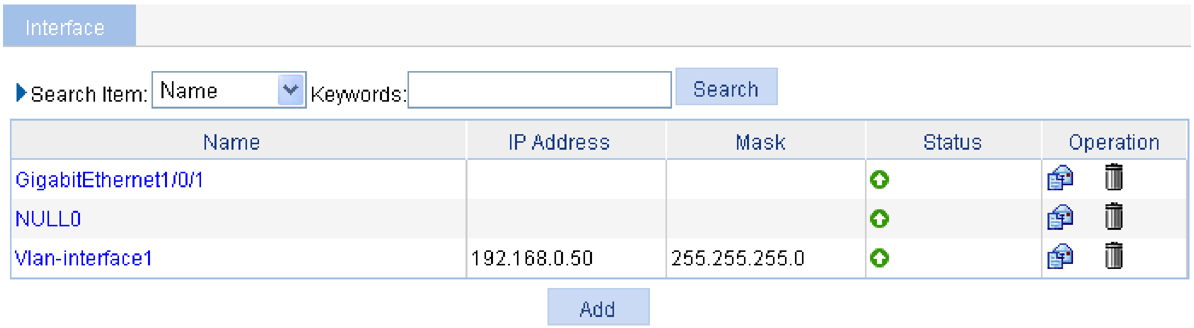
Items marked with an asterisk(*) are required

- Set VLAN ID 2.
- Click **Apply**.

Setting IP Address

Select **Device** > **Interface** in the navigation tree to enter the page shown in Figure 2-3. Click **Add** to enter the page for creating an interface, as shown in Figure 2-4.

Figure 2-3 Interface management page



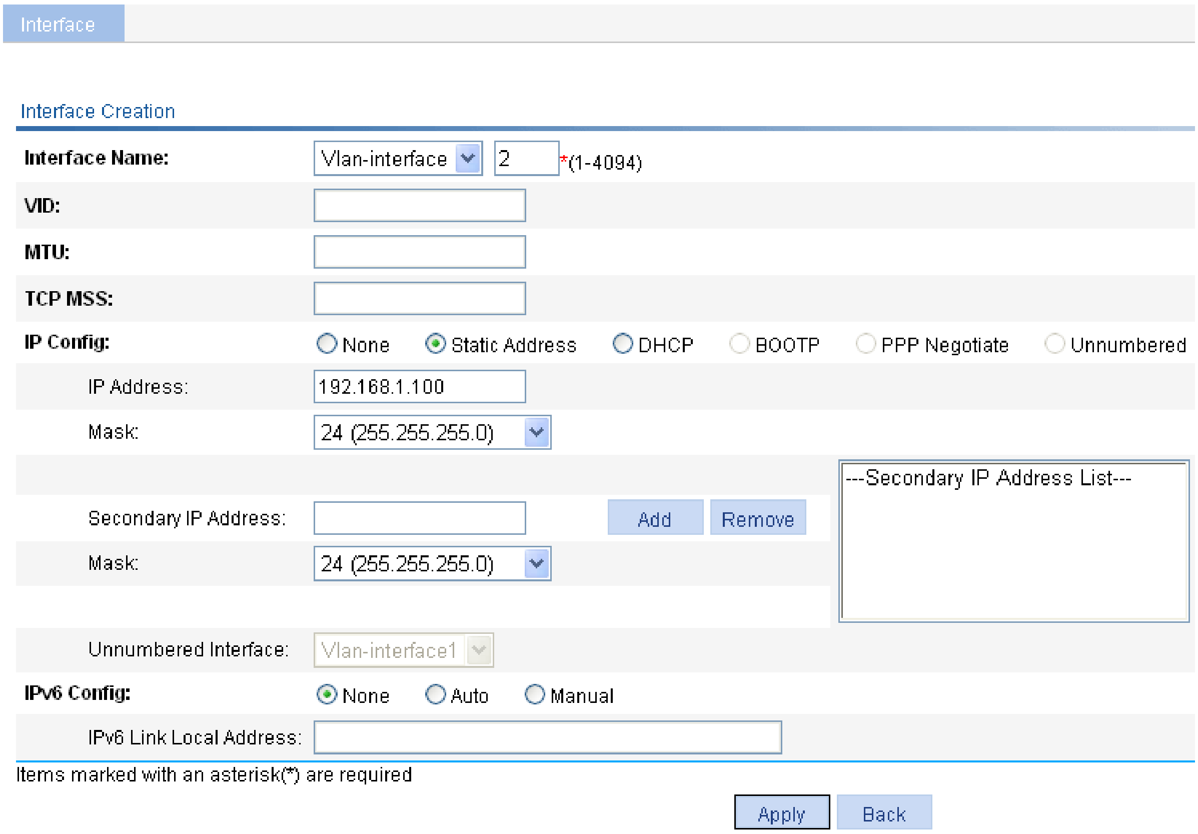
Interface

Search Item: Name Keywords: Search

Name	IP Address	Mask	Status	Operation
GigabitEthernet1/0/1			●	
NULL0			●	
Vlan-interface1	192.168.0.50	255.255.255.0	●	

Add

Figure 2-4 Create an interface



Interface

Interface Creation

Interface Name:	Vlan-interface 2 *(1-4094)
VID:	
MTU:	
TCP MSS:	
IP Config:	○ None ● Static Address ○ DHCP ○ BOOTP ○ PPP Negotiate ○ Unnumbered
IP Address:	192.168.1.100
Mask:	24 (255.255.255.0)
Secondary IP Address:	Add Remove
Mask:	24 (255.255.255.0)
Unnumbered Interface:	Vlan-interface1
IPv6 Config:	● None ○ Auto ○ Manual
IPv6 Link Local Address:	

---Secondary IP Address List---

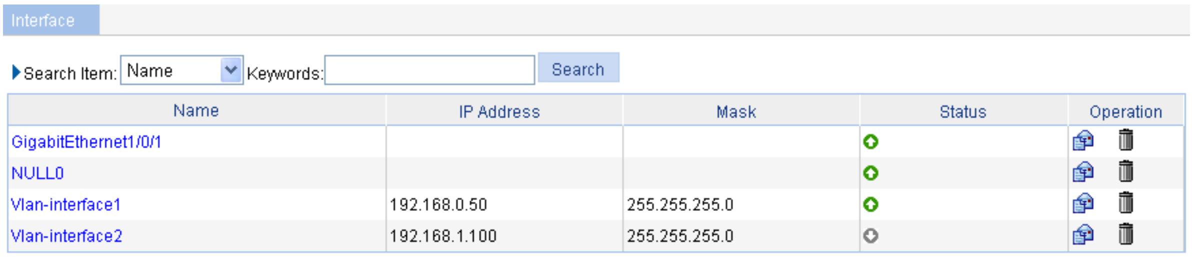
Items marked with an asterisk(*) are required

Apply Back

- Choose Vlan-interface 2.
- Choose **Static Address**.
- Set the primary IP address **192.168.1.100**.
- Set the mask 24.
- Click **Apply**.

Configuration verification

Figure 2-5 View the IP address of VLAN 2



Name	IP Address	Mask	Status	Operation
GigabitEthernet1/0/1			●	
NULL0			●	
Vlan-interface1	192.168.0.50	255.255.255.0	●	
Vlan-interface2	192.168.1.100	255.255.255.0	○	

Configuration guidelines

When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

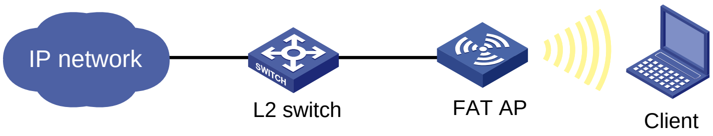
3 WLAN Access Configuration

Wireless Service Configuration Example

Network requirement

As shown in Figure 3-1, it is required that the client access the wireless network by passing plain text authentication.

Figure 3-1 WLAN service configuration

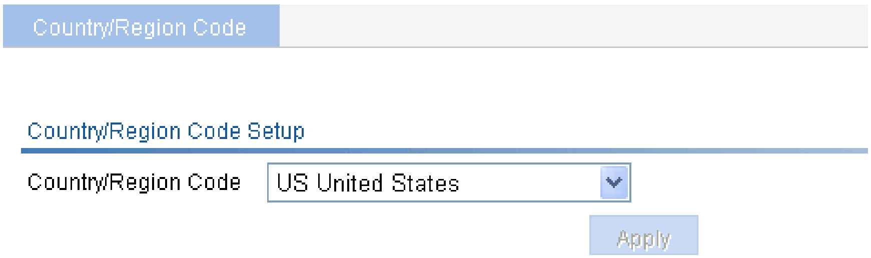


Configuration procedure

1) Select a correct country/region code

Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

Figure 3-2 Set a country/region code



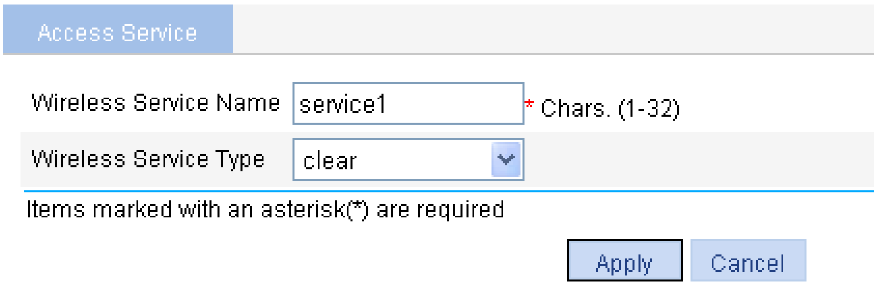
Country/Region Code: US United States

2) Configure a wireless service

# Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-3:

Figure 3-3 Create a wireless service



Wireless Service Name: service1 * Chars. (1-32)

Wireless Service Type: clear

Items marked with an asterisk(*) are required

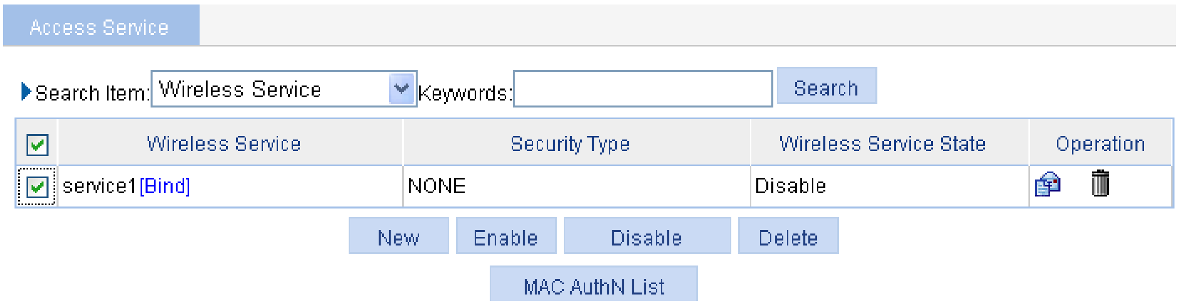
- Set the service name as **service1**.
- Select the wireless service type **clear**.

- Click **Apply**.

3) Bind a radio to the wireless service and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the page for enabling wireless service, as shown in Figure 3-4:

Figure 3-4 Enable the wireless service



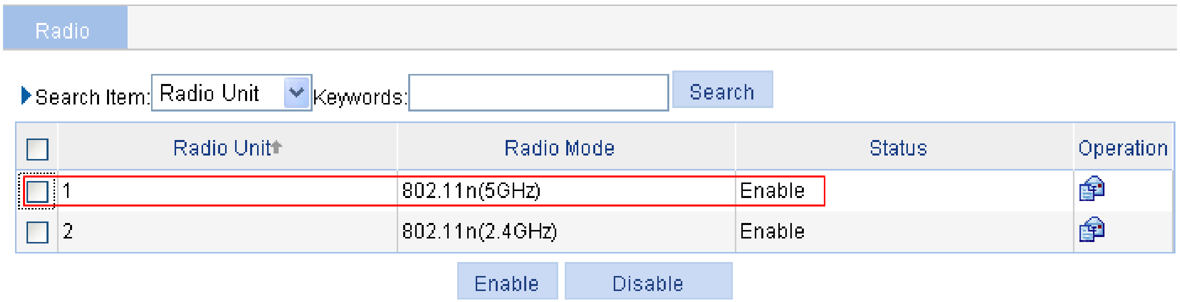
☑	Wireless Service	Security Type	Wireless Service State	Operation
☑	service1 [Bind]	NONE	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Set the **service1** check box.
- Click **Enable**.

4) Enable 802.11n radio (By default, the 802.11n (2.4GHz) radio is enabled.)

Select **Radio > Radio** from the navigation tree to enter the **Radio** page, as shown in Figure 3-5. Make sure that 802.11n (5GHz) radio is enabled.

Figure 3-5 Enable 802.11n (5GHz) radio

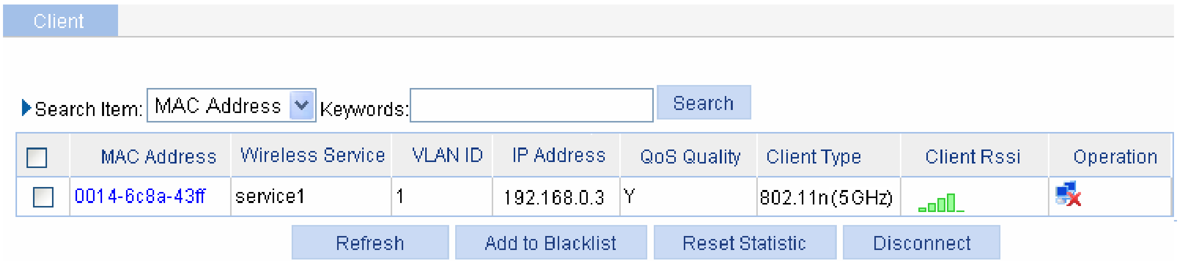


□	Radio Unit	Radio Mode	Status	Operation
□	1	802.11n(5GHz)	Enable	
□	2	802.11n(2.4GHz)	Enable	

Configuration verification

- Select **Summary** > **Client** from the navigation tree to enter the page as shown in Figure 3-6 to view the online clients.

Figure 3-6 View the online clients



□	MAC Address	Wireless Service	VLAN ID	IP Address	QoS Quality	Client Type	Client Rssi	Operation
□	0014-6c8a-43ff	service1	1	192.168.0.3	Y	802.11n(5GHz)		

Note

The IP addresses of clients obtained by the AP can be displayed only when ARP snooping is enabled. By default, ARP snooping is enabled.

- The client can be pinged successfully on the AP.

Configuration guidelines

Note the following when configuring a wireless service:

- Select a correct country/region code.
- Make sure that radio is enabled.
- When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

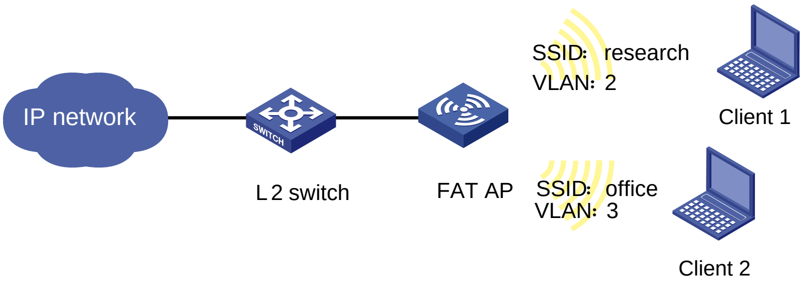
Access Service Based VLAN Configuration Example

Network requirements

As shown in Figure 3-7, it is required to configure the AP to provide multiple wireless access services. that use different wireless security policies, and are bound to different VLANs to implement isolation between wireless access users. More specifically,

- Set up a wireless service named **research**, and configure it to use PSK authentication. Clients that access the WLAN are in VLAN 2.
- Set up a wireless service named **office**, and configure it to use clear text authentication. Clients that access the WLAN are in VLAN 3.

Figure 3-7 Network diagram for access service-based VLAN configuration



Configuration procedure

1) Select a correct country/region code

Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configure a wireless service named **research**.

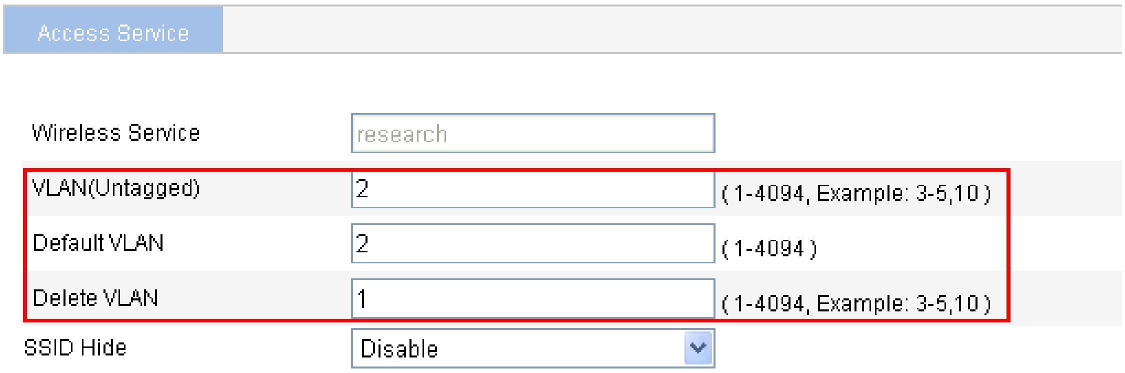
Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **Create** to enter the page for creating a wireless service.

- Configure the name of the wireless service as **research**.
- Select the wireless service type **crypto**.
- Click **Apply**.

# After the wireless service is created, the system is automatically navigated to the wireless service page, where you can perform the VLAN settings (before this operation, select **Network** > **VLAN** and create VLAN 2 first).

Figure 3-8 Set the VLANs



Wireless Service: research

VLAN(Untagged): 2 (1-4094, Example: 3-5,10)

Default VLAN: 2 (1-4094)

Delete VLAN: 1 (1-4094, Example: 3-5,10)

SSID Hide: Disable

- Type **2** in the **VLAN (Untagged)** text box.
- Type **2** in the **Default VLAN** text box.
- Type **1** in the **Delete VLAN** text box.

Note

For related configuration, refer to PSK Authentication Configuration Example. You can strictly follow the configuration example to configure the PSK configuration.

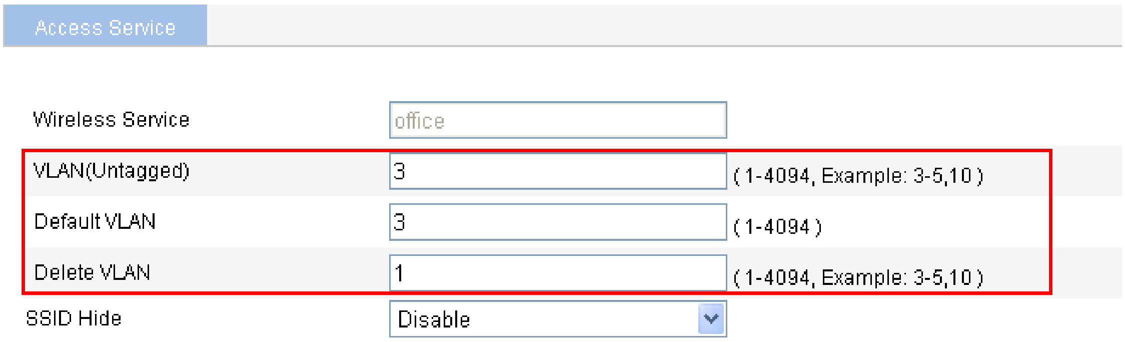
3) Configure a wireless service named **office**.

Create a wireless service.

- Configure the wireless service name as **office**.
- Select the wireless service type **clear**.
- Click **Apply**.

# After the wireless service is created, the system is automatically navigated to the wireless service page, where you can configure the VLANs (Create VLAN 3 in the **Network** > **VLAN** page).

Figure 3-9 Set the VLANs



Wireless Service: office

VLAN(Untagged): 3 (1-4094, Example: 3-5,10)

Default VLAN: 3 (1-4094)

Delete VLAN: 1 (1-4094, Example: 3-5,10)

SSID Hide: Disable

- Type **3** in the **VLAN (Untagged)** text box.
- Type **3** in the **Default VLAN** text box.
- Type **1** in the **Delete VLAN** text box.

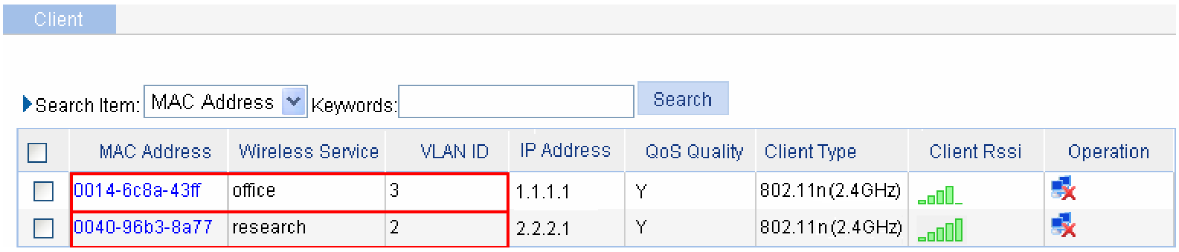
- Click **Apply**.

# Bind the corresponding radio to wireless services **office** and **research** respectively, enable the wireless services **office** and **research**, and enable the radios.

4) Verify the configuration

Select **Summary** > **Client** from the navigation tree, and enter the page shown in Figure 3-10 to view the online clients.

Figure 3-10 View the online clients



Client

Search Item: MAC Address Keywords: Search

□	MAC Address	Wireless Service	VLAN ID	IP Address	QoS Quality	Client Type	Client Rssi	Operation
□	0014-6c8a-43ff	office	3	1.1.1.1	Y	802.11n(2.4GHz)		
□	0040-96b3-8a77	research	2	2.2.2.1	Y	802.11n(2.4GHz)		

On this page, you can see that client 2, which accesses the SSID **office**, is in VLAN 3, while client 1, which accesses the SSID **research**, is in VLAN 2. Because the two clients are in different VLANs, they cannot access each other.

Configuration guidelines

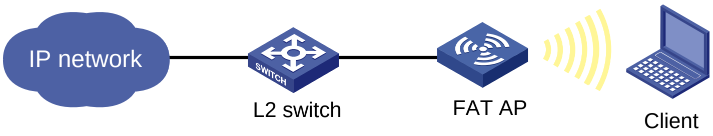
When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

PSK Authentication Configuration Example

Network requirements

As shown in Figure 3-11, it is required that the client access the wireless network by passing PSK authentication. The PSK key configuration on the client is the same as that on the AP, that is, **12345678**.

Figure 3-11 Network diagram for PSK authentication configuration



Configuration procedure

1) Select a correct country/region code

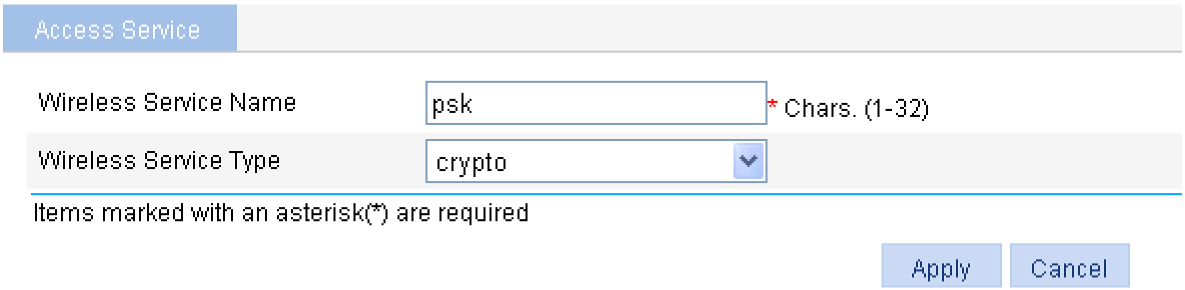
Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configure a wireless service

# Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-12:

Figure 3-12 Create a wireless service



Access Service

Wireless Service Name: psk * Chars. (1-32)

Wireless Service Type: crypto

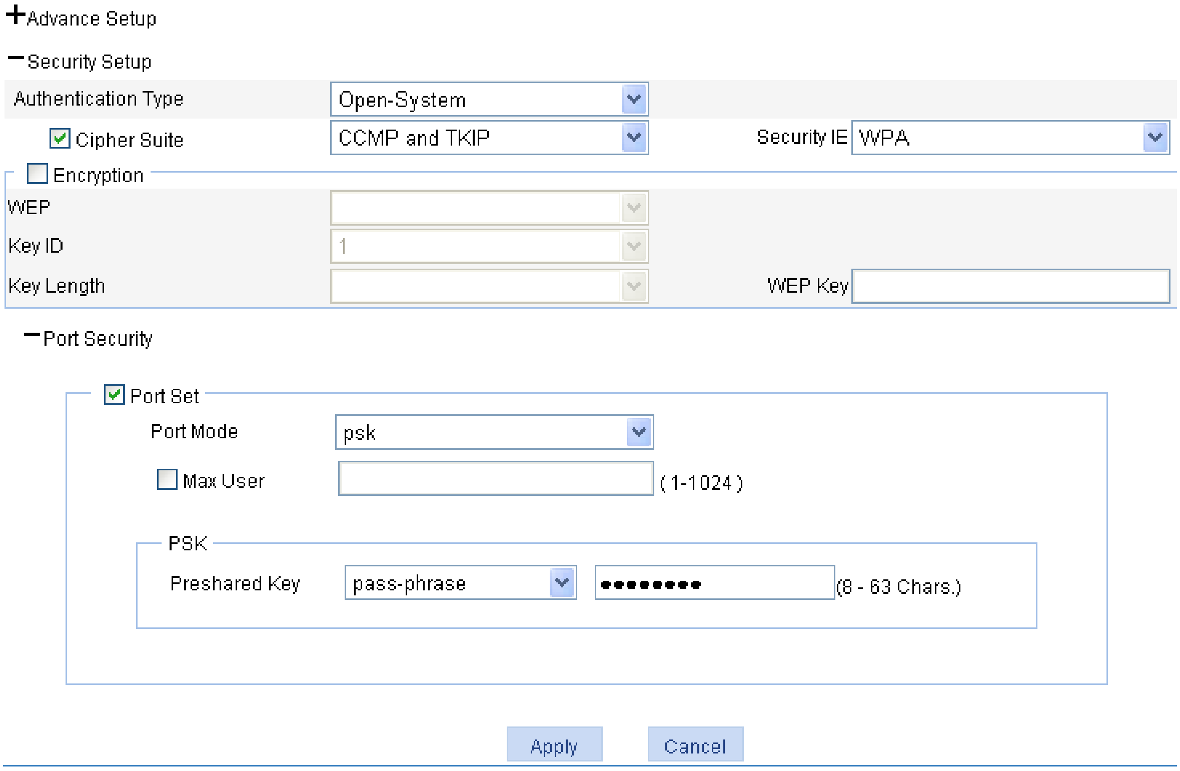
Items marked with an asterisk(*) are required

- Set the service name to **psk**.
- Select the wireless service type **crypto**.
- Click **Apply**.

3) Configure the wireless service

After you create a wireless service, you will enter the wireless service configuration page. You need to perform security setup when configuring PSK authentication, as shown in Figure 3-13:

Figure 3-13 Security setup



+Advance Setup

−Security Setup

Authentication Type: Open-System

☑ Cipher Suite: CCMP and TKIP

Security IE: WPA

□ Encryption

WEP:

Key ID: 1

Key Length:

WEP Key:

−Port Security

☑ Port Set

Port Mode: psk

□ Max User: (1-1024)

PSK

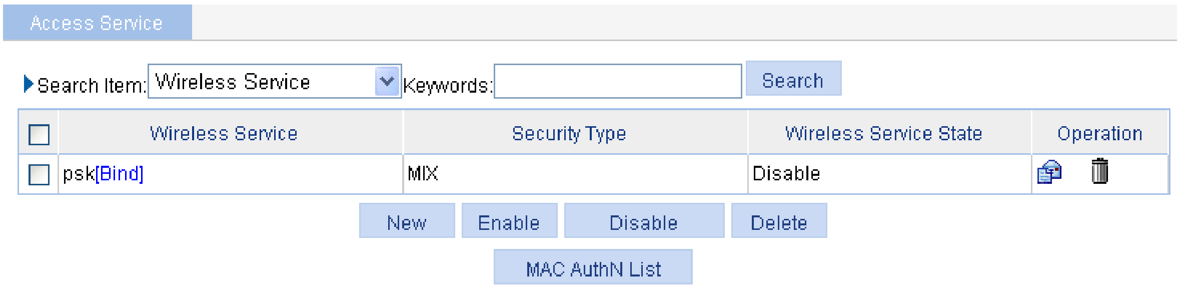
Preshared Key: pass-phrase ●●●●●●●●● (8 - 63 Chars.)

- Select the **Open-System** from the **Authentication Type** drop-down list.
- Select **Cipher Suite** check box, select **CCMP and TKIP** (select an encryption type as needed), and then select **WPA** from the **Security IE** drop-down list.
- Select the **Port Set** check box, and select **psk** from the **Port Mode** drop-down list.
- Select **pass-phrase** from the **Preshared Key** drop-down list, and type key ID **12345678**.
- Click **Apply**.

4) Bind the radio to the wireless service, and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the page for enabling a wireless service, as shown in Figure 3-14:

Figure 3-14 Bind the radio to and enable the wireless service



□	Wireless Service	Security Type	Wireless Service State	Operation
□	psk[Bind]	MIX	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Select the **psk** check box.
- Click **Enable**.

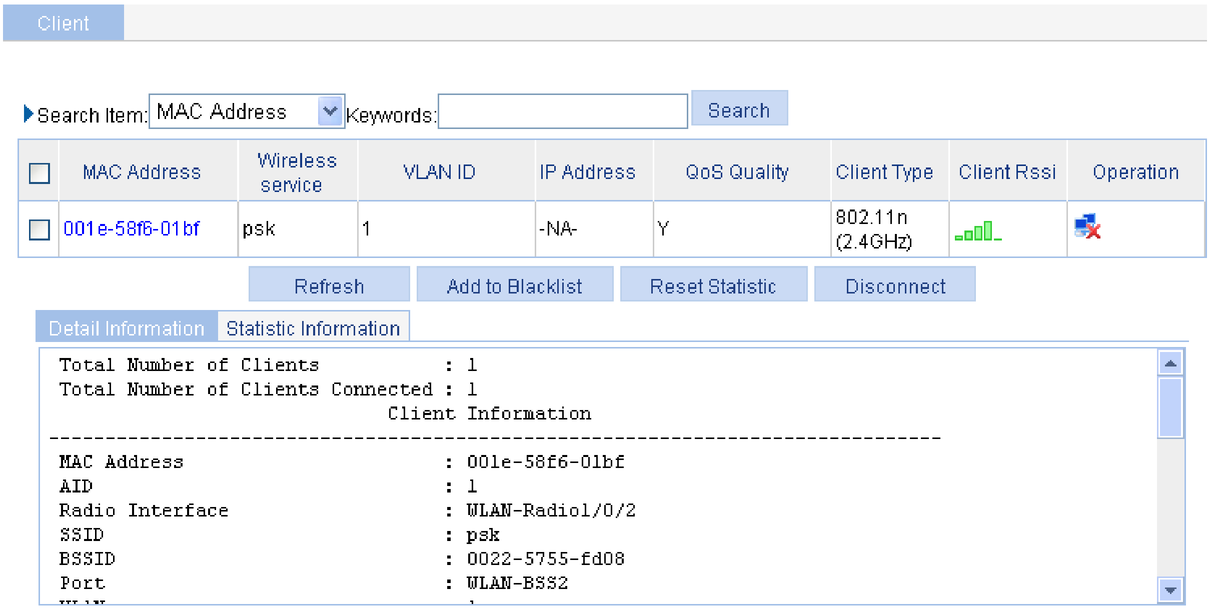
5) Enable 802.11n (2.4GHz) radio (By default, 802.11n (2.4GHz) radio is enabled. Therefore, this step is optional.)

Select **Radio > Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11n (2.4GHz) radio is enabled.

Configuration verification

The same PSK pre-shared key is configured on the client. The client can successfully associate with the AP (as shown in Figure 3-15)and can access the WLAN network.

Figure 3-15 The client associates with the AP



□	MAC Address	Wireless service	VLAN ID	IP Address	QoS Quality	Client Type	Client Rssi	Operation
□	001e-58f6-01bf	psk	1	-NA-	Y	802.11n (2.4GHz)		

```
 Total Number of Clients           : 1
 Total Number of Clients Connected : 1
                             Client Information
------------------------------------------------------------------------------
 MAC Address                       : 001e-58f6-01bf
 AID                               : 1
 Radio Interface                   : WLAN-Radio1/0/2
 SSID                              : psk
 BSSID                             : 0022-5755-fd08
 Port                              : WLAN-BSS2
```

Configuration guidelines

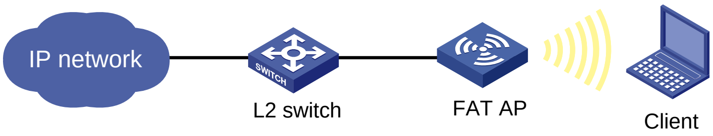
When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

Local MAC Authentication Configuration Example

Network requirements

As shown in Figure 3-16, configure the fat AP to perform MAC authentication on the client.

Figure 3-16 Network diagram for local MAC authentication configuration



Configuration procedure

1) Select a correct country/region code

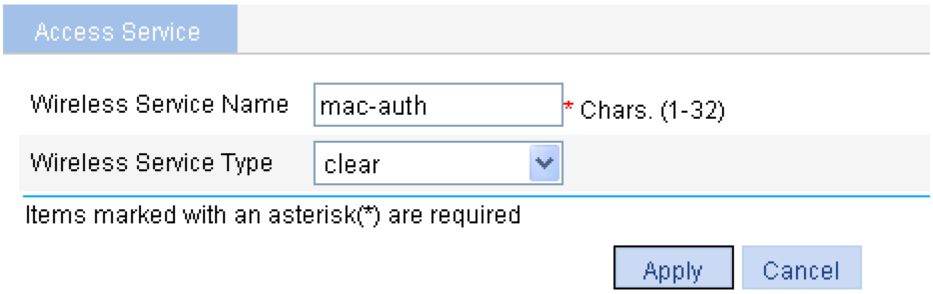
Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configure a wireless service

# Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-17:

Figure 3-17 Create a wireless service



Wireless Service Name: mac-auth * Chars. (1-32)

Wireless Service Type: clear

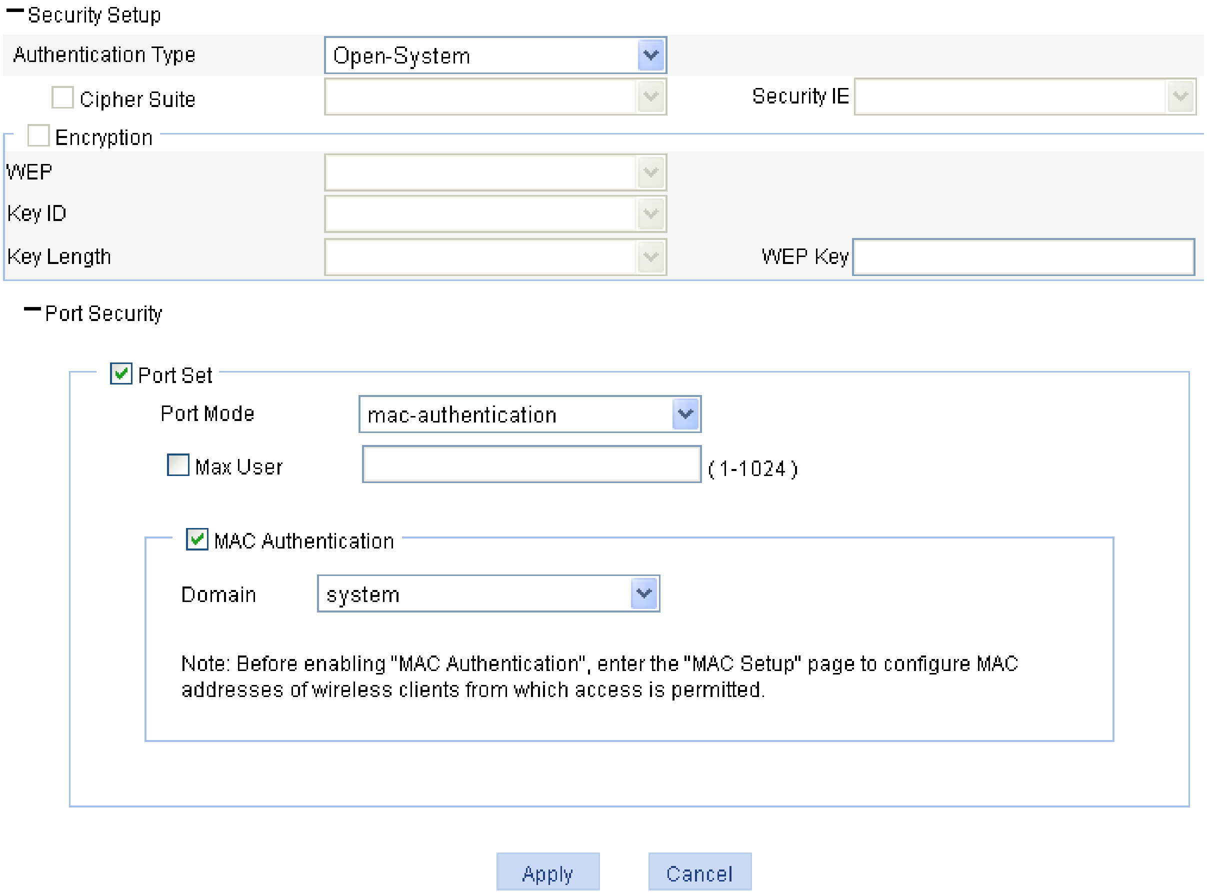
Items marked with an asterisk(*) are required

- Set the service name to **mac-auth**.
- Select the wireless service type **clear**.
- Click **Apply**.

3) Configure the wireless service

After you have created a wireless service, you will enter the wireless service configuration page. You need to perform security setup when configuring MAC authentication, as shown in Figure 3-18:

Figure 3-18 Security setup



— Security Setup

Authentication Type	Open-System		
□ Cipher Suite		Security IE	

□ Encryption

WEP			
Key ID			
Key Length		WEP Key	

— Port Security

☑ Port Set

Port Mode: mac-authentication

□ Max User (1-1024)

☑ MAC Authentication

Domain: system

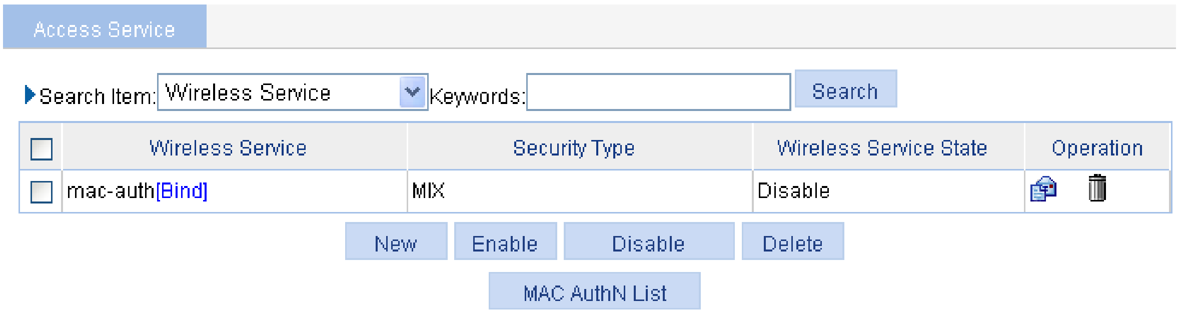
Note: Before enabling "MAC Authentication", enter the "MAC Setup" page to configure MAC addresses of wireless clients from which access is permitted.

- Select the **Open-System** from the **Authentication Type** drop-down list.
- Select the **Port Set** check box, and select **mac-authentication** from the **Port Mode** drop-down list.
- Select **MAC Authentication** check box, and select **system** from the **Domain** drop-down list (you can select **Authentication** > **AAA** from the navigation tree, click the **Domain Setup** tab, and create a domain in the **Domain Name** drop-down combo box).
- Click **Apply**.

4) Bind the radio to the wireless service, and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the page for enabling a wireless service, as shown in Figure 3-19:

Figure 3-19 Bind the radio to and enable the wireless service



Search Item: Wireless Service Keywords:

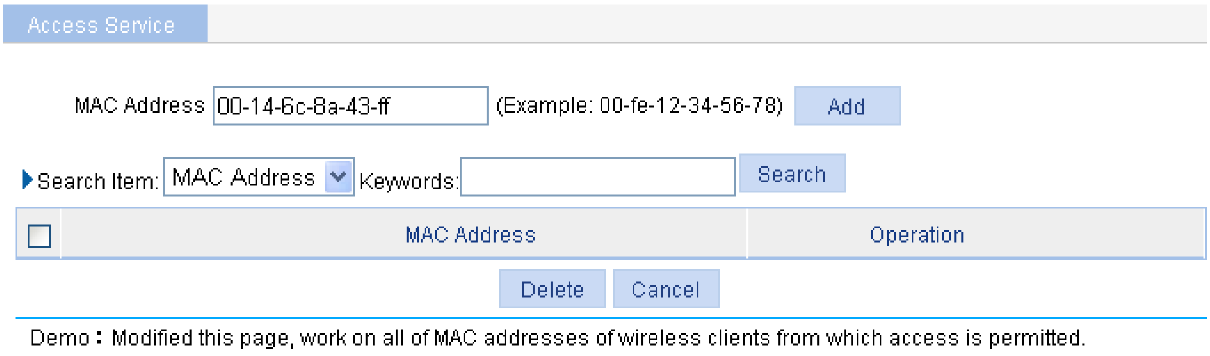
□	Wireless Service	Security Type	Wireless Service State	Operation
□	mac-auth[Bind]	MIX	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Select the **mac-auth** check box.
- Click **Enable**.

5) Configure a MAC authentication list

Select **Wireless Service** > **Access Service** from the navigation tree, and click **MAC Authentication List** to enter the page for configuring a MAC authentication list, as shown in Figure 3-20:

Figure 3-20 Add a MAC authentication list



Demo：Modified this page, work on all of MAC addresses of wireless clients from which access is permitted.

- Add a local user in the **MAC Address** box. **00-14-6c-8a-43-ff** is used in this example.
- Click **Add**.

6) Enable 802.11n (2.4GHz) radio (By default, 802.11n (2.4GHZ) radio is enabled. Therefore, this step is optional.)

Select **Radio > Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11n (2.4GHz) is enabled.

Configuration verification

- If the MAC address of the client is in the MAC authentication list, the client can pass authentication and access the WLAN network.
- The client can be pinged on the AP.

Configuration guidelines

When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

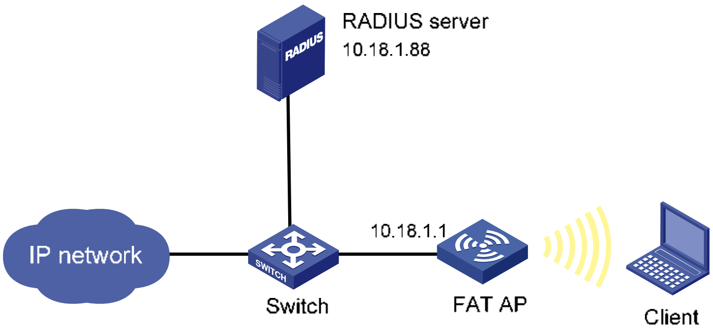
Remote MAC Authentication Configuration Example

Network requirements

It is required to perform remote MAC authentication on the client. More specifically,

- Use the intelligent management center (iMC) as the RADIUS server for authentication, authorization, and accounting (AAA). On the RADIUS server, configure the client’s username and password as the MAC address of the client and the shared key as **expert**. The IP address of the RADIUS server is 10.18.1.88.
- The IP address of the AP is 10.18.1.1. On the AP, configure the shared key for communication with the RADIUS server as **expert**, and configure the AP to remove the domain name of a username before sending it to the RADIUS server.

Figure 3-21 Remote MAC authentication



Configuration procedure

1) Configure the IP address of the fat AP

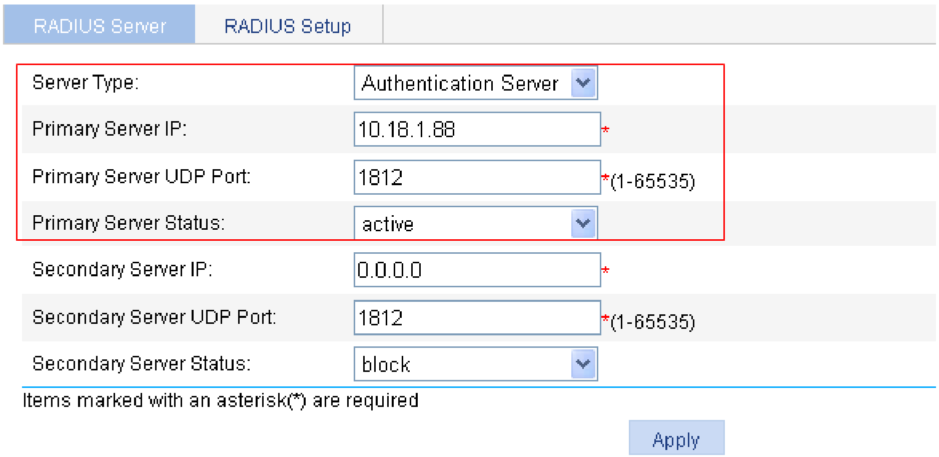
In the **Network** > **VLAN** page, create a VLAN on the fat AP, and configure the VLAN interface in the **Device** > **Interface Management** page.

2) Configure a RADIUS scheme

# Configure the RADIUS authentication server.

From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears. Perform the following configuration, as shown in Figure 3-22.

Figure 3-22 Configure the RADIUS authentication server



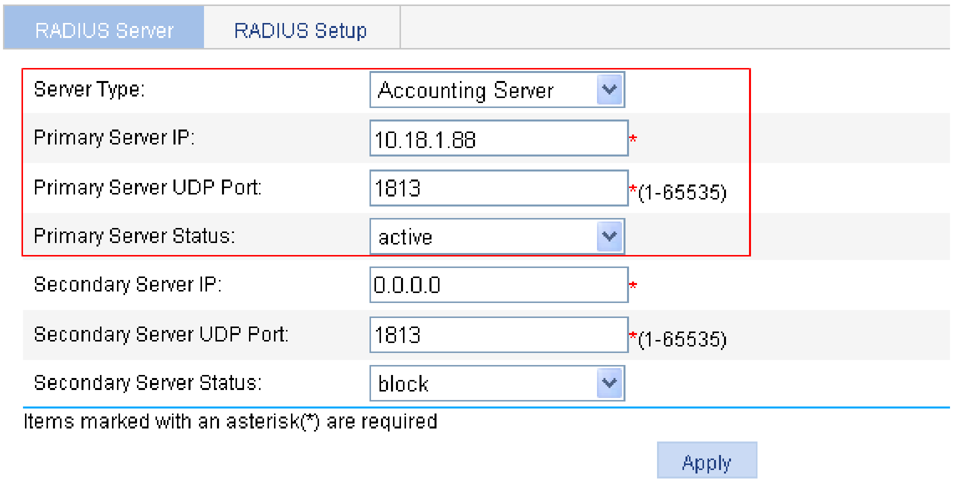
Server Type:	Authentication Server
Primary Server IP:	10.18.1.88 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	active
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	block

Items marked with an asterisk(*) are required

- Select **Authentication Server** as the server type.
- Enter **10.18.1.88** as the IP address of the primary authentication server
- Enter **1812** as the UDP port of the primary authentication server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the RADIUS accounting server, as shown in Figure 3-23.

Figure 3-23 Configure the RADIUS accounting server



Server Type:	Accounting Server	
Primary Server IP:	10.18.1.88	*
Primary Server UDP Port:	1813	*(1-65535)
Primary Server Status:	active	
Secondary Server IP:	0.0.0.0	*
Secondary Server UDP Port:	1813	*(1-65535)
Secondary Server Status:	block	

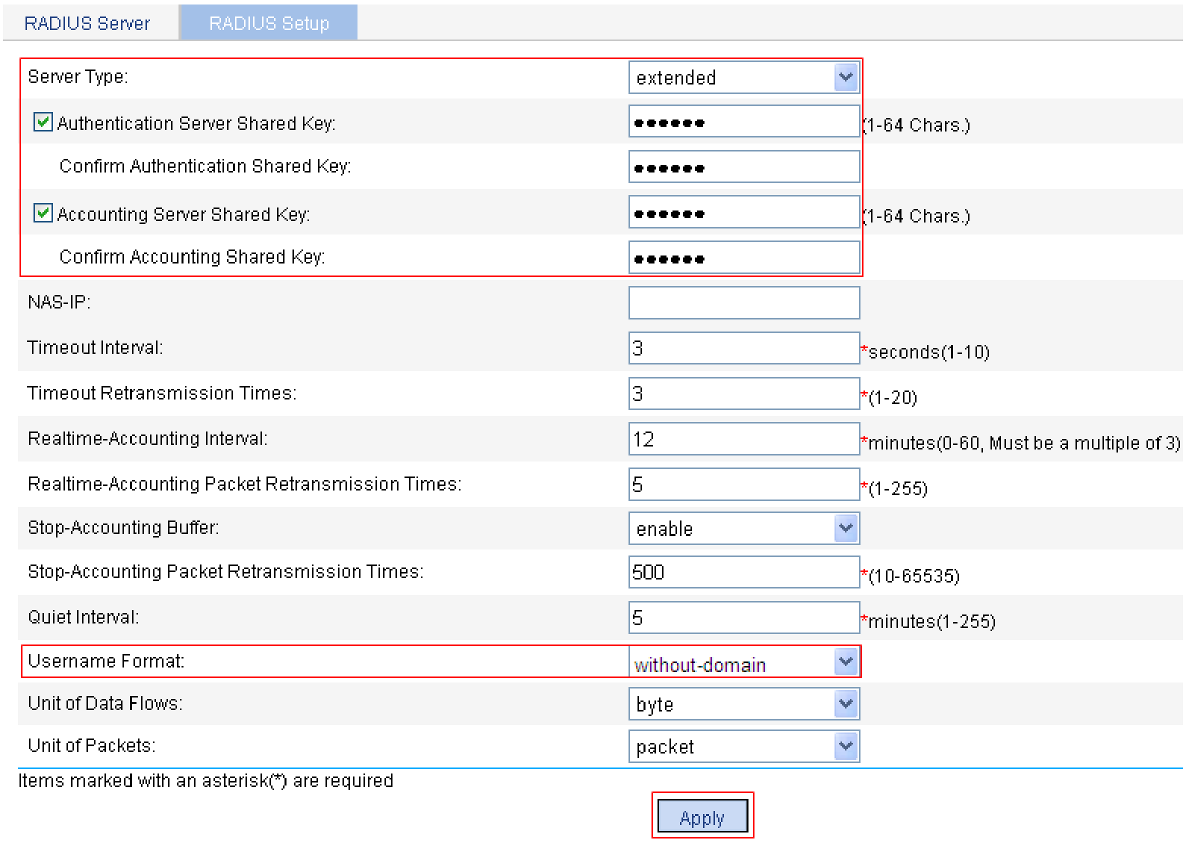
Items marked with an asterisk(*) are required

- Select **Accounting Server** as the server type.
- Enter **10.18.1.88** as the IP address of the primary accounting server.
- Enter **1813** as the UDP port of the primary accounting server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the parameters for communication between the AP and the RADIUS servers.

- Select the **RADIUS Setup** tab and configure the parameters, as shown in Figure 3-24.

Figure 3-24 Configure RADIUS parameters



Server Type:	extended	
☑ Authentication Server Shared Key:	••••••	(1-64 Chars.)
Confirm Authentication Shared Key:	••••••	
☑ Accounting Server Shared Key:	••••••	(1-64 Chars.)
Confirm Accounting Shared Key:	••••••	
NAS-IP:		
Timeout Interval:	3	*seconds(1-10)
Timeout Retransmission Times:	3	*(1-20)
Realtime-Accounting Interval:	12	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	without-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	

Items marked with an asterisk(*) are required

- Select **extended** as the server type.

- Select the **Authentication Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Authentication Shared Key** text box.
- Select the **Accounting Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Accounting Shared Key** text box.
- Select **without-domain** for **Username Format**.
- Click **Apply**

3) Configure AAA

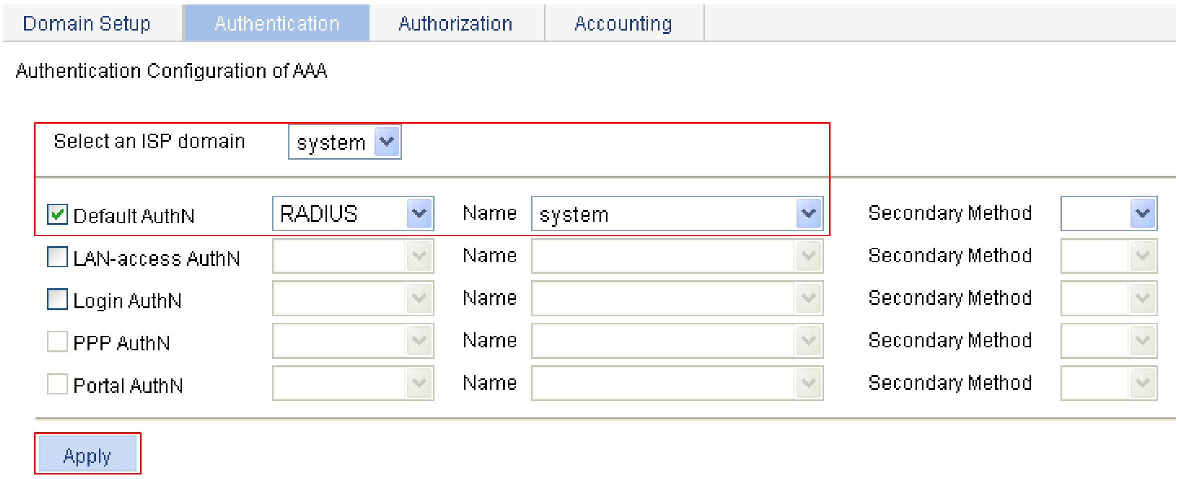
# Create an ISP domain.

- From the navigation tree, select **Authentication** > **AAA**. The domain setup page appears. In this example, the default domain **system** is used (you can create and configure a new ISP domain as needed).

# Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab, as shown in Figure 3-25.

Figure 3-25 Configure the AAA authentication method for the ISP domain



Authentication Configuration of AAA

Select an ISP domain: system

☑ Default AuthN	RADIUS	Name	system	Secondary Method	
□ LAN-access AuthN		Name		Secondary Method	
□ Login AuthN		Name		Secondary Method	
□ PPP AuthN		Name		Secondary Method	
□ Portal AuthN		Name		Secondary Method	

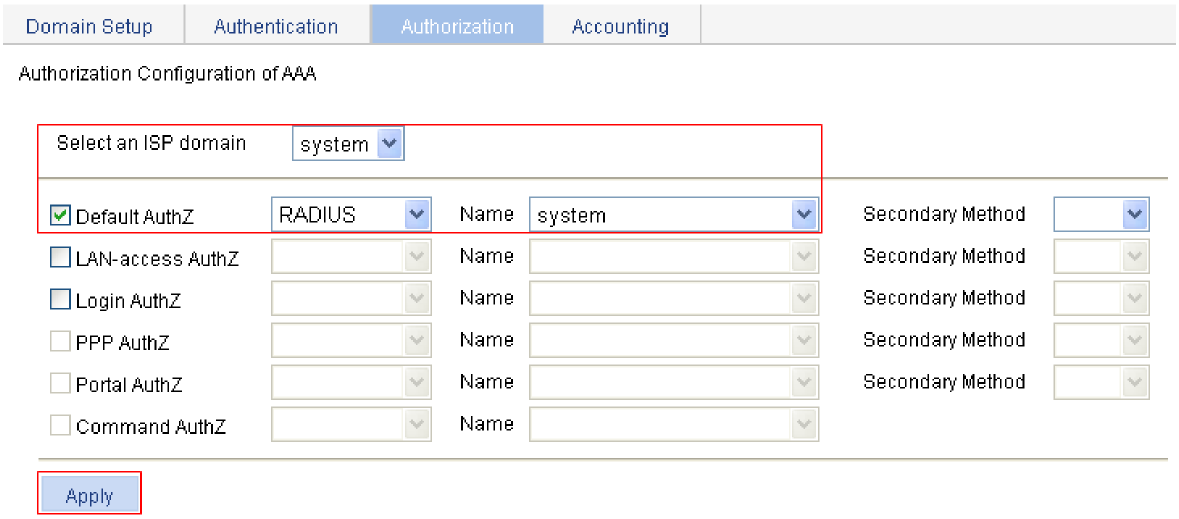
Perform the following configuration, as shown in Figure 3-25.

- Select the ISP domain name **system**.
- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab, as shown in Figure 3-26.

Figure 3-26 Configure the AAA authorization method for the ISP domain



Domain Setup | Authentication | Authorization | Accounting

Authorization Configuration of AAA

Select an ISP domain: system

☑ Default AuthZ: RADIUS — Name: system — Secondary Method:

☐ LAN-access AuthZ: — Name: — Secondary Method:

☐ Login AuthZ: — Name: — Secondary Method:

☐ PPP AuthZ: — Name: — Secondary Method:

☐ Portal AuthZ: — Name: — Secondary Method:

☐ Command AuthZ: — Name:

Apply

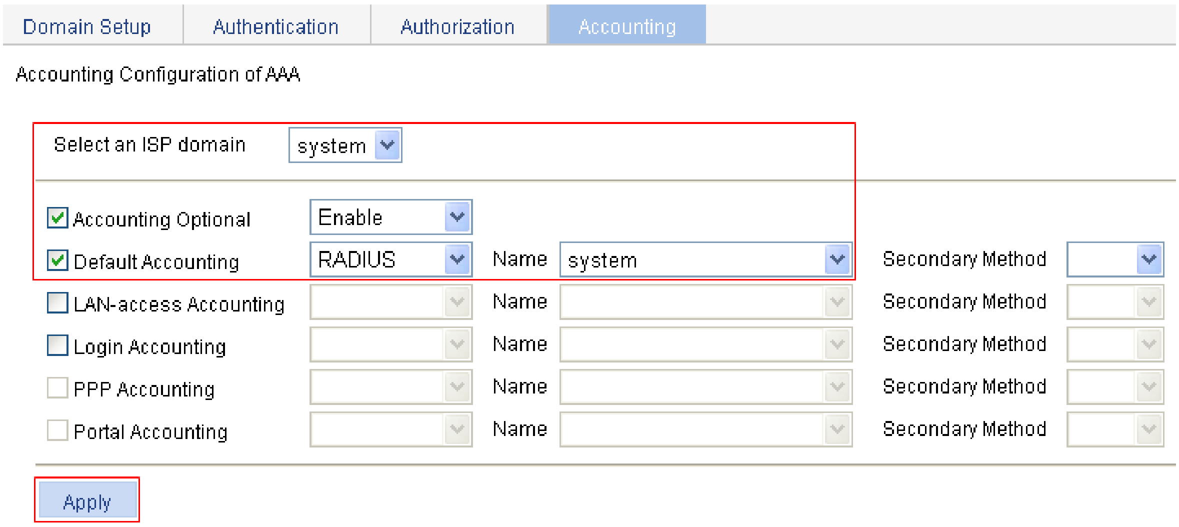
Perform the following configuration, as shown in Figure 3-26.

- Select the domain name **system**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA accounting method for the ISP domain, and enable **Accounting Optional**.

- Select the **Accounting** tab, as shown in Figure 3-27.

Figure 3-27 Configure the AAA accounting method for the ISP domain



Domain Setup | Authentication | Authorization | Accounting

Accounting Configuration of AAA

Select an ISP domain: system

☑ Accounting Optional: Enable

☑ Default Accounting: RADIUS — Name: system — Secondary Method:

☐ LAN-access Accounting: — Name: — Secondary Method:

☐ Login Accounting: — Name: — Secondary Method:

☐ PPP Accounting: — Name: — Secondary Method:

☐ Portal Accounting: — Name: — Secondary Method:

Apply

Perform the following configuration, as shown in Figure 3-27.

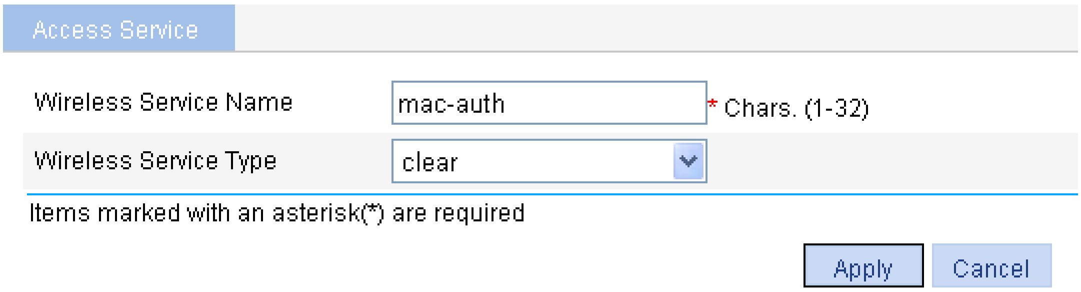
- Select the domain name **system**.
- Select the **Accounting Optional** checkbox and then select **Enable**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

4) Configure wireless service

Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-28:

Figure 3-28 Create a wireless service



Access Service

Wireless Service Name: mac-auth * Chars. (1-32)

Wireless Service Type: clear

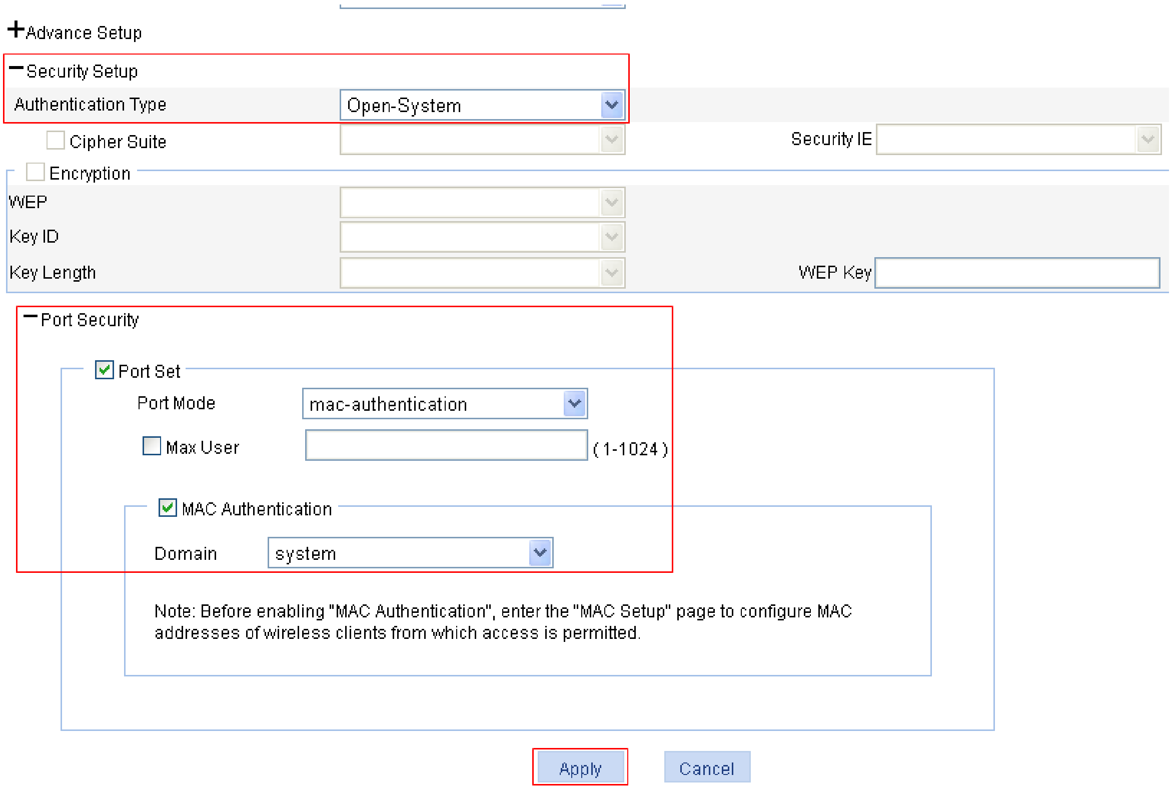
Items marked with an asterisk(*) are required

- Set the wireless service name as **mac-auth**.
- Select the wireless service type **clear**.
- Click **Apply**.

5) Configure MAC authentication

After you create a wireless service, you will enter the wireless service configuration page. Then you can configure MAC authentication on the **Security Setup** area, as shown in Figure 3-29:

Figure 3-29 Security setup



+Advance Setup

−Security Setup

Authentication Type: Open-System

□ Cipher Suite

Security IE

□ Encryption

WEP

Key ID

Key Length

WEP Key

−Port Security

☑ Port Set

Port Mode: mac-authentication

□ Max User (1-1024)

☑ MAC Authentication

Domain: system

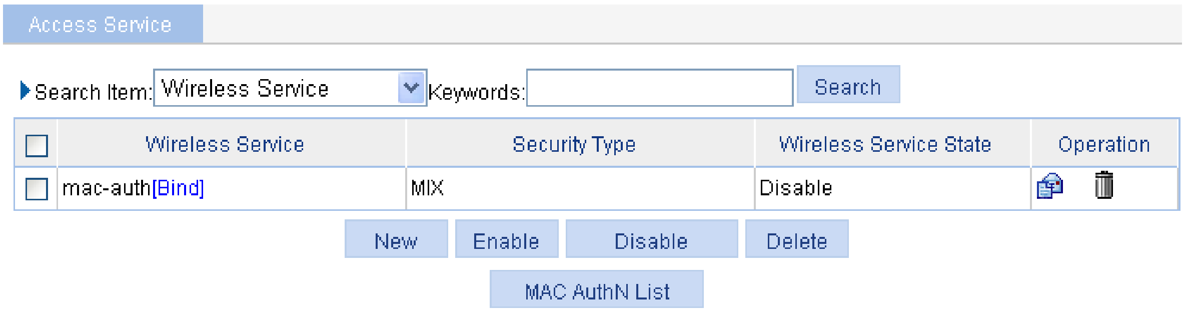
Note: Before enabling "MAC Authentication", enter the "MAC Setup" page to configure MAC addresses of wireless clients from which access is permitted.

- Select **Open-System** from the **Authentication Type** drop-down list.
- Select the **Port Set** check box, and select **mac-authentication** from the **Port Mode** drop-down list.
- Select **MAC Authentication** check box, and select **system** from the **Domain** drop-down list.
- Click **Apply**.

6) Bind the radio to the wireless service and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the page as shown in the following figure.

Figure 3-30 Bind the radio to the wireless service and enable the wireless service



Search Item: Wireless Service Keywords:

□	Wireless Service	Security Type	Wireless Service State	Operation
□	mac-auth[Bind]	MIX	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Select the **mac-auth** check box.
- Click **Enable**.

7) Enable 802.11g radio (By default, the 802.11g radio is enabled. Therefore, this step is optional.)

Select **Radio** > **Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11g is enabled.

8) Configure the RADIUS server (iMC)

Note

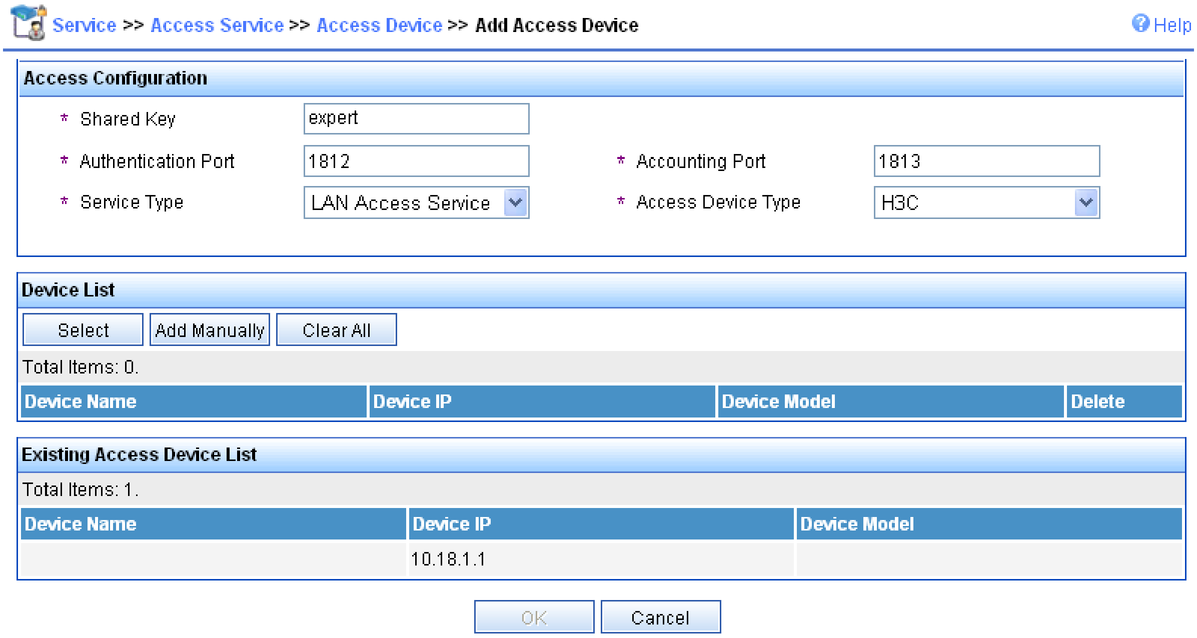
The following takes the iMC (iMC PLAT 3.20-R2602 and iMC UAM 3.60-E6102) as an example to illustrate the basic configuration of the RADIUS server.

# Add an access device.

Log in to the iMC management platform. Select the **Service** tab, and then select **Access Service** > **Access Device** from the navigation tree to enter the access device configuration page. Click **Add** on the page to enter the configuration page as shown in Figure 3-31:

- Input **expert** as the **Shared Key**.
- Add ports **1812**, and **1813** for **Authentication Port** and **Accounting Port** respectively.
- Select **LAN Access Service** for **Service Type**.
- Select **H3C** for **Access Device Type**.
- Select or manually add the access device (the AP) with the IP address 10.18.1.1.

Figure 3-31 Add access device



Service >> Access Service >> Access Device >> Add Access Device

Help

Access Configuration

* Shared Key: expert

* Authentication Port: 1812

* Accounting Port: 1813

* Service Type: LAN Access Service

* Access Device Type: H3C

Device List

Select | Add Manually | Clear All

Total Items: 0.

Device Name	Device IP	Device Model	Delete

Existing Access Device List

Total Items: 1.

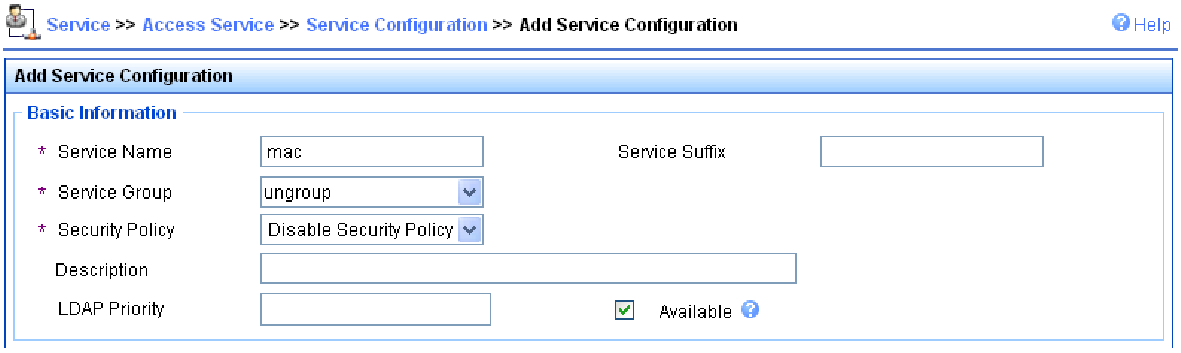
Device Name	Device IP	Device Model
	10.18.1.1	

OK | Cancel

# Add service.

Select the **Service** tab, and then select **Access Service** > **Service Configuration** from the navigation tree to enter the add service page. Then click **Add** on the page to enter the following configuration page. Set the service name as **mac**, and keep the default values for other parameters.

Figure 3-32 Add service



Service >> Access Service >> Service Configuration >> Add Service Configuration

Help

Add Service Configuration

Basic Information

* Service Name: mac

Service Suffix:

* Service Group: ungroup

* Security Policy: Disable Security Policy

Description:

LDAP Priority:

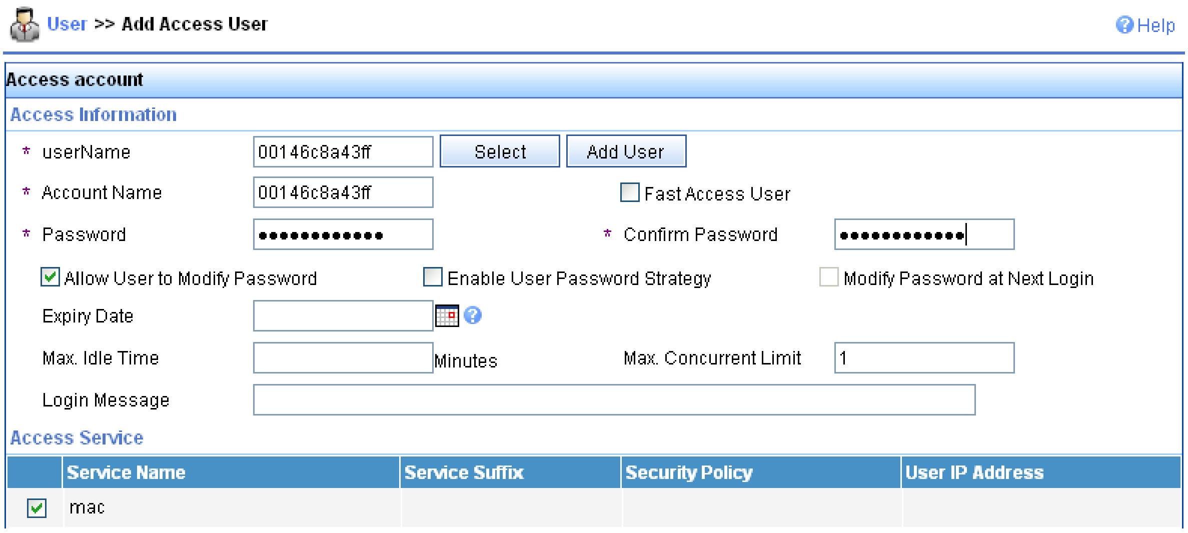
☑ Available

# Add account.

Select the **User** tab, and then select **User** > **All Access Users** from the navigation tree to enter the user page. Then, click **Add** on the page to enter the page as shown in Figure 3-33.

- Enter username **00146c8a43ff**.
- Set the account name and password both as **00146c8a43ff**.
- Select the service **mac**.

Figure 3-33 Add account



User >> Add Access User

Help

Access account

Access Information

* userName 00146c8a43ff Select Add User

* Account Name 00146c8a43ff □ Fast Access User

* Password ●●●●●●●●●●●● * Confirm Password ●●●●●●●●●●●●

☑ Allow User to Modify Password □ Enable User Password Strategy □ Modify Password at Next Login

Expiry Date

Max. Idle Time Minutes Max. Concurrent Limit 1

Login Message

Access Service

	Service Name	Service Suffix	Security Policy	User IP Address
☑	mac			

Configuration verification

During authentication, the client does not need to input the username or password. After the client passes MAC authentication, the client can associate with the AP and access the WLAN. You can view the online clients by selecting **Summary** > **Client**.

Configuration guidelines

When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

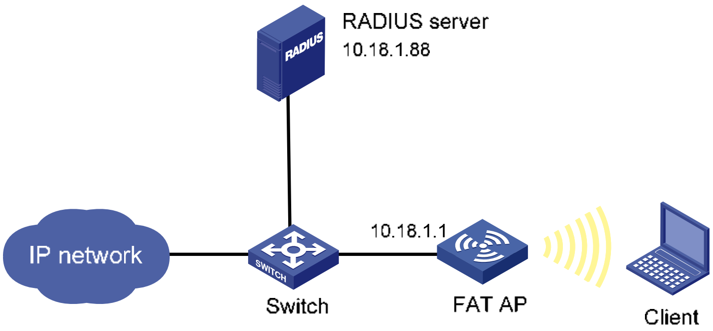
Remote 802.1X Authentication Configuration Example

Network requirements

It is required to perform remote 802.1X authentication on the client. More specifically,

- Use the CAMS or iMC as a RADIUS server for AAA. On the RADIUS server, configure the client’s username as **user**, password as **dot1x**, and shared key as **expert**. The IP address of the RADIUS server is 10.18.1.88.
- On the AP, configure the shared key as **expert**, and configure the AP to remove the domain name of a username before sending it to the RADIUS server. The IP address of the AP is 10.18.1.1.

Figure 3-34 Remote 802.1X authentication



Configuration procedure

1) Configure the IP address of the fat AP

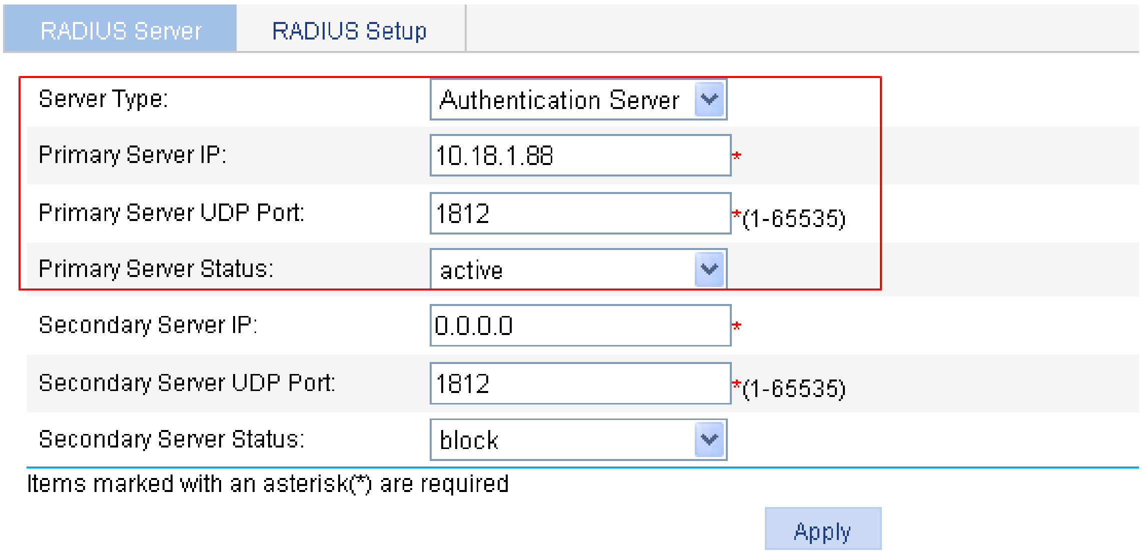
In the **Network** > **VLAN** page, create a VLAN on the fat AP, and in the **Device** > **Interface Management** page, configure the VLAN interface.

2) Configure a RADIUS scheme

# Configure the RADIUS authentication server.

From the navigation tree, select **Authentication** > **RADIUS**. The RADIUS server configuration page appears.

Figure 3-35 Configure the RADIUS authentication server



Server Type:	Authentication Server
Primary Server IP:	10.18.1.88 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	active
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	block

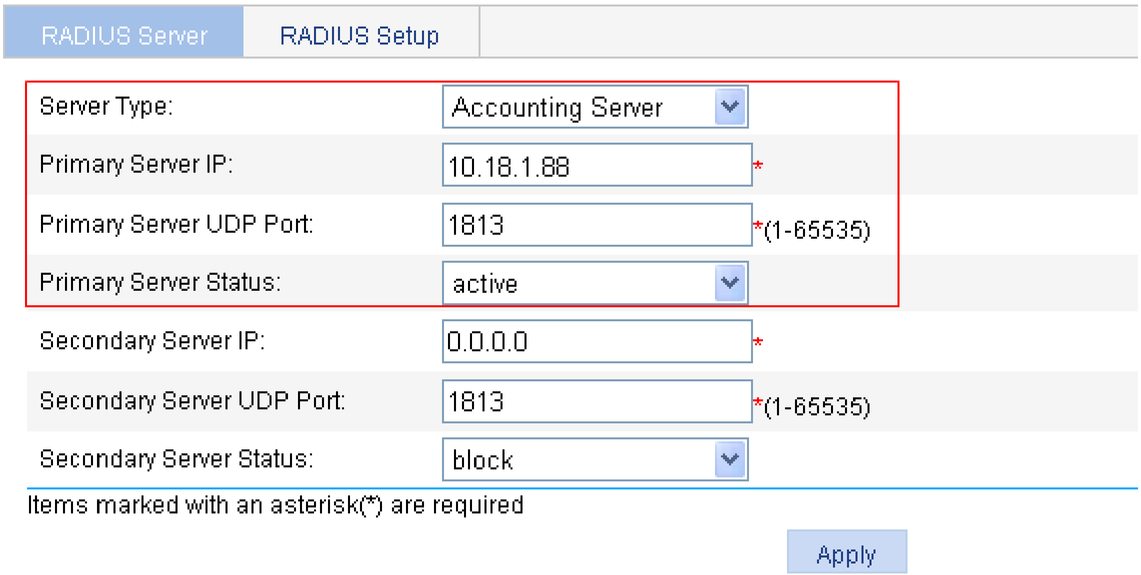
Items marked with an asterisk(*) are required

Perform the following configuration, as shown in Figure 3-35.

- Select **Authentication Server** as the server type.
- Enter **10.18.1.88** as the IP address of the primary authentication server
- Enter **1812** as the UDP port of the primary authentication server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the RADIUS accounting server.

Figure 3-36 Configure the RADIUS accounting server



Server Type:	Accounting Server
Primary Server IP:	10.18.1.88 *
Primary Server UDP Port:	1813 *(1-65535)
Primary Server Status:	active
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1813 *(1-65535)
Secondary Server Status:	block

Items marked with an asterisk(*) are required

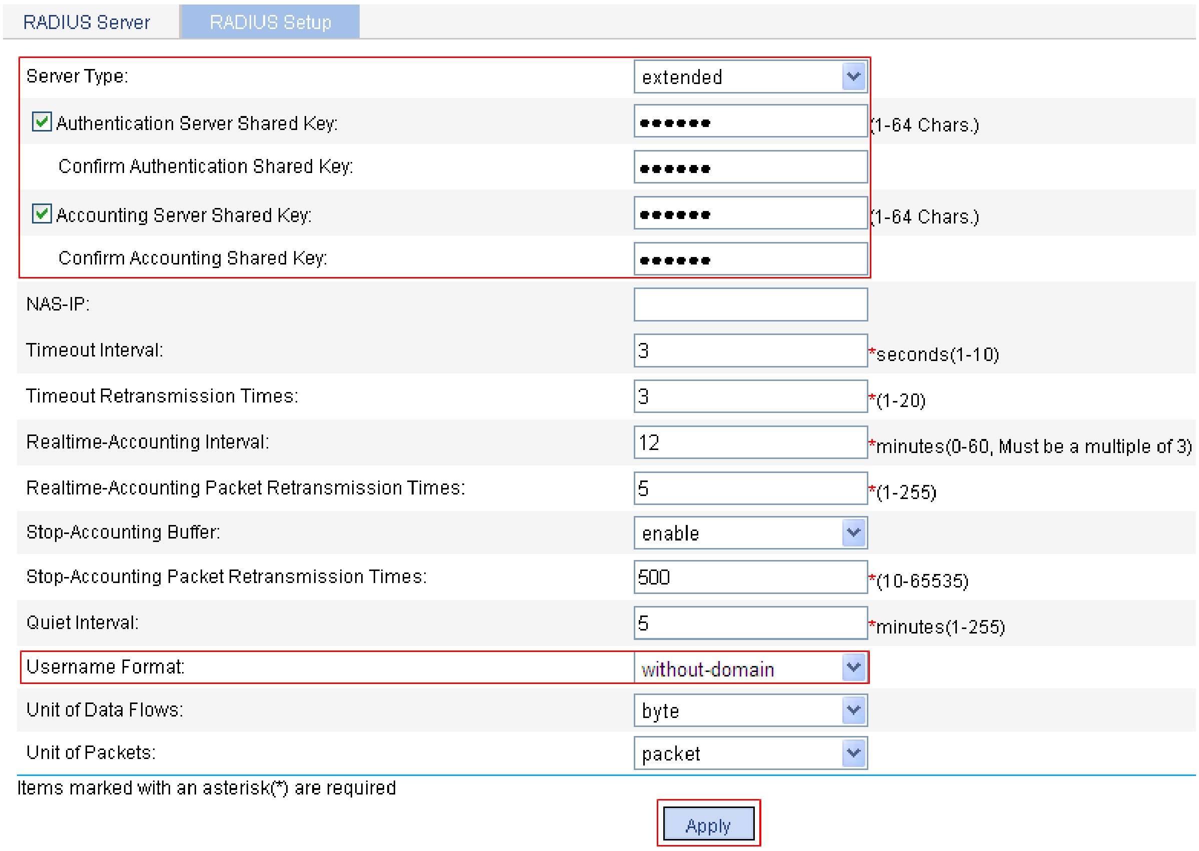
Perform the following configuration, as shown in Figure 3-36.

- Select **Accounting Server** as the server type.
- Enter **10.18.1.88** as the IP address of the primary accounting server.
- Enter **1813** as the UDP port of the primary accounting server.
- Select **active** as the primary server status.
- Click **Apply**.

# Configure the parameters for communication between the AP and the RADIUS servers.

- Select the **RADIUS Setup** tab and configure the parameters, as shown in Figure 3-37.

Figure 3-37 Configure RADIUS parameters



Server Type:	extended	
☑ Authentication Server Shared Key:	••••••	(1-64 Chars.)
Confirm Authentication Shared Key:	••••••	
☑ Accounting Server Shared Key:	••••••	(1-64 Chars.)
Confirm Accounting Shared Key:	••••••	
NAS-IP:		
Timeout Interval:	3	*seconds(1-10)
Timeout Retransmission Times:	3	*(1-20)
Realtime-Accounting Interval:	12	*minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)
Stop-Accounting Buffer:	enable	
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)
Quiet Interval:	5	*minutes(1-255)
Username Format:	without-domain	
Unit of Data Flows:	byte	
Unit of Packets:	packet	

Items marked with an asterisk(*) are required

- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Authentication Shared Key** text box.
- Select the **Accounting Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Accounting Shared Key** text box.
- Select **without-domain** for **Username Format**.
- Click **Apply**.

3) Configure AAA

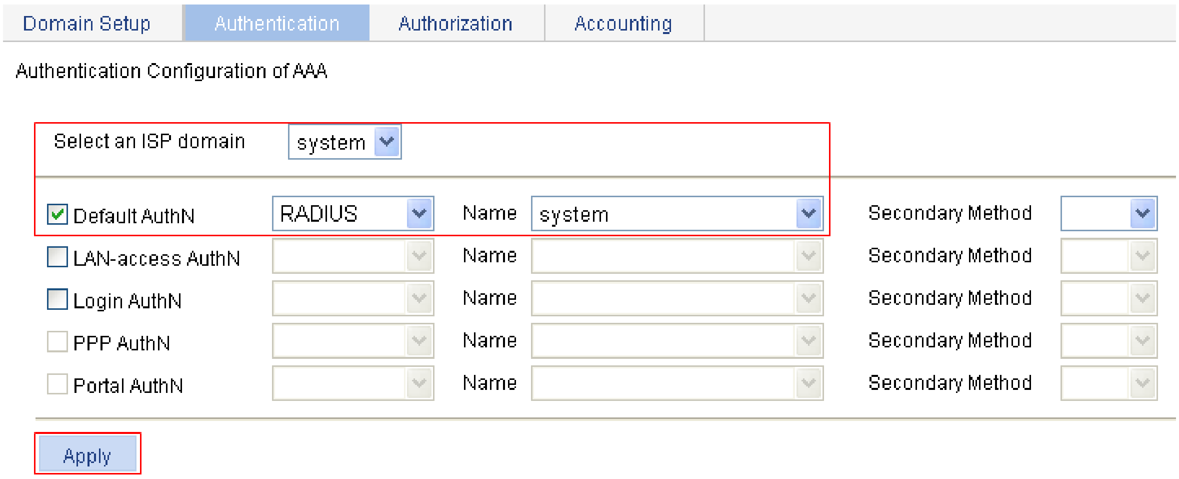
# Create an ISP domain.

- From the navigation tree, select **Authentication** > **AAA**. The domain setup page appears. In this example, the default domain **system** is used (you can create and configure a new ISP domain as needed).

# Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab, as shown in Figure 3-38.

Figure 3-38 Configure the AAA authentication method for the ISP domain



Authentication Configuration of AAA

Select an ISP domain: system

☑ Default AuthN: RADIUS — Name: system — Secondary Method:
□ LAN-access AuthN — Name — Secondary Method
□ Login AuthN — Name — Secondary Method
□ PPP AuthN — Name — Secondary Method
□ Portal AuthN — Name — Secondary Method

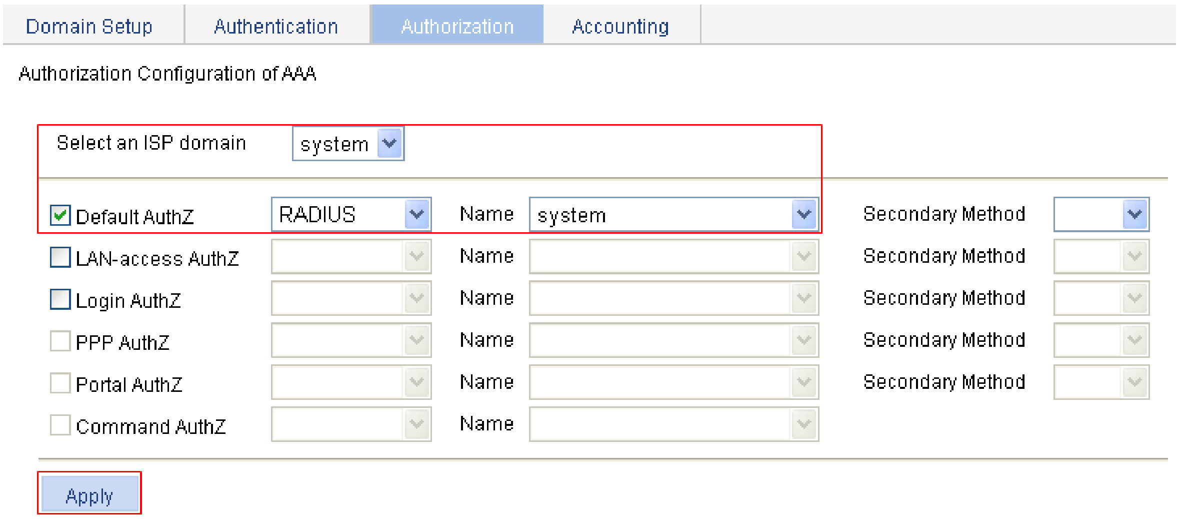
Perform the following configuration, as shown in Figure 3-38.

- Select the ISP domain name **system**.
- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab, as shown in Figure 3-39.

Figure 3-39 Configure the AAA authorization method for the ISP domain



Authorization Configuration of AAA

Select an ISP domain: system

☑ Default AuthZ: RADIUS — Name: system — Secondary Method:
□ LAN-access AuthZ — Name — Secondary Method
□ Login AuthZ — Name — Secondary Method
□ PPP AuthZ — Name — Secondary Method
□ Portal AuthZ — Name — Secondary Method
□ Command AuthZ — Name

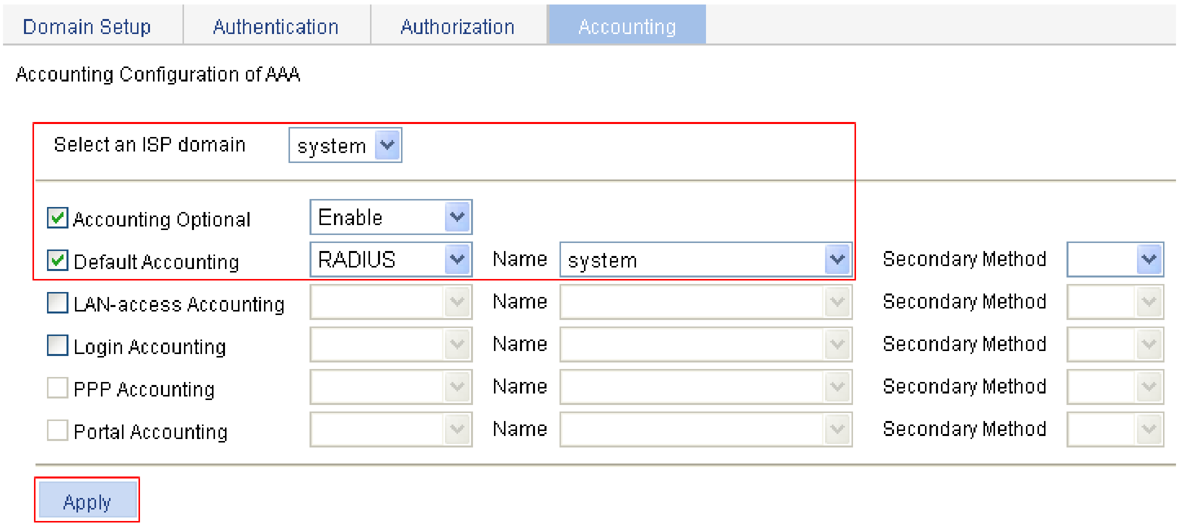
Perform the following configuration, as shown in Figure 3-39.

- Select the domain name **system**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

# Configure the AAA accounting method for the ISP domain, and enable **Accounting Optional**.

- Select the **Accounting** tab, as shown in Figure 3-40.

Figure 3-40 Configure the AAA accounting method for the ISP domain



Accounting Configuration of AAA

Select an ISP domain: system

☑ Accounting Optional	Enable				
☑ Default Accounting	RADIUS	Name	system	Secondary Method	
□ LAN-access Accounting		Name		Secondary Method	
□ Login Accounting		Name		Secondary Method	
□ PPP Accounting		Name		Secondary Method	
□ Portal Accounting		Name		Secondary Method	

Perform the following configuration, as shown in Figure 3-40.

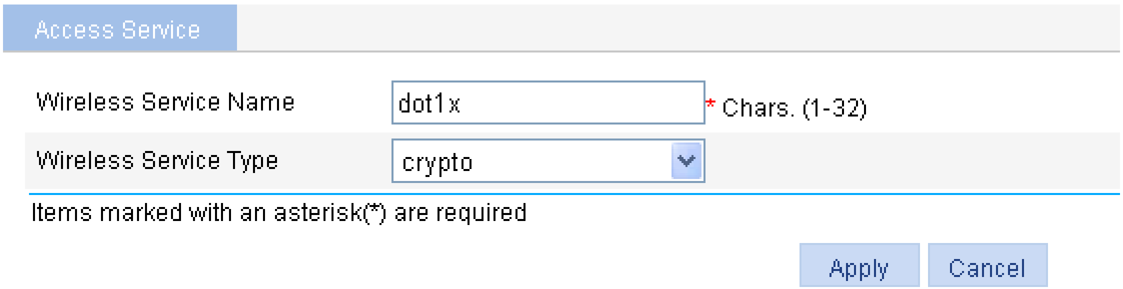
- Select the domain name **system**.
- Select the **Accounting Optional** checkbox and then select **Enable**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

4) Configure wireless service

# Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-41:

Figure 3-41 Create a wireless service



Wireless Service Name: dot1x * Chars. (1-32)

Wireless Service Type: crypto

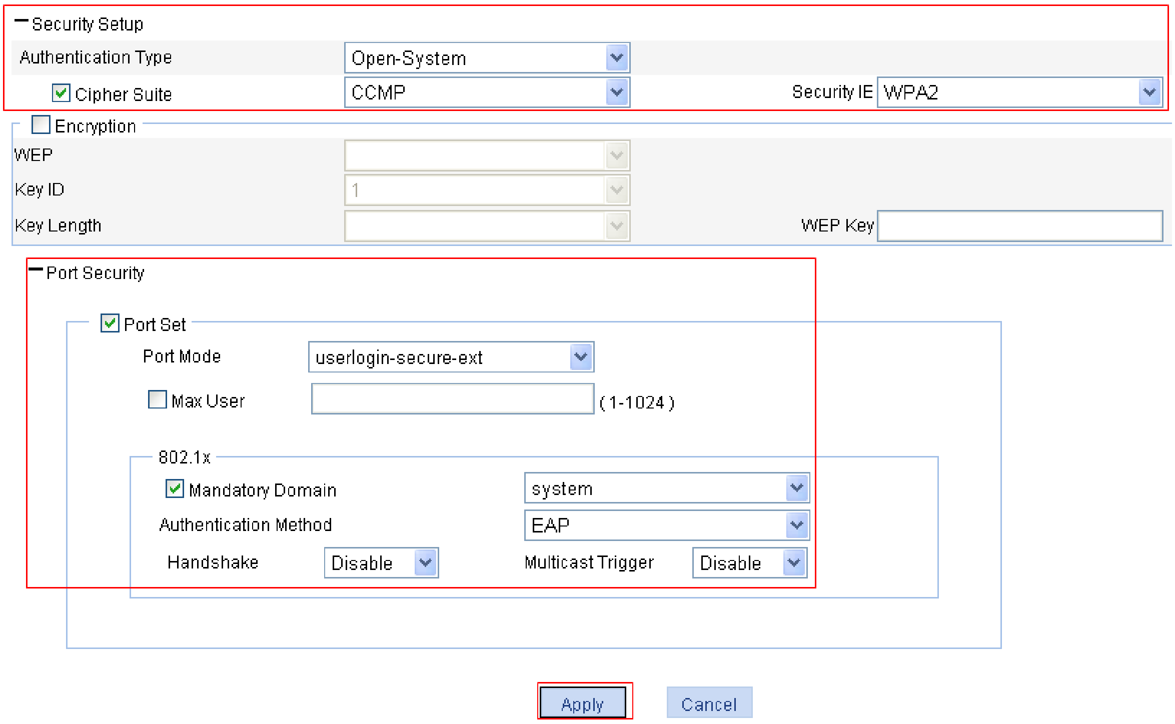
Items marked with an asterisk(*) are required

- Set the service name as **dot1x**.
- Select the wireless service type **crypto**.
- Click **Apply**.

5) Configure 802.1X authentication

After you create a wireless service, you will enter the wireless service configuration page. Then you can configure 802.1X authentication on the **Security Setup** area, as shown in Figure 3-42:

Figure 3-42 Security setup



- Security Setup

Authentication Type: Open-System

☑ Cipher Suite: CCMP   Security IE: WPA2

☐ Encryption

WEP:

Key ID: 1

Key Length: WEP Key:

- Port Security

☑ Port Set

Port Mode: userlogin-secure-ext

☐ Max User   (1-1024)

802.1x

☑ Mandatory Domain: system

Authentication Method: EAP

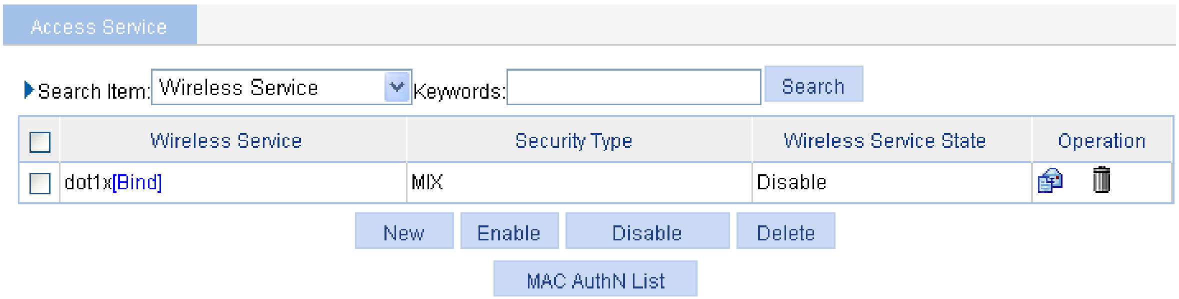
Handshake: Disable   Multicast Trigger: Disable

- Select **Open-System** from the **Authentication Type** drop-down list.
- Select the **Cipher Suite** check box, select **CCMP** from the **Cipher Suite** drop-down list, and select **WPA2** from the **Security IE** drop-down list.
- Select the **Port Set** check box, and select **userlogin-secure-ext** from the **Port Mode** drop-down list.
- Select **system** from the **Mandatory Domain** drop-down list.
- Select **EAP** from the **Authentication Method** drop-down list.
- You are recommended to disable **Handshake** and **Multicast Trigger**.
- Click **Apply**.

6) Bind the radio to the wireless service and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the page as shown in the following figure.

Figure 3-43 Bind the radio to the wireless service and enable the wireless service



Search Item: Wireless Service   Keywords:

☐	Wireless Service	Security Type	Wireless Service State	Operation
☐	dot1x[Bind]	MIX	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Select the **dot1x** check box.
- Click **Enable**.

7) Enable 802.11g radio (By default, the 802.11g radio is enabled. Therefore, this step is optional.)

Select **Radio** > **Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11g is enabled.

8) Configure the RADIUS server (iMC)

Note

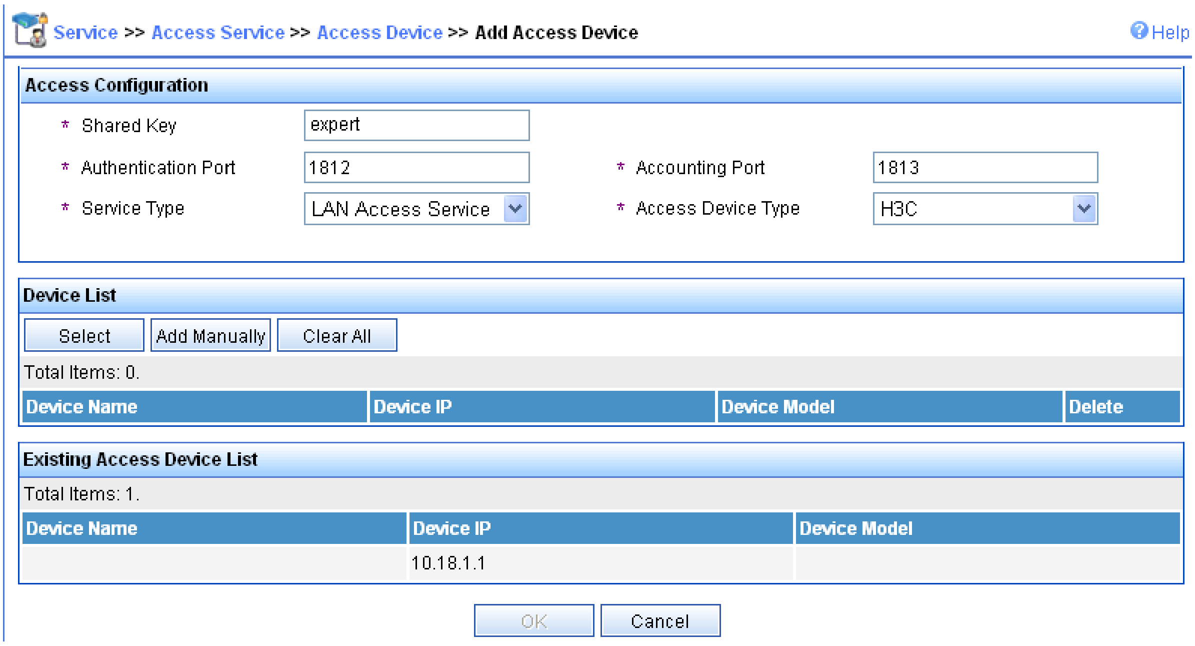
The following takes the iMC (iMC PLAT 3.20-R2602 and iMC UAM 3.60-E6102) as an example to illustrate the basic configuration of the RADIUS server.

# Add an access device.

Log in to the iMC management platform. Select the **Service** tab, and then select **Access Service** > **Access Device** from the navigation tree to enter the access device configuration page. Click **Add** on the page to enter the configuration page as shown in Figure 3-44:

- Input **expert** as the **Shared Key**.
- Add ports **1812**, and **1813** for **Authentication Port** and **Accounting Port** respectively.
- Select **LAN Access Service** for **Service Type**.
- Select **H3C** for **Access Device Type**.
- Select or manually add the access device (the AP) with the IP address 10.18.1.1.

Figure 3-44 Add access device



Service >> Access Service >> Access Device >> Add Access Device

Access Configuration

* Shared Key	expert		
* Authentication Port	1812	* Accounting Port	1813
* Service Type	LAN Access Service	* Access Device Type	H3C

Device List

Total Items: 0.

Device Name	Device IP	Device Model	Delete

Existing Access Device List

Total Items: 1.

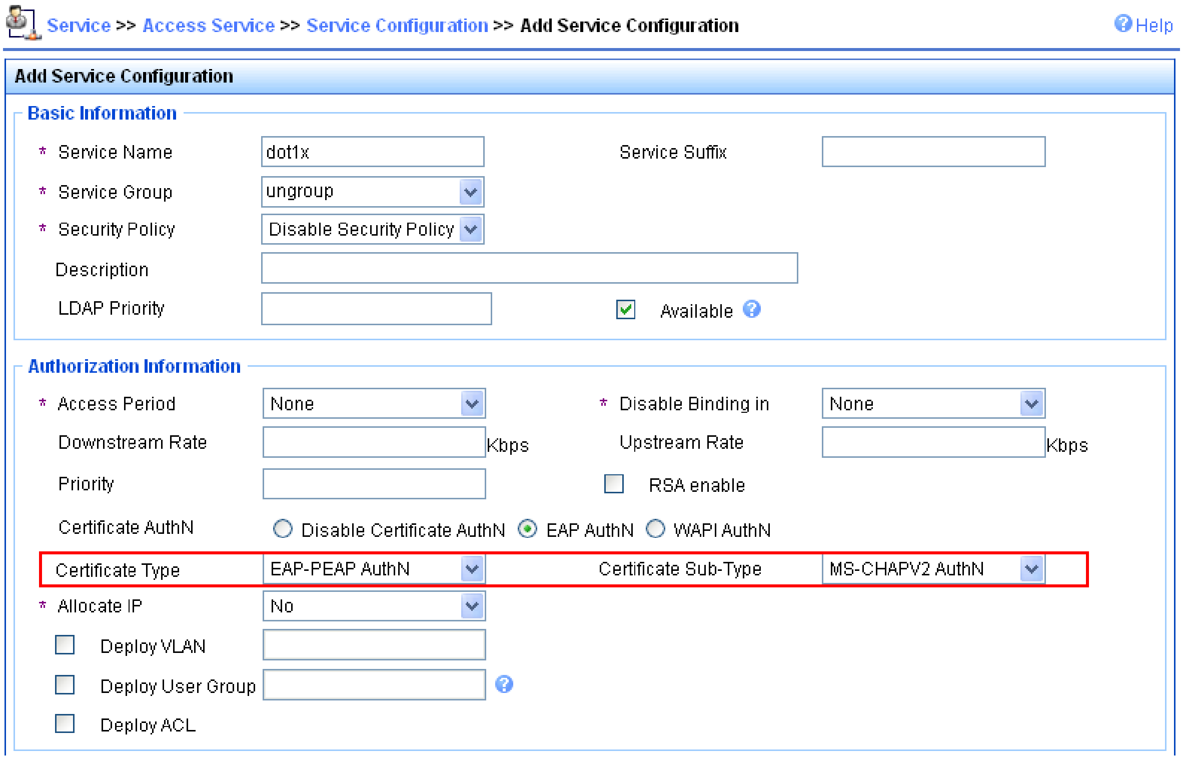
Device Name	Device IP	Device Model
	10.18.1.1	

# Add service.

Select the **Service** tab, and then select **Access Service** > **Service Configuration** from the navigation tree to enter the add service page. Then click **Add** on the page to enter the following configuration page.

- Set the service name as **dot1x.**
- Set the **Certificate Type** to **EAP-PEAP AuthN** and the **Certificate Sub Type** to **MS-CHAPV2 AuthN**.

Figure 3-45 Add service


Service >> Access Service >> Service Configuration >> Add Service Configuration

Help

Add Service Configuration

Basic Information

* Service Name: dot1x

Service Suffix:

* Service Group: ungroup

* Security Policy: Disable Security Policy

Description:

LDAP Priority:

☑ Available

Authorization Information

* Access Period: None

* Disable Binding in: None

Downstream Rate: Kbps

Upstream Rate: Kbps

Priority:

□ RSA enable

Certificate AuthN: ○ Disable Certificate AuthN ● EAP AuthN ○ WAPI AuthN

Certificate Type: EAP-PEAP AuthN

Certificate Sub-Type: MS-CHAPV2 AuthN

* Allocate IP: No

□ Deploy VLAN

□ Deploy User Group

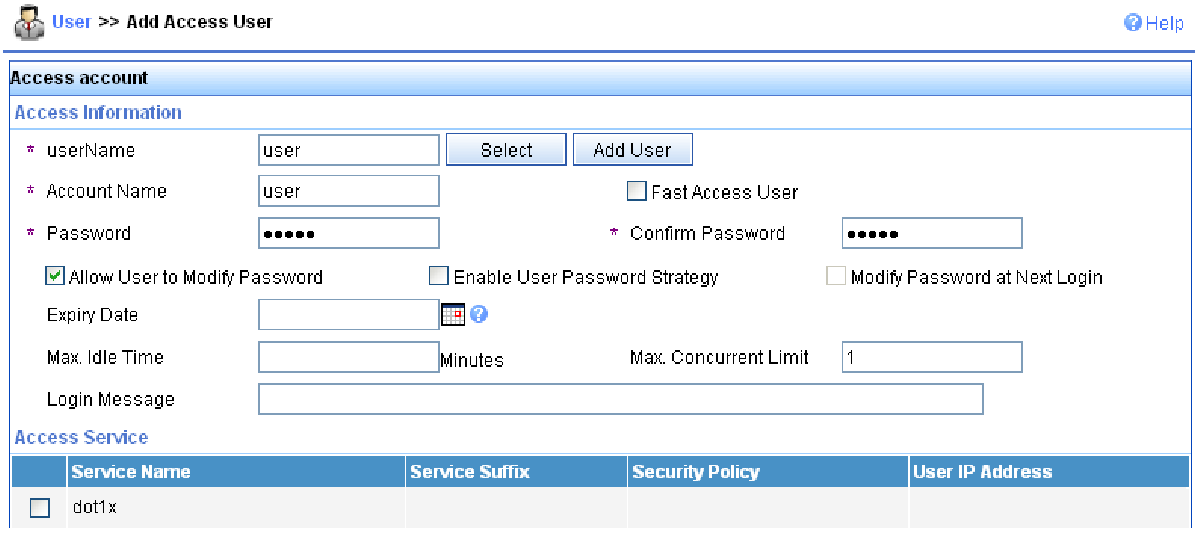
□ Deploy ACL

# Add account.

Select the **User** tab, and then select **User** > **All Access Users** from the navigation tree to enter the user page. Then, click **Add** on the page to enter the page shown in Figure 3-46.

- Enter username **user**.
- Set the account name as **user** and password as **dot1x**.
- Select the service **dot1x**.

Figure 3-46 Add account


User >> Add Access User

Help

Access account

Access Information

* userName: user [Select] [Add User]

* Account Name: user

□ Fast Access User

* Password: •••••

* Confirm Password: •••••

☑ Allow User to Modify Password

□ Enable User Password Strategy

□ Modify Password at Next Login

Expiry Date:

Max. Idle Time: Minutes

Max. Concurrent Limit: 1

Login Message:

Access Service

	Service Name	Service Suffix	Security Policy	User IP Address
□	dot1x			

Configuration verification

- After inputting username **user** and password **dot1x** in the popup dialog box, the client can associate with the AP and access the WLAN.

- You can view the online clients by selecting **Summary** > **Client**.

Configuration guidelines

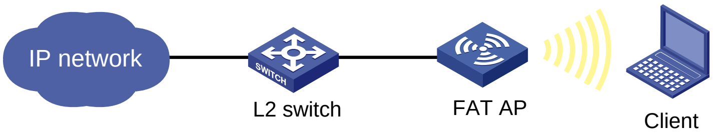
When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

802.11n Configuration Example

Network requirements

As shown in Figure 3-47, configure the AP supporting 802.11n to provide wireless access for 802.11n clients.

Figure 3-47 Network diagram for wireless service configuration



Configuration procedure

1) Select a correct country/region code

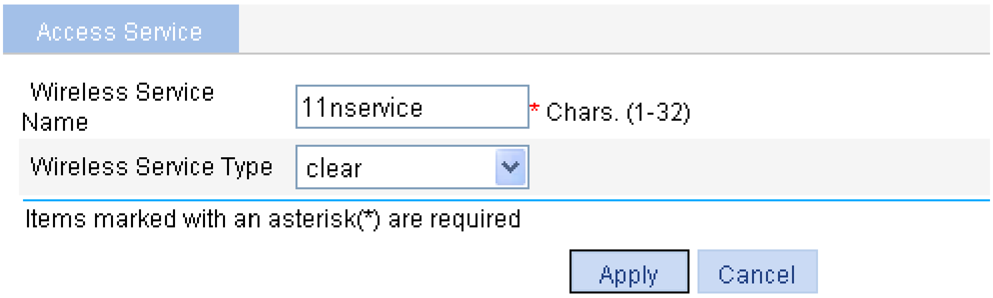
Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configure a wireless service

# Create a wireless service.

Select **Wireless Service** > **Access Service** from the navigation tree, and click **New** to enter the page for creating a wireless service, as shown in Figure 3-48:

Figure 3-48 Create a wireless service



Wireless Service Name: 11nservice * Chars. (1-32)

Wireless Service Type: clear

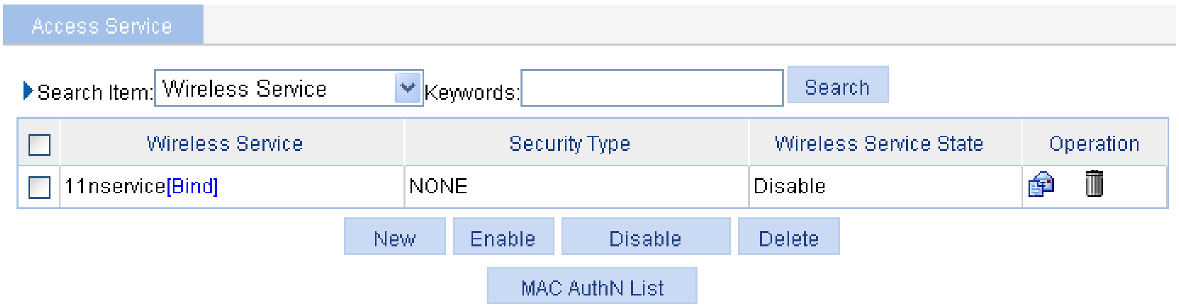
Items marked with an asterisk(*) are required

- Set the service name to **11nservice**.
- Select the wireless service type **clear**.
- Click **Apply**.

3) Bind the radio to the wireless service and enable the wireless service

Select **Wireless Service** > **Access Service** from the navigation tree to enter the pages as shown in Figure 3-49:

Figure 3-49 Bind the radio to the wireless service and enable the wireless service



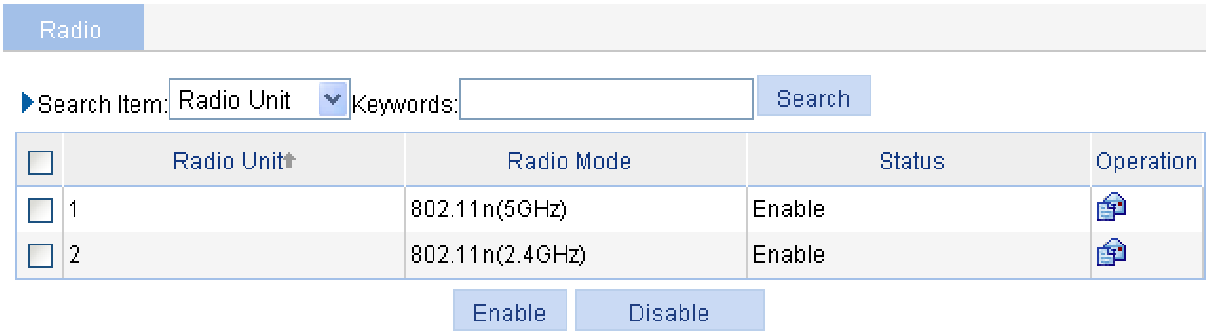
□	Wireless Service	Security Type	Wireless Service State	Operation
□	11nservice[Bind]	NONE	Disable	

- Click the **Bind** link in the **Wireless Service** column, select the target radio, and click **Bind**.
- Select the **11nservice** check box.
- Click **Enable**.

4) Enable 802.11n (2.4GHZ) radio (By default, 802.11n (2.4GHZ) radio is enabled. Therefore, this step is optional.)

Select **Radio > Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11n (2.4GHZ) is enabled.

Figure 3-50 Enable the radio

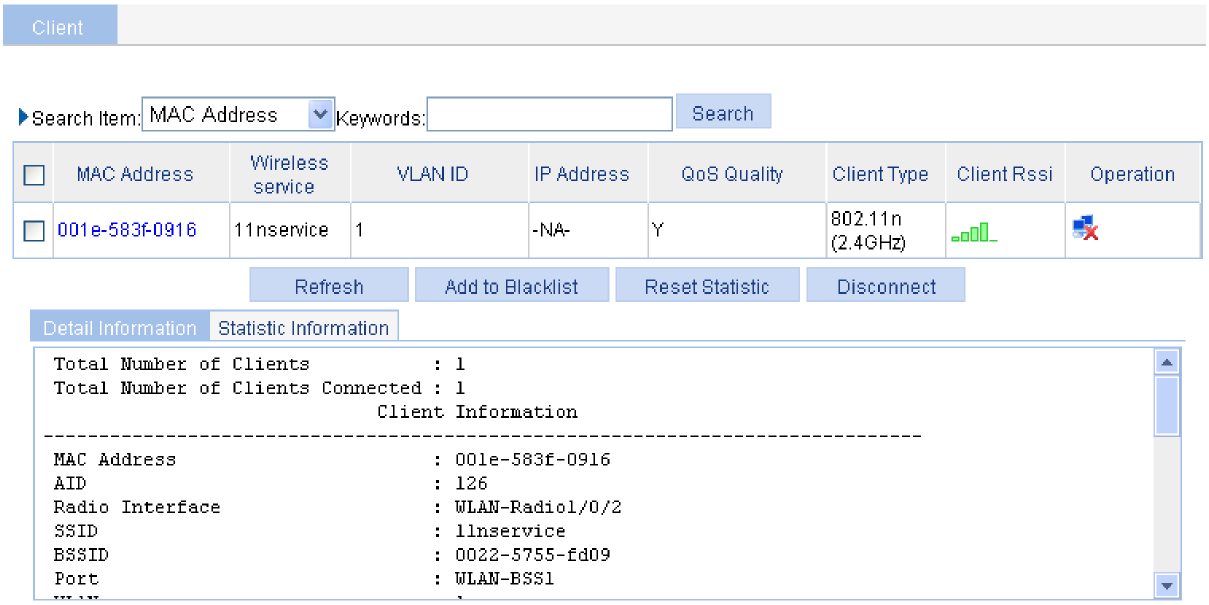


□	Radio Unit	Radio Mode	Status	Operation
□	1	802.11n(5GHz)	Enable	
□	2	802.11n(2.4GHz)	Enable	

Configuration verification

- Select **Summary** > **Client** from the navigation tree to enter the page displaying online clients, as shown in Figure 3-51.

Figure 3-51 View online clients



□	MAC Address	Wireless service	VLAN ID	IP Address	QoS Quality	Client Type	Client Rssi	Operation
□	001e-583f-0916	11nservice	1	-NA-	Y	802.11n (2.4GHz)	▂▄▆	✕

```
 Total Number of Clients           : 1
 Total Number of Clients Connected : 1
                              Client Information
--------------------------------------------------------------------------------
 MAC Address                       : 001e-583f-0916
 AID                               : 126
 Radio Interface                   : WLAN-Radio1/0/2
 SSID                              : 11nservice
 BSSID                             : 0022-5755-fd09
 Port                              : WLAN-BSS1
```

Configuration guidelines

When configuring 802.11n, note that:

- To modify the 802.11n radio setup and 802.11n rates, shut down the radio first.
- Select **Radio > Radio** from the navigation tree, select the AP to be configured, and click the corresponding icon to enter the radio configuration page, where you can modify the 802.11n-related parameters, including **Bandwidth Mode**, **A-MSDU**, **A-MPDU**, **Short GI**, and **Client 802.11n Only** (permitting only 802.11n users to access the wireless network).
- Make sure that 802.11n (2.4GHZ) is enabled.
- Select **Radio** > **Rate** from the navigation tree to modify the 802.11n rate.
- When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

4 WDS Configuration

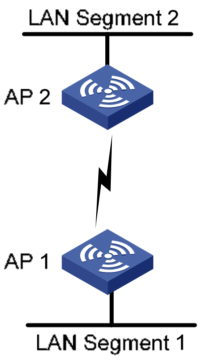
WDS Configuration Example

Network requirements

As shown in Figure 4-1:

- AP 1 and AP 2 are connected to different LAN segments.
- The WDS link between AP 1 and AP 2 is formed in 802.11n (2.4GHZ) radio mode.

Figure 4-1 Network diagram for WDS configuration



Configuration procedure

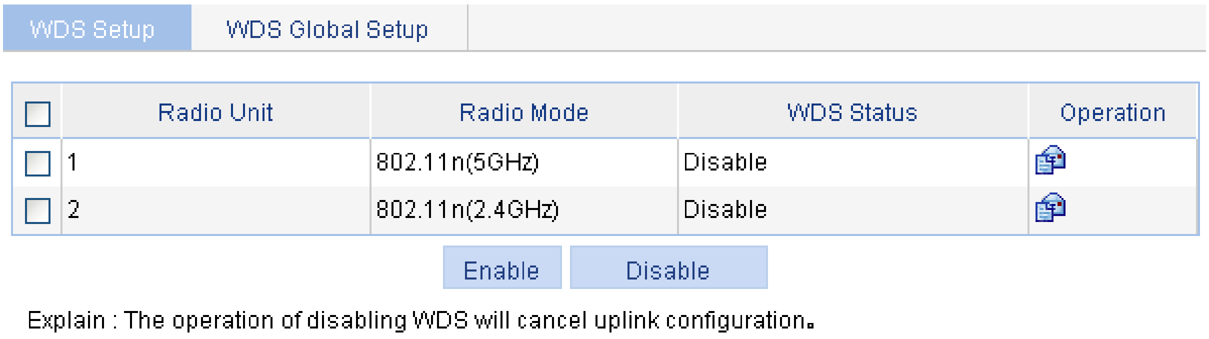
1) Select a correct country/region code

Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configure WDS

Select **Wireless Service** > **WDS** from the navigation tree to enter the **WDS Setup** page, as shown in Figure 4-2.

Figure 4-2 WDS setup page

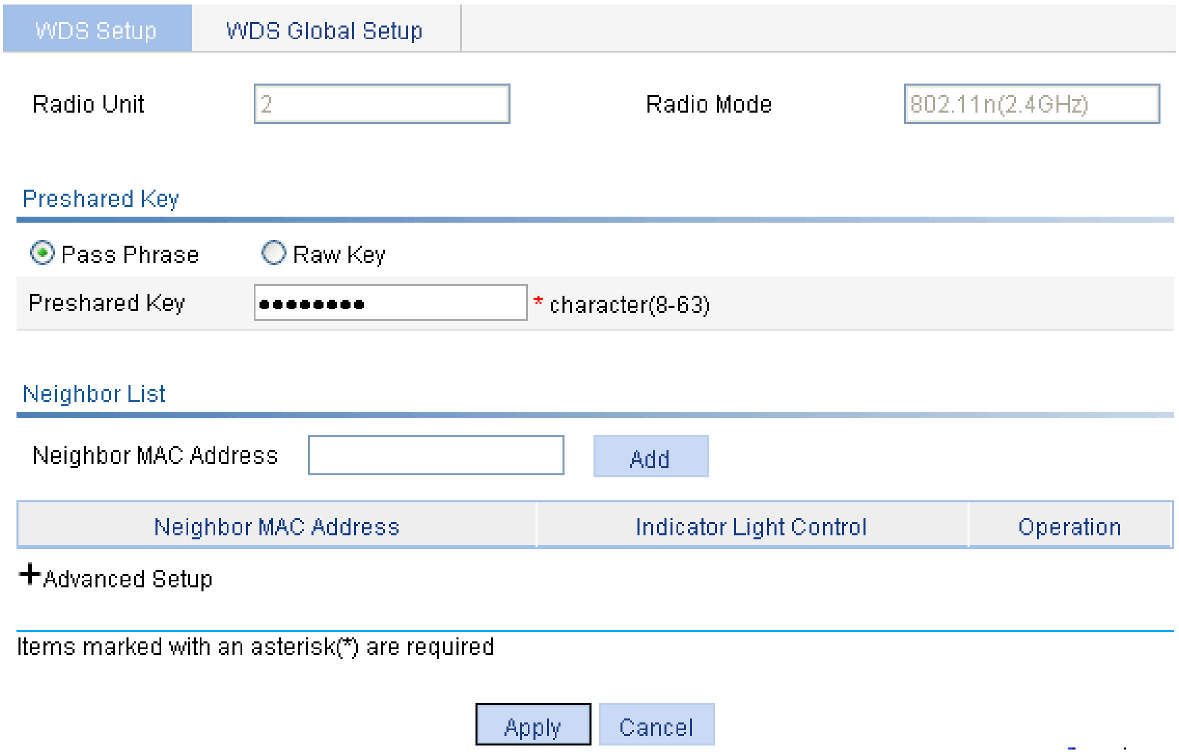


□	Radio Unit	Radio Mode	WDS Status	Operation
□	1	802.11n(5GHz)	Disable	📋
□	2	802.11n(2.4GHz)	Disable	📋

Explain : The operation of disabling WDS will cancel uplink configuration。

Find the radio unit to be configured in the list, and click the corresponding 📋 icon to enter the **WDS Setup** page shown in Figure 4-3.

Figure 4-3 WDS setup page



Radio Unit: 2
Radio Mode: 802.11n(2.4GHz)

Preshared Key

● Pass Phrase ○ Raw Key

Preshared Key: ●●●●●●●●● * character(8-63)

Neighbor List

Neighbor MAC Address:

Neighbor MAC Address	Indicator Light Control	Operation

+Advanced Setup

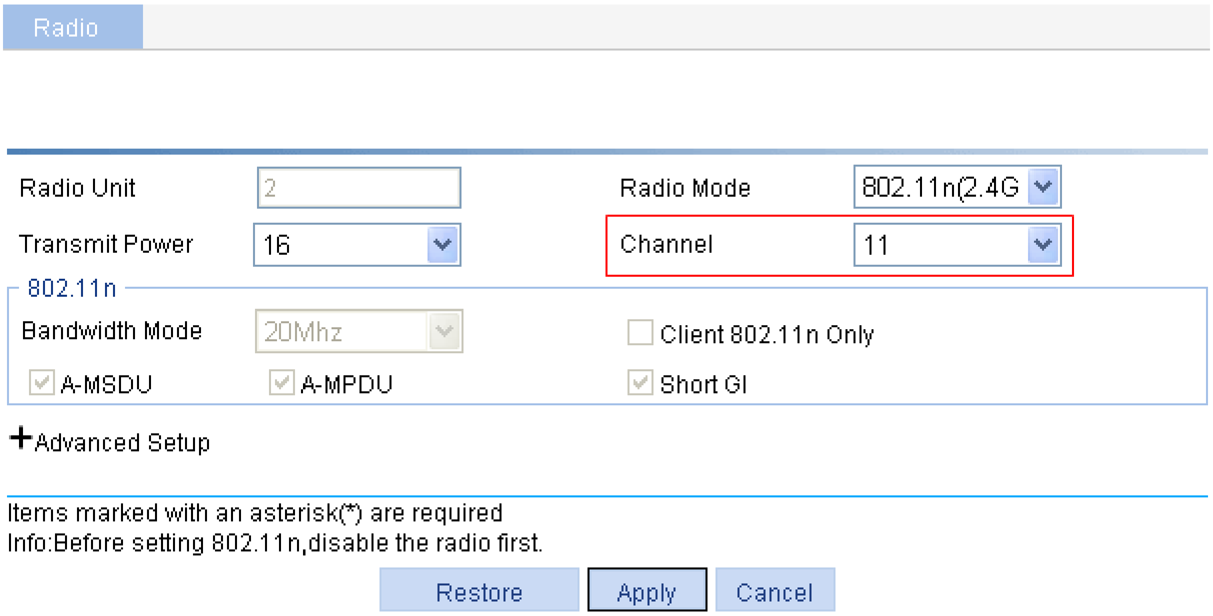
Items marked with an asterisk(*) are required

- Select the **Pass Phrase** check box, and input **12345678** in the **Preshared Key** input box.
- Do not set the neighbor MAC address, indicating that the AP can establish a WDS link with any other AP.
- Click **Apply**.

3) Configure the same working channel.

Select **Radio > Radio** from the navigation tree, select the radio unit to be configured in the list, and click the corresponding icon to enter the **Radio** page, as shown in Figure 4-4.

Figure 4-4 Configure the working channel



Radio Unit: 2
Radio Mode: 802.11n(2.4G
Transmit Power: 16
Channel: 11

802.11n

Bandwidth Mode: 20Mhz
□ Client 802.11n Only
☑ A-MSDU ☑ A-MPDU ☑ Short GI

+Advanced Setup

Items marked with an asterisk(*) are required
Info:Before setting 802.11n,disable the radio first.

Select the channel to be used from the **Channel** drop-down list.

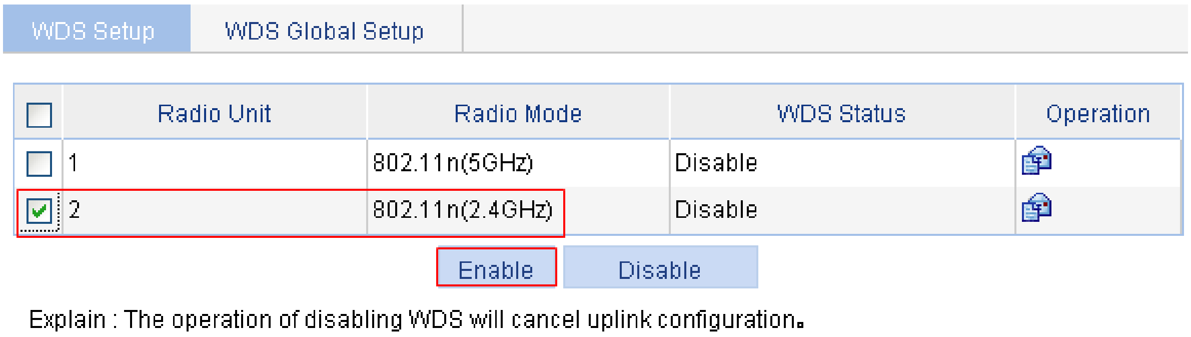
Enable 802.11n (2.4GHz) radio (By default, 802.11n (2.4GHZ) radio is enabled. Therefore, this step is optional.)

Select **Radio > Radio** from the navigation tree to enter the **Radio** page. Make sure that 802.11n (2.4GHz) is enabled.

4) Enable WDS

Select **Wireless Service** > **WDS** from the navigation tree to enter the **WDS Setup** page.

Figure 4-5 WDS setup page



□	Radio Unit	Radio Mode	WDS Status	Operation
□	1	802.11n(5GHz)	Disable	
☑	2	802.11n(2.4GHz)	Disable	

Explain : The operation of disabling WDS will cancel uplink configuration。

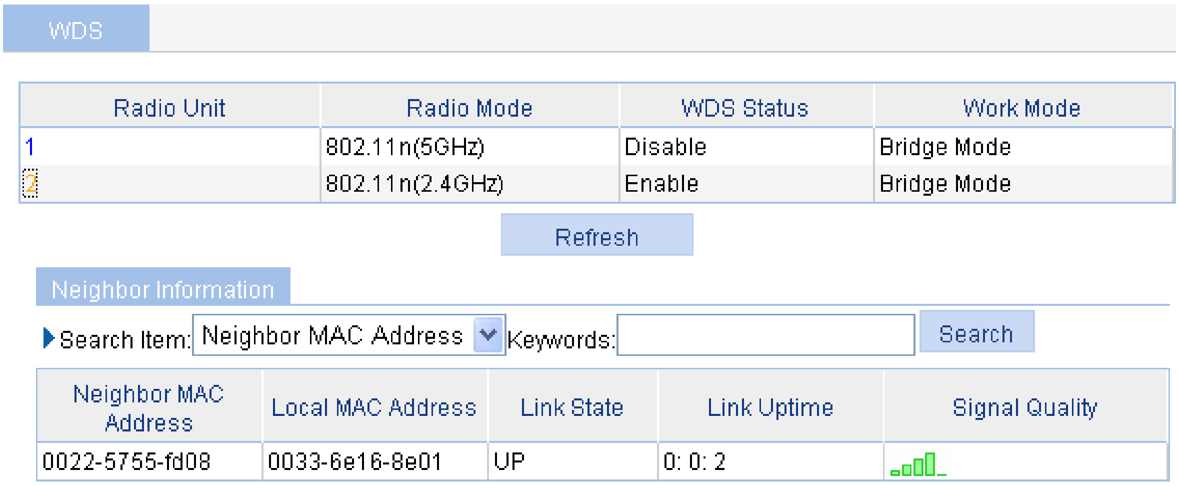
Select the checkbox corresponding to 802.11n (2.4GHz), and click **Enable**.

Configuration verification

- Check the WDS link status.

Select **Summary** > **WDS** from the navigation tree to enter the page displaying WDS information.

Figure 4-6 The page displaying WDS information



Radio Unit	Radio Mode	WDS Status	Work Mode
1	802.11n(5GHz)	Disable	Bridge Mode
2	802.11n(2.4GHz)	Enable	Bridge Mode

Search Item: Neighbor MAC Address

Neighbor MAC Address	Local MAC Address	Link State	Link Uptime	Signal Quality
0022-5755-fd08	0033-6e16-8e01	UP	0: 0: 2	

Configuration guidelines

- The output information of a WDS link includes: neighbor MAC address, local MAC address, link state, link uptime, and signal quality.
- When five green bars are displayed for the signal quality, the signal is of the highest quality; if yellow bars are displayed, the signal is weak. In this case, you should check whether the antennas in use match the current radio, whether the antennas are connected correctly, and whether the maximum power of the current radio is too low.
- When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

WDS Point-to-Multipoint Configuration Example

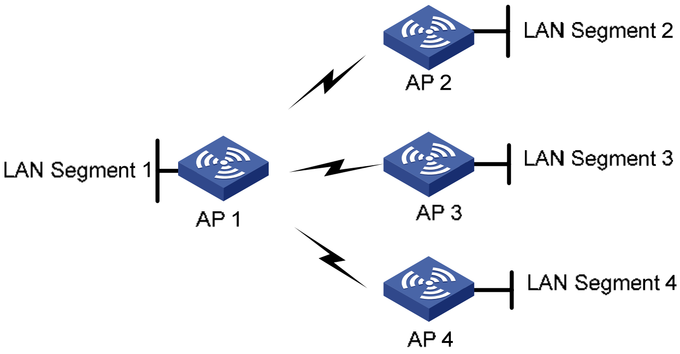
Network requirements

As shown in 0, it is required that AP 1 establish a WDS link with AP 2, AP 3, and AP 4 respectively.

The WDS configuration is the same as the normal WLAN WDS configuration. Note the following when configuring WDS:

- Configure a neighbor MAC address for each radio interface (otherwise, WDS links may be established between AP 2, AP 3 and AP 4).
- Set the maximum number of WDS links allowed. The default value is 2. It should be set to **3** for AP 1 in this example.

Figure 4-7 Network diagram for WDS configuration



Configuration procedure

WDS configuration is the same as normal WLAN WDS configuration. Refer to WDS Configuration Example for details.

Configuration verfication

Display WDS link status:

- It is displayed on the WDS link status page of AP 1 (which you can enter by selecting **Summary** > **WDS** from the navigation tree) that AP 1 has established a WDS link with AP 2, AP 3 and AP 4 respectively.
- It is displayed on the WDS link status page of AP 2, AP 3 and AP 4 (which you can enter by selecting **Summary** > **WDS**) that AP 2, AP 3 and AP 4 have respectively established a WDS link with AP 1.

Configuration guidelines

When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

5 Repeater Mode Configuration

Repeater Mode Configuration Example

Network Requirements

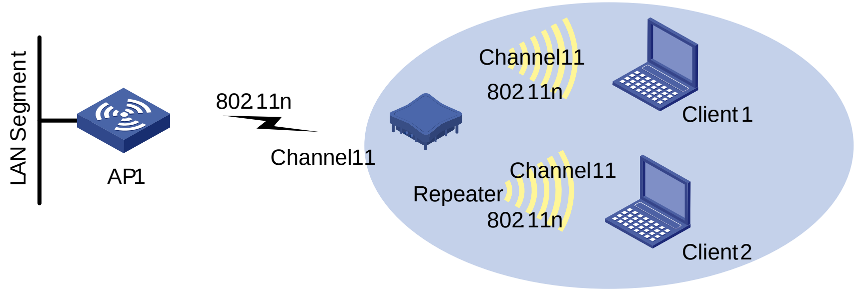
As shown in Figure 5-1:

AP1 connects to the wired network. The AP acting as a repeater needs to set up a WDS link with AP 1. At the same time, the repeater needs to provide wireless access service for clients.

To satisfy the requirements above:

- Use the 802.11n (2.4GHz) radio to set up a WDS link between AP 1 and the repeater.
- Use the 802.11n (2.4GHz) radio to connect clients to the repeater.
- The channel of the WDS link between AP 1 and the repeater must be the same as that of the access service. In this example, channel 11 in 802.11n (2.4GHz) radio mode is used as the working channel.
- Configure WDS on AP 1. For the detailed configuration procedure, refer to Configuration procedure.
- Configure WDS and access service on the repeater.

Figure 5-1 Network diagram for repeater mode configuration



Configuration procedure

Perform the following configurations on the repeater:

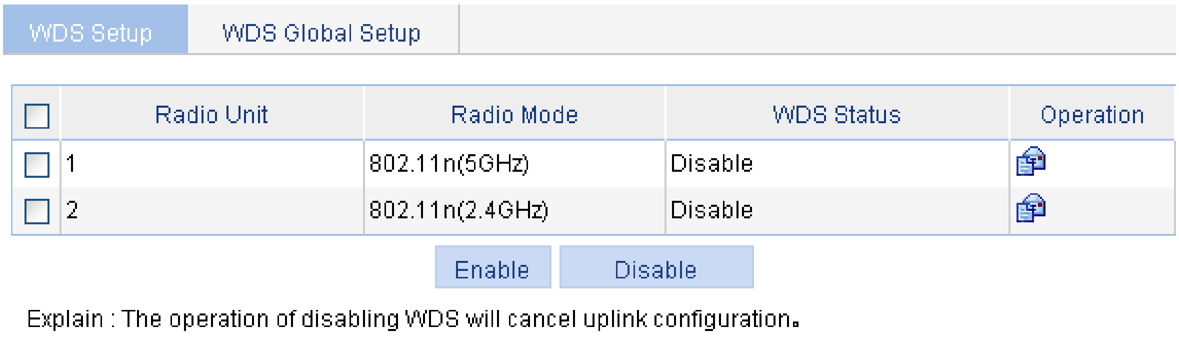
1) Select a correct country/region code

Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Configuring WDS

Select **Wireless Service** > **WDS** from the navigation tree to enter the **WDS Setup** page shown in Figure 5-2.

Figure 5-2 WDS setup page

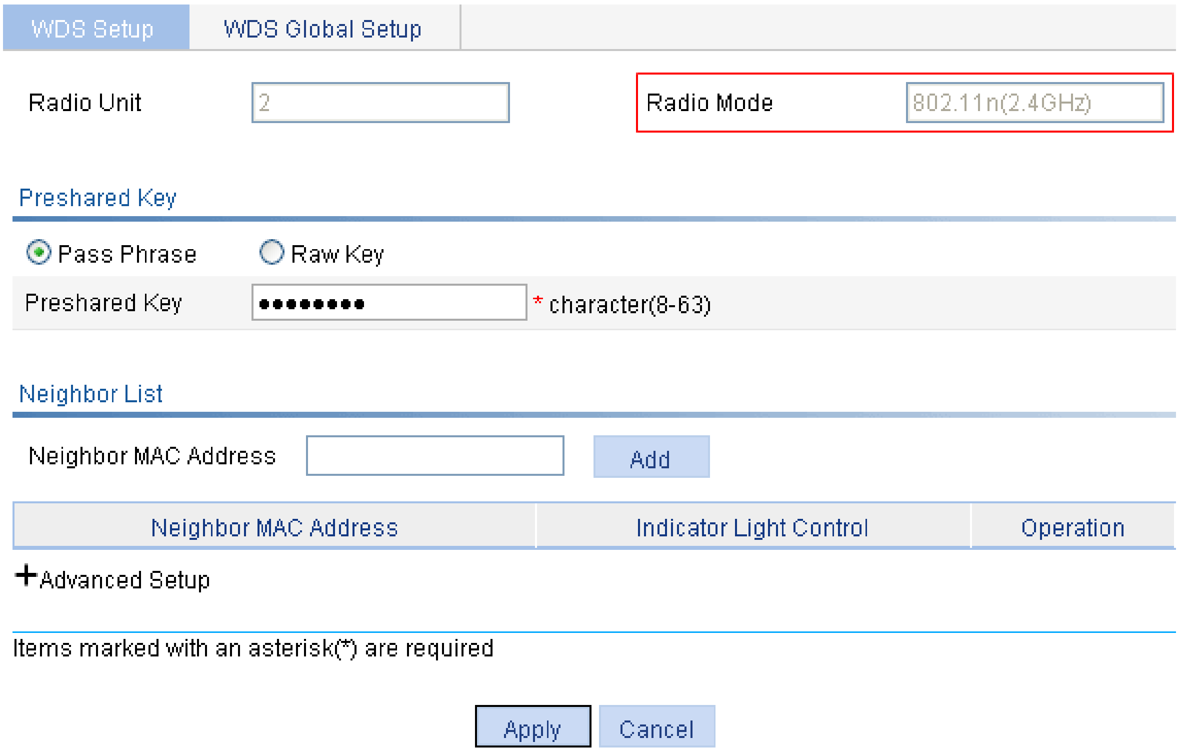


□	Radio Unit	Radio Mode	WDS Status	Operation
□	1	802.11n(5GHz)	Disable	
□	2	802.11n(2.4GHz)	Disable	

Explain : The operation of disabling WDS will cancel uplink configuration。

Select the 802.11n radio mode in the list and click the corresponding icon in the **Operation** column to enter the page shown in Figure 5-3.

Figure 5-3 WDS setup page



Radio Unit: 2

Radio Mode: 802.11n(2.4GHz)

Preshared Key

● Pass Phrase ○ Raw Key

Preshared Key: ●●●●●●●●● * character(8-63)

Neighbor List

Neighbor MAC Address:

Neighbor MAC Address	Indicator Light Control	Operation

Items marked with an asterisk(*) are required

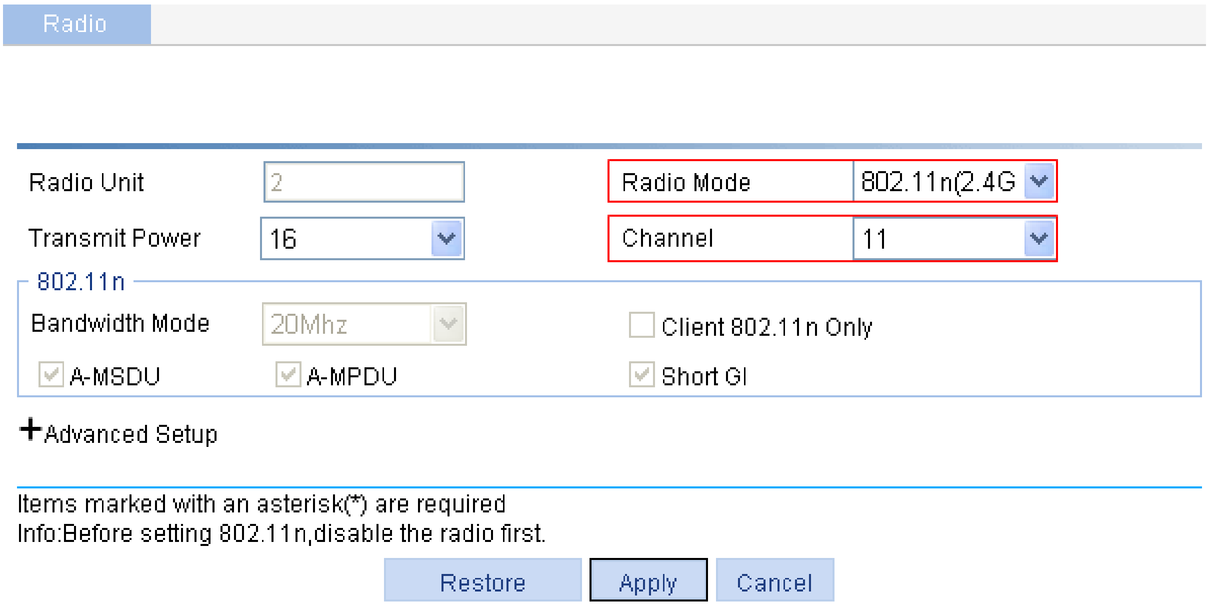
- Select the **Pass Phrase** option and input 12345678 in the **Preshared Key** text box.
- Click **Apply**.

3) Configuring the working channel

# Configure the working channel.

Select **Radio** > **Radio Setup** from the navigation tree, find the radio to be configured in the list, and click the corresponding icon to enter the page shown in Figure 5-4.

Figure 5-4 Configure the same channel



Radio Unit	2	Radio Mode	802.11n(2.4G
Transmit Power	16	Channel	11

802.11n

Bandwidth Mode 20Mhz

□ Client 802.11n Only

☑ A-MSDU ☑ A-MPDU ☑ Short GI

+Advanced Setup

Items marked with an asterisk(*) are required

Info:Before setting 802.11n,disable the radio first.

Select **11** in the **Channel** drop-down list.

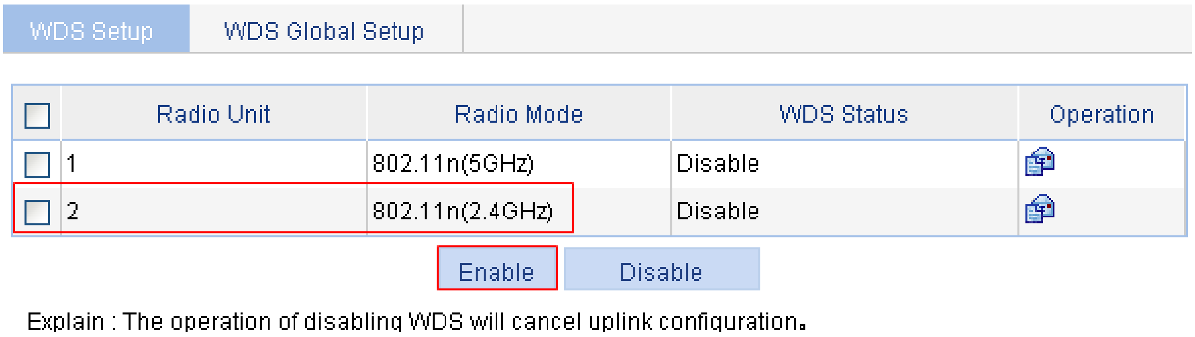
# Enable 802.11n (2.4GHz) radio. (By default, 802.11n (2.4GHZ) radio is enabled. Therefore, this step is optional.)

Select **Radio** > **Radio Setup** from the navigation tree to enter the **Radio Setup** page. Make sure that 802.11n (2.4GHz) is enabled.

4) Enabling WDS

Select **Wireless Service** > **WDS** from the navigation tree to enter the **WDS Setup** page shown in Figure 5-5.

Figure 5-5 WDS setup page



□	Radio Unit	Radio Mode	WDS Status	Operation
□	1	802.11n(5GHz)	Disable	📋
□	2	802.11n(2.4GHz)	Disable	📋

Explain : The operation of disabling WDS will cancel uplink configuration。

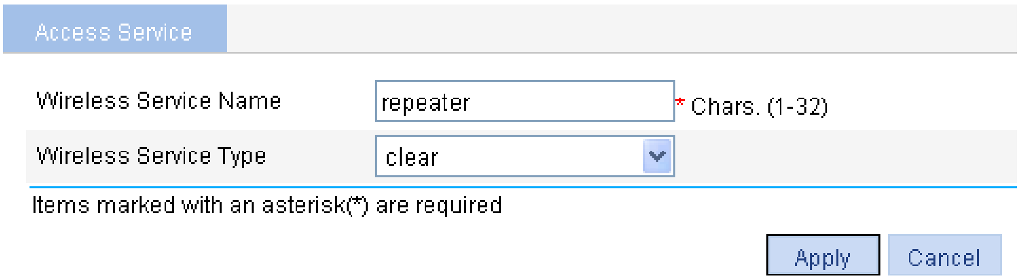
Select the check box corresponding to 802.11n (2.4GHz) and click **Enable**.

5) Configuring the access service

Note

For how to configure the access service on the repeater, refer to Wireless Service Configuration Example. You can strictly follow the steps in Wireless Service Configuration Example to configure the access service on the repeater.

Figure 5-6 Configure the access service



Access Service

Wireless Service Name	repeater * Chars. (1-32)
Wireless Service Type	clear

Items marked with an asterisk(*) are required

Note

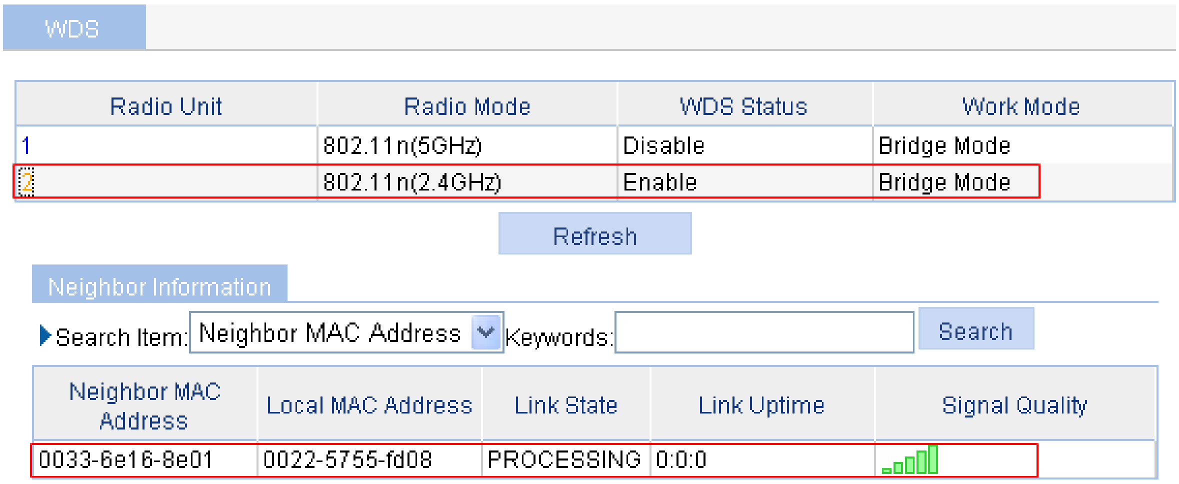
When configuring access service on the repeater, make sure that the radio mode of the repeater is the same as that of WDS.

Configuration verification

# Verify that the WDS link has been established for the repeater.

Select **Summary** > **WDS** from the navigation tree to enter the **WDS** page displaying the WDS information, as shown in Figure 5-7. Click radio unit 2 to see the neighbor information.

Figure 5-7 The page displaying WDS information



WDS

Radio Unit	Radio Mode	WDS Status	Work Mode
1	802.11n(5GHz)	Disable	Bridge Mode
2	802.11n(2.4GHz)	Enable	Bridge Mode

Neighbor Information

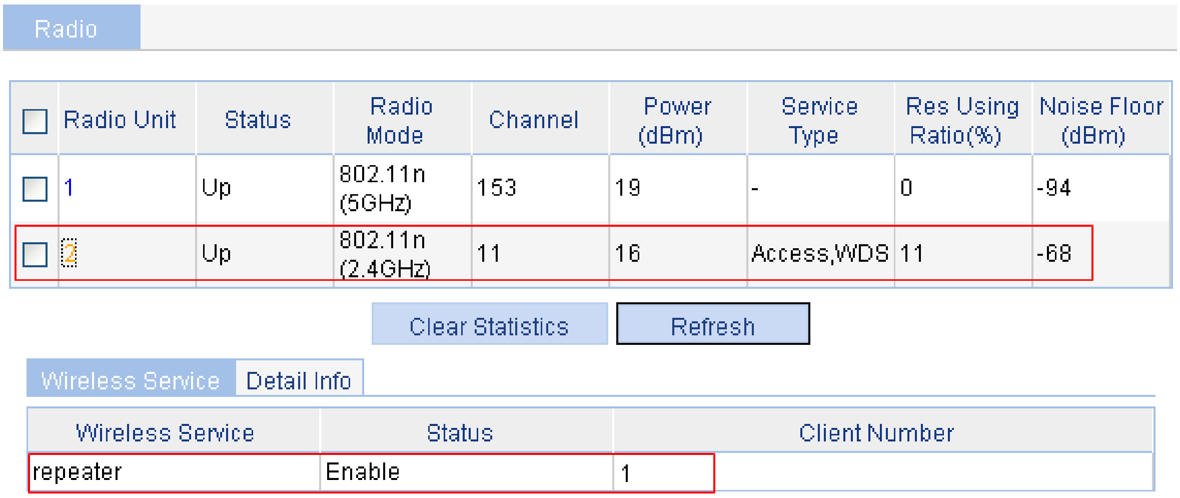
Search Item: Neighbor MAC Address Keywords:

Neighbor MAC Address	Local MAC Address	Link State	Link Uptime	Signal Quality
0033-6e16-8e01	0022-5755-fd08	PROCESSING	0:0:0	

# Verify that the repeater mode has been configured successfully.

Select **Summary** > **Radio** from the navigation tree, and the page displaying radio information appears, as shown in Figure 5-8. On the page, you can see that the 802.11n (2.4GHz) radio mode on the repeater provides both access and mesh services, and one user has accessed the wireless network through the repeater.

Figure 5-8 The page displaying radio information



□	Radio Unit	Status	Radio Mode	Channel	Power (dBm)	Service Type	Res Using Ratio(%)	Noise Floor (dBm)
□	1	Up	802.11n (5GHz)	153	19	-	0	-94
□	2	Up	802.11n (2.4GHz)	11	16	Access,WDS	11	-68

Wireless Service	Status	Client Number
repeater	Enable	1

Configuration guidelines

When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

6 Workgroup Bridge Mode Configuration

Workgroup Bridge Mode Configuration Example

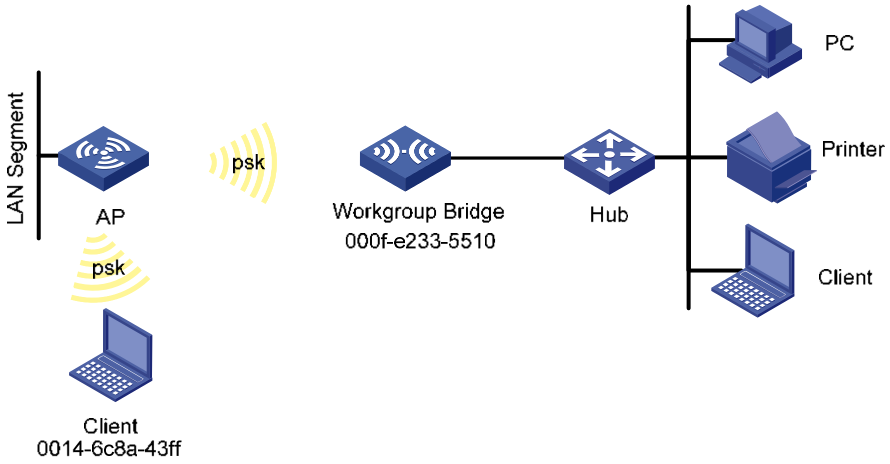
Network requirements

As shown in Figure 6-1, an AP working as a workgroup bridge accesses the wireless network as a client. The Ethernet interface of the workgroup bridge connects to multiple hosts or printers in the wired network, and thus the wired network is connected to the wireless network through the workgroup bridge.

The detailed requirements are as follows:

- The AP accesses the wired LAN, and the workgroup bridge with MAC address 000f-e2333-5510 accesses the AP as a client.
- The workgroup bridge accesses the wireless service **psk** by passing the RSN(CCMP)+PSK authentication.
- Client with MAC address 0014-6c8a-43ff also accesses the wireless service **psk**.

Figure 6-1 Network diagram for workgroup bridge mode configuration



Configuration procedure

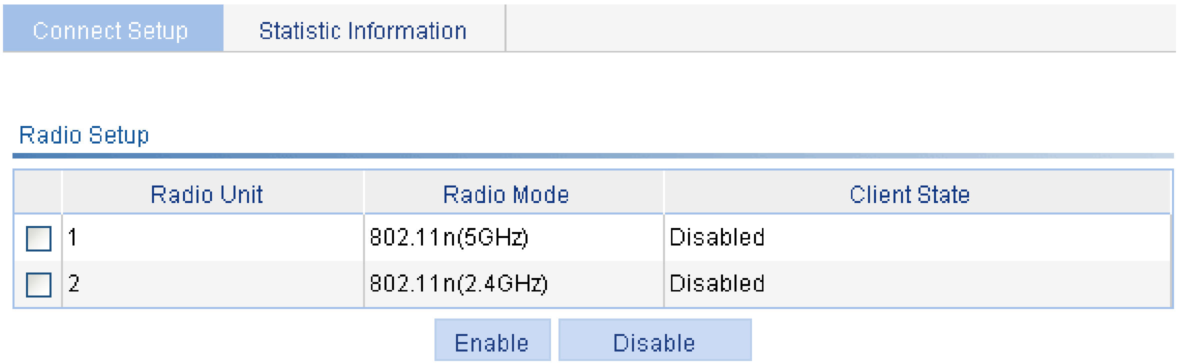
1) Select a correct country/region code

Select **Advanced** > **Country/Region Code** from the navigation tree to enter the page for setting a country/region code, as shown in Figure 3-2.

2) Enable the client mode

Select **Wireless Service** > **Client Mode** from the navigation tree and click **Connect Setup** to enter the page shown in 1).

Figure 6-2 Enable the client mode

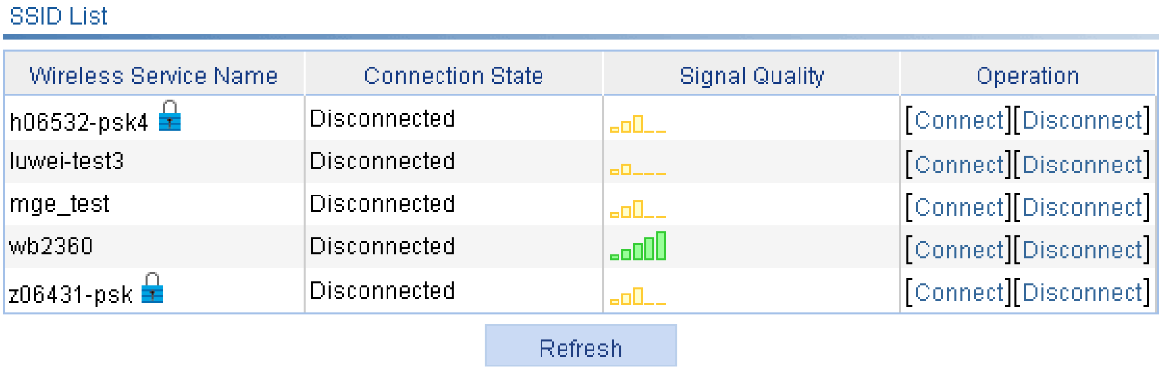


Radio Setup

□	Radio Unit	Radio Mode	Client State
□	1	802.11n(5GHz)	Disabled
□	2	802.11n(2.4GHz)	Disabled

Select the check box corresponding to 802.11n (2.4GHz) and click **Enable**. With the client mode enabled, you can check the existing wireless services in the wireless service list.

Figure 6-3 Check the wireless service list



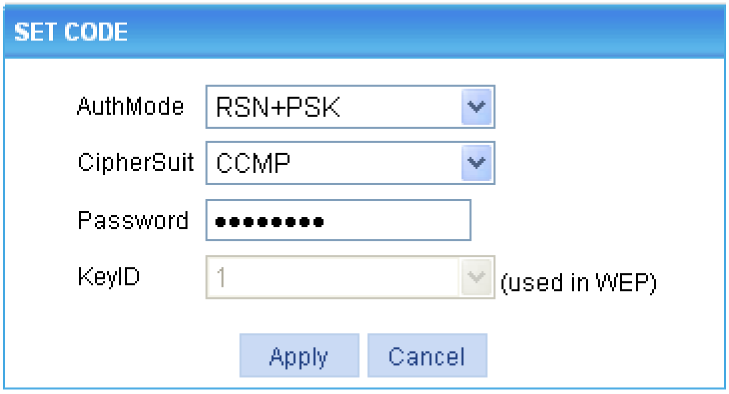
SSID List

Wireless Service Name	Connection State	Signal Quality	Operation
h06532-psk4	Disconnected		[Connect][Disconnect]
luwei-test3	Disconnected		[Connect][Disconnect]
mge_test	Disconnected		[Connect][Disconnect]
wb2360	Disconnected		[Connect][Disconnect]
z06431-psk	Disconnected		[Connect][Disconnect]

3) Connect the wireless service

Click the **Connect** icon of the wireless service **psk** in the wireless service list, and a **SET CODE** dialog box shown in Figure 6-4 appears.

Figure 6-4 SET CODE



SET CODE

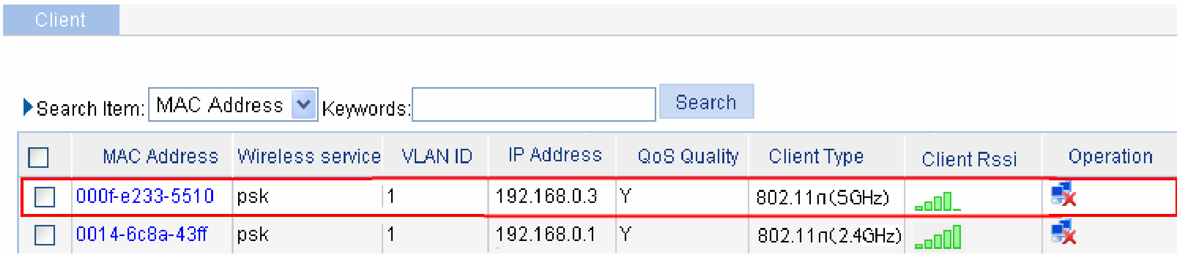
AuthMode	RSN+PSK
CipherSuit	CCMP
Password	●●●●●●●●●
KeyID	1 (used in WEP)

- Specify the **AuthMode** as **RSN+PSK**.
- Specify the **CipherSuite** as **CCMP**.
- Set the **Password** to that on the AP, **12345678**.
- Click **Apply**.

Configuration verification

On the AP shown in Figure 6-1, select **Summary** > **Client** from the navigation tree to enter the page shown in Figure 6-5, where you can check that the workgroup bridge is online.

Figure 6-5 Check that the workgroup bridge is online



Client

Search Item: MAC Address Keywords: Search

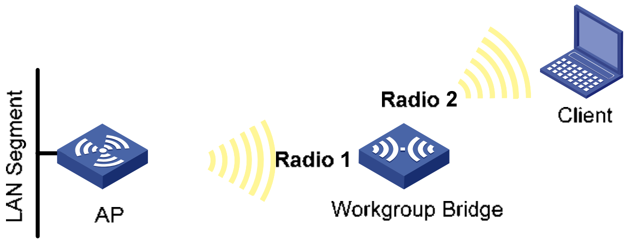
□	MAC Address	Wireless service	VLAN ID	IP Address	QoS Quality	Client Type	Client Rssi	Operation
□	000f-e233-5510	psk	1	192.168.0.3	Y	802.11n(5GHz)	▂▄▆	✕
□	0014-6c8a-43ff	psk	1	192.168.0.1	Y	802.11n(2.4GHz)	▂▄▆█	✕

- You can see that the client with MAC address 0014-6c8a-43ff and the workgroup bridge with MAC address 000f-e2333-5510 have been successfully associated with the AP.
- The wired devices on the right (such as printers and PCs) can access the wireless network through the workgroup bridge.

Configuration guidelines

- As shown in Figure 6-6, if the workgroup bridge uses two radio interfaces at the same time, the client connecting to radio 2 can access the AP through the workgroup bridge.

Figure 6-6 Network diagram for a workgroup bridge using two radio interfaces at the same time



- When satisfied with the configuration Save Configuration to File to ensure it is not lost when the Access Point restarts.

7 Save Configuration over reboot

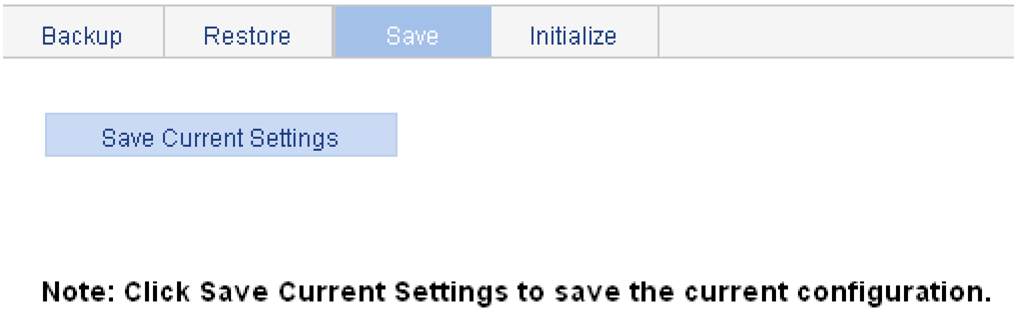
Save Configuration to File

To avoid losing the applied configuration changes when the Access Point reboots:

Select **Device**> **Configuration** from the navigation tree, and then click the **Save** tab to enter the save configuration confirmation page, as shown in Figure 7-1.

- Click the **Save Current Settings** button to save the current configuration to the configuration file.

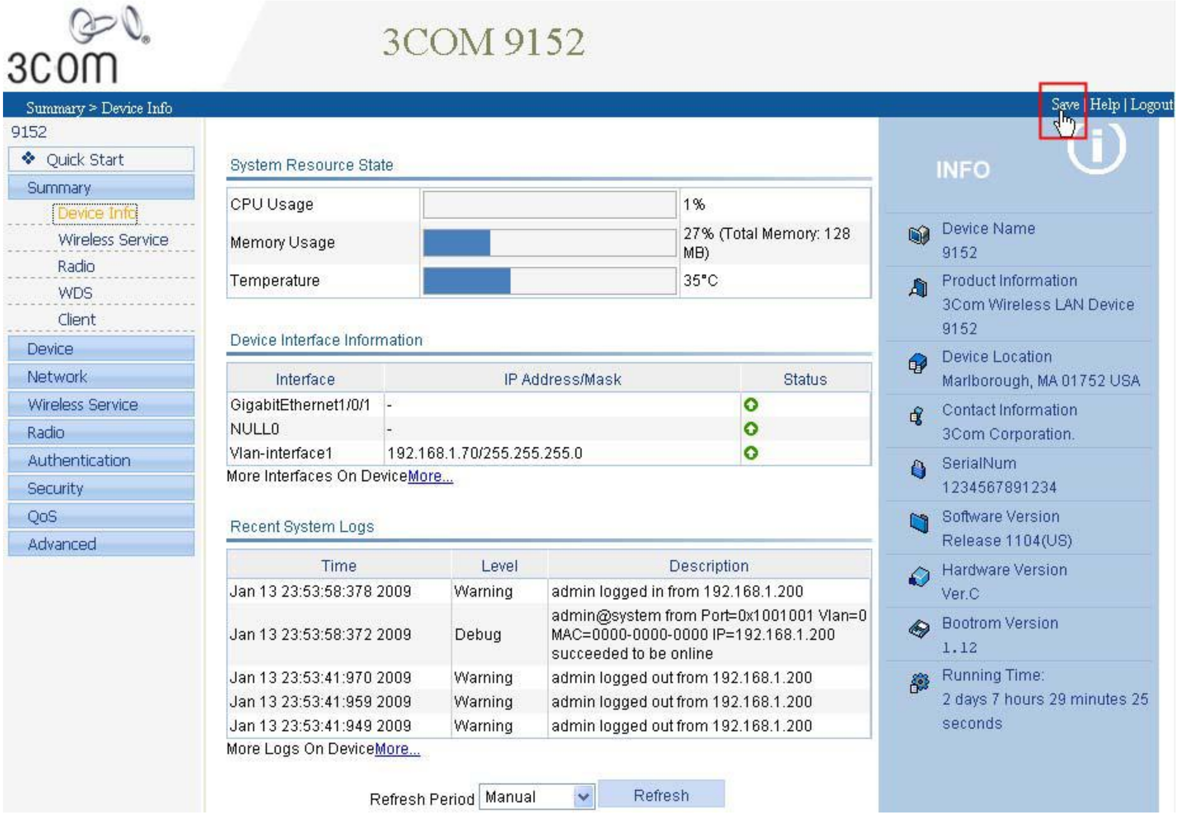
Figure 7-1 Save configuration confirmation



Note: Click Save Current Settings to save the current configuration.

- Or Click the **Save** button on the right f the title area to save the current configuration to the configuration file.

Figure 7-2 Save configuration confirmation



System Resource State

CPU Usage		1%
Memory Usage		27% (Total Memory: 128 MB)
Temperature		35°C

Device Interface Information

Interface	IP Address/Mask	Status
GigabitEthernet1/0/1	-	○
NULL0	-	○
Vlan-interface1	192.168.1.70/255.255.255.0	○

More Interfaces On DeviceMore...

Recent System Logs

Time	Level	Description
Jan 13 23:53:58:378 2009	Warning	admin logged in from 192.168.1.200
Jan 13 23:53:58:372 2009	Debug	admin@system from Port=0x1001001 Vlan=0 MAC=0000-0000-0000 IP=192.168.1.200 succeeded to be online
Jan 13 23:53:41:970 2009	Warning	admin logged out from 192.168.1.200
Jan 13 23:53:41:959 2009	Warning	admin logged out from 192.168.1.200
Jan 13 23:53:41:949 2009	Warning	admin logged out from 192.168.1.200

More Logs On DeviceMore...

Refresh Period Manual Refresh

Device Name
9152

Product Information
3Com Wireless LAN Device 9152

Device Location
Marlborough, MA 01752 USA

Contact Information
3Com Corporation.

SerialNum
1234567891234

Software Version
Release 1104(US)

Hardware Version
Ver.C

Bootrom Version
1.12

Running Time:
2 days 7 hours 29 minutes 25 seconds

The configuration from the last saved current settings will be installed from the configuration file (**.cfg** file or **.xml** file) at the next startup. Any settings applied but not saved to the configuration file will be lost when the Access Point next restarts.

Note

- Saving the configuration takes a period of time.
- The system does not support the operation of saving configuration of two or more consecutive users. If such a case occurs, the system prompts the latter users to try later.