ADMINISTRATION GUIDE

Cisco Small Business

AP541N Dual-band Single-radio Access Point

OL-20285-01

Contents

1

Getting Started

The Cisco AP541N Dual-band Single-radio Access Point is an advanced, standards-based solution for wireless networking in businesses of any size. The access point enables wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The access point operates in Standalone Mode. In Standalone Mode, the access point acts as an individual access point in the network, and you manage it by using the *Access Point Configuration Utility*, or SNMP.

This document describes how to perform the setup, management, and maintenance of the access point in Standalone Mode. Before you power on a new access point, review the following sections to check required hardware and software components, client configurations, and compatibility issues. Make sure you have everything you need for a successful launch and test of your new or extended wireless network.

This chapter contains the following topics:

- **Administrator Computer Requirements**
- **Connecting the Access Point to a PC**
- **Troubleshooting Your Connection**
- **Configuring the Access Point by using the Getting Started Page**
- **Verifying the Installation**
- **Configuring Security on the Wireless Access Point**

To manage the access point by using the Web interface, the access point needs an IP address. If you use VLANs or IEEE 802.1X Authentication (port security) on your network, you might need to configure additional settings on the access point before it can connect to the network.

NOTE The WLAN AP is not designed to function as a gateway to the Internet. To connect your WLAN to other LANs or the Internet, you need a gateway device.

Administrator Computer Requirements

Table 1 describes the minimum requirements for the personal computer for the initial configuration and administration of the access point through a *Access Point Configuration Utility*.

Table 1 Requirements for Configuration

Required Software or Component	Description
Ethernet Connection to the Access Point	The computer used to configure the access point must be connected to the access point by an Ethernet cable. The IP address must be on the same subnet as the access point. The subnet mask must match the subnet mask of the access point. The **Administration PC IP Address** section describes the procedure for changing these parameters on a PC running Windows.
Web Browser and Operating System	The following Web browsers can be used to display the access point Configuration Utility Web pages: ▪ Microsoft® Internet Explorer® version 6.x or 7.x (with up-to-date patch level for either major version) and Mozilla Firefox 3.x on Microsoft Windows® XP or Microsoft Windows 2000 ▪ Mozilla Firefox 3.x on Redhat® Linux® version 2.4 or later The Web browser must have JavaScript™ enabled to support the interactive features of the Configuration Utility interface.
Security Settings	Ensure that security is disabled on the wireless client used initially to configure the access point. Once the device has been configured, security can be enabled.

Administration PC IP Address

We recommend that if you are starting from the default configuration or this is the first time the device will be configured that you configure the device before you deploy it in the network by using the access point default static IP address (*192.168.10.10*). To do so, the PC IP address must be on the same subnet as the access point.

Verify that your PC IP address is set to an address on the same subnet as the access point:

STEP 1 From the Windows **Start** menu, choose **Settings** > **Control Panel**.

STEP 2 On the Control Panel dialog box, click **Network**.

STEP 3 In the Network dialog box select **TCP/IP** for your PC Ethernet card, then click **Properties**.

STEP 4 In the IP Address window, click **Specify an IP address**.

STEP 5 In the IP Address field, enter an IP address that is in the same subnet as the access point IP address. (The default access point IP address is *192.168.10.10*. The default subnet mask is **255.255.255.0**.) For example, you can set the:

PC IP address to *192.168.10.250*
PC IP subnet mask to *255.255.255.0*

STEP 6 In the Subnet Mask field, type **255.255.255.0**.

STEP 7 Click **OK**.

STEP 8 If you are prompted to restart your PC, click **Yes**.

Connecting the Access Point to a PC

To configure the access point, you can connect the access point directly to an administration PC or through the network to an administration PC.

If you are not using CCA to configure the access point, we recommend that you configure the device before deploying it in the network by following the instructions in the **"Connect the Access Point to an Administration PC"** section. Otherwise, follow the instructions in the **"Connecting the Access Point to the PC through a Network Connection"**

Connect the Access Point to an Administration PC

You can connect the access point to a administration PC directly or through the network. We recommend that you connect the access point directly to the PC unless you are using CCA to configure the access point.

Connecting the Access Point to the PC by using a Direct Cable Connection

To connect the access point to an administration PC, use a direct-cable connection:

STEP 1 Connect one end of an Ethernet straight-through or crossover cable to the network port on the access point, as shown in **Figure 1**.

STEP 2 Connect the other end of the cable to the Ethernet port on the PC.

Figure 1 Connecting the Access Point Using a Direct-Cable Connection

If you use this method, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to the PC but instead is connected to the LAN (either by using a hub or a switch).

STEP 3 Connect the power adapter to the power port on the back of the access point.

STEP 4 Plug the other end of the power cord into a power outlet.

STEP 5 Configure the access point by following the instructions in the **"Display the Configuration Utility By Using the Default IP Address"** section.

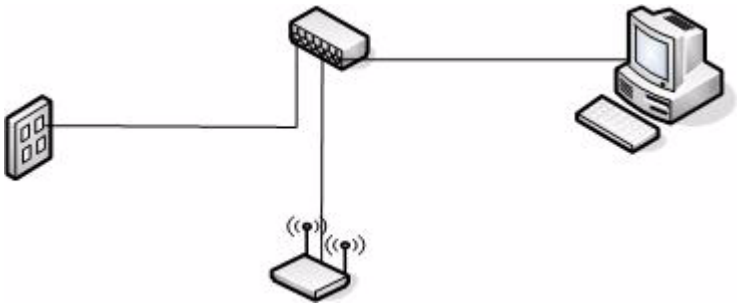
Connecting the Access Point to the PC through a Network Connection

To connect the access point to an administration PC through the network:

STEP 1 Connect one end of an Ethernet straight-through or crossover cable to the network port on the access point, as shown in **Figure 2**.

STEP 2 Connect the other end to the same hub or switch where your PC is connected.

Figure 2 Connecting the Access Point Using a LAN Connection



The hub or switch you use must permit broadcast signals from the access point to reach the other devices on the network.

STEP 3 If you are not using PoE, connect the power adapter to the power port on the back of the access point, then plug the other end of the power cord into a power outlet.

Launching the Access Point Configuration Utility

This section contains information for the for launching the *Access Point Configuration Utility*:

- Using the default static IP address of the switch. Follow the instructions in the **"Display the Configuration Utility By Using the Default IP Address"** section.
- Using Cisco Configuration Assistant (CCA). Follow the instructions in the **"Display the Configuration Utility by Using Cisco Configuration Assistant 2.1 or higher"** section.
- Using the an IP address assigned to the switch through DHCP. Follow the instructions in the **"Display the Configuration Utility by Using Another IP Address"** section.

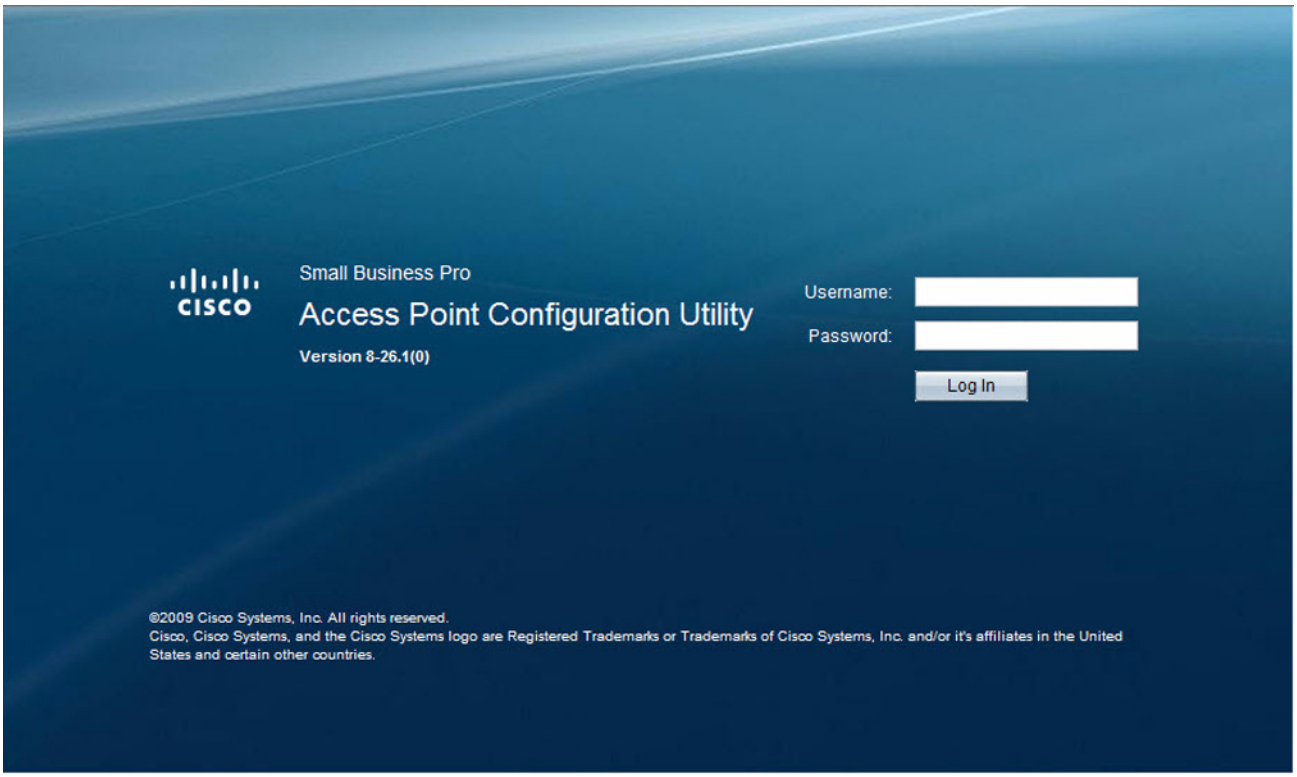
Display the Configuration Utility By Using the Default IP Address

To access the *Access Point Configuration Utility*, enter the default static IP address of the access point into a Web browser, do the following:

STEP 1 Enter the Cisco AP541N default static IP address in the address bar and press **Enter**. For example, **http://***192.168.10.10*.

The **Login** window displays, as shown in **Figure 3**.

Figure 3 Login Window

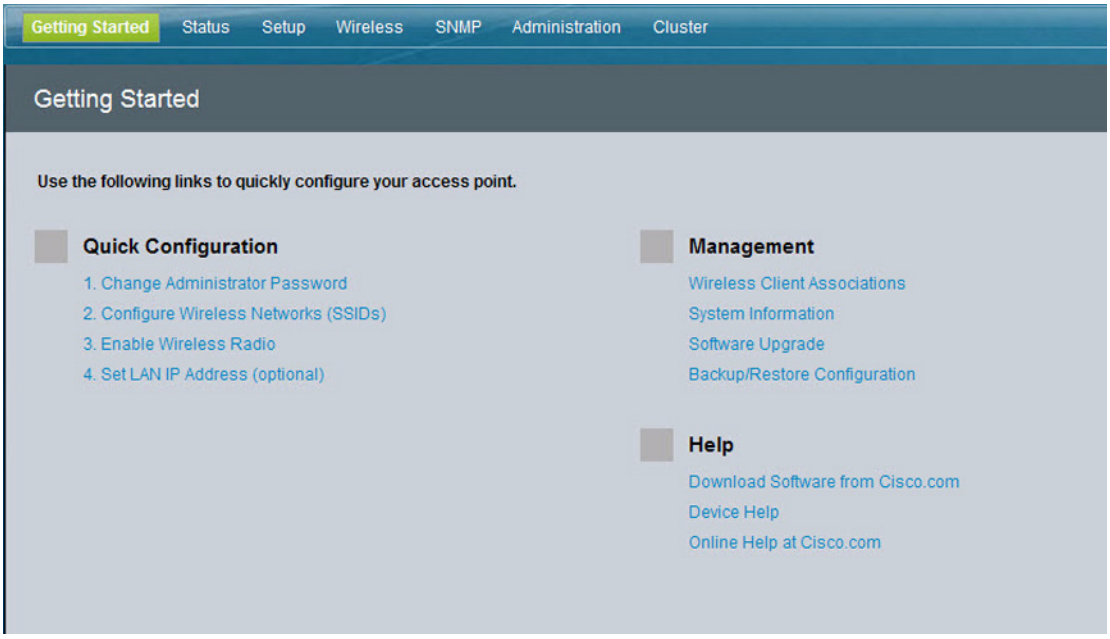


STEP 2 Enter the login information:

Username = **cisco**
Default password `cisco`. (Passwords are case sensitive.)

When you log in, the **Getting Started** page for the access point Configuration Utility is displayed, as shown in **Figure 4**.

Figure 4 Getting Started Page



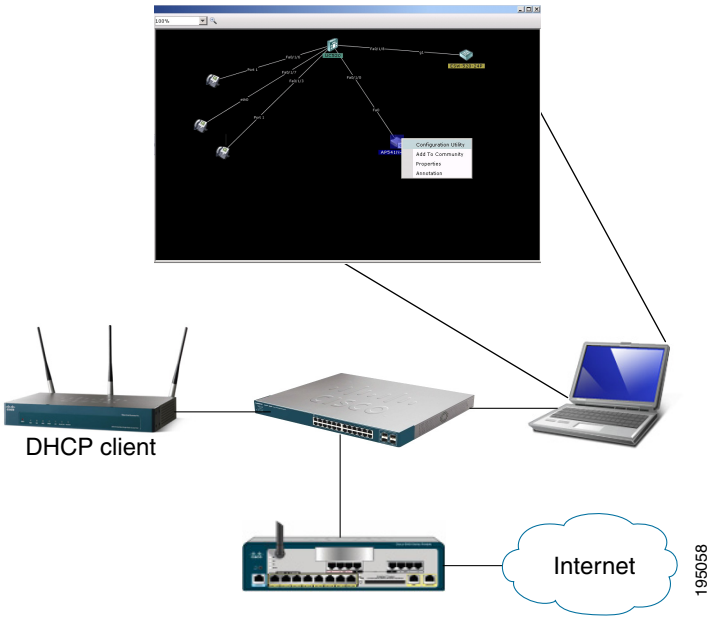
STEP 3 Update the Cisco AP541N software with the latest version by clicking the **Software Upgrade** link, as shown in **Figure 4**.

Next, we recommend that you:

- Change the password by clicking **Change Administrator Password**.
- Configure the SSID and enable wireless security, by clicking **Configure Wireless Networks (SSIDs)**.
- Enable the wireless radio, by clicking **Enable Wireless Radio**.
- Assign a new static IP address to the access point if your network devices are configured with static IP addresses, by clicking **Set LAN IP Address**.

Display the Configuration Utility by Using Cisco Configuration Assistant 2.1 or higher

Use Cisco Configuration Assistant 2.1 or higher (CCA) to configure the access point when it is deployed in a Cisco Smart Business Communications System (SBCS) network with a UC520 or SR520.



This procedure assumes you are familiar with CCA. You can find additional information about CCA at **http://www.cisco.com/en/US/products/ps7287/tsd_products_support_series_home.html**

To configure the access point by using CCA:

STEP 1 Connect the Ethernet port on the access point to a switch port on a SBCS device.

STEP 2 Power on the Cisco AP541N.

STEP 3 Connect a PC with CCA installed to any access switch port on the UC520 or SR520.

STEP 4 Create a new CCA site by entering a name and the IP address of the UC520 or SR520.

STEP 5 Connect to the CCA site by using the appropriate login credentials.

STEP 6 Click **Window** > **Topology View**.

When you have connected to the CCA site and the devices have been discovered, the Topology Map includes the Cisco AP541N.

NOTE Non-Cisco devices connected to the switch are not shown in the Topology map.

STEP 7 **Right-click** the access point to display the options: Configuration Utility, Properties, and Annotation.

STEP 8 Click **Configuration Utility.**

The *Access Point Configuration Utility* displays in a new window, as shown in **Figure 4**.

Next, we recommend that you:

- Change the password by clicking **Change Administrator Password**.
- Configure the SSID and enable wireless security, by clicking **Configure Wireless Networks (SSIDs)**.
- Enable the wireless radio, by clicking **Enable Wireless Radio**.
- Assign a new static IP address to the access point if your network devices are configured with static IP addresses, by clicking **Set LAN IP Address**.

Display the Configuration Utility by Using Another IP Address

You can display the *Access Point Configuration Utility* by using an IP address assigned to the access point during a previous configuration or by a DHCP server.

When you power on the access point, the built-in DHCP client searches for a DHCP server on the network to obtain an IP address and other network information. If the access point does not find a DHCP server on the network, the access point uses its default static IP address (`192.168.10.10`) unless you have assigned it a static IP address (and specified a static IP addressing policy) or until the access point successfully receives network information from a DHCP server.

CAUTION If the access point IP address is changed, either by a DHCP server or manually, your link to the access point will be lost and you must enter the new IP address to use the *Access Point Configuration Utility*.

To configure the access point by using an IP address other than the default static IP address:

STEP 1 Power on the Cisco AP541N.

STEP 2 If you used a DHCP server on your network to automatically configure network information for the access point, enter the IP address assigned to the access point by the DHCP server into the Web browser.

If you have access to the DHCP server on your network and know the MAC address of your access point, you can view the new IP address associated with the MAC address of the access point. Otherwise, we recommend that you disconnect the access point from the network, reset it to the default configuration by using the procedure in the **"Resetting the Device by using the Reset Button"** section, and configuring the device by using the procedure in the **"Display the Configuration Utility By Using the Default IP Address"** section.

If you replaced the default static IP address with a new static IP address, enter the new IP address of the access point into the Web browser

The **Login** window displays, as shown in **Figure 3**.

STEP 3 Enter the login information:

Username is **cisco**
Default password is `cisco` (passwords are case sensitive)

When you log in, the **Getting Started** page for the access point Configuration Utility is displayed, as shown in **Figure 4**.

STEP 4 Update the Cisco AP541N software with the latest version by clicking the **Software Upgrade** link, as shown in **Figure 4**.

Next, we recommend that you:

- Change the password by clicking **Change Administrator Password**.
- Configure the SSID and enable wireless security, by clicking **Configure Wireless Networks (SSIDs)**.
- Enable the wireless radio, by clicking **Enable Wireless Radio**.
- Assign a new static IP address to the access point if your network devices are configured with static IP addresses, by clicking **Set LAN IP Address**.

CAUTION If you do not have a DHCP server on your internal network, and do not plan to use one, we recommend assigning a new static IP address so that if you bring up another WLAN Cisco AP541N on the same network, the IP address for each access point is unique. If the IP address is not unique, a conflict results causing unpredictable results.

To change the connection type and assign a static IP address by using the *Access Point Configuration Utility*, see **LAN Settings, page 35**.

Troubleshooting Your Connection

If you cannot display the login window, you can test the IP address by using the **ping** command. If you do not know the IP address, you can configure the device by resetting the device to the factory defaults and accessing the *Access Point Configuration Utility* by using the factory default static IP address.

Using the Ping Command to Test the Connection

If you cannot display the configuration utility, you can test the ability of the PC to communicate with the access point by using **ping**. To use **ping** on a PC running Windows:

STEP 1 Verify that the Cisco AP541N is powered on and the LEDs indicate the appropriate links.

STEP 2 Open a command window by using **Start** > **Run** and enter **cmd**.

STEP 3 At the **Command** window prompt enter **ping** and the *access point IP address*. For example **ping** *192.168.10.10* (the default static IP address of the access point).

If successful, you should get a reply similar to the following:

```
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
```

If it fails, likely you are using the wrong access point IP address and you will get a reply similar to the following:

```
Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
```

Possible Cause of Failure

The most likely cause of connectivity failure is an incorrect IP address.

The Web browser is pointed to the wrong IP address. Or, your PC might be configured with an IP address that is not in the same subnet as the access point.

DHCP is enabled on the Cisco AP541N by default. When a DHCP server is enabled on your network and the access point is connected to the network, the DHCP server replaces the default static IP address with a DHCP server–assigned IP address. If this happens before you display the *Access Point Configuration Utility* window, you must use the assigned IP address to display the utility. If this happens during configuration, the *Access Point Configuration Utility* will lose connectivity.

You can query the DHCP server for the new IP address or disconnect the access point from the network and reset the device to use the static default access point IP address by using the **Resetting the Access Point to the Factory Default Configuration, page 114** procedure.

Resetting the Device by using the Reset Button

To use the **Reset** button to reboot or reset the access point, do the following:

- To **reboot** the access point, press the **Reset** button. Do not hold it for more than 10 seconds.
- To **restore** the access point to the factory default settings:

  1. Disconnect the access point from the network or disable all DHCP servers on your network.

  2. With the power on, press-and-hold the **Reset** button for more than 10 seconds.

Configuring the Access Point by using the Getting Started Page

From the **Getting Started** page, you can use the following links to quickly configure your access point:

- **Access Point Configuration**
- **Access Point Management Page**
- **Wireless Configuration Page**

Access Point Configuration

To change the access point IP address, password, and VLAN configuration, do the following:

STEP 1 Click **Change Administrator Password** to provide a new administration password for the access point. (The username is **cisco** and it cannot be changed. The default password is *cisco*.)

STEP 2 If you do not have a DHCP server on the network and do not plan to use one, click Change IP Address to change the connection type from DHCP to static IP and set a static IP address and subnet mask.

NOTE We recommend that you assign a new static IP address. Otherwise, if you bring up another Cisco AP541N on the same network, the IP address for each access point will not be unique; duplicating an IP address on a network will create a conflict.

Also, if you change the static IP address, you will lose connectivity. To reestablish connectivity, enter the new IP address into your Web browser and log into the Configuration Utility.

To change the connection type and assign a static IP address, see **LAN Settings, page 35**.

STEP 3 If your network uses VLANs, you might need to configure the management VLAN ID or untagged VLAN ID on the access point for it to work with your network.

For information about how to configure VLAN information, see **LAN Settings, page 35**.

STEP 4 If your network uses Dynamic WEP port security for network access control, you must configure the 802.1X supplicant information on the access point. For information about how to configure the 802.1X user name and password, see **Configuring 802.1X Authentication, page 38**.

Access Point Management Page

Click **System Information** to view the device information. For more information, see **Device Information, page 22**.

As new versions of the Access Point software become available, you can upgrade the software on your devices to take advantage of new features and enhancements. For more information, see **Software Upgrade, page 117**.

For information on how to backup and restore the configuration, go to **Access Point Configuration, page 113**.

Wireless Configuration Page

For information about the wireless radio settings, see **Configuring Wireless Radio Settings, page 153**.

To configure the SSID, Guest Access, and Security Configuration, see **Modifying Virtual Access Point Settings, page 50**.

Wireless Client Requirements

The access point provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running. The access point supports multiple client operating systems. Clients can be laptop or desktop computers, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

To connect to the access point, wireless clients need the software and hardware described in **Table 2**.

Table 2 Requirements for Wireless Clients

Required Component	Description
Wi-Fi Client Adapter	Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11n modes are supported.)
Wireless Client Software	Client software, such as Microsoft Windows Supplicant, configured to associate with the access point.
Client Security Settings	Security should be disabled on the client used to do initial configuration of the access point. If the Security mode on the access point is set to anything other than plain text, wireless clients must have a profile set to the same authentication mode used by the access point and provide a valid username and password, certificate, or user identity required by the authentication server. Security modes are Static WEP, IEEE 802.1X, WPA with RADIUS server, and WPA-PSK. For information about configuring security on the access point, see **Configuring the Wireless Distribution System, page 85**.

Verifying the Installation

Make sure the access point is connected to the LAN and associating with wireless clients on the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune the access point by modifying the advanced configuration features.

STEP 1 Connect the access point to the LAN.

If you configured the access point by using a direct cable connection from your computer to the access point, do the following:

a. Disconnect the cable from the computer and the access point.

b. Mount the access point in the desired location.

c. Connect an Ethernet cable from the access point to the LAN.

d. Power on the access point.

e. Connect your computer to the LAN by using an Ethernet cable or a wireless card.

If you configured the access point and an administrator PC by connecting both to a network hub or switch, your access point is already connected to the LAN. The next step is to test some wireless clients.

STEP 2 Test the access point by trying to detect it and associate with it from a wireless client. For information about requirements for the client devices, see **Wireless Client Requirements, page 16**.

NOTE The access point is not designed for multiple, simultaneous configuration changes. If more than one administrator is logged onto the Configuration Utility and is making changes to the configuration, there is no guarantee that all configuration changes specified by multiple users will be applied.

CAUTION By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN, including unauthorized devices. An important next step is to configure security. Continue with **Configuring Security on the Wireless Access Point, page 19** for more information.

Configuring Security on the Wireless Access Point

You configure secure wireless client access by configuring security for each virtual access point (VAP) that you enable. You can configure up to 16 VAPs per wireless radio that simulate multiple access points in one physical access point. For each VAP, you can configure a unique security mode to control wireless client access.

Each wireless radio has 16 VAPs, with VAP IDs from 0-15. VAP 0, VAP 1, and VAP 2 have different default settings than VAPs 3-15. By default, VAP 0, VAP 1, and VAP 2 are enabled.

VAP0 has the following default settings:

- VLAN ID: 1
- SSID: cisco-data
- Broadcast SSID: Enabled
- Security: None
- MAC Authentication Type: Disabled
- Station Isolation: Disabled
- HTTP Redirect: Disable

VAP1 has the following default settings:

- VLAN ID: 100
- SSID: cisco-voice
- Broadcast SSID: Enabled
- Security: None
- MAC Authentication Type: Disabled

- Station Isolation: Disabled
- HTTP Redirect: Disable

VAP2 has the following default settings:

- VLAN ID: 1
- SSID: cisco-scan
- Broadcast SSID: Enabled
- Security: WPA Personal
- WPA Versions: WPA2
- Cipher Suites: CCMP (AES)
- Key: intermec
- MAC Authentication Type: Disabled
- Station Isolation: Disabled
- HTTP Redirect: Disable

VAP3-15 are disabeld by default, but when they are enabled they will have the following default settings:

- VLAN ID: 1
- SSID: Virtual Access Point x (where *x* is the VAP ID)
- Broadcast SSID: Enabled
- Security: None
- MAC Authentication Type: Disabled
- Station Isolation: Disabled
- HTTP Redirect: Disable

To prevent unauthorized access to the access point, we recommend that you select and configure a security option other than None for the default VAP and for each VAP that you enable.

For information about how to configure the security settings on each VAP, see **Configuring the Wireless Distribution System, page 85**.

2

Status

The Status page provides information on the following:

- **Device Information**
- **Network Interfaces**
- **Traffic Statistics**
- **Associated Clients**
- **Rogue AP Detection**

Device Information

From the **Device Information** page, you can view hardware and product information.

Figure 5 Device Information

Table 3 describes the fields shown on the **Device Information** page.

Table 3 Device Information Page

Field	Description
Product Identifier	Identifies the AP hardware model.
Hardware Version	Identifies the AP hardware version.
Software Version	Shows version information for the software installed on the AP. As new versions of the WLAN AP software become available, you can upgrade the software.
Serial Number	Shows the AP serial number.
Device Name	Generic name to identify the type of hardware.
Device Description	Provides information about the product hardware.

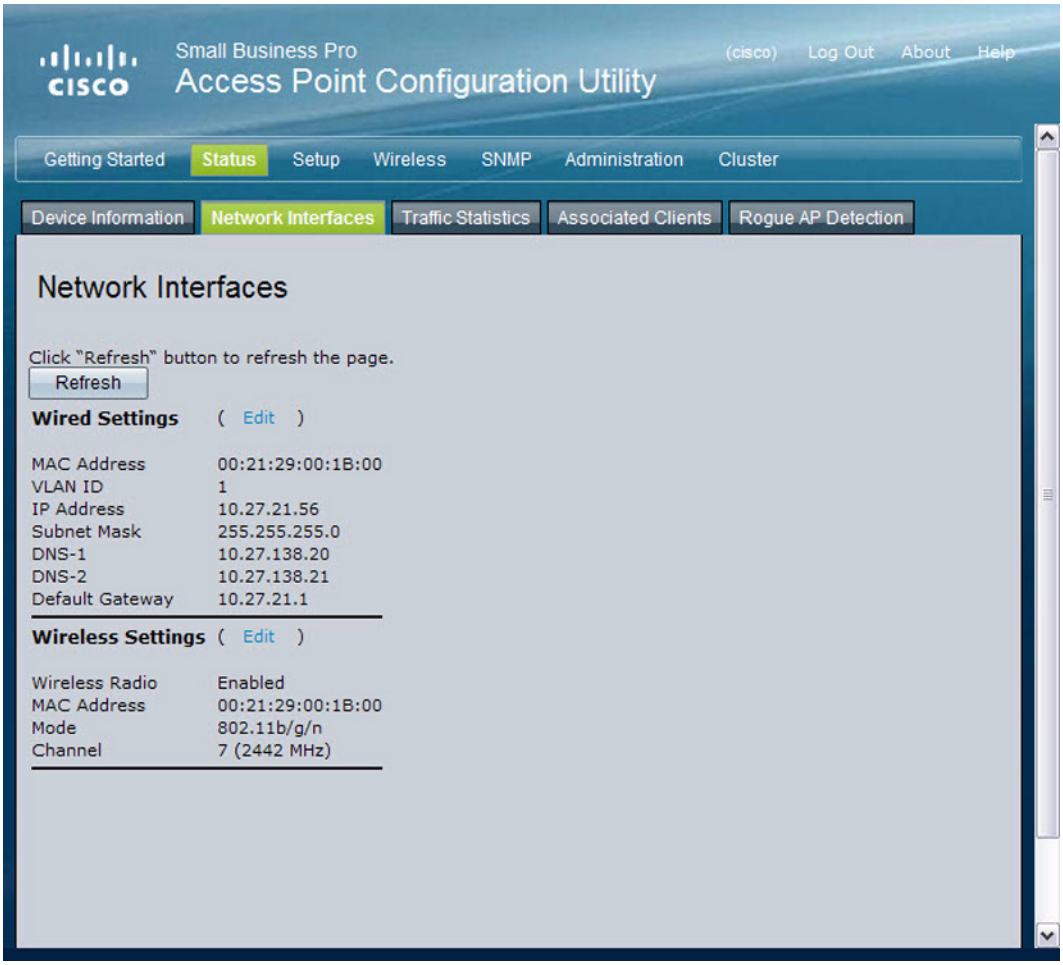
Table 3 Device Information Page

Field	Description
System Uptime	The amount of time that the AP has been operational since its last power-up/reboot.

Network Interfaces

The Network Interface Status window displays the current **Wired Settings** and the **Wireless Settings** of the access point. Click **Refresh** to refresh the page.

Figure 6 Interface Status



Wired Settings

The Wired Settings include the MAC address, management VLAN ID, IP address, subnet mask, and DNS information. To change any of these settings, click **Edit** to be redirected to the **Setup > LAN Settings** page.

For information about configuring these settings, see **LAN Settings, page 35**.

Wireless Settings

The **Wireless Settings** section indicates the status of the wireless radio, and includes the Radio Mode and Channel. The **Wireless Settings** section also shows the MAC address (read-only) associated with each wireless radio interface.

To change the Radio Mode or Channel settings, click **Edit**. You are redirected to the **Wireless > Radio Settings** page.

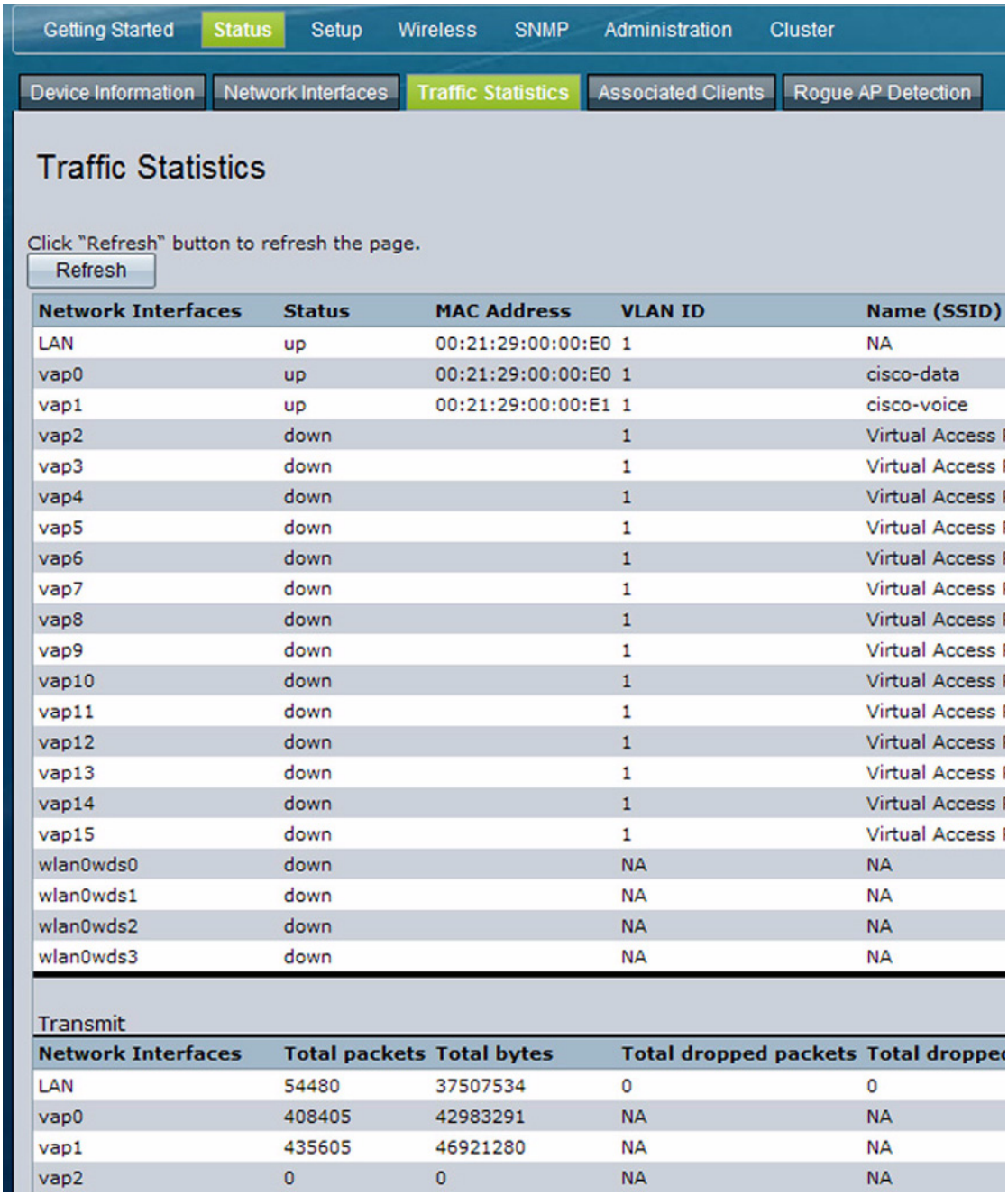
For information about configuring these settings, see **Modifying Wireless Radio Settings, page 47** and **Modifying Advanced Settings, page 74**.

Traffic Statistics

The **Traffic Statistics** page provides basic information about the access point, a real-time display of the transmit and receive statistics for the Ethernet interface, and VAP (Virtual Access Point) statistics. The transmit and receive statistics are totals since the access point was last started. If you reboot the access point, these figures indicate transmit and receive totals since the reboot.

To view transmit and receive statistics for the access point, click the **Traffic Statistics** tab. Click **Refresh** to refresh the page.

Figure 7 **Viewing Traffic Statistics**



Network Interfaces	Status	MAC Address	VLAN ID	Name (SSID)
LAN	up	00:21:29:00:00:E0	1	NA
vap0	up	00:21:29:00:00:E0	1	cisco-data
vap1	up	00:21:29:00:00:E1	1	cisco-voice
vap2	down		1	Virtual Access
vap3	down		1	Virtual Access
vap4	down		1	Virtual Access
vap5	down		1	Virtual Access
vap6	down		1	Virtual Access
vap7	down		1	Virtual Access
vap8	down		1	Virtual Access
vap9	down		1	Virtual Access
vap10	down		1	Virtual Access
vap11	down		1	Virtual Access
vap12	down		1	Virtual Access
vap13	down		1	Virtual Access
vap14	down		1	Virtual Access
vap15	down		1	Virtual Access
wlan0wds0	down		NA	NA
wlan0wds1	down		NA	NA
wlan0wds2	down		NA	NA
wlan0wds3	down		NA	NA

Transmit

Network Interfaces	Total packets	Total bytes	Total dropped packets	Total droppe
LAN	54480	37507534	0	0
vap0	408405	42983291	NA	NA
vap1	435605	46921280	NA	NA
vap2	0	0	NA	NA

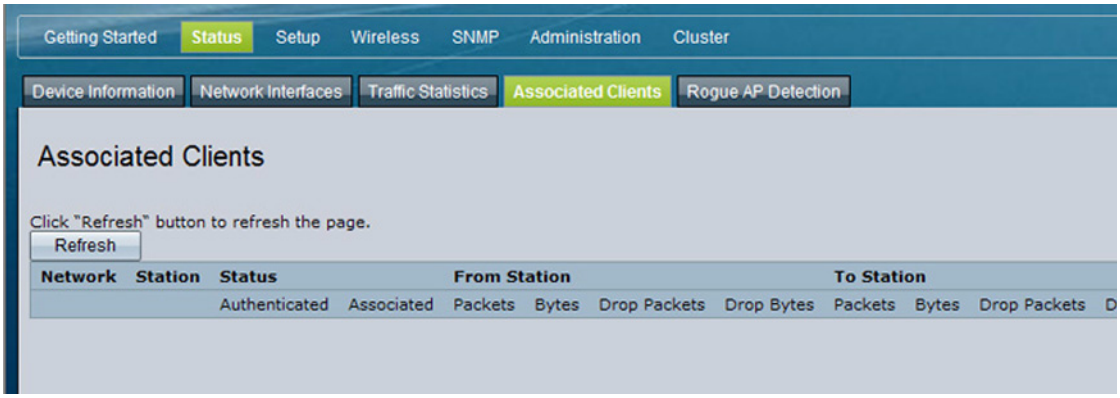
Table 4 Traffic Statistics Description

Field	Description
Network Interfaces	The name of the Ethernet or VAP interfaces.
Status	Shows whether the interface is up or down.
MAC Address	MAC address for the specified interface. Each VAP interface has a unique MAC address.
VLAN ID	A virtual LAN (VLAN) ID is used to establish multiple networks on the same access point. The VLAN ID is configured on the Wireless > VAP tab. (See **Bandwidth Utilization, page 90**.)
Name (SSID)	The network name, also known as the SSID, is an alphanumeric key that uniquely identifies a VAP. The name (SSID) is configured on the VAP tab. (See **Bandwidth Utilization, page 90**.) **NA** means either that the entry is not applicable or is not supported.
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) on that interface.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) on that interface.
Total Dropped Packets	Indicates total number of packets sent (in Transmit table) or received (in Received table) on that interface that were dropped. **NA** means that the drop and error counters for the VAP interfaces and the WDS interfaces are not supported.
Total Dropped Bytes	Indicates total number of bytes sent (in Transmit table) or received (in Received table) on that interface that were dropped. **NA** means that the drop and error counters for the VAP interfaces and the WDS interfaces are not supported.
Errors	Displays the total number of transmit and receive errors detected by the AP. **NA** means that the drop and error counters for the VAP interfaces and the WDS interfaces are not supported.

Associated Clients

To view the client stations associated with the access point, click the **Associated Clients** tab.

Figure 8 Viewing Client Association Information



The associated stations are displayed along with information about packet traffic transmitted and received for each station. Click **Refresh** to refresh the page.

Table 5 describes the fields on the **Associated Clients** page.

Table 5 Associated Clients Field Descriptions

Field	Description
Network	Shows which VAP the client is associated with. For example, an entry of wlan0vap2 means the client is associated with Wireless Radio 1, VAP 2.
Station	Shows the MAC address of the associated wireless client.

Table 5 Associated Clients Field Descriptions

Field	Description
Status	The Authenticated and Associated Status shows the underlying IEEE 802.11 authentication and association status that is present no matter which type of security the client uses to connect to the access point. This status does not show the IEEE 802.1X authentication or association status. Some points to keep in mind with regard to this field are: ▪ If the AP security mode is None or Static WEP, the authentication and association status of clients showing on the Client Associations tab will be in line with what is expected; that is, if a client shows as authenticated to the access point, it will be able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.) ▪ If the access point uses IEEE 802.1X or WPA security, however, it is possible for a client association to show on this tab as authenticated (by using IEEE 802.11 security) but actually not be authenticated to the access point by using the second layer of security.
From Station	Shows the number of packets and bytes received from the wireless client and the number of packets and bytes that were dropped after being received.
To Station	Shows the number of packets and bytes transmitted from the access point to the wireless client and the number of packets and bytes that were dropped upon transmission.

Link Integrity Monitoring

The access point provides link integrity monitoring to continually verify its connection to each associated client. To do this, the access point sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect when a client goes out of range, even during periods when no normal traffic is exchanged. The client connection drops off the list within 300 seconds if these data packets are not acknowledged, even if no disassociation message is received.

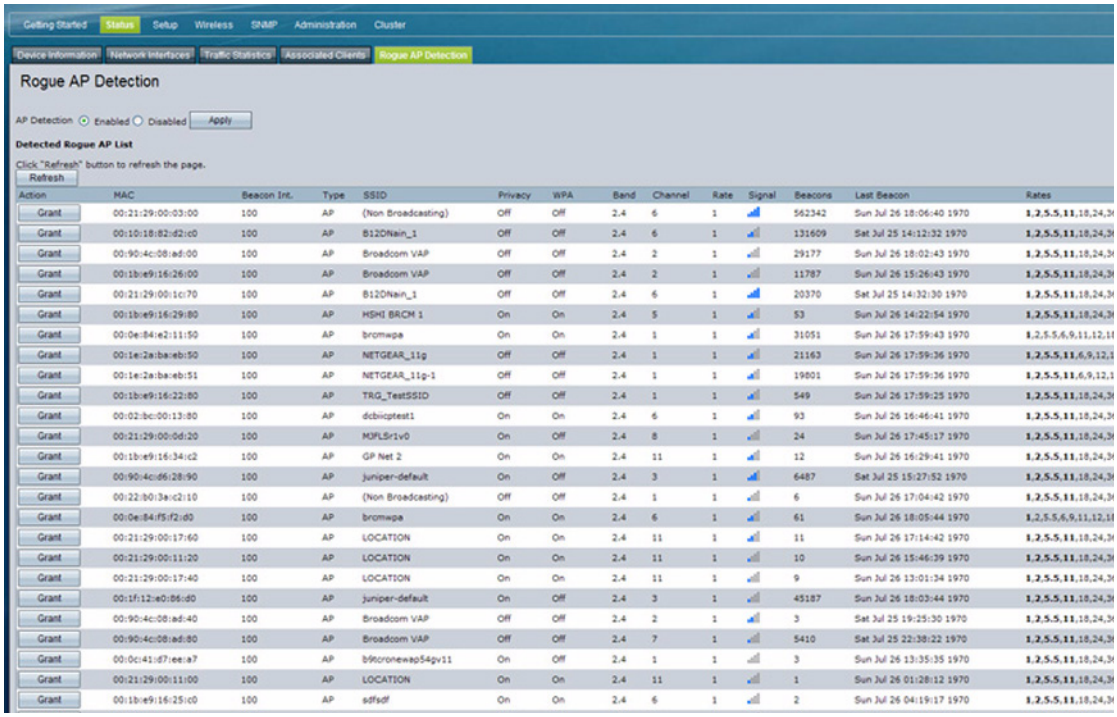
Rogue AP Detection

A Rogue AP is an access point that has been installed on a secure network without authorization from a system administrator. Rogue access points pose a security threat because anyone with access to the premises can ignorantly or maliciously install a wireless access point that might allow unauthorized parties to access the network.

The **Rogue AP Detection** page displays information about all access points detected by the Cisco AP541N in the vicinity of the network. If the access point listed as a rogue is actually a legitimate access point, you can add it to the Known AP List. Click **Refresh** to refresh the page.

NOTE The Detected Rouge AP List and Known AP List provide information. The Cisco AP541N does not have any control over the access points on the lists and cannot apply any security policies to access points detected through the RF scan.

Figure 9 Viewing Neighboring Access Points



You must enable the access point detection to collect information about other access points within range. Table 6 describes the information provided on neighboring access points.

Table 6 Neighboring Access Point Information

Field	Description
AP Detection	To enable neighbor access point detection and collect information about neighbor access points, click **Enabled**. (default) To disable neighbor access point detection, click **Disabled**. To save the setting, click **Apply**.

Table 6 Neighboring Access Point Information

Field	Description
Action	If an access point is in the Detected Rogue AP List, you can click **Grant** to move the access point from the Detected Rogue AP List to the Known AP List. If an access point is in the Known AP List, click the **Delete** button to move the access point from the Known AP List to the Detected Rogue AP List. **NOTE:** The Detected Rouge AP List and Known AP List provide information only; the Cisco AP541N does not have any control over the access points on the list and cannot apply any security policies to access points detected through the RF scan.
MAC	Shows the MAC address of the detected access point.
Beacon Int.	Shows the Beacon interval of another access point. Beacon frames are transmitted by an access point at regular intervals to announce their existence on the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval for your access point is set on the **Wireless > Advanced Settings** page. (See **Modifying Advanced Settings, page 74**.)
Type	Indicates the type of device: ▪ **AP** indicates the detected device is an access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. ▪ **Ad hoc** designation indicates a neighboring station running in ad hoc mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as *peer-to-peer* mode or an *Independent Basic Service Set* (IBSS).

Table 6 Neighboring Access Point Information

Field	Description
SSID	The Service Set Identifier (SSID) for another, detected access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. The SSID is set on the **Virtual Access Point** tab. (See **Bandwidth Utilization, page 90**.)
Privacy	Indicates whether there is any security on the neighboring access point. ▪ **Off** indicates that the Security mode on the neighboring access point is set to None (no security). ▪ **On** indicates that the neighboring access point has some security in place. Security is configured on the access point from the **Virtual Access Point** page.
WPA	Indicates whether WPA security is on or off for the detected access point.
Band	This indicates the IEEE 802.11 mode being used on the detected access point. (For example, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.) The number shown indicates the mode according to the following map: ▪ **2.4** indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes) ▪ **5** indicates IEEE 802.11a mode, 802.11n mode, or a combination of modes.

Table 6 Neighboring Access Point Information

Field	Description
Channel	Shows the Channel on which the detected access point is broadcasting. The channel defines the portion of the wireless radio spectrum that the wireless radio uses for transmitting and receiving. The channel for your access point is set in **Wireless > Advanced Settings**. (See **Modifying Advanced Settings, page 74**.)
Rate	Shows the rate (in megabits per second) at which the detected access point is currently transmitting. The current rate is always one of the rates shown in Supported Rates.
Signal	Indicates the strength of the wireless radio signal emitting from the detected access point. If you hover the mouse pointer over the bars, a number appears and shows the strength in decibels (dB).
Beacons	Shows the total number of beacons received from the detected access point since it was first discovered.
Last Beacon	Shows the date and time of the last beacon received from the detected access point.
Rates	Shows supported and basic (advertised) rate sets for the detected access point. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the **Wireless > Advanced Settings** page. (See **Modifying Advanced Settings, page 74**.)

Save or Import a List of Known Access Points

To save the Known AP List to a file, click **Save**. The list contains the MAC addresses of all access points that have been added to the Known AP List. By default, the filename is `Rogue2.cfg`. You can use a text editor or Web browser to open the file and view its contents.

Use the Import feature to import a list of known access points from a saved list. The list might be from another Cisco access point or created from a text file. If the MAC address of an access point appears in the Known AP List, it will not be shown as a rogue.

The file you import must be a plain-text file with a .txt or .cfg extension. Entries in the file are MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55. Separate the entries with a single space. For the access point to accept the file, it must contain only MAC addresses.

To import an access point list from a file, do the following:

STEP 1 Choose whether to replace the existing Known AP List or add the entries in the imported file to the Known AP List.

- Select the **Replace** radio button to import the list and replace the entire contents of the Known AP List.
- Select the **Merge** radio button to import the list and add the access points in the imported file to the access points currently displayed in the Known AP List.

STEP 2 Click **Browse** and choose the file to import.

STEP 3 Click **Import**.

Once the import is complete, the screen refreshes and the MAC addresses of the access points listed in the imported file appear in the Known AP List.

3

Setup

LAN Settings

The default wired LAN interface settings, including the default DHCP and VLAN parameters, might not work correctly for your network.

By default, the DHCP client on the access point broadcasts requests for network information. To use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

The access point default management VLAN is `VLAN 1`. This VLAN is also the default untagged VLAN. If you have configured the management VLAN on your network with a different VLAN ID, you must change the VLAN ID of the access point management VLAN.

To configure the LAN interface settings, click the **LAN Settings** tab.

Figure 10 LAN Settings

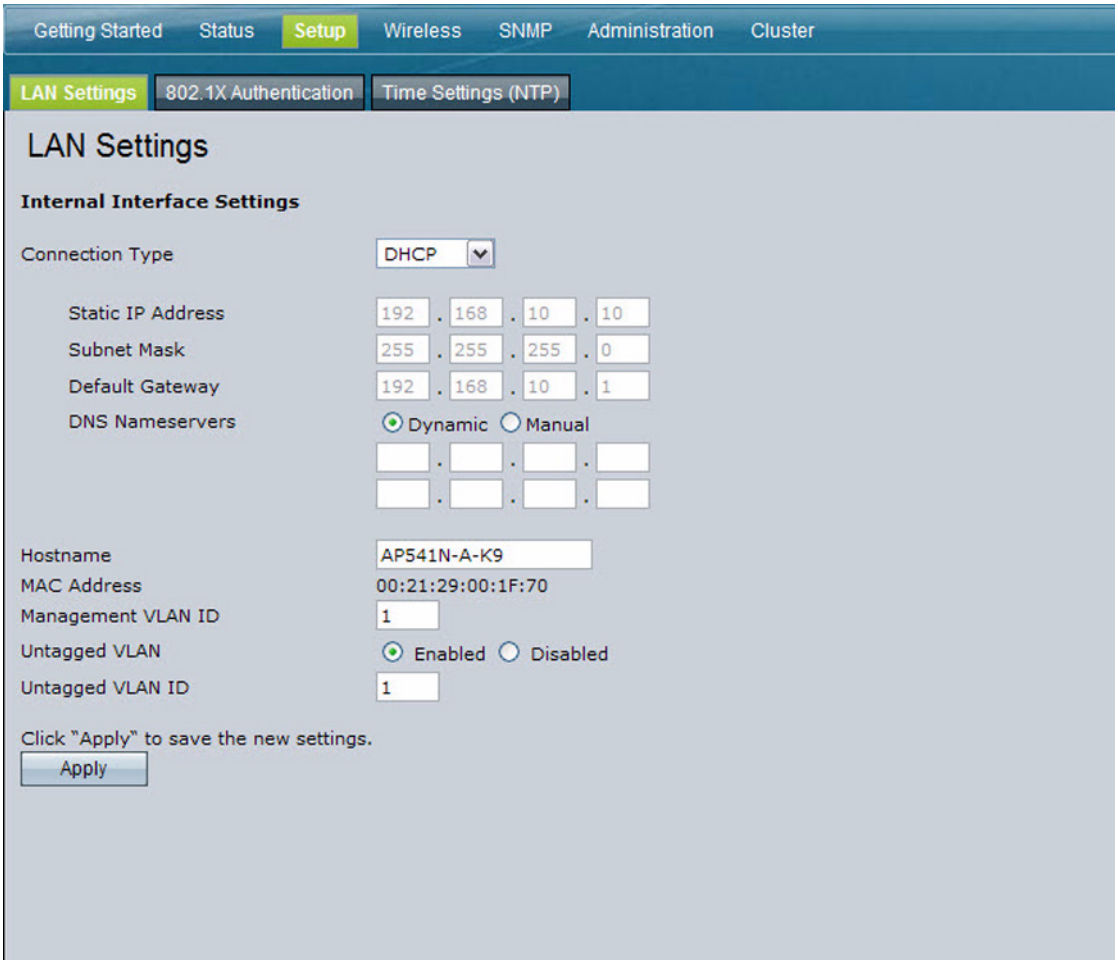


Table 7 describes the fields to view or configure on the **LAN Settings** page.

Table 7 LAN Settings Field Descriptions

Field	Description
Hostname	DNS name (host name) for the access point. The DNS name has the following requirements: ▪ Maximum of 20 characters ▪ Only letters, numbers and dashes. Double quote (") is not a valid character. ▪ Must start with a letter and end with either a letter or a number
MAC Address	MAC address for the Ethernet port on this access point. This is a read-only field that you cannot change.
Management VLAN ID	Enter a number between 1 and 4094 for the management VLAN ID used on your network. The default management VLAN ID is 1.
Untagged VLAN	Enable or disable VLAN tagging. If you enable the untagged VLAN, all traffic is tagged with a VLAN ID. By default all traffic on the access point uses VLAN 1, the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS.
Untagged VLAN ID	Provide a number between 1 and 4094 for the untagged VLAN ID. Traffic on the VLAN that you specify in this field is not tagged with a VLAN ID.
Connection Type	If you select **DHCP**, the access point acquires its IP address, subnet mask, DNS, and gateway information from a DHCP server. If you select **Static IP**, you must enter information in the Static IP Address, Subnet Mask, and Default Gateway fields.
Static IP Address	The static IP address of the access point. This field is disabled if you use DHCP as the connection type.

Table 7 LAN Settings Field Descriptions

Field	Description
Subnet Mask	**Subnet Mask** of the access point.
Default Gateway	**Default Gateway** of the access point.
DNS Nameservers	DNS mode. In **Dynamic** mode, the IP addresses for the DNS servers are assigned automatically by using DHCP. This option is only available if you specified DHCP for the Connection Type. In **Manual** mode, you must assign the IP addresses of the DNS Nameservers that resolve domain names.

NOTE After you configure the wired settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Configuring 802.1X Authentication

On networks that use IEEE 802.1X, port-based network access control, a supplicant (client) cannot gain access to the network until the 802.1X authentication server grants access. If your network uses 802.1X, you must configure the 802.1X authentication information that the access point can supply to the authentication server.

To configure the access point 802.1X supplicant user name and password, click the **802.1X Authentication** tab and configure the fields shown in Table 8.

Figure 11 IEEE 802.1X Authentication

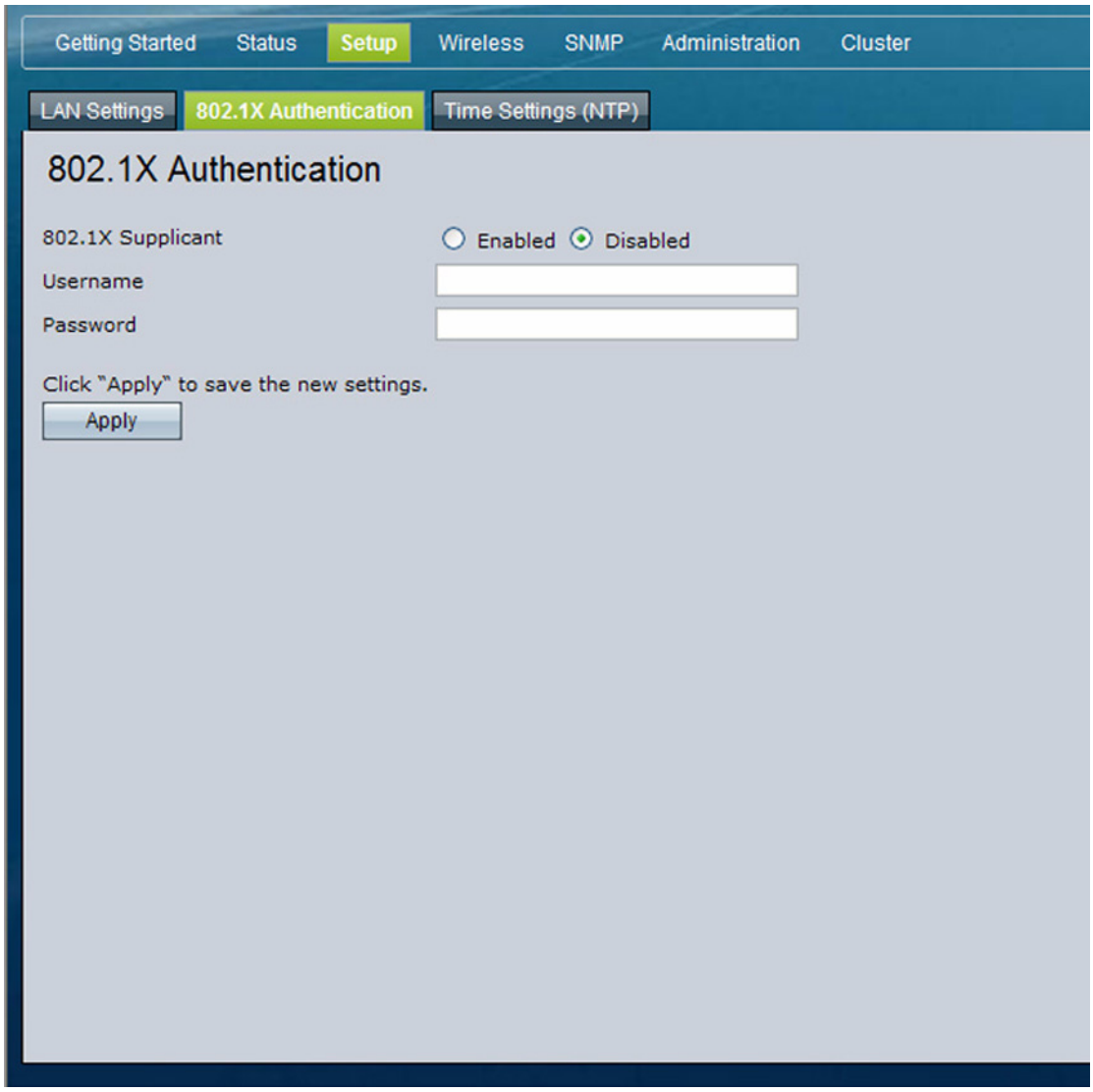


Table 8 IEEE 802.1X Authentication Field Descriptions

Field	Description
802.1X Supplicant	Click **Enabled** to enable the Administrative status of the 802.1X Supplicant. Click **Disabled** to disable the Administrative status of the 802.1X Supplicant.

Table 8 IEEE 802.1X Authentication Field Descriptions

Field	Description
Username	Enter the MD5 username for the access point to use when responding to requests from an 802.1X authentication server. The username can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case letters, numbers, and special symbols such as @ and #. Double quote (") is not a valid character. **NOTE:** If the 802.1X Supplicant is Disabled, the Username field is not editable.
Password	Enter the MD5 password for the access point to use when responding to requests from an 802.1X authentication server. The password can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case letters, numbers, and special symbols such as @ and #. Double quote (") is not a valid character. **NOTE:** If the 802.1X Supplicant is Disabled, the Password field is not editable.

NOTE After you configure the settings on the Authentication page, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Enabling the Network Time Protocol

The Network Time Protocol (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp is used to indicate the date and time of each event in log messages.

By using NTP, the AP can obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information.

See http://www.ntp.org for more information about NTP.

To configure the NTP that the access point uses manually as shown in **Figure 12 on page 42** or by using a server as shown in **Figure 13 on page 43**, click the **Time** tab and update the fields as described in **Table 9**.

Figure 12 Manually Enabling Network Time Protocol

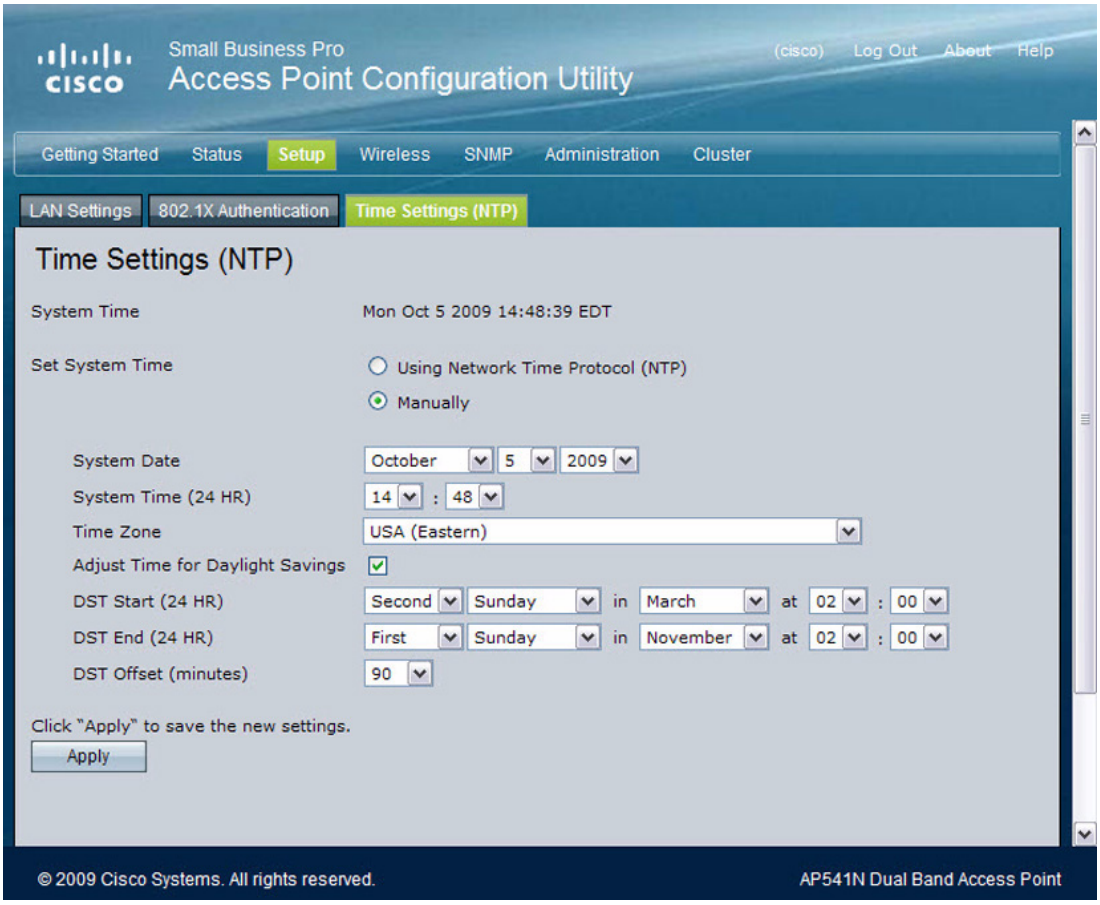


Figure 13 Enabling Network Time Protocol Server

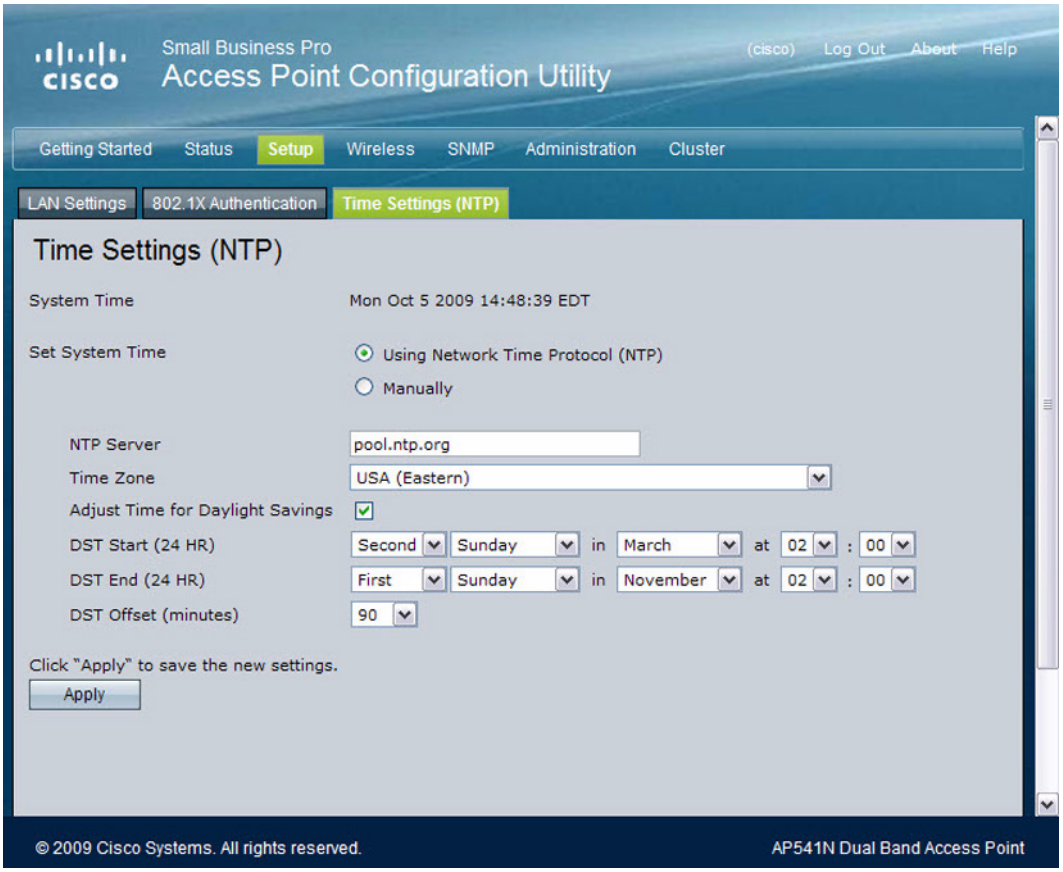


Table 9 TIme Settings (NTP)

Field	Description
System Time	Shows the current system time.
Set System Time	To permit the AP to poll an NTP server, click **Using Network Time Protocol (NTP)**. To set the system time manually, click **Manually**.
NTP Server	This field appears when you select **Using Network Time Protocol (NTP)** in the **Set System Time** field. If using NTP, specify the server by host name or IP address. Using the IP address is not recommended as the IP address is more likely to change.
Time Zone	Select the international time zone in which the AP is operating, for example **USA (Eastern)**.
System Date	This field appears when you select **Manually** in the **Set System Time** field. Use the **System Date** list to select month, day, and year.
System Time (24 HR)	This field appears when you select **Manually** in the **Set System Time** field. Use the **System Time** list to select hours and minutes. All times are relative to the local time zone.

Table 9 TIme Settings (NTP)

Field	Description
Adjust Time for Daylight Savings	Select the Daylight Savings option to adjust the system time for Daylight Savings Time (DST). Fields appear in order to select the date and time to start and end DST.
DST Start (24 HR)	Use this field to configure Daylight Savings Time to start. The start time is relative to standard time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere. From the week list, select the week of the month (**First, Second, ..., Last**). From the day list, select the day of the week (**Sunday**, **Monday**...). From the month list, select the month (**January**, **February**...). Specify the time (24-hour format) by selecting the hours and minutes.
DST End (24 HR)	Use this field to configure Daylight Savings Time to end. The end time is relative to Daylight Savings Time. From the week list, select the week of the month (**First, Second, ..., Last**). From the day list, select the day of the week (**Sunday**, **Monday**...). From the month list, select the month (**January**, **February**...). Specify the time (24-hour format) by selecting the hours and minutes.
DST Offset (minutes)	From the **DST Offset** list, select the number of minutes to add during Daylight Savings Time (**15** to **120** in 15-minute increments).

NOTE After you configure the Time settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

4

Wireless

Modifying Wireless Radio Settings

Wireless settings configure the wireless radio in the access point (802.11 mode and channel) and to the network interface to the access point (AP MAC address).

To configure the wireless interface, click the **Wireless Radio Settings** tab.

Figure 14 Wireless Interface Configuration

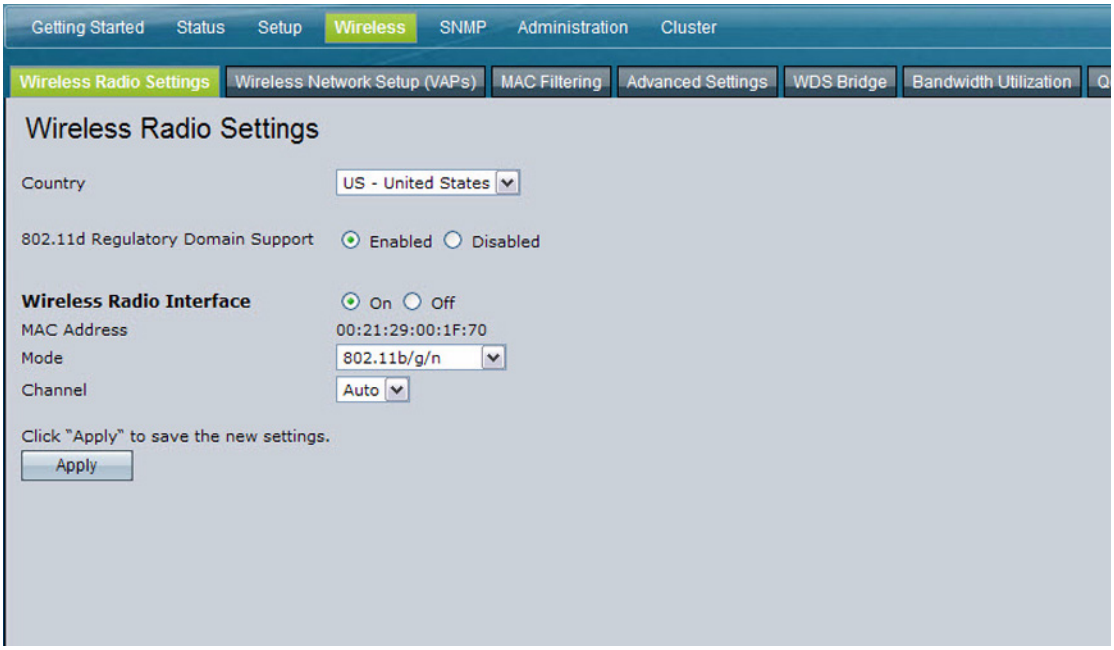


Table 10 describes the fields and configuration options available on the **Radio Settings** page.

Table 10 Radio Settings Field Descriptions

Field	Description
Country	The country in which the access point is operating. Wireless regulations vary from country to country. Make sure you select the correct country code so that the access point complies with the regulations in your country. The country code selection affects the wireless radio modes the access point can support as well as the list of channels and transmit power of the wireless radio.
802.11d Regulatory Domain Support	Enabling support for IEEE 802.11d (World Mode) on the access point causes the access point to broadcast which country it is operating in as a part of its beacons and probe responses. This allows client stations to operate in any country without reconfiguration. Disabling 802.11d prevents the country code setting from being broadcast in the beacons. However, this only applies to wireless radios configured to operate in the *g* band (2.4 GHz band). For wireless radios operating in the *a* band (5 GHz band), the access point software configures support for 802.11h. When 802.11h is supported, the country code information is broadcast in the beacons. To enable 802.11d regulatory domain support, click **Enabled**. To disable 802.11d regulatory domain support, click **Disabled**.
Wireless Radio Interface	Turns the wireless radio interface on or off.
MAC Address	Indicates the Media Access Control (MAC) addresses for the interface. This page shows the MAC addresses for Radio Interface One. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the interface.

Table 10 Radio Settings Field Descriptions

Field	Description
Mode	The Physical Layer (PHY) standard the wireless radio uses. **NOTE:** If the Wireless Radio Interface is set to **Off**, the Mode cannot be changed. **NOTE:** The modes available on your access point depend on the country code setting. Select one of the following modes for the wireless radio interface: ▪ 802.11a. Only 802.11a clients can connect to the access point. ▪ 802.11b/g. 802.11b and 802.11g clients can connect to the access point. ▪ 802.11a/n. 802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the access point. ▪ 802.11b/g/n (default). 802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the access point. ▪ 2.4 GHz 802.11n. Only 802.11n clients operating in the 2.4-GHz frequency can connect to the access point. ▪ 5 GHz 802.11n.Only 802.11n clients operating in the 5-GHz frequency can connect to the access point.

Table 10 Radio Settings Field Descriptions

Field	Description
Channel	Select the **Channel**. **NOTE:** If Radio Interface is set to **Off**, the Channel cannot be changed. The range of available channels is determined by the mode of the wireless radio interface and the country code setting. If you select Auto for the channel setting, the access point scans all available channels, immediately selects a channel, and begins operation. If interference or errors occur on that channel, another channel is automatically selected. The Channel defines the portion of the wireless radio spectrum the wireless radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).

NOTE After you configure the wireless settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Modifying Virtual Access Point Settings

To change VAP 0 or to enable and configure additional VAPs, select the **Virtual Access Points (SSIDs)** tab in the **Wireless** section.

VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple access points in one physical access point. The Cisco AP541N supports up to 16 VAPs.

NOTE Note that only those VAPs which have non-default configuration are displayed when the page initially loads. To configure additional VAPs, click **Add Another** to expose new (empty) VAP entries.

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

You can configure each VAP to use a different VLAN, or you can configure multiple VAPs to use the same VLAN. VAP0, which is always enabled, is assigned to VLAN 1 by default. VAP1 is also enabled by default and assigned to VLAN 100.

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

You can configure up to four global IPv4 RADIUS servers. One of the servers always acts as a primary while the others act as backup servers. The network type and accounting mode are common across all configured RADIUS servers. You can configure each VAP to use the global RADIUS server settings, which is the default, or you can configure a per-VAP RADIUS server set. You can also configure separate RADIUS server settings for each VAP.

The Global RADIUS server settings are collapsed when the page initially loads. To show (expand) the Global RADIUS server settings section of the page, click the right arrow icon to the left of the Global RADIUS server settings section title. To collapse the Global RADIUS server settings section, click the down arrow icon to the left of the Global RADIUS server settings section title.

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

NOTE Before you configure VLANs on the access point, be sure to verify that the switch and DHCP server the access point uses can support IEEE 802.1Q VLAN encapsulation.

To configure multiple VAPs, click the **VAP** tab.

Figure 15 Configuring Virtual Access Points

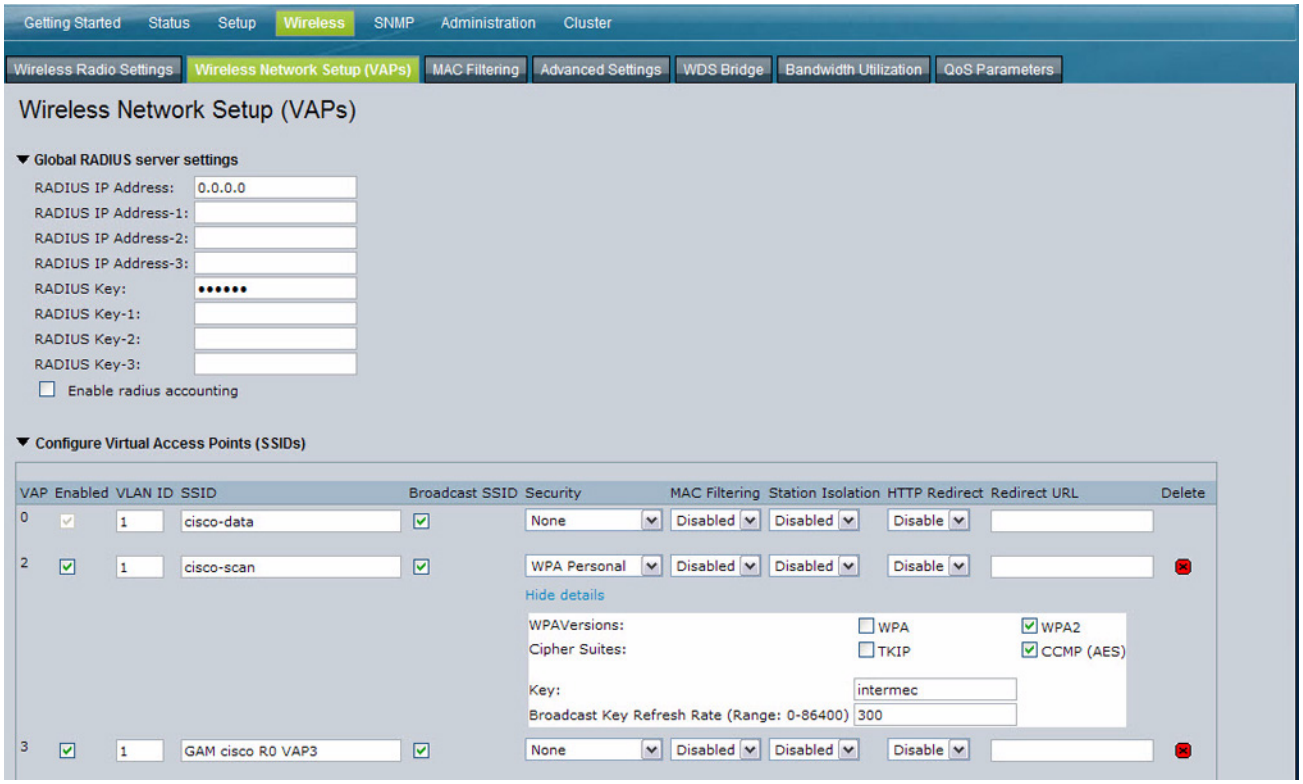


Table 11 describes the fields and configuration options on the VAP page.

Table 11 VAP Field Descriptions

Field	Description
RADIUS IP Address	Enter the address for the primary global RADIUS server. By default, each VAP uses the global RADIUS settings that you define for the access point at the top of the VAP page. When the first wireless client tries to authenticate with the access point, the access point sends an authentication request to the primary server. If the primary server responds to the authentication request, the access point continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify.

Table 11 VAP Field Descriptions

Field	Description
RADIUS IP Address 1–3	Enter up to three IPv4 addresses to use as the backup RADIUS servers. If authentication fails with the primary server, each configured backup server is tried in sequence. The address must be valid in order for the access point to attempt to contact the server.
RADIUS Key	Enter the RADIUS key in the text box. The *RADIUS Key* is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the access point and on your RADIUS server. The text you enter is displayed as large dot characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1–3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so forth.
Enable Radius Accounting	**Select this option** to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so forth. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
VAP	You can configure up to 16 VAPs for each wireless radio. VAP0 is the physical wireless radio interface. To disable VAP0, you must disable the wireless radio. Due to the dependency of the WDS links with the VAP0 security mode, VAP0 cannot be configured to **None**, **Static WEP**, or **802.1X** if the WDS links have **WPA Personal** as the security mode. If you need to change the security of VAP0 from **WPA Personal** or **WPA Enterprise** to **None**, **Static WEP**, or **802.1X**, then remove the WPA security mode for all the WDS links.

Table 11 VAP Field Descriptions

Field	Description
Enabled	You can enable or disable a configured network. ▪ To enable the specified network, select the **Enabled** option beside the appropriate VAP. ▪ To disable the specified network, clear the **Enabled** option beside the appropriate VAP. If you disable the specified network, you lose the VLAN ID you entered.
VLAN ID	When a wireless client connects to the access point by using this VAP, the access point tags all traffic from the wireless client with the VLAN ID you enter in this field unless you enable the untagged VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is 1–4094. If you use RADIUS-based authentication for clients, you can optionally add the following attributes to the appropriate file in the RADIUS or AAA server to configure a VLAN for the client: ▪ Tunnel-Type ▪ Tunnel-Medium-Type ▪ Tunnel-Private-Group-ID The RADIUS-assigned VLAN ID overrides the VLAN ID you configure on the **VAP** page. You configure the untagged and management VLAN IDs on the Ethernet Settings page. For more information, see **LAN Settings, page 35**.

Table 11 VAP Field Descriptions

Field	Description
SSID	Enter a name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. Double quote (") is not a valid character. You can use the same SSID for multiple VAPs, or you can choose a unique SSID for each VAP. **NOTE:** If you are connected as a wireless client to the same access point that you are administering, resetting the SSID will cause you to lose connectivity to the access point. You will need to reconnect to the new SSID after you save this new setting.
Broadcast SSID	Specify whether to allow the access point to broadcast the *Service Set Identifier* (SSID) in its beacon frames. The Broadcast SSID parameter is disabled by default. When the VAP does not broadcast its SSID, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect. ▪ To enable the SSID broadcast, select the **Broadcast SSID** check box. ▪ To prohibit the SSID broadcast, clear the **Broadcast SSID** check box. **NOTE:** Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

Table 11 VAP Field Descriptions

Field	Description
Security	Select one of the following **Security** modes for this VAP: ▪ None ▪ Static WEP ▪ Dynamic WEP ▪ IEEE 802.1X ▪ WPA Personal ▪ WPA Enterprise If you select a security mode other than **None**, additional fields appear. These fields are explained in the **"Security (Mode)"** section.
MAC Auth Type	You can configure a global list of MAC addresses that are allowed or denied access to the network. The drop-down menu for this feature allows you to select the type of MAC authentication to use: ▪ **Disabled**: Do not use MAC authentication. ▪ **Local**: Use the MAC authentication list that you configure on the Wireless Connection Control page. ▪ **RADIUS**: Use the MAC authentication list on the external RADIUS server. For more information about MAC authentication, see **Client Connection Control, page 71**.

Table 11 VAP Field Descriptions

Field	Description
Station Isolation	Select from the drop-down menu to configure Station Isolation for this VAP: ▪ When Station Isolation is **disabled**, wireless clients can communicate with one another normally by sending traffic through the access point. ▪ When Station Isolation is **enabled**, the access point blocks communication between wireless clients on the same VAP. The access point still allows data traffic between its wireless clients and wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP.
Redirect Mode	Enable the HTTP redirect feature to redirect wireless clients to a custom Web page. When redirect mode is enabled, the user is redirected to the URL you specify after the wireless client associates with an access point and the user opens a Web browser on the client to access the Internet. The custom Web page must be located on an external Web server and might contain information such as the company logo and network usage policy. **NOTE:** The wireless client is redirected to the external Web server only once, when it is first associated with the access point.
Redirect URL	Specify the URL where the Web browser is to be redirected after the wireless client associates with the access point and sends HTTP traffic. Length is 1 to 120 alphanumeric and special characters, in the form "^[A-Za-z]+://[A-Za-z0-9-]+\.[A-Za-z0-9]+"). For example: http://cisco.com.
Delete	Click the red x Delete icon to remove the configuration for a particular VAP. When a VAP is deleted, all of its configuration is restored to its default configuration settings. The entry is removed from the list of displayed VAPs. **NOTE:** VAP0 corresponds to the physical wireless radio interface and cannot be deleted. The Delete icon is not displayed for this VAP.

NOTE After you configure the VAP settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Security (Mode)

The Security mode you set here is specifically for this VAP.

When the page initially loads, any VAP that has a security mode other than **None** will have a **Show details** link below the **Security** selection box. Click the **Show details** link to show the current security settings. When showing the current security settings, the link changes to **Hide details**. Click **Hide details** to collapse the current security settings.

None (Plain-text)

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

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Static WEP is not the most secure mode available, but it offers more protection than setting the security mode to None (Plain-text) as it does prevent an outsider from easily sniffing out unencrypted wireless traffic.

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called RC4.)

If you use Static WEP, the following rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP, and all clients must have one of the WEP keys specified on the access point in order to de-code AP-to-station data transmissions.
- The access point must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (access point and clients). For example if the access point defines `abc123` key as WEP key 3, then the client stations must define that same string as WEP key 3.
- Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)
- On some wireless client software, you can configure multiple WEP keys and define a client station "transfer key index", and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring access points cannot decode each other's transmissions.
- You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Table 12 describes the WEP fields.

Table 12 WEP Field Descriptions

Field	Description
Transfer Key Index	Select a key index from the drop-down menu. Key indexes 1 through 4 are available. The default is 1. The transfer key index indicates which WEP key the access point will use to encrypt the data it transmits.
Key Length	Specify the length of the key by clicking one of the radio buttons: ▪ 64 bits ▪ 128 bits

Table 12 WEP Field Descriptions

Field	Description
Key Type	Select the key type by clicking one of the radio buttons: ▪ ASCII ▪ Hex
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for each key. The keys you enter depend on the key type selected: ▪ ASCII. Includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. ▪ Hex. Includes digits 0 to 9 and the letters A to F. Use the same number of characters for each key as specified in the Characters Required field. These are the RC4 WEP keys shared with the stations using the access point. Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the access point. **Characters Required:** The number of characters you enter into the WEP Key fields is determined by the Key length and Key type you select. For example, if you use 128-bit ASCII keys, you must enter 13 characters in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.

Table 12 WEP Field Descriptions

Field	Description
802.1X Authentication	The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an access point when static WEP is the security mode. Specify the authentication algorithm you want to use by choosing one of the following options: ▪ **Open system** authentication allows any client station to associate with the access point whether that client station has the correct WEP key or not. This algorithm is also used in plaintext, Dynamic WEP, IEEE 802.1X, and WPA modes. When the authentication algorithm is set to Open System, any client can associate with the access point. **NOTE** Just because a client station is allowed to *associate* does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point. ▪ **Shared key** authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key will not be able to associate with the access point. ▪ **Both Open system and Shared key.** When you select both authentication algorithms: - Client stations configured to use WEP in shared key mode must have a valid WEP key to associate with the access point. - Client stations configured to use WEP as an open system (shared key mode not enabled) are able to associate with the access point, even if they do not have the correct WEP key.

IEEE 802.1X Authentication

IEEE 802.1X is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1X provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of an external RADIUS server to authenticate users. The access point requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

You can use any of a variety of authentication methods that the IEEE 802.1X mode supports, including certificates, Kerberos, and public key authentication. You must configure the client stations to use the same authentication method the access point uses.

NOTE After you configure the security settings, you must click **Apply** to apply the changes and to save the settings.

Table 13 IEEE 802.1X

Field	Description
Use Global RADIUS Server Settings	By default each VAP uses the global RADIUS settings that you define for the access point at the top of the VAP page. However, you can configure each VAP to use a different set of RADIUS servers. To use the global RADIUS server settings, make sure the check box is selected. To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the following fields.
RADIUS IP Address	Enter the address for the primary RADIUS server for this VAP.

Table 13 IEEE 802.1X

Field	Description
RADIUS IP Address 1–3	Enter up to three IPv4 addresses to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.
RADIUS Key	Enter the RADIUS key in the text box. The *RADIUS Key* is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the access point and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1–3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so forth.
Enable RADIUS Accounting	Select this option to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so forth. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Session Key Refresh Rate	Enter a value to set the interval at which the access point will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Dynamic WEP

Dynamic WEP mode uses IEEE 802.1X, the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages are sent over an IEEE 802.11 wireless network by using a protocol called EAP Encapsulation Over LANs (EAPOL). Dynamic WEP mode provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of an external RADIUS server to authenticate users. The AP requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

You can use any of a variety of authentication methods that the Dynamic WEP mode supports, including certificates, Kerberos, and public key authentication. You must configure the client stations to use the same authentication method the access point uses.

Table 14 Dynamic WEP

Field	Description
Use Global RADIUS Server Settings	By default each VAP uses the global RADIUS settings that you define for the AP at the top of the VAP page. However, you can configure each VAP to use a different set of RADIUS servers. To use the global RADIUS server settings, make sure the check box is selected. To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the following fields.
RADIUS IP Address	Enter the address for the primary RADIUS server for this VAP.
RADIUS IP Address 1–3	Enter up to three IPv4 addresses to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.

Table 14 Dynamic WEP

Field	Description
RADIUS Key	Enter the RADIUS key in the text box. The *RADIUS Key* is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1–3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.
Enable RADIUS Accounting	Select this option to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Session Key Refresh Rate	Enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

NOTE After you configure the security settings, you must click **Apply** to apply the changes and to save the settings.

WPA Personal

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

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

Table 15 WPA Personal Field Descriptions

Field	Description
WPA Versions	Select the types of client stations you want to support: **WPA.** If all client stations on the network support the original WPA but none support the newer WPA2, select WPA. **WPA2.** If all client stations on the network support WPA2, we suggest using WPA2, as it provides the best security by supporting the IEEE 802.11i standard. **WPA and WPA2.** If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients that support it. This WPA configuration allows more interoperability, at the expense of some security.

Table 15 WPA Personal Field Descriptions

Field	Description
Cipher Suites	Select the cipher suite you want to use: ▪ TKIP ▪ CCMP (AES) ▪ TKIP and CCMP (AES) Both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the access point: ▪ A valid TKIP key ▪ A valid AES-CCMP key Clients not configured to use a WPA Personal cannot associate with the access point.
Key	The Pre-shared Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

WPA Enterprise

WPA Enterprise with RADIUS is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes CCMP (AES), and TKIP mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users.

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

Table 16 WPA Enterprise Field Descriptions

Field	Description
WPA Versions	Select the types of client stations you want to support: ▪ **WPA.** If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA. ▪ **WPA2.** If all client stations on the network support WPA2, we suggest using WPA2, as it provides the best security by supporting the IEEE 802.11i standard. ▪ **WPA and WPA2.** If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both WPA and WPA2. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients that support it. This WPA configuration allows more interoperability, at the expense of some security.
Enable pre-authentication	If in WPA Versions you selected only WPA2 or both WPA and WPA2, you can enable pre-authentication for WPA2 clients. Click **Enable pre-authentication** if you want WPA2 wireless clients to send a pre-authentication packet. The pre-authentication information is relayed from the access point the client is using to the target access point. Enabling this feature can speed up authentication for roaming clients that connect to multiple access points. This option does not apply if you selected only WPA for WPA Versions because WPA does not support this feature.

Table 16 WPA Enterprise Field Descriptions

Field	Description
Cipher Suites	Select the cipher suite you want to use: ▪ TKIP ▪ CCMP (AES) ▪ TKIP and CCMP (AES) By default both TKIP and CCMP are selected. When both TKIP and CCMP are selected, client stations configured to use WPA with RADIUS must have one of the following: ▪ A valid TKIP RADIUS IP address and RADIUS Key ▪ A valid CCMP (AES) IP address and RADIUS Key
Active Server	Displays which RADIUS server is in use. You can manually change from this server to a different server by selecting the desired server in the dropdown box. **NOTE:** The Active Server is not stored across reboots. The first configured RADIUS server is selected when the device is rebooted or reset.
Use Global RADIUS Server Settings	By default each VAP uses the global RADIUS settings that you define for the access point at the top of the VAP page. However, you can configure each VAP to use a different set of RADIUS servers. To use the global RADIUS server settings, make sure the check box is selected. To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the fields.
RADIUS IP Address	Enter the address for the primary RADIUS server for this VAP.
RADIUS IP Address 1–3	Enter up to three IPv4 addresses to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.

Table 16 WPA Enterprise Field Descriptions

Field	Description
RADIUS Key	Enter the RADIUS key in the text box. The *RADIUS Key* is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the access point and on your RADIUS server. The text you enter is displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1–3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so forth.
Enable RADIUS Accounting	**Select this option** to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so forth. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Session Key Refresh Rate	Enter a value to set the interval at which the access point will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

NOTE After you configure the security settings, you must click **Apply** to apply the changes and to save the settings.

Client Connection Control

A Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example `00:DC:BA:09:87:65`. Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

You can use the *Access Point Configuration Utility* on the access point or use an external RADIUS server to control access to the network through the access point based on the MAC address of the wireless client. This feature is called MAC Authentication or MAC Filtering. To control access, you configure a global list of MAC addresses locally on the access point or on an external RADIUS server. Then, you set a filter to specify whether the clients with those MAC addresses are allowed or denied access to the network. When a wireless client attempts to associate with an access point, the access point looks up the MAC address of the client in the local Stations List or on the RADIUS server. If it is found, the global allow or deny setting is applied. If it is not found, the opposite is applied.

On the **Virtual Access Point Settings** page, the MAC Auth Type setting controls whether the access point uses the station list configured locally on the **Client Connection Control** page or the external RADIUS server. The Allow/Block filter setting on the **Client Connection Control** page determines whether the clients in the station list (local or RADIUS) can access the network through the access point. For more information about setting the MAC authentication type, see **Configuring the Wireless Distribution System, page 85**.

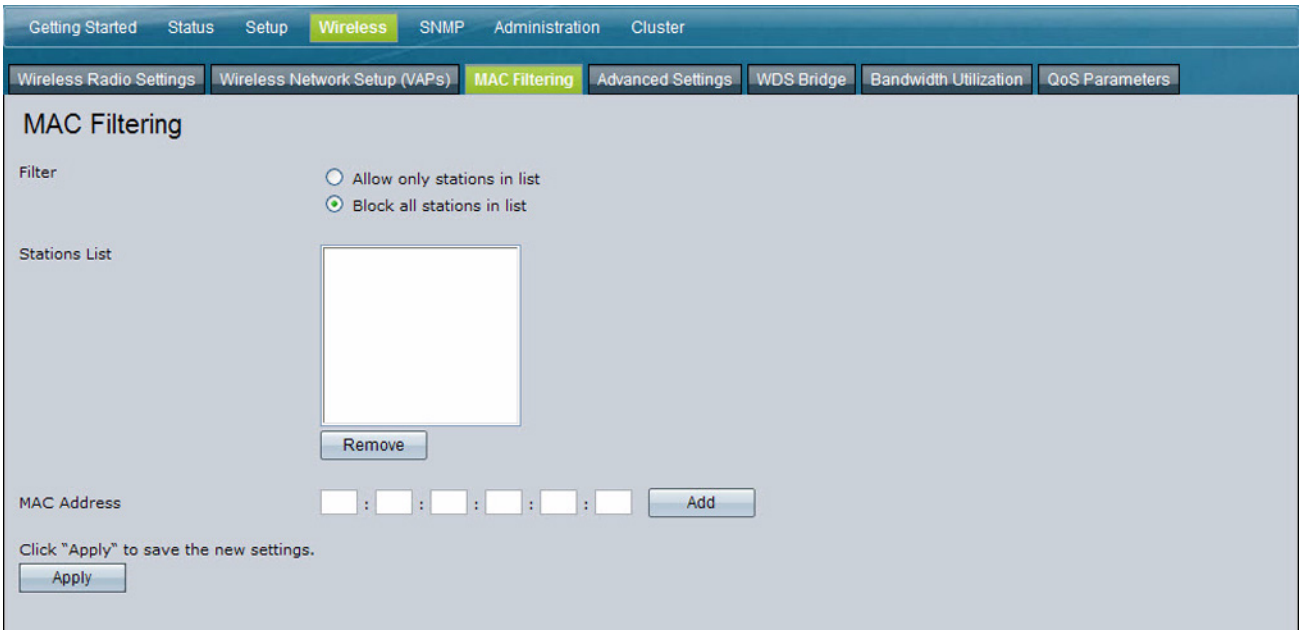
Configuring a MAC Filter and Station List on the Access Point

The **Client Connection Control** page allows you to control access to access point based on MAC addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *deny* access to the stations listed.

When you enable MAC Authentication and specify a list of approved MAC addresses, only clients with a listed MAC address can access the network. If you specify MAC addresses to deny, all clients can access the network except for the clients on the *deny* list.

To enable filtering by MAC address, click the **Client Connection Control** tab.

Figure 16 Configuring MAC Authentication



NOTE Global MAC Authentication settings apply to all VAPs.

Table 17 describes the fields and configuration options available on the **MAC Authentication** page

Table 17 MAC Authentication Field Descriptions

Field	Description
Filter	To set the MAC Address Filter, select one of the following options: ▪ **Allow only stations in list.** Any station that is in the Stations List is allowed access to the network through the access point; all other stations are denied. ▪ **Block all stations in list.** Only the stations that appear in the list are denied access to the network through the access point. All other stations are permitted access. **NOTE:** The filter you select is applied to the clients in the station list, regardless of whether that station list is local or on the RADIUS server.

Table 17 MAC Authentication Field Descriptions

Field	Description
Stations List	This is the local list of clients that are either permitted or denied access to the network through the access point. To add a MAC Address to the local Stations List, enter its 48-bit MAC address into the MAC Address text boxes, then click Add. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click Remove. The stations in the list will either be allowed or denied access based on how you set the filter in the previous field. **NOTE:** If the MAC authentication type for the VAP is set to **Local**, the access point uses the Stations List to permit or deny the clients access to the network. If the MAC authentication type is set to **RADIUS**, the access point ignores the MAC addresses configured in this list and uses the list that is stored on the RADIUS server. The MAC authentication type is set on the VAP configuration page.

NOTE After you configure local MAC Authentication settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Configuring MAC Authentication on the RADIUS Server

If you use RADIUS MAC authentication for MAC-based access control, you must configure a station list on the RADIUS server. The station list contains client MAC address entries, and the format for the list is described in the following table.

Table 18 Configuring MAC Authentication on the RADIUS Server

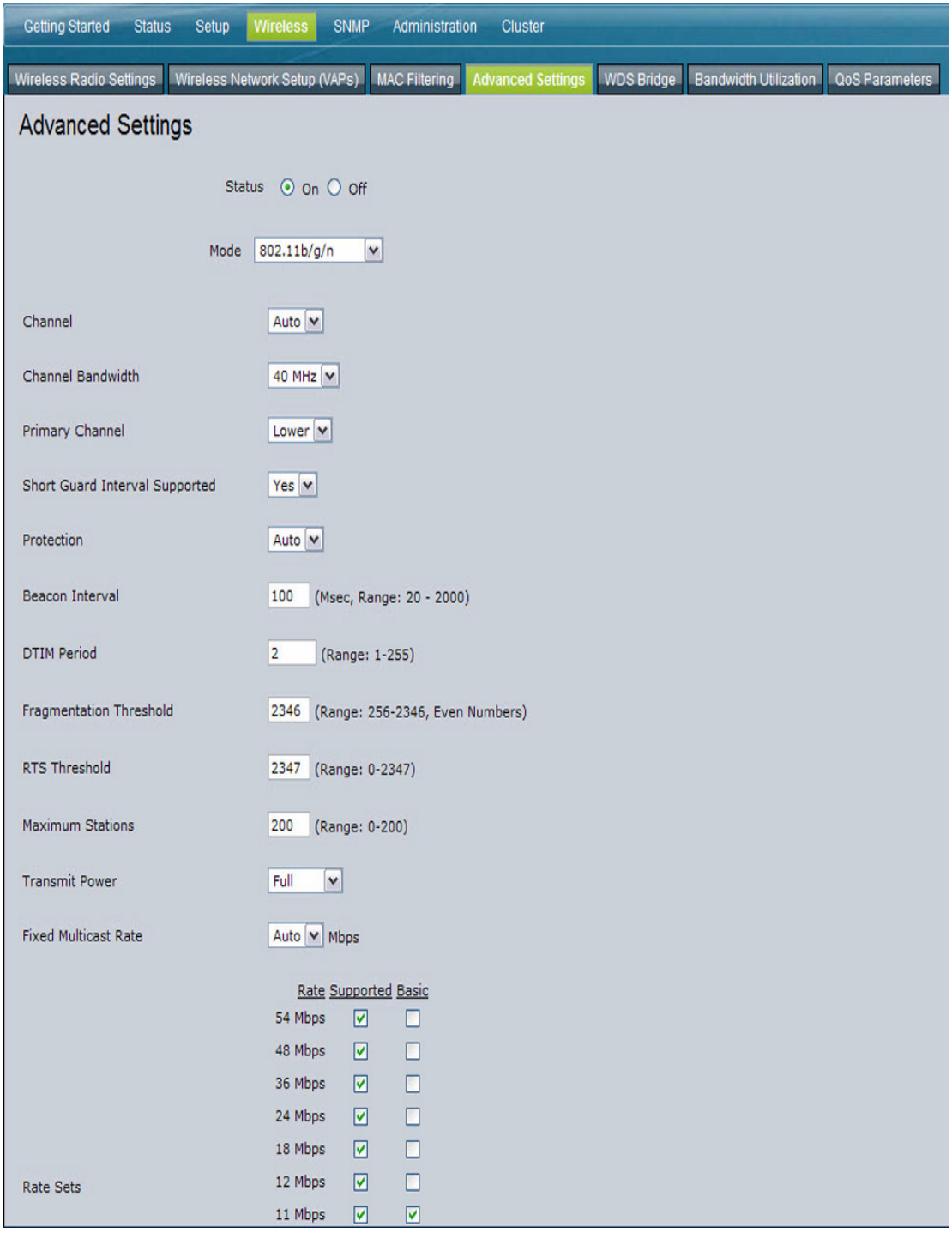
RADIUS Server Attribute	Description	Value
User-Name (1)	MAC address of the client station.	Valid Ethernet MAC Address.
User-Password (2)	A fixed global password used to lookup a client MAC entry.	NOPASSWORD

Modifying Advanced Settings

The advanced wireless settings directly control the behavior of the wireless radio in the access point and its interaction with the physical medium; that is, how and what type of electromagnetic waves the access point emits.

To specify the wireless radio settings, click the **Advanced Settings** tab.

Figure 17 Configuring the Wireless Radio Settings



Different settings display depending on the mode you select. Table 19 describes the fields and configuration options for the Advanced Settings page.

Table 19 Advanced Settings Field Descriptions

Field	Description
Status (On/Off)	Specify whether you want the wireless radio on or off by clicking **On** or **Off**. If you turn off a wireless radio, the access point sends disassociation frames to all the wireless clients it was supporting so that the wireless radio can be gracefully shutdown and the clients can start the association process with other available access points. **NOTE:** If Status is set to **Off**, then all fields are not able to be edited.
Mode	The **Mode** defines the Physical Layer (PHY) standard used by the wireless radio. **NOTE:** The modes available on your access point depend on the country code setting. Select one of the following modes for the wireless radio interface: ▪ 802.11a ▪ 802.11b/g ▪ 802.11a/n ▪ 802.11b/g/n ▪ 5 GHz 802.11n ▪ 2.4 GHz 802.11n

Table 19 Advanced Settings Field Descriptions

Field	Description
Channel	The range of available channels is determined by the mode of the wireless radio interface and the country code setting. If you select **Auto** for the channel setting, and Auto channel is configured, the access point scans available channels, immediately selects a channel and begins operation. If interference or errors occur on that channel, another channel is automatically selected. The channel defines the portion of the wireless radio spectrum the wireless radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).
Channel Bandwidth	This field is available only if the wireless radio mode includes 802.11n. The 802.11n specification allows a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. Select a value to set the use of the channel bandwidth. The default is 20-MHz.

Table 19 Advanced Settings Field Descriptions

Field	Description
Primary Channel	This field is available only if the radio mode includes 802.11n. This setting can be changed only when the channel bandwidth is set to 40 MHz. A 40-MHz channel can consist of two contiguous 20-MHz channels in the same frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients. Select one of the following options: ▪ **Upper**. Set the Primary Channel as the upper 20-MHz channel in the 40-MHz band. ▪ **Lower**. Set the Primary Channel as the lower 20-MHz channel in the 40-MHz band.
Short Guard Interval Supported	This field is available only if the radio mode includes 802.11n. The guard interval is the dead time, in nanoseconds, between OFDM symbols. It prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10 percent improvement in data throughput. Select one of the following options: ▪ **Yes**. The access point transmits data using a 400 ns guard Interval when communicating with clients that also support the short guard interval. ▪ **No**. The access point transmits data using an 800 ns guard interval.

Table 19 Advanced Settings Field Descriptions

Field	Description
STBC Mode	This field is available only if the radio mode includes 802.11n. Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams. Select one of the following options: ▪ **On**. The access point transmits the same data stream on multiple antennas at the same time. ▪ **Off**. The access point does not transmit the same data on multiple antennas.
Protection	The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (**Auto**). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the access point. You can disable (**Off**) these protection mechanisms; however, when protection is off, legacy clients or access points within range can be affected by 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and access points from 802.11g transmissions. **Note:** This setting does not affect the ability of the client to associate with the access point.
Beacon Interval	Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). Enter a value from 20 to 2000 milliseconds.

Table 19 Advanced Settings Field Descriptions

Field	Description
DTIM Period	Specify a DTIM period from 1 to 255 beacons. The Delivery Traffic Information Map (DTIM) message is an element included in some beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point and are awaiting pick-up. The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the access point awaiting pickup. The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the access point at every beacon. If you set this field to 10, clients will check on every 10th beacon.

Table 19 Advanced Settings Field Descriptions

Field	Description
Fragmentation Threshold	Specify a number between 256 and 2,346 to set the frame size threshold in bytes. The fragmentation threshold must be set to an even number within the range. The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold you set, the fragmentation function is activated and the packet is sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation is not used. Setting the threshold to the largest value (2346 bytes) effectively disables fragmentation. Fragmentation plays no role when Aggregation is enabled. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help *improve* network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) might help with some interference problems; for example, with microwave ovens. By default, fragmentation is off. We recommend not using fragmentation unless you suspect that there is wireless radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

Table 19 Advanced Settings Field Descriptions

Field	Description
RTS Threshold	Specify a Request to Send (RTS) Threshold value between 0 and 2347. The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. Changing the RTS threshold can help control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Maximum Stations	Specify the maximum number of stations allowed to access this access point at any one time. You can enter a value between 0 and 200.

Table 19 Advanced Settings Field Descriptions

Field	Description
Transmit Power	Select the value for the transmit power level for this access point: ▪ Low ▪ Medium ▪ High ▪ Full The default value, which is **Full**, can be more cost-efficient than a lower level since it gives the access point a maximum broadcast range and reduces the number of access points needed. To increase capacity of the network, place access points closer together and reduce the value of the transmit power. This helps reduce overlap and interference among access points. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
Fixed Multicast Rate	Select the multicast traffic transmission rate you want the access point to support.

Table 19 Advanced Settings Field Descriptions

Field	Description
Rate Sets	Check the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise: ▪ **Rate** is expressed in megabits per second. ▪ **Supported** indicates rates that the access point supports. You can check multiple rates (click a check box to select or de-select a rate). The access point automatically chooses the most efficient rate based on factors like error rates and distance of client stations from the access point. ▪ **Basic** indicates rates that the access point will advertise to the network for the purposes of setting up communication with other access points and client stations on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets.
Broadcast/ Multicast Rate Limiting	Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. By default the **Multicast/Broadcast Rate Limiting** option is enabled. When **Multicast/Broadcast Rate Limiting** is disabled, the Rate Limit and Rate Limit Burst fields cannot be modified.
Rate Limit	Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1; the max value is 100 packets per second (pps). Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination. The default rate limit setting is 100 packets per second.
Rate Limit Burst	Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit. The rate limit burst range is 1-150 packets per second. The default rate limit burst setting is 150 packets per second.

Configuring the Wireless Distribution System

The Wireless Distribution System (WDS) allows you to connect multiple access points. With WDS, access points communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. You can configure the access point in point-to-point or point-to-multipoint bridge mode based on the number of links to connect.

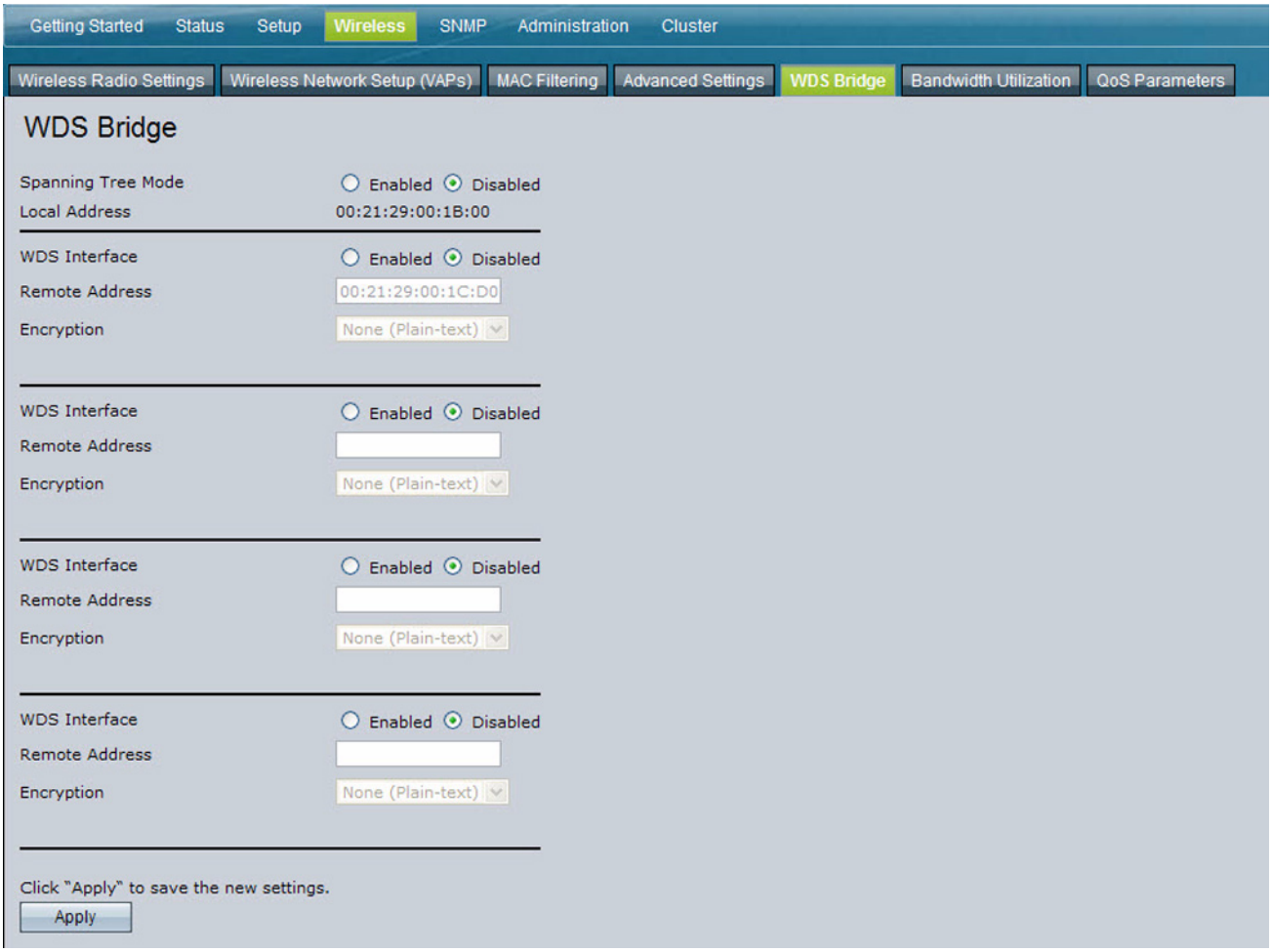
In the point-to-point mode, the access point accepts client associations and communicates with wireless clients and other repeaters. The access point forwards all traffic meant for the other network over the tunnel that is established between the access points. The bridge does not add to the hop count. It functions as a simple OSI layer 2 network device.

In the point-to-multipoint bridge mode, one access point acts as the common link between multiple access points. In this mode, the central access point accepts client associations and communicates with the clients and other repeaters. All other access points associate only with the central access point that forwards the packets to the appropriate wireless bridge for routing purposes.

The access point can also act as a repeater. In this mode, the access point serves as a connection between two access points that might be too far apart to be within cell range. When acting as a repeater, the access point does not have a wired connection to the LAN and repeats signals by using the wireless connection. No special configuration is required for the access point to function as a repeater, and there are no repeater mode settings. Wireless clients can still connect to an access point that is operating as a repeater.

To specify the details of traffic exchange from this access point to others, click the **WDS Bridge** tab.

Figure 18 Configuring WDS Bridge Settings



Before you configure WDS on the access point, note the following guidelines:

- When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address might appear only once on the WDS page for a particular access point.
- Both access points participating in a WDS link must be on the same wireless radio channel and use the same IEEE 802.11 mode. (See **Modifying Advanced Settings, page 74** for information on configuring the Radio mode and channel.)

- When 802.11h is operational, setting up two WDS links can be difficult. See Modifying Advanced Settings, page 74.
- If you use WPA encryption on the WDS link, VAP0 must use WPA Personal or WPA Enterprise as the security mode.

To configure WDS on this access point, describe each remote access point intended to receive and send information to this access point. For each destination access point, configure the fields listed in Table 20.

Table 20 WDS Bridge Settings

Field	Description
Spanning Tree Mode	Spanning Tree Protocol (STP) prevents switching loops. STP is recommended if you configure WDS links. Select **Enabled** to use STP Select **Disabled** to turn off STP links (not recommended)
Local Address	The MAC address for this access point.
Remote Address	The MAC address of the destination access point; the access point on the other end of the WDS link to which data will be sent and from which data will be received. Click the drop-down arrow to the right of the **Remote Address** field to see a list of all the available MAC addresses and their associated SSIDs on the network. Select the appropriate MAC address from the list. **NOTE:** The SSID displayed in the drop-down list is the SSID of the remote access point.
Encryption	You can use no encryption, WEP, or WPA (PSK) on the WDS link. If you are unconcerned about security issues on the WDS link, you might decide not to set any type of encryption. Alternatively, if you have security concerns you can choose between Static WEP and WPA (PSK). In WPA (PSK) mode, the access point uses WPA2-PSK with CCMP (AES) encryption over the WDS link. **NOTE:** To configure WPA-PSK on any WDS link, VAP0 of the selected wireless radio must be configured for WPA-PSK or WPA-Enterprise.

If you select **None** as your preferred WDS encryption option, you will not be asked to fill in any more fields on the **WDS** page. All data transferred between the two access points on the WDS link will be unencrypted.

NOTE To disable a WDS link, you must remove the value configured in the Remote Address field.

WEP on WDS Links

Table 21 describes the additional fields that appear when you select WEP as the encryption type.

Table 21 WEP on WDS Links

Field	Description
Encryption	WEP
WEP	Select this option if you want to set WEP encryption on the WDS link.
Key Length	If WEP is enabled, specify the length of the WEP key: 64 bits 128 bits
Key Type	If WEP is enabled, specify the WEP key type: ASCII Hex
Characters Required	The number of characters required in the WEP key. The field updates automatically based on how you set Key Length and Key Type.
WEP Key	Enter a string of characters. If you selected ASCII, enter any combination of 0–9, a–z, and A–Z. If you selected HEX, enter hexadecimal digits (any combination of 0–9 and a–f or A–F). These are the RC4 encryption keys shared with the stations using the access point.

WPA/PSK on WDS Links

Table 22 describes the additional fields that appear when you select WPA/PSK as the encryption type.

NOTE To configure WPA-PSK on any WDS link, VAP0 of the selected wireless radio must be configured for WPA-PSK or WPA-Enterprise.

Table 22 WPA/PSK on WDS Links

Field	Description
Encryption	WPA (PSK)
SSID	Enter an appropriate name for the new WDS link you have created. This SSID should be different from the other SSIDs used by this access point. However, it is important that the same SSID is also entered at the other end of the WDS link. If this SSID is not the same for both access points on the WDS link, they will not be able to communicate and exchange data. The SSID can be any alphanumeric combination.
Key	Enter a unique shared key for the WDS bridge. This unique shared key must also be entered for the access point at the other end of the WDS link. If this key is not the same for both access points, they will not be able to communicate and exchange data. The WPA-PSK key is a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numerics, and special symbols such as @ and #.

NOTE After you configure the WDS settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Bandwidth Utilization

You can set network utilization thresholds on the access point to maintain the speed and performance of the wireless network as clients associate and disassociate with the access point.

To configure load balancing and set limits and behavior to be triggered by a specified utilization rate of the access point, click the **Bandwidth Utilization** tab and update the fields shown in the following figure.

Figure 19 Configuring Bandwidth Utilization

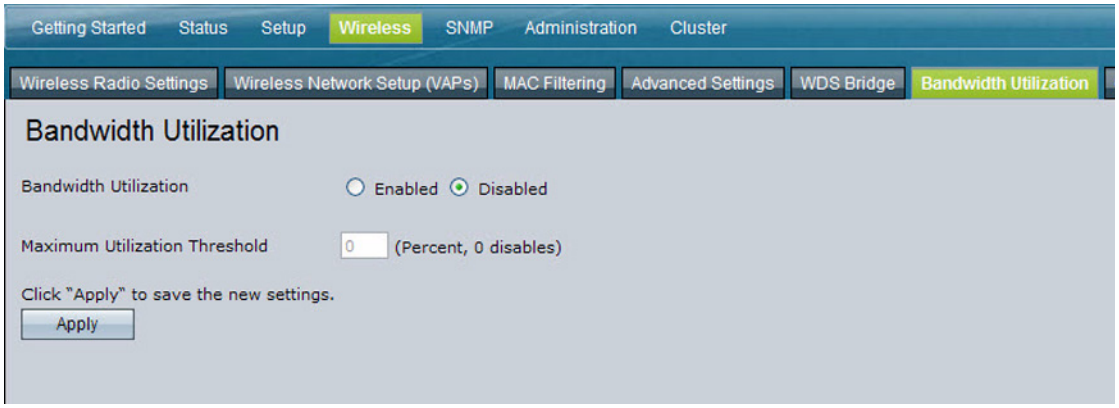


Table 23 Bandwidth Utilization

Field	Description
Bandwidth Utilization	Enable or disable bandwidth utilization: To enable bandwidth utilization this access point, click **Enable**. To disable bandwidth utilization on this access point, click **Disable**.
Maximum Utilization Threshold	Provide the percentage of network bandwidth utilization allowed on the wireless radio before the access point stops accepting new client associations. The default is 0, which means that all new associations are allowed regardless of the utilization rate.

NOTE After you configure the bandwidth utilization settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Configuring Quality of Service (QoS)

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the access point.

Configuring QoS on the access point consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through *Contention Windows*) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station.

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

The default values for the access point and station EDCA parameters are those suggested by the Wi-Fi Alliance in the WMM specification. In normal use these values should not need to be changed. Changing these values will affect the QoS provided.

To set up queues for QoS, click the **QoS** tab under the **Services** heading and configure settings as described in **Table 24**.

Figure 20 Configuring QoS Settings

Table 24 QoS Parameters

Field	Description
AP EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from AP-to-station: **Data 0 (Voice)**—High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)**—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)**—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)**—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Table 24 QoS Parameters (Continued)

Field	Description
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified for Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for **cwMin** are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for cwMin must be less than or equal to the value for cwMax.
cwMax (Maximum Contention Window)	The value specified for the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for **cwMax** are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for cwMax must be higher than or equal to the value for cwMin.

Table 24 QoS Parameters (Continued)

Field	Description
Max. Burst	The **Max. Burst** is an AP EDCA parameter and only applies to traffic flowing from the access point to the client station. This value specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999.0.
Wi-Fi Multimedia Settings	
Wi-Fi MultiMedia (WMM)	Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the access point control *downstream* traffic flowing from the access point to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point. If WMM disabled, all the fields below it are not able to be edited. To disable WMM, click **Disabled**. To enable WMM, click **Enabled**.

Table 24 QoS Parameters (Continued)

Field	Description
Station EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from station-to-AP: **Data 0 (Voice)**—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)**—Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)**—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)**—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	This parameter is used by the algorithm that determines the initial random wait time for data transmission during a period of contention for access point resources. The value specified here in the Minimum Contention Window is the upper limit from which the initial random backoff wait time will be determined. The first random number generated will be a number between 0 and the number specified here. If the timer expires before the data frame is sent, a retry counter is incremented and the random backoff value is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.

Table 24 QoS Parameters (Continued)

Field	Description
cwMax (Maximum Contention Window)	The value specified here in the *Maximum Contention Window* is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.
TXOP Limit	The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the access point. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a client has the right to initiate transmissions towards the access point. The TXOP Limit maximum value is 65535.
Other QoS Settings	
No Acknowledgement	Select On to specify that the access point should not acknowledge frames with QosNoAck as the service class value.
Automatic Power Save Delivery	Select On to enable Automatic Power Save Delivery (APSD), which is a power management method. APSD is recommended if VoIP phones access the network through the access point.

NOTE After you configure the QoS settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

5

SNMP

Configuring SNMP on the Access Point

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The access point supports SNMP versions 1, 2, and 3. Unless specifically noted, all configuration parameters on this page apply to SNMPv1 and SNMPv2c only.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in Management Information Bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as access points, routers, switches, bridges, hubs, servers, or printers.

The access point can function as an SNMP managed device for seamless integration into network management systems such as HP OpenView.

From the **SNMP** page, you can start or stop control of SNMP agents, configure community passwords, access MIBs, and configure SNMP Trap destinations.

From the pages under the SNMP heading, you can manage SNMPv3 users and their security levels and define access control to the SNMP MIBs. For information about how to configure SNMPv3 views, groups, users, and targets, see **Configuring SNMP Views, page 101**.

To configure SNMP, click the **General** tab under the **SNMP** heading and update the fields described in **Table 25 on page 98**.

Figure 21 Modifying SNMP Settings

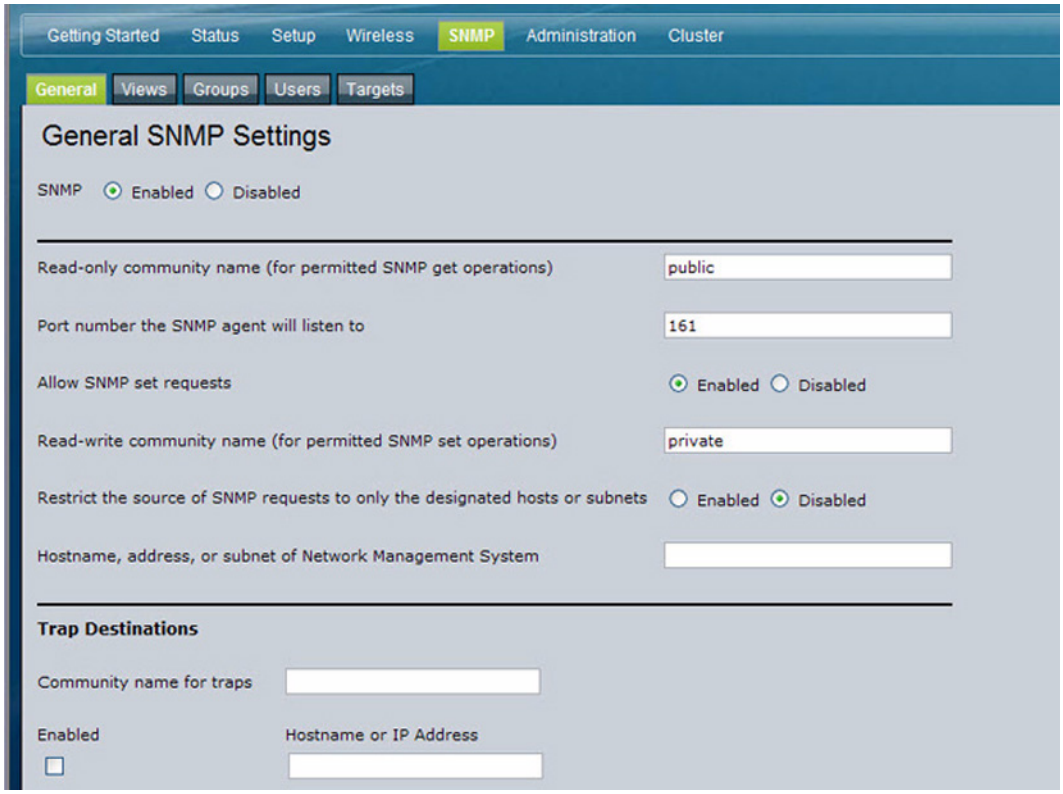


Table 25 SNMP Settings

Field	Description
SNMP Enabled/Disabled	You can specify the SNMP administrative mode on your network. By default SNMP is disabled. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**. After changing the mode, you must click **Apply** to save your configuration changes. **NOTE:** If you disable SNMP, all remaining fields on the SNMP page are disabled. This is a global SNMP parameter that applies to SNMPv1, SNMPv2c, and SNMPv3.

Table 25 SNMP Settings (Continued)

Field	Description
Read-only community name (for permitted SNMP get operations)	Enter a read-only community name. The community name, as defined in SNMPv2c, acts as a simple authentication mechanism to restrict the machines on the network that can request data to the SNMP agent. The name functions as a password, and the request is assumed to be authentic if the sender knows the password. The community name can be in any alphanumeric format. Double quote (") is not a valid character.
Port number the SNMP agent will listen to	By default, an SNMP agent only listens to requests from port 161. However, you can configure this parameter so that the agent listens to requests on another port. Enter the port number on which you want the SNMP agents to listen to requests. **NOTE:** This is a global SNMP parameter that applies to SNMPv1, SNMPv2c, and SNMPv3.
Allow SNMP set requests	You can choose whether or not to allow SNMP set requests on the access point. Enabling SNMP set requests means that machines on the network can execute configuration changes by using the SNMP agent on the access point to the Cisco System MIB. To enable SNMP set requests, click **Enabled**. To disable SNMP set requests click **Disabled**.
Read-write community name (for permitted SNMP set operations)	If you have enabled SNMP set requests you can set a read-write community name. Setting a community name is similar to setting a password. Only requests from the machines that identify themselves with this community name will be accepted. The community name can be in any alphanumeric format. Double quote (") is not a valid character.

Table 25 SNMP Settings (Continued)

Field	Description
Restrict the source of SNMP requests to only the designated hosts or subnets	You can restrict the source of permitted SNMP requests. To restrict the source of permitted SNMP requests, click **Enabled**. To permit any source submitting an SNMP request, click **Disabled**.
Hostname, address or subnet of Network Management System	Specify the IPv4 DNS hostname or subnet of the machines that can execute *get* and *set* requests to the managed devices. As with community names, this provides a level of security on SNMP settings. The SNMP agent only accepts requests from the hostname or subnet specified here. To specify a subnet, enter one or more subnetwork address ranges in the form *address/mask_length* where *address* is an IP address and *mask_length* is the number of mask bits. Both formats *address/mask* and *address/mask_length* are supported. Individual hosts can be provided for this, i.e. I.P Address or Hostname. For example, if you enter a range of `192.168.1.0/24` this specifies a subnetwork with address `192.168.1.0` and a subnet mask of `255.255.255.0`. The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute get and set requests on the managed device. Given the example above, the machines with addresses from `192.168.1.1` through `192.168.1.254` can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by `.255` in the range is always reserved for the broadcast address). As another example, if you enter a range of `10.10.1.128/25`, machines with IP addresses from `10.10.1.129` through `10.10.1.254` can execute SNMP requests on managed devices. In this example, `10.10.1.128` is the network address and `10.10.1.255` is the broadcast address. 126 addresses are designated.

Table 25 SNMP Settings (Continued)

Field	Description
Community name for traps	Enter the global community string associated with SNMP traps. Traps sent from the device provide this string as a community name. The community name can be in any alphanumeric format. Special characters are not permitted. Double quote (") is not a valid character.
Hostname or IP address	Enter the DNS hostname of the computer to which you want to send SNMP traps. An example of a DNS hostname is: `snmptraps.foo.com`. Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can add up to a maximum of three DNS hostnames. Select the **Enabled** check box beside the appropriate hostname.

NOTE After you configure the SNMP settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Configuring SNMP Views

A MIB view is combination of a set of view subtrees or a family of view subtrees where each view subtree is a subtree within the managed object naming tree. You can create MIB views to control the OID range that SNMPv3 users can access.

A MIB view called **all** that contains all management objects supported by the system is created by default.

NOTE If you create an *excluded* view subtree, create a corresponding *included* entry with the same view name to allow subtrees outside of the excluded subtree to be included. For example, to create a view that excludes the subtree 1.3.6.1.4, create an *excluded* entry with the OID 1.3.6.1.4. Then, create an *included* entry with OID .1 with the same view name.

Figure 22 SNMPv3 Views

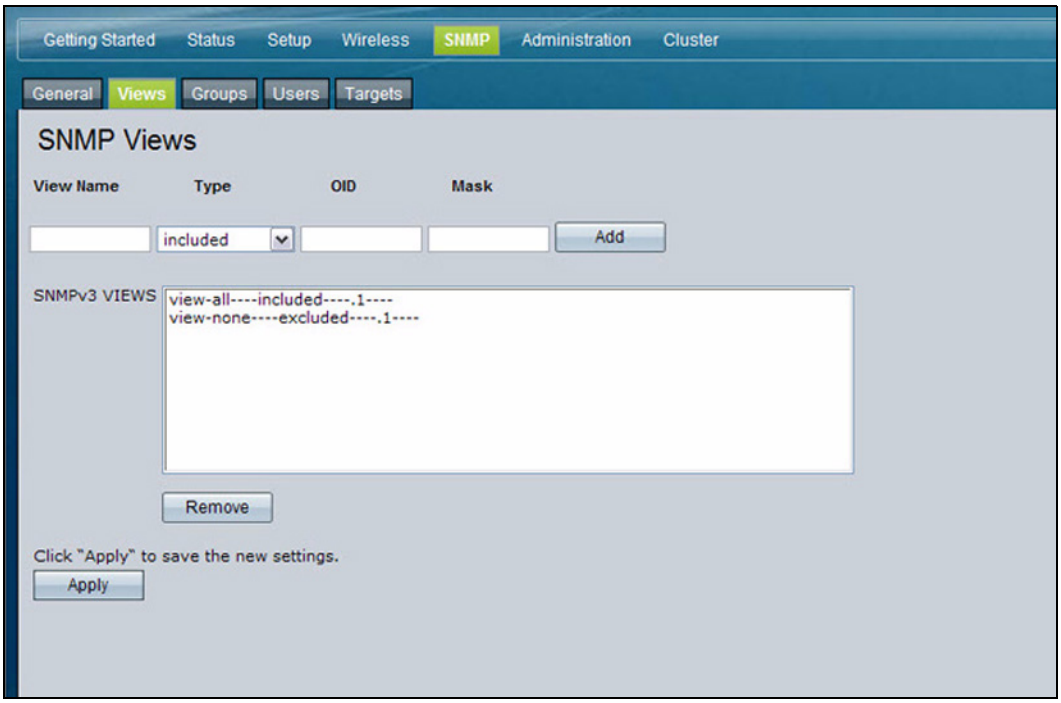


Table 26 describes the fields you can configure on the SNMPv3 Views page.

Table 26 SNMPv3 Views

Field	Description
View Name	Enter a name to identify the MIB view. View names can contain up to 32 alphanumeric characters. Double quote (") is not a valid character.
Type	Specifies whether to include or exclude the view subtree or family of subtrees from the MIB view.

Table 26 SNMPv3 Views

Field	Description
OID	Enter an OID string for the subtree to include or exclude from the view. OID string is 256 characters in length. For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.
Mask	The OID mask is 47 characters in length. The format of the OID mask is xx.xx.xx...or xx.xx.xx... and is 16 octets in length. Each octet is 2 hexadecimal characters separated by either a "." (period) or ":" (colon). Only hex characters are accepted in this field. For example, OID mask FA.80 is 11111010.10000000. A family mask is used to define a family of view subtrees. The family mask indicates which sub-identifiers of the associated family OID string are significant to the family's definition. A family of view subtrees allows control access to one row in a table, in a more efficient manner.
SNMPv3 Views	This field shows the MIB views on the access point. To remove a view, select it and click **Remove**.

NOTE After you configure the SNMPv3 Views settings, you must click **Apply** to apply the changes and to save the settings.

Configuring SNMP Groups

SNMPv3 groups allow you to combine users into groups of different authorization and access privileges.

By default, the access point has three groups:

- **RO**—A read-only group with no authentication and no data encryption. No security is provided by this group. By default, users of this group have read access to the default all MIB view, which can be modified by the user.
- **RWAuth**—A read/write group using authentication, but no data encryption. Users in this group send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. By default, users of this group have read and write access to default all MIB view, which can be modified by the user.

- **RWPriv**—A read/write group using authentication and data encryption. Users in this group use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined. By default, users of this group have read and write access to default all MIB view, which can be modified by the user.

RWPriv, RWAuth, and RO groups are defined by default.

To define additional groups, navigate to the **SNMP Groups** page and configure the settings that Table 27 describes.

Figure 23 SNMPv3 Groups

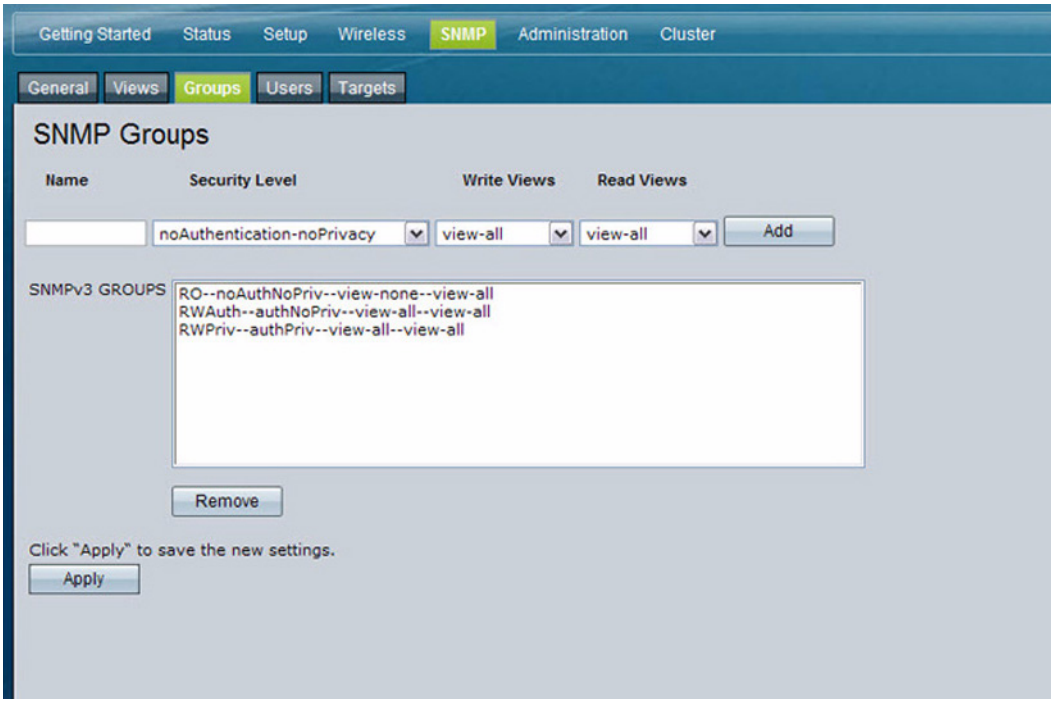


Table 27 SNMPv3 Groups

Field	Description
Name	Specify a name to use to identify the group. The default group names are RWPriv, RWAuth, and RO. Group names can contain up to 32 alphanumeric characters. Double quote (") is not a valid character.

Table 27 SNMPv3 Groups

Field	Description
Security Level	Select one of the following security levels for the group: **noAuthentication-noPrivacy**—No authentication and no data encryption (no security). **Authentication-noPrivacy**—Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. **Authentication-Privacy**—Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption. For groups that require authentication, encryption, or both, you must define the MD5 and DES key/passwords on the SNMPv3 Users page.
Write Views	Select the write access to management objects (MIBs) for the group: **write-all**—The group can create, alter, and delete MIBs. **write-none**—The group is not allowed to create, alter, or delete MIBS.
Read Views	Select the read access to management objects (MIBs) for the group: **view-all**—The group is allowed to view and read all MIBs. **view-none**—The group cannot view or read MIBs.
SNMPv3 Groups	This field shows the default groups and the groups that you have defined on the access point. To remove a group, select the group and click **Remove**.

NOTE After you configure the SNMPv3 Groups settings, you must click **Apply** to apply the changes and to save the settings.

Configuring SNMP Users

From the **SNMP Users** page, you can define multiple users, associate the desired security level to each user, and configure security keys.

For authentication, only MD5 type is supported, and for encryption only DES type is supported. There are no default SNMPv3 users on the access point.

Figure 24 SNMPv3 Users

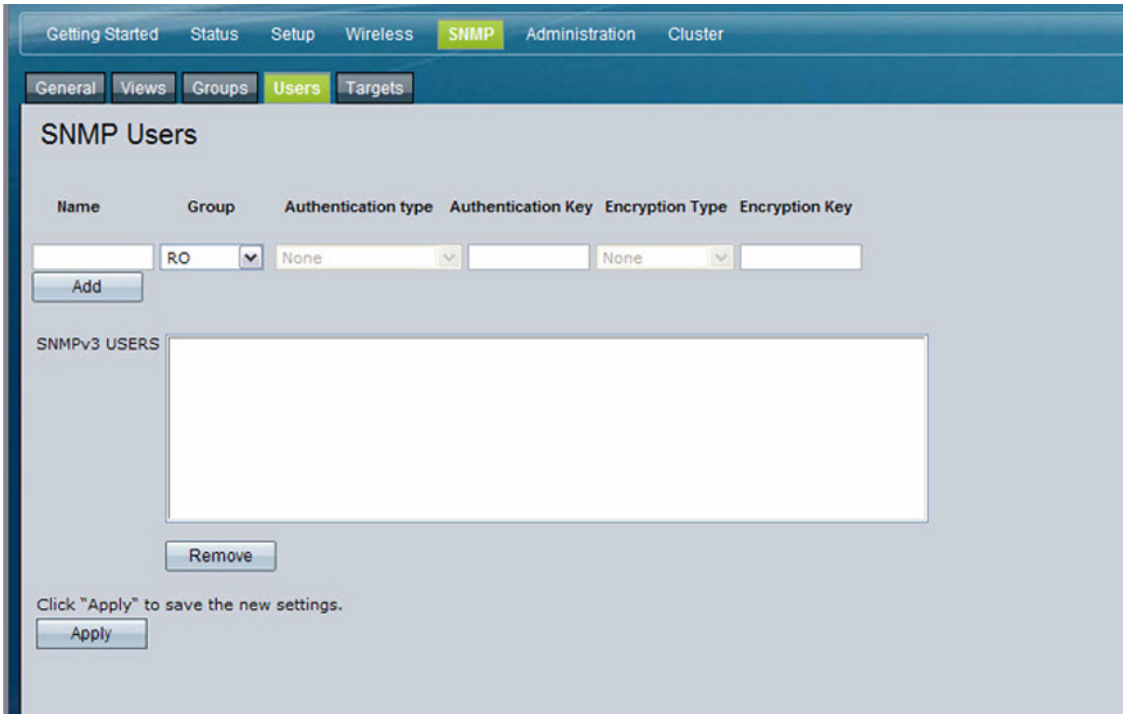


Table 28 describes the fields to configure SNMPv3 users.

Table 28 SNMP v3 Users

Field	Description
Name	Enter the user name to identify the SNMPv3 user. User names can contain up to 32 alphanumeric characters. Double quote (") is not a valid character.
Group	Map the user to a group. The default groups are RWAuth, RWPriv, and RO. You can define additional groups on the **SNMP Groups** page.

Table 28 SNMP v3 Users (Continued)

Field	Description
Authentication Type	Select the type of authentication to use on SNMP requests from the user: **MD5**—Require MD5 authentication on SNMPv3 requests from the user. **None**—SNMPv3 requests from this user require no authentication.
Authentication Key	If you specify **MD5** as the authentication type, enter a password to enable the SNMP agent to authenticate requests sent by the user. The passphrase must be between 8 and 32 characters in length.
Encryption Type	Select the type of privacy to use on SNMP requests from the user: **DES**—Use DES encryption on SNMPv3 requests from the user. **None**—SNMPv3 requests from this user require no privacy.
Encryption Key	If you specify **DES** as the privacy type, enter a key to use to encrypt the SNMP requests. The passphrase must be between 8 and 32 characters in length.
SNMPv3 Users	This field shows the users that you have defined on the access point. To remove a user, select the user and click **Remove**.

NOTE After you configure the SNMPv3 Users settings, you must click **Apply** to apply the changes and to save the settings.

SNMP Targets

SNMPv3 Targets send trap messages to the SNMP manager. Each target is identified by a target name and associated with target IP address, UDP port, and SNMP user name.

Figure 25 SNMPv3 Target

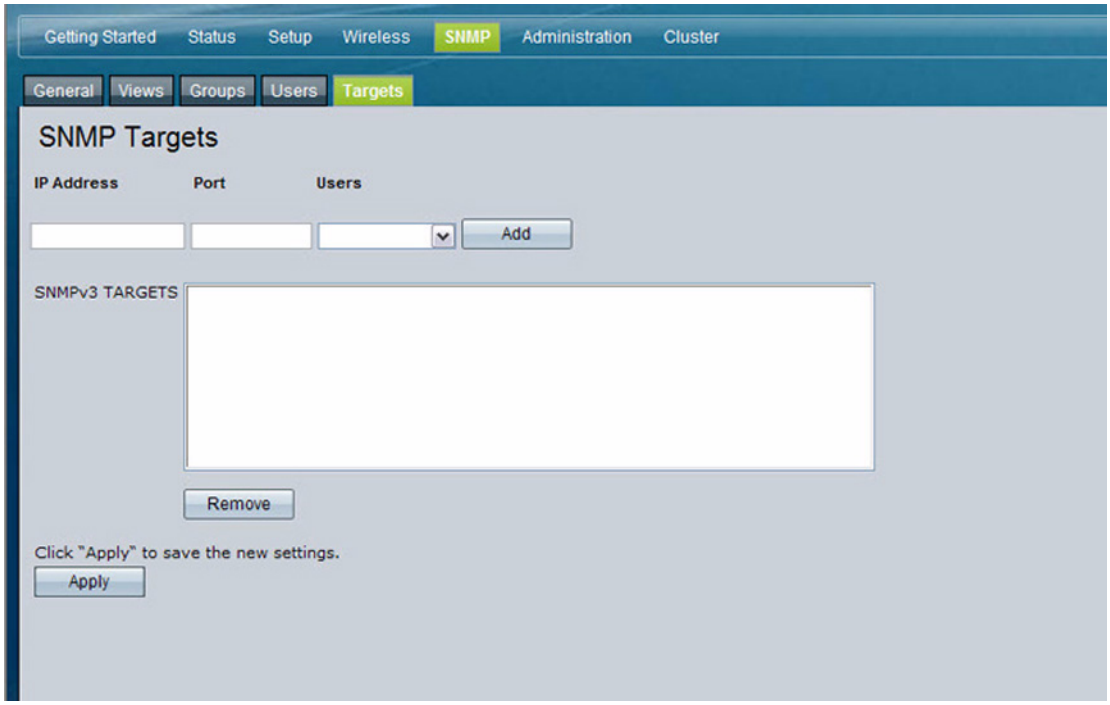


Table 29 SNMPv3 Targets

Field	Description
IP Address	Enter the IP address of the remote SNMP manager to receive the target.
Port	Enter the UDP port to use for sending SNMP targets.
Users	Enter the name of the SNMP user to associate with the target.To configure SNMP users, see **Configuring SNMP Users, page 106**.
SNMPv3 Targets	This field shows the SNMPv3 Targets on the access point. To remove a target, select it and click **Remove**.

NOTE After you configure the SNMPv3 Target settings, you must click **Apply** to apply the changes and to save the settings.

6

Administration

Administrator

Use this page to configure the administrator information and to provide a new administration password for the access point. The default password is `cisco`.

NOTE As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.

Figure 26 Administrator Configuration Page

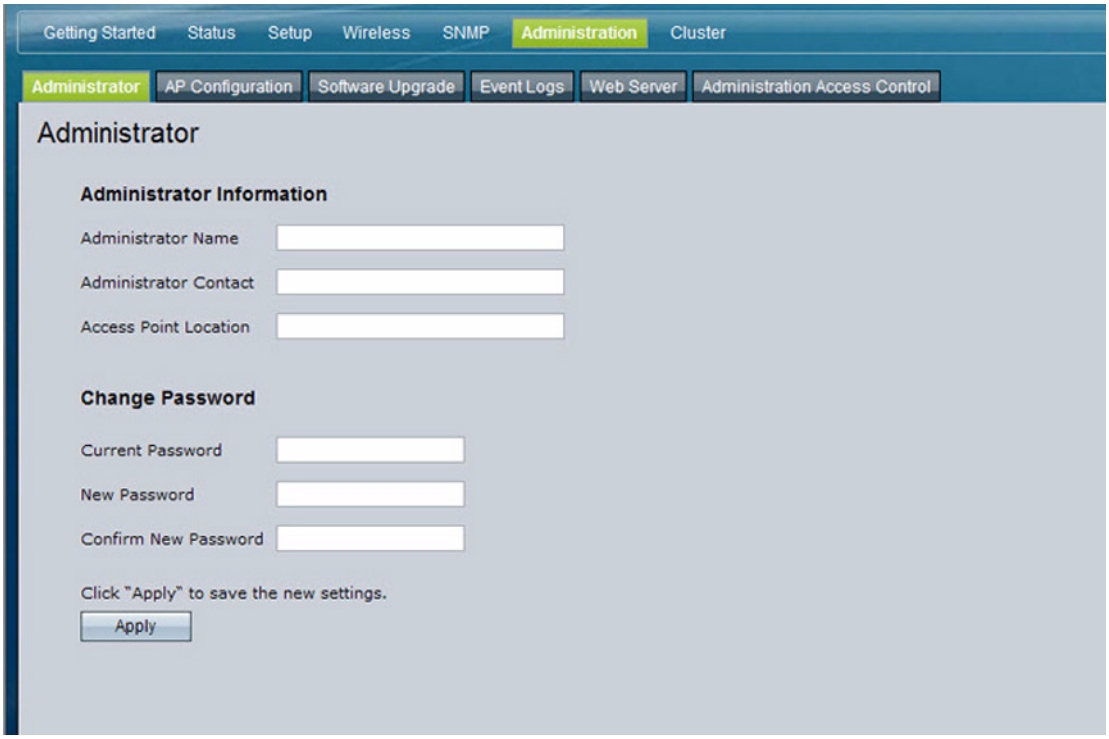


Table 30 describes the fields and configuration options on the **Administrator** page.

Table 30 Administrator Page

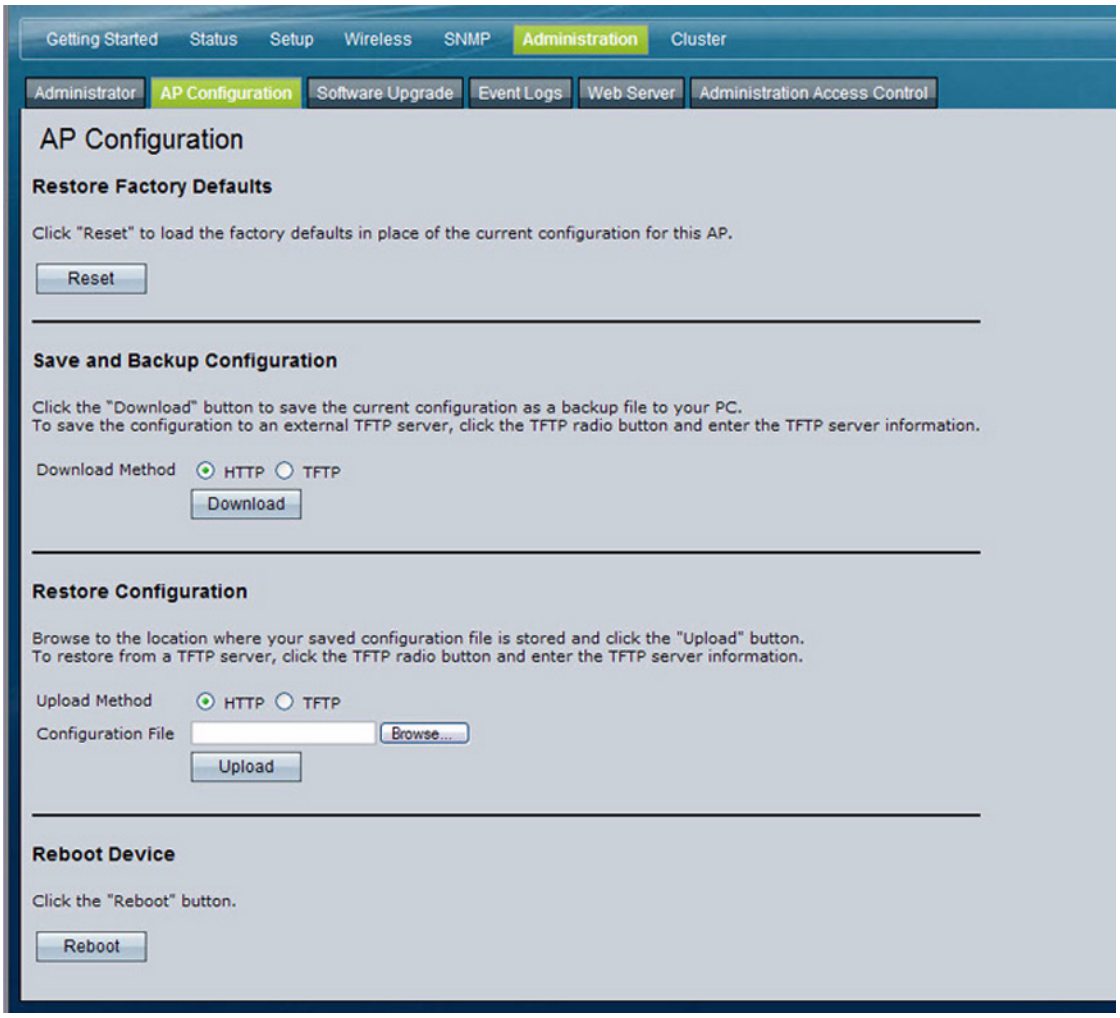
Field	Description
Administrator Name	Enter the name of the administrator. You can use up to 64 alphanumeric and symbols characters. [ASCII values 32 to 126 excluding double quote(")].
Administrator Contact	Enter the e-mail address or phone number of the person to contact regarding issues related to the access point. You can use up to 255 alphanumeric and symbols characters. (ASCII values 32 to 126 excluding double quote.)
Access Point Location	Enter the physical location of the access point, for example *Conference Room A*. You can use up to 255 alphanumeric and symbols characters. (ASCII values 32 to 126 excluding double quote.)
Current Password	Enter the current administrator password. You must correctly enter the current password before you are able to change it.
New Password	Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type. The administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces.
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.

NOTE After you configure the settings on the Administrator page, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Access Point Configuration

The access point configuration file is in XML format and contains all of the information about the access point settings. You can download the configuration file to a management station to manually edit the content or to save as a back-up copy. When you upload a configuration file to the access point, the configuration information in the XML file is applied to the access point. Click the **AP Configuration** tab to access the configuration management page, which Figure 27 shows.

Figure 27 Configuration Management Page



Resetting the Access Point to the Factory Default Configuration

If you are experiencing problems with the access point and have tried all other troubleshooting measures, click **Reset**. This restores factory defaults and clears all settings, including settings such as the password or wireless settings. You can also use the **Reset** button to reset the system to the default configuration.

Saving the Current Configuration to a Backup File

You can use HTTP or TFTP to transfer files to and from the access point. After you download a configuration file to the management station, you can manually edit the file, which is in XML format. Then, you can upload the edited configuration file to apply those configuration settings to the access point.

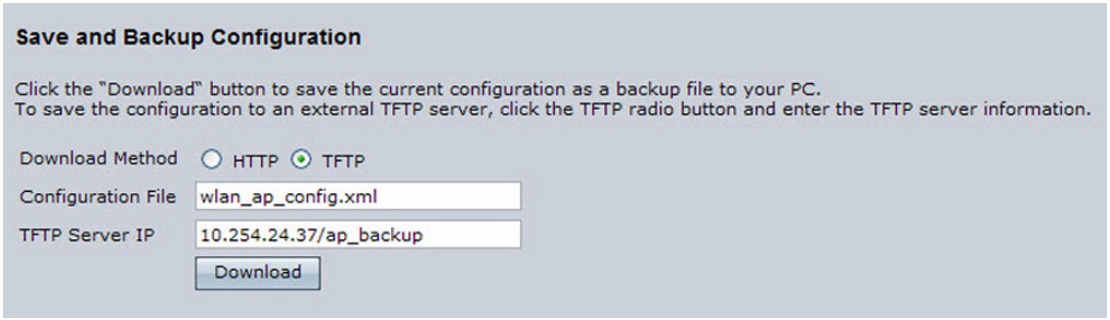
Saving the Current Configuration by using TFTP

Use the following steps to save a copy of the current settings on an access point to a backup configuration file by using TFTP:

STEP 1 If it is not already selected, click the radio button for using TFTP to download the file.

STEP 2 Enter a name for the backup file in the **Configuration File** field, including the .xml file name extension and the path to the directory where you want to save the file.

STEP 3 Enter the IP address of the TFTP server.



STEP 4 Click **Download** to save the file.

Saving the Current Configuration by using HTTP

Use the following steps to save a copy of the current settings on an access point to a backup configuration file by using HTTP:

STEP 1 Click the HTTP radio button.

STEP 2 Click the **Download** button. A File Download or Open dialog box displays.

STEP 3 From the dialog box, choose the **Save** option. A file browser dialog box opens.

STEP 4 Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

You can keep the default file name (config.xml) or rename the backup file, but be sure to save the file with an .xml extension.

Restoring the Configuration from a Previously Saved File

You can use HTTP or TFTP to transfer files to and from the access point. After you download a configuration file to the management station, you can manually edit the file, which is in XML format. Then, you can upload the edited configuration file to apply those configuration settings to the access point.

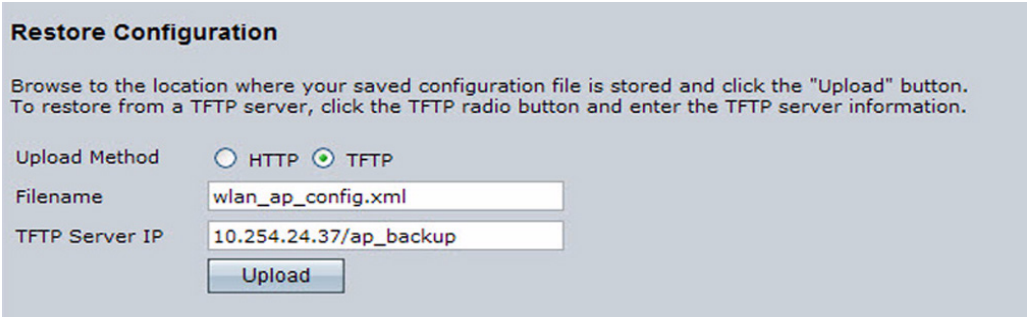
Restoring the Current Configuration by using TFTP

Use the following procedures to restore the configuration on an access point to previously saved settings by using TFTP:

STEP 1 If it is not already selected, click the **TFTP** radio button.

STEP 2 Enter a name for the backup file in the **Filename** field, including the .xml file name extension and the path to the directory that contains the configuration file to upload.

STEP 3 Enter the IP address of the TFTP server.



STEP 4 Click the **Restore** button.

The access point reboots. A reboot confirmation dialog and follow-on rebooting status message displays. Please wait for the reboot process to complete, which might take several minutes.

The Configuration Utility is not accessible until the access point has rebooted.

Restoring the Current Configuration by Using HTTP

Use the following steps to save a copy of the current settings on an access point to a backup configuration file by using HTTP:

STEP 1 Clear the **Use TFTP to upload the file** option.

When you clear the radio button, the Server IP field is disabled.

STEP 2 Enter the name of the file to restore.

STEP 3 Click **Restore**.

A **File Upload** or **Choose File** dialog box displays.

STEP 4 Navigate to the directory that contains the file, then select the file to upload and click **Open**.

NOTE Only those files saved as .xml backup configuration files are valid to use with Restore; for example, `ap_config.xml`.

STEP 5 Click **Restore**.

The access point reboots. A reboot confirmation dialog and follow-on rebooting status message displays. Please wait for the reboot process to complete, which might take several minutes.

The Configuration Utility is not accessible until the access point has rebooted.

Rebooting the Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the access point. To reboot the access point, click the **Reboot** button on the **Configuration** page.

Software Upgrade

As new versions of the access point software become available, you can upgrade the software on your devices to take advantage of new features and enhancements. The access point uses a TFTP client for software upgrades. You can also use HTTP to perform software upgrades.

NOTE When you upgrade the software, the access point retains the existing configuration information.

NOTE By default, the access point uses HTTP for software upgrades instead of TFTP.

Upgrading the Software by using TFTP

Use the following steps to upgrade the software on an access point by using TFTP:

STEP 1 Click the **Software Upgrade** tab in the **Administration** section.

Information about the current software version is displayed and an option to upgrade a new software image is provided.

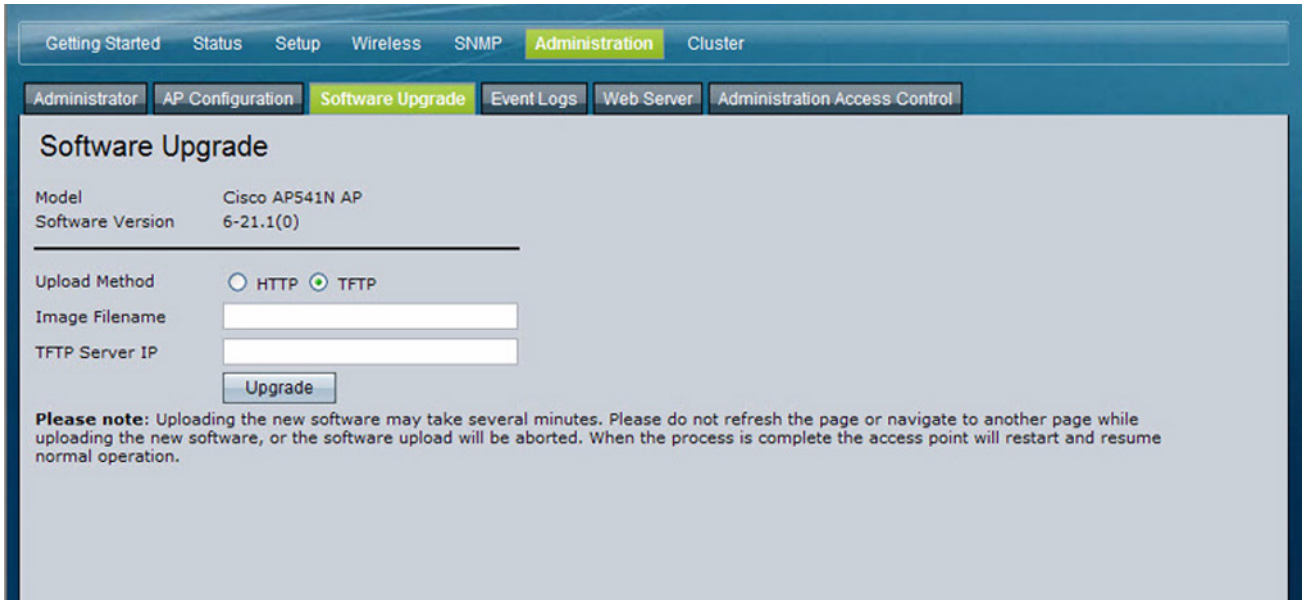
STEP 2 Make sure the **Upload Method TFTP** radio button is selected.

STEP 3 Enter a name for the image file in the **New Software Image** field, including the path to the directory that contains the image to upload.

For example, to upload the *ap_upgrade.tar* image located in the */share/builds/ap* directory, enter */share/builds/ap/ap_upgrade.tar* in the **New Software Image** field.

The software upgrade file supplied must be a *tar* file. Do not attempt to use *bin* files or files of other formats for the upgrade; these types of files will not work.

STEP 4 Enter the IP address of the TFTP server in the **Server IP** field.



STEP 5 Click **Upgrade**.

Upon clicking **Upgrade**, a popup confirmation window is displayed that describes the upgrade process.

STEP 6 Click **OK** to confirm the upgrade and start the process.

NOTE The software upgrade process begins once you click **Upgrade** and then **OK** in the popup confirmation window.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point restarts. The access point resumes normal operation with the same configuration settings it had before the upgrade.

STEP 7 To verify that the software upgrade completed successfully, check the software version shown on the **Software Upgrade** tab (and also on the **Summary** section). If the upgrade was successful, the updated version name or number is indicated.

Upgrading the Software by Using HTTP

Use the following steps to upgrade the software on an access point by using HTTP:

STEP 1 Clear the **Upload Method TFTP** option.

When you clear the radio button, the Server IP field is disabled.

STEP 2 If you know the path to the **New Software Image** file, enter it in the **New Software Image** field. Otherwise, click the **Browse** button and locate the software image file.

The software upgrade file supplied must be a *tar* file. Do not attempt to use *bin* files or files of other formats for the upgrade; these types of files will not work.

STEP 3 Click **Upgrade** to apply the new software image.

Upon clicking **Upgrade** for the software upgrade, a popup confirmation window is displayed that describes the upgrade process.

STEP 4 Click **OK** to confirm the upgrade and start the process.

NOTE The software upgrade process begins when you click **Upgrade** and then **OK** in the popup confirmation window.

The upgrade process might take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in progress. When the upgrade is complete, the access point restarts. The access point resumes normal operation with the same configuration settings it had before the upgrade.

STEP 5 To verify that the software upgrade completed successfully, check the software version shown on the **Software Upgrade** tab. (It is also shown in the **Summary** section). If the upgrade was successful, the updated version name or number is indicated.

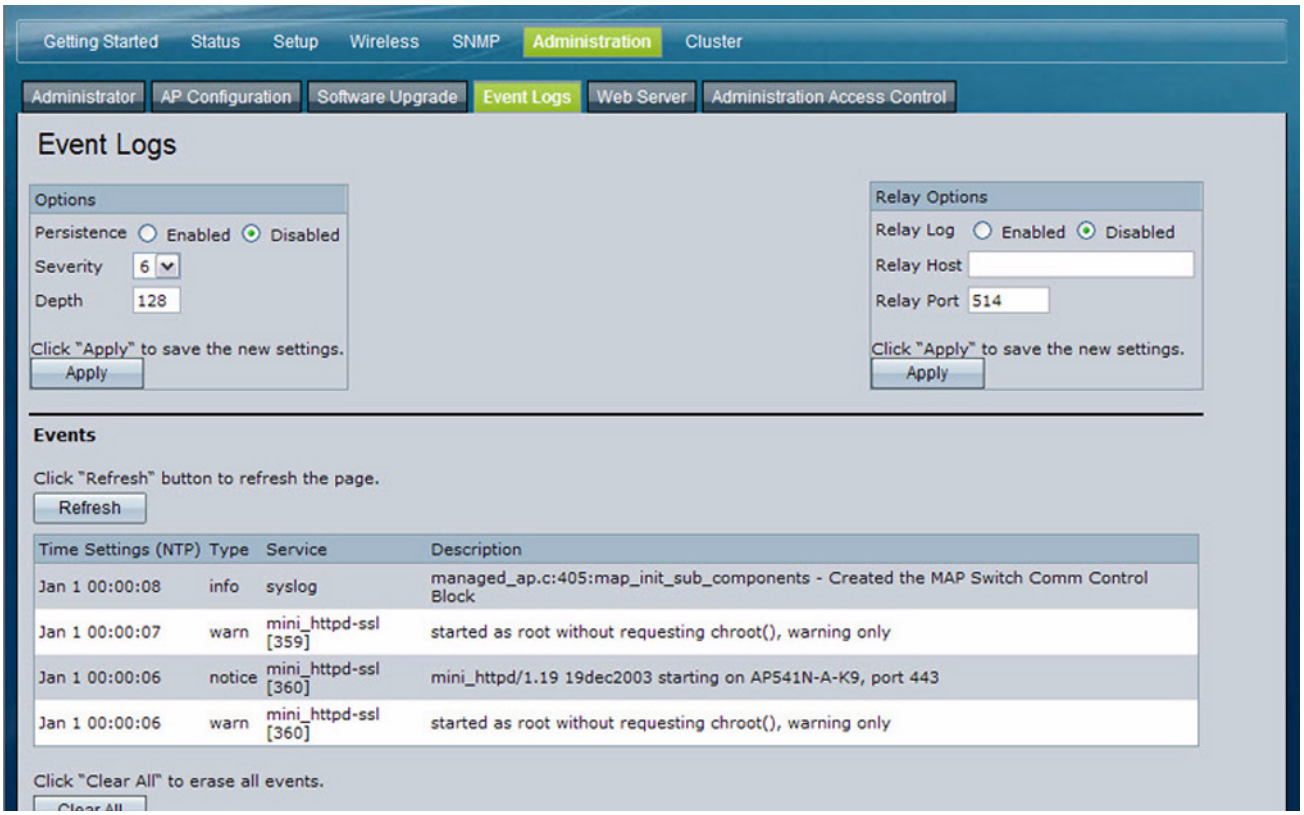
Event Logs

The **Events** page shows real-time system events on the access point such as wireless clients associating with the access point and being authenticated.

You can view the most recent events generated by this access point and configure logging settings. You can enable and configure persistent logging to write system event logs to non-volatile memory so that the events are not erased when the system reboots. And you can enable a remote log relay host to capture all system events and errors in a Kernel Log.

To view system events, click the **Events** tab.

Figure 28 Event Logs



Click **Refresh** to refresh the page.

NOTE The access point acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as Greenwich Mean Time). You need to convert the reported time to your local time. For information on setting the network time protocol, see **Enabling the Network Time Protocol, page 41**.

Configuring Persistent Logging Options

If the system unexpectedly reboots, log messages can help you diagnose the cause. However, log messages are erased when the system reboots unless you enable persistent logging.

WARNING Enabling persistent logging can wear out the flash (non-volatile) memory and degrade network performance. You should only enable persistent logging to debug a problem. Make sure you disable persistent logging after you finish debugging the problem.

To configure persistent logging on the **Event Logs** page, set the persistence, severity, and depth options as described in **Table 31**, and then click **Apply.**

Figure 29 Persistent Logging Options

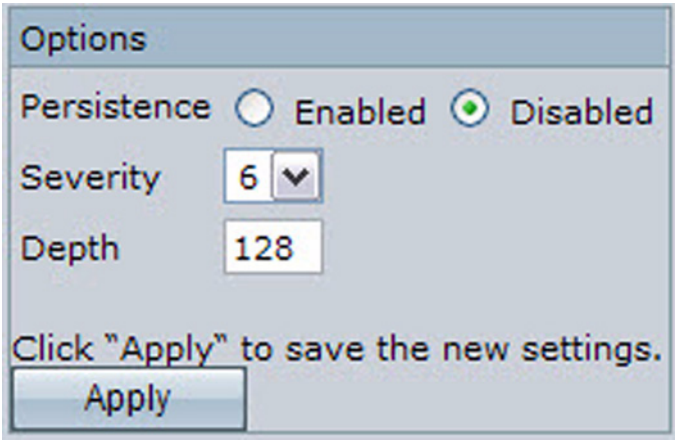


Table 31 Logging Options

Field	Description
Persistence	Choose **Enabled** to save system logs to non-volatile memory so that the logs are not erased when the access point reboots. Choose **Disabled** to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
Severity	Specify the severity level of the log messages to write to non-volatile memory. For example, if you specify 2, critical, alert, and emergency logs are written to non-volatile memory. Error messages with a severity level of 3–7 are written to volatile memory. **0**—emergency **1**—alert **2**—critical **3**—error **4**—warning **5**—notice **6**—info **7**—debug
Depth	You can store up to 128 messages in non-volatile memory. Once the number you configure in this field is reached, the oldest log event is overwritten by the new log event.

NOTE To apply your changes, click **Apply**. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

Configuring the Log Relay Host for Kernel Messages

The Kernel Log is a comprehensive list of system events (shown in the System Log) and kernel messages such as error conditions, like dropping frames.

You cannot view kernel log messages directly from the *Access Point Configuration Utility* for an access point. You must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. Then, you can configure the access point to send syslog messages to the remote server.

Remote log server collection for access point syslog messages provides the following features:

- Allows aggregation of syslog messages from multiple access points
- Stores a longer history of messages than kept on a single access point
- Triggers scripted management operations and alerts

To use Kernel Log relaying, you must configure a remote server to receive the syslog messages. The procedure to configure a remote log host depends on the type of system you use as the remote host.

NOTE The syslog process will default to use port 514. We recommend keeping this default port. However; If you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process.

Enabling or Disabling the Log Relay Host on the Events Page

To enable and configure Log Relaying on the **Event Logs** page, set the Log Relay options as described in Log Relay Host, page 124, and then click **Apply.**

Figure 30 Log Relay Host

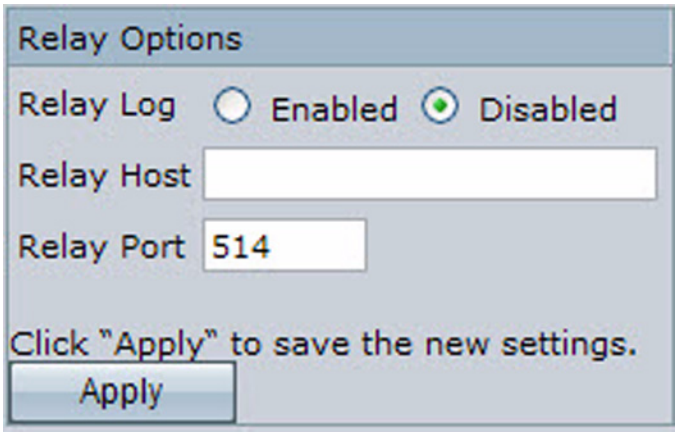


Table 32 Log Relay Host

Field	Description
Relay Log	Choose to either enable or disable use of the Log Relay Host. If you select the **Relay Log** radio button, the Log Relay Host is enabled and the Relay Host and Relay Port fields are editable.
Relay Host	Specify the IP Address or DNS name of the remote log server.
Relay Port	Specify the Port number for the syslog process on the Relay Host. The default port is 514.

NOTE To apply your changes, click **Apply**. Changing some settings might cause the access point to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

If you enabled the Log Relay Host, clicking **Apply** activates remote logging. The access point sends its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you disabled the Log Relay Host, clicking **Apply** disables remote logging.

Configuring the Web Server Settings

The access point can be managed through HTTP or secure HTTP (HTTPS) sessions. By default both HTTP and HTTPS access are enabled. Either access type can be disabled.

To configure the Web server settings, click the Web Server tab.

Figure 31 Configuring Web Server Settings

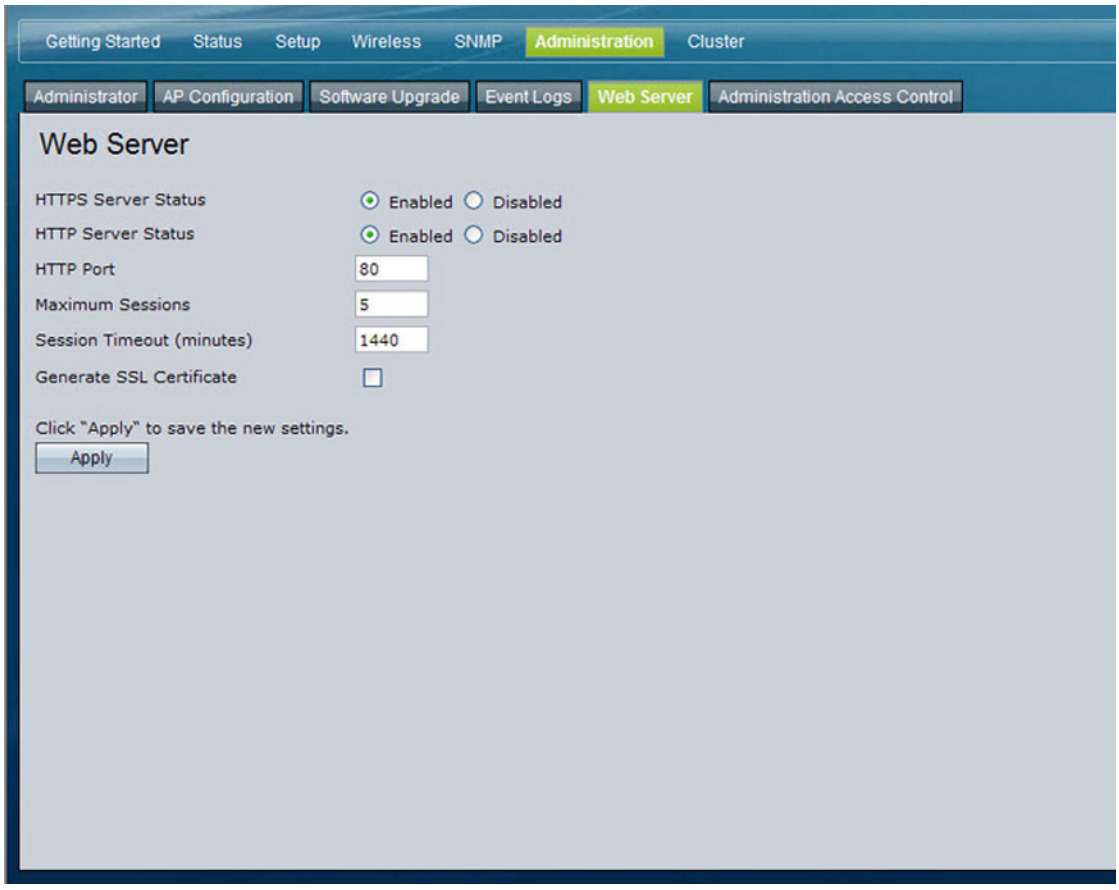


Table 33 Web Server Settings

Field	Description
HTTPS Server Status	**Enable** or **disable** access through a Secure HTTP Server (HTTPS). This setting is independent of the HTTP server status setting.
HTTP Server Status	**Enable** or **disable** access through HTTP. This setting is independent of the HTTPS server status setting.
HTTP Port	Specify the port number for HTTP traffic. (The default is 80.)
Maximum Sessions	Specify the maximum number of HTTP and HTTPS connections permitted to the access point Web server that are allowed at the same time. The permitted range is 1–10. The number you enter affects the number of connections to the access point Configuration Utility. It has no impact on the number of wireless clients allowed to associate with the access point.
Session Timeout	Enter the number of minutes a HTTP or HTTPS session remains idle before the session is terminated. The valid range is 1–1440 minutes (24 hours).
Generate SSL Certificate	Select this option to generate a new SSL certificate for the secure Web server. This should be done once the access point has an IP address to ensure that the common name for the certificate matches the IP address of the access point. Generating a new SSL certificate restarts the secure Web server. The secure connection will not work until the new certificate is accepted on the browser.

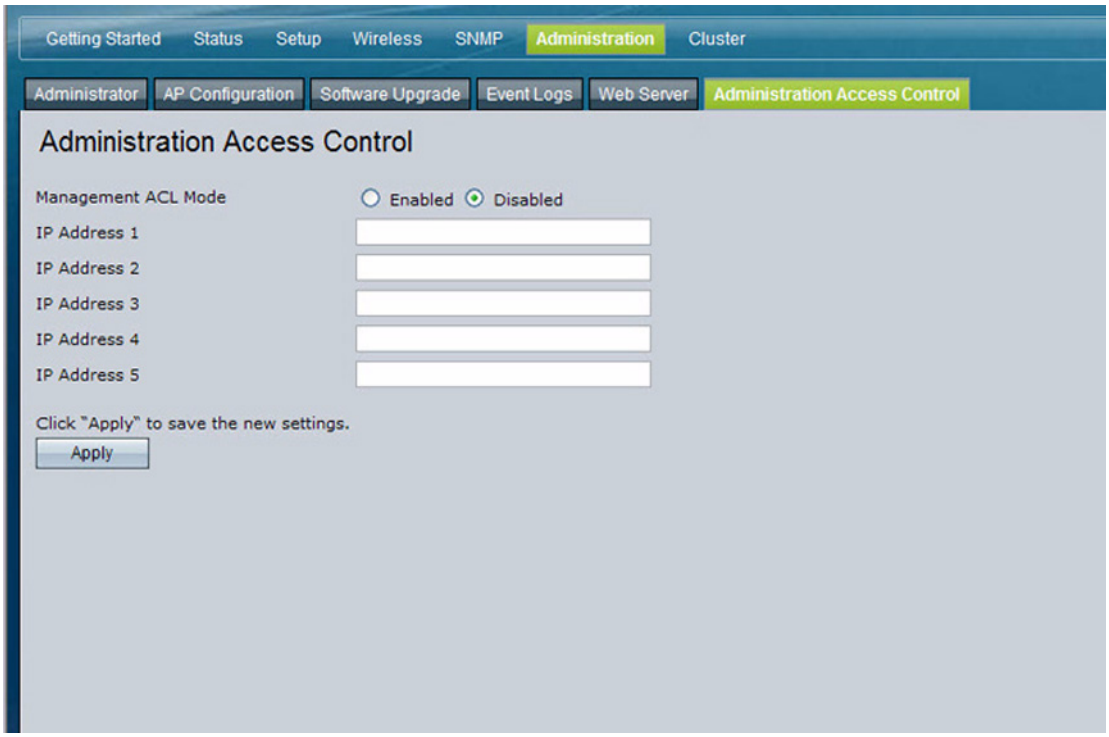
NOTE Click **Apply** to apply the changes and to save the settings. If you disable the protocol you are currently using to access the access point management interface, the current connection will end and you will not be able to access the access point by using that protocol until it is enabled.

Creating an Administration Access Control List

You can create an access control list (ACL) that lists up to five IPv4 hosts that are authorized to access the access point management interface by Web, Telnet, and SNMP. If this feature is disabled, anyone can access the management interface from any network client by supplying the correct access point username and password.

To create an access list, click the Administration Access Control tab.

Figure 32 Management ACL



NOTE After you configure the settings, click **Apply** to apply the changes and to save the settings.

Table 34 Management ACL

Field	Description
Management ACL Mode	**Enable** or **disable** the management ACL feature. At least one IPv4 address should be configured before enabling Management ACL Mode. If **enabled**, only the IP addresses you specify will have Web, Telnet, SSH and SNMP access to the management interface.
IP Address (1–5)	Enter up to five IPv4 addresses that are allowed management access to the access point. Use dotted-decimal format (for example, *192.168.10.10*0).

7

Clustering Multiple Access Points

The Cisco AP541N supports access point clusters. A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity rather than a series of separate wireless devices.

Managing Access Points in the Cluster

The access point cluster is a dynamic, configuration-aware group of access points in the same subnet of a network. Each cluster can have up to 10 members. The cluster provides a single point of administration and enables you to view the deployment of access points as a single wireless network rather than a series of separate wireless devices. A network subnet can have multiple clusters. Clusters can share various configuration information, such as VAP settings and QoS queue parameters.

A cluster can be formed between two access points if the following conditions are met:

- The access points use the same radio mode. (For example, both radios use 802.11g.)
- The access points are connected on the same bridged segment.
- The access points joining the cluster have the same Cluster Name.
- Clustering mode is enabled on both access points.

NOTE For two access points to be in the same cluster, they do not need to have the same number of radios; however, the supported capabilities of the radios should be same.

Clustering Single and Dual Radio Access Points

Clusters can contain a mixture of access points with two radios and access points with a single radio. When the configuration of a single-radio access point in the cluster changes, the access point propagates the change to the first radio of all cluster members. The configuration of the second radio on any dual-radio access points in the cluster is not affected.

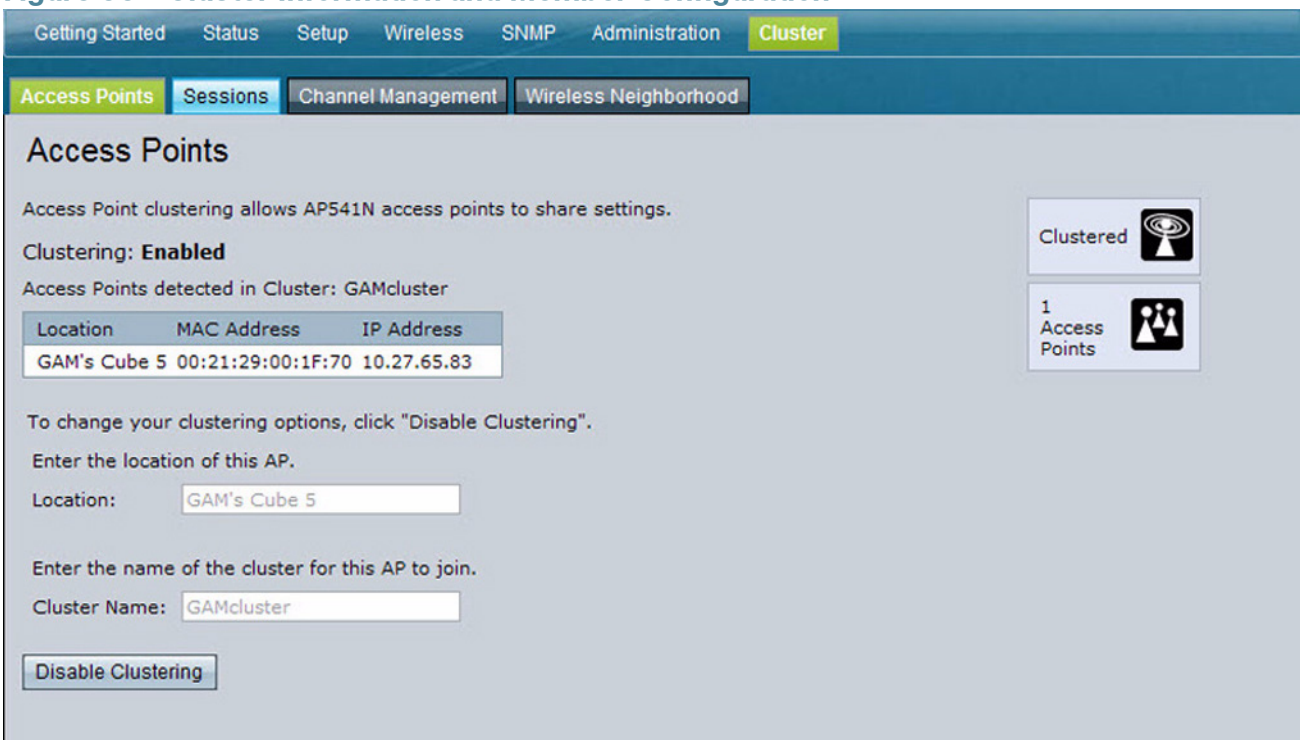
If a cluster contains only single-radio access points and a dual radio access point joins the cluster, then only radio 1 on the dual-radio access point is configured with the cluster configuration. Radio 2 on the access point remains as it was prior to joining the cluster. However, if the cluster already has at least one dual-radio access point, then the second radio of the access point joining the cluster is configured with the cluster settings.

Viewing and Configuring Cluster Members

The **Access Points** tab allows you to start or stop clustering on an access point, view the cluster members, and configure the location and cluster name for a cluster member. From the **Access Points** page, you can also click the IP address of each cluster member to navigate to configuration settings and data on an access point in the cluster.

To view information about cluster members and to configure the location and cluster of an individual member, click the **Access Points** tab.

Figure 33 Cluster Information and Member Configuration



If clustering is currently disabled on the access point, the **Enable Clustering** button is visible. If clustering is enabled, the **Disable Clustering** button is visible. You can enter clustering option information whether clustering is enabled or disabled.

Table 35 describes the configuration and status information available on the cluster **Access Points** page when clustering is enabled.

Table 35 Access Points in the Cluster

Field	Description
Status	If the status field is visible, the access point is enabled for clustering. If clustering is not enabled, then the access point is operating in stand-alone mode and none of the information in this table is visible. To disable clustering on the access point, click **Disable Clustering**.
Location	Description of where the access point is physically located.

Table 35 Access Points in the Cluster

Field	Description
MAC Address	Media Access Control (MAC) address of the access point. The address shown here is the MAC address for the bridge (`br0`). This is the address by which the access point is known externally to other networks.
IP Address	The IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.

Table 36 describes the cluster information to configure for a member.

Table 36 Clustering Options

Field	Description
Location	Enter a description of where the access point is physically located. The location can be a maximum of 64 characters in length. All alphanumeric characters except double quote (") are valid. Null or empty space is not allowed.
Cluster Name	Enter the name of the cluster for the access point to join. The name can be a maximum of 64 characters in length. All alphanumeric characters except double quote (") are valid. Null or empty space is not allowed. The cluster name is not sent to other access points in the cluster. You must configure the same cluster name on each access point that is a member of the cluster. The cluster name must be unique for each cluster you configure on the network.

Removing an Access Point from the Cluster

To remove an access point from the cluster, do the following.

STEP 1 Go to the **Administration** pages for the clustered access point.

STEP 2 Click the **Cluster > Access Points** tab in the Administration pages.

STEP 3 Click **Disable Clustering**.

The change is shown under **Status** for that access point as `standalone` (instead of `cluster`).

Adding an Access Point to a Cluster

To add an access point that is currently in standalone mode back into a cluster, do the following.

STEP 1 Go to the **Administration** pages for the standalone access point.

STEP 2 Click the **Cluster > Access Points** tab in the Administration pages for the standalone access point.

The **Access Points** tab for a standalone access point indicates that the current mode is standalone and provides a button for adding the access point to a cluster (group).

STEP 3 Click **Enable Clustering**.

The access point is now a cluster member. Its Status (Mode) on the **Cluster > Access Points** tab now indicates **Cluster** instead of **Not Clustered**.

Navigating to Configuration Information for a Specific Access Point

All access points in a cluster reflect the same configuration. In this case, it does not matter to which access point you actually connect to for administration of the cluster.

There might be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. In this case, you can navigate to the **Administration** page for individual access points by clicking the IP address links on the **Access Points** tab.

All clustered access points are shown on the **Cluster > Access Points** page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

Navigating to an Access Point by Using its IP Address in a URL

You can also link to the **Administration** pages of a specific access point, by entering the IP address for that access point as a URL directly into a Web browser address bar in the following form:

http://IPAddressOfAccessPoint

where *IPAddressOfAccessPoint* is the address of the particular access point you want to monitor or configure.

Managing Cluster Sessions

The **Sessions** page shows information on client stations associated with access points in the cluster. Each client is identified by its MAC address, along with the access point (location) to which it is currently connected.


NOTE When accessing the **Cluster - Sessions** page, a maximum of 20 clients are reported per radio. To see all the associated clients, access the **Client Associations** page of the access point.

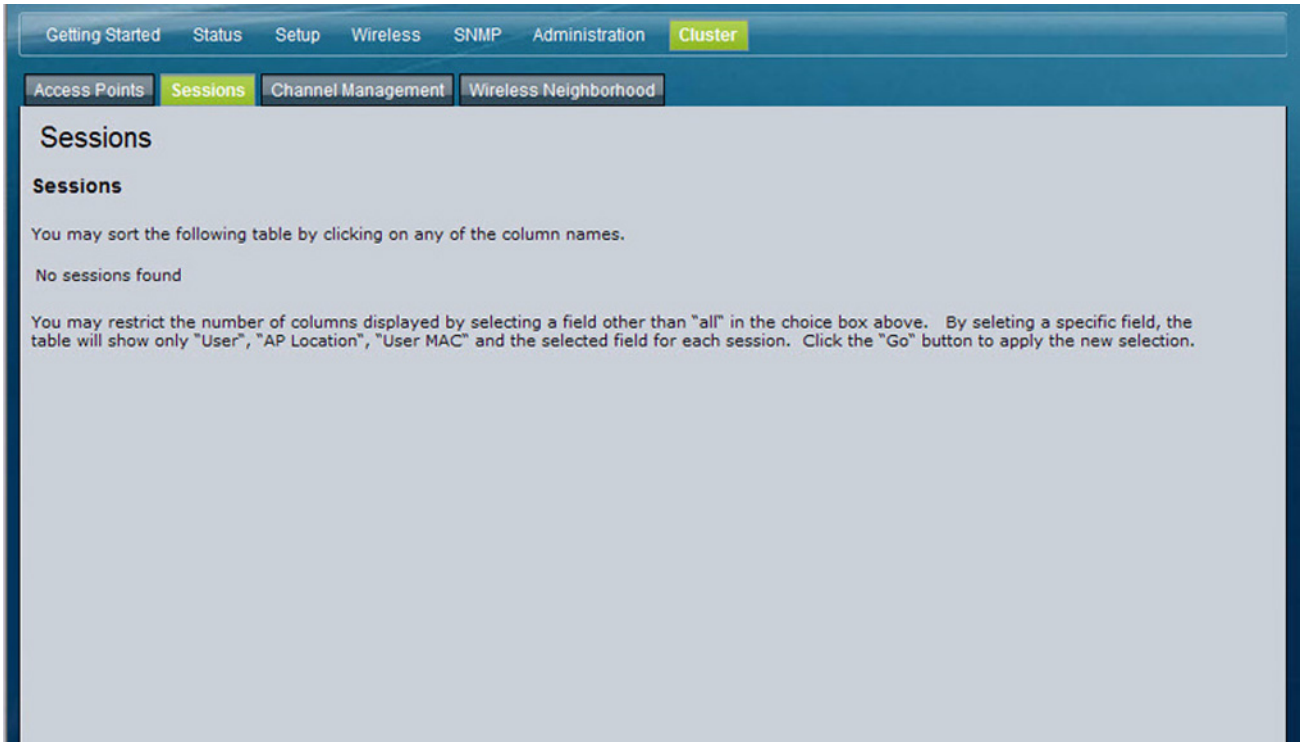
To view a particular statistic for client sessions, select an item from the **Display** dropdown list and click **Go**. You can view information about idle time, data rate, signal strength and so forth; all of which are described in detail in Table 37.

A session in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the client logs on to the network, and the session ends when the client either logs off intentionally or loses the connection for some other reason.

NOTE A session is not the same as an association, which describes a client connection to a particular access point. A client network connection can shift from one clustered access point to another within the context of the same session. A client station can roam between access points and maintain the session.

To manage sessions associated with the cluster, click the **Sessions** tab.

Figure 34 Session Management



Details about the session information shown is described in Table 37.

Table 37 Session Management

Field	Description
AP Location	Indicates the physical location of the access point. The location can be a maximum of 64 characters in length. All alphanumeric characters except double quote (") are valid. Null or empty space is not allowed.
Cluster Name	Enter the name of the cluster for the access point to join. The name can be a maximum of 64 characters in length. All alphanumeric characters except double quote (") are valid. Null or empty space is not allowed. The cluster name is not sent to other access points in the cluster. You must configure the same cluster name on each access point that is a member of the cluster. The cluster name must be unique for each cluster you configure on the network.
User MAC	Indicates the MAC address of the wireless client device. A MAC address is a hardware address that uniquely identifies each node of a network.
Idle	Indicates the amount of time this station has remained inactive. A station is considered to be idle when it is not receiving or transmitting data.
Rate	The speed at which this access point is transferring data to the specified client. The data transmission rate is measured in *megabits per second* (Mbps). This value should fall within the range of the advertised rate set for the mode in use on the access point. For example, 6 to 54 Mbps for 802.11a.

Table 37 Session Management

Field	Description
Signal	Strength of the radio frequency (RF) signal the client receives from the access point. The measure used for this is a value known as *Received Signal Strength Indication* (RSSI), and will be a value between 0 and 100. RSSI is determined by a mechanism implemented on the network interface card (NIC) of the client station.
Receive Total	Number of total packets received by the client during the current session.
Transmit Total	Number of total packets transmitted to the client during this session.
Error Rate	Percentage of time frames are dropped during transmission on this access point.

Sorting Session Information

To sort the information shown in the tables by a particular indicator, click the column label by which you want to order things. For example, if you want to see the table rows ordered by signal strength, click the **Signal** column label. The entries are sorted by signal strength.

Configuring and Viewing Channel Management Settings

When Channel Management is enabled, the access point automatically assigns radio channels used by clustered access points. The automatic channel assignment reduces mutual interference (or interference with other access points outside of its cluster) and maximizes Wi-Fi bandwidth to help maintain the efficiency of communication over the wireless network.

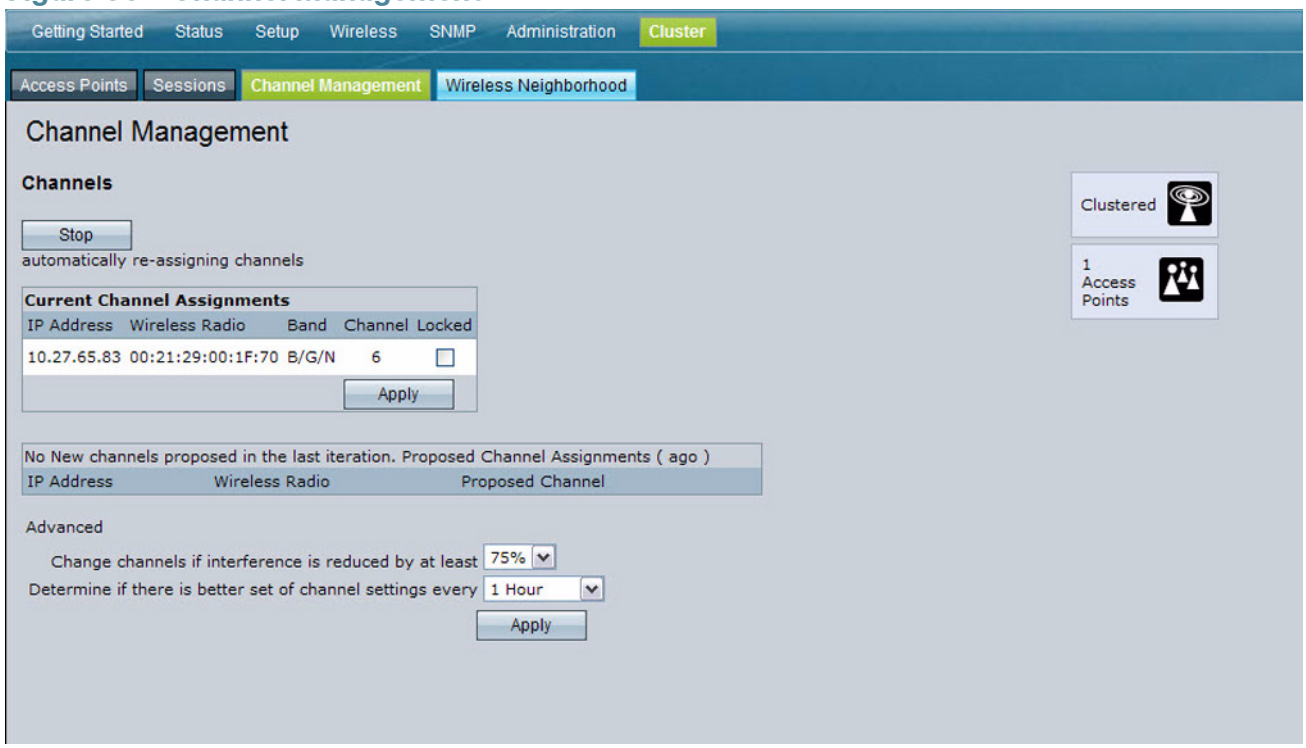
You must start channel management to get automatic channel assignments; it is disabled by default on a new access point.

At a specified interval, the Channel Manager maps access points to channel use and measures interference levels in the cluster. If significant channel interference is detected, the Channel Manager automatically re-assigns some or all of the access points to new channels per an efficiency algorithm (or *automated channel plan*).

The Channel Management page shows previous, current, and planned channel assignments for clustered access points. By default, automatic channel assignment is disabled. You can start channel management to optimize channel usage across the cluster on a scheduled interval.

To configure and view the channel assignments for the cluster members, click the **Channel Management** tab.

Figure 35 Channel Management



From this page, you can view channel assignments for all access points in the cluster and stop or start automatic channel management. By using the Advanced settings on the page, you can modify the interference reduction potential that triggers channel re-assignment, change the schedule for automatic updates, and re-configure the channel set used for assignments.

Stopping/Starting Automatic Channel Assignment

By default, automatic channel assignment is disabled (off).

NOTE Channel Management overrides the default cluster behavior, which is to synchronize radio channels of all access points across a cluster. When Channel Management is enabled, the radio Channel is not synced across the cluster to other access points.

- Click **Start** to resume automatic channel assignment.

  When automatic channel assignment is enabled, the Channel Manager periodically maps radio channels used by clustered access points and, if necessary, re-assigns channels on clustered access points to reduce interference with cluster members or other access points outside the cluster.

- Click **Stop** to stop automatic channel assignment. (No channel usage maps or channel re-assignments will be made. Only manual updates will affect the channel assignment.)

NOTE The proposed channel assignment will not take effect if the **Channel** field on the **Wireless Radio** page is set to **auto**. The channel must be set to a static channel.

Viewing Current Channel Assignments and Setting Locks

The **Current Channel Assignments** section shows a list of all access points in the cluster by IP Address. The display shows the band on which each access point is broadcasting (a/b/g/n), the current channel used by each access point, and an option to lock an access point on its current radio channel so that it cannot be re-assigned to another.

Table 38 provides details about Current Channel Assignments.

Table 38 Channel Assignments

Field	Description
IP Address	IP Address for the access point.

Table 38 Channel Assignments

Field	Description
Wireless Radio	MAC address of the radio.
Band	Band on which the access point is broadcasting.
Channel	Radio channel on which this access point is currently broadcasting.
Locked	Click **Locked** to force the access point to remain on the current channel. When Locked is selected (enabled) for an access point, automated channel management plans do not re-assign the access point to a different channel as a part of the optimization strategy. Instead, access points with locked channels are factored in as requirements for the plan. If you click **Apply**, you will see that locked access points show the same channel for the Current Channel and Proposed Channel fields. The locked access points keep their current channels.

Viewing the Last Proposed Set of Changes

The *Proposed Channel Assignments* shows the last channel plan. The plan lists all access points in the cluster by IP Address, and shows the current and proposed channels for each access point. Locked channels will not be re-assigned and the optimization of channel distribution among access points will take into account the fact that locked access points must remain on their current channels. access points that are not locked may be assigned to different channels than they were previously using, depending on the results of the plan.

Table 39 Last Proposed Changes

Field	Description
IP Address	IP address for the access point.
Wireless Radio	Radio channel on which this access point is currently broadcasting.
Proposed Channel	Radio channel to which this access point would be re-assigned if the Channel Plan is executed.

Configuring Advanced Settings

The advanced settings allow you to customize and schedule the channel plan for the cluster. If you use Channel Management as provided (without updating Advanced Settings), channels are automatically fine-tuned once every hour if interference can be reduced by 25 percent or more. Channels are reassigned even if the network is busy. The appropriate channel sets will be used (b/g for access points using IEEE 802.11b/g and a for access points using IEEE 802.11a).

The default settings are designed to satisfy most scenarios where you would need to implement channel management.

Use **Advanced Settings** to modify the interference reduction potential that triggers channel re-assignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments. If there are no fields showing in the Advanced section, click the toggle button to display the settings that modify timing and details of the channel planning algorithm.

Table 40 Advanced Channel Management Settings

Field	Description
Change channels if interference is reduced by at least	Specify the minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is 75 percent. Use the drop-down menu to choose percentages ranging from 5 percent to 75 percent. This setting lets you set a gating factor for channel re-assignment so that the network is not continually disrupted for minimal gains in efficiency. For example, if channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce interference by 30 percent, then channels will not be reassigned. However; if you re-set the minimal channel interference benefit to 25 percent and click **Apply**, the proposed channel plan will be implemented and channels reassigned as needed.

Table 40 Advanced Channel Management Settings

Field	Description
Determine if there is better set of channels every	Use the dropdown menu to specify the schedule for automated updates. A range of intervals is provided, from 30 Minutes to 6 Months The default is 1 Hour (channel usage reassessed and the resulting channel plan applied every hour).

Click **Apply** under Advanced settings to apply these settings.

Advanced settings will take affect when they are applied and influence how automatic channel management is performed.

Viewing Wireless Neighborhood Information

The Wireless Neighborhood shows all access points within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and nonmembers.

NOTE When accessing the **Cluster - Wireless Neighborhood** page, a maximum of 20 detected access points are reported per access point. To see all the detected access points, directly access the **Neighboring Access Points** page of the specific access point.

For each neighbor access point, the Wireless Neighborhood view shows identifying information (SSID or Network Name, IP address, MAC address) along with radio statistics (signal strength, channel, beacon interval). You can click on an access point to get additional statistics about the access points in radio range of the currently selected access point.

The Wireless Neighborhood view can help you:

- Detect and locate unexpected (or *rogue*) access points in a wireless domain so that you can take action to limit associated risks
- Verify coverage expectations. By assessing which access points are visible at what signal strength from other access points, you can verify that the deployment meets your planning goals.
- Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the color coded table.

Figure 36 Wireless Neighborhood

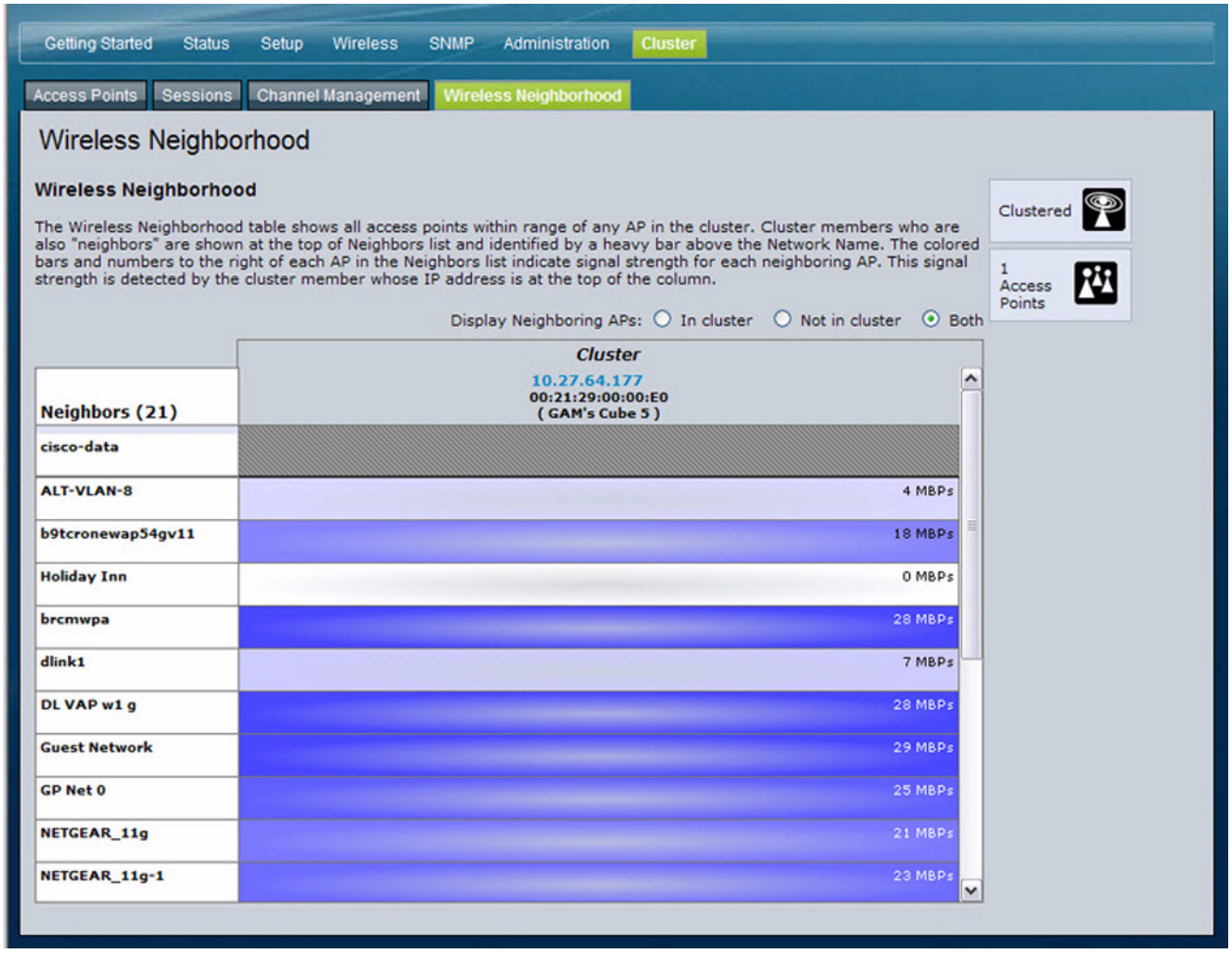


Table 41 describes the Wireless Neighborhood information.

Table 41 Wireless Neighborhood Information

Field	Description
Display neighboring APs	Click one of the following radio buttons to change the view: **In cluster**—Shows only neighbor access points that are members of the cluster **Not in cluster**—Shows only neighbor access points that are not cluster members **Both**—Shows all neighbor access points (cluster members and non-members)
Cluster	The Cluster list at the top of the table shows IP addresses for all access points in the cluster. (This is the same list of cluster members shown on the **Cluster > Access Points** tab.) If there is only one access point in the cluster, only a single IP address column will be displayed here; indicating that the access point is clustered with itself. You can click on an IP address to view more details on a particular access point.

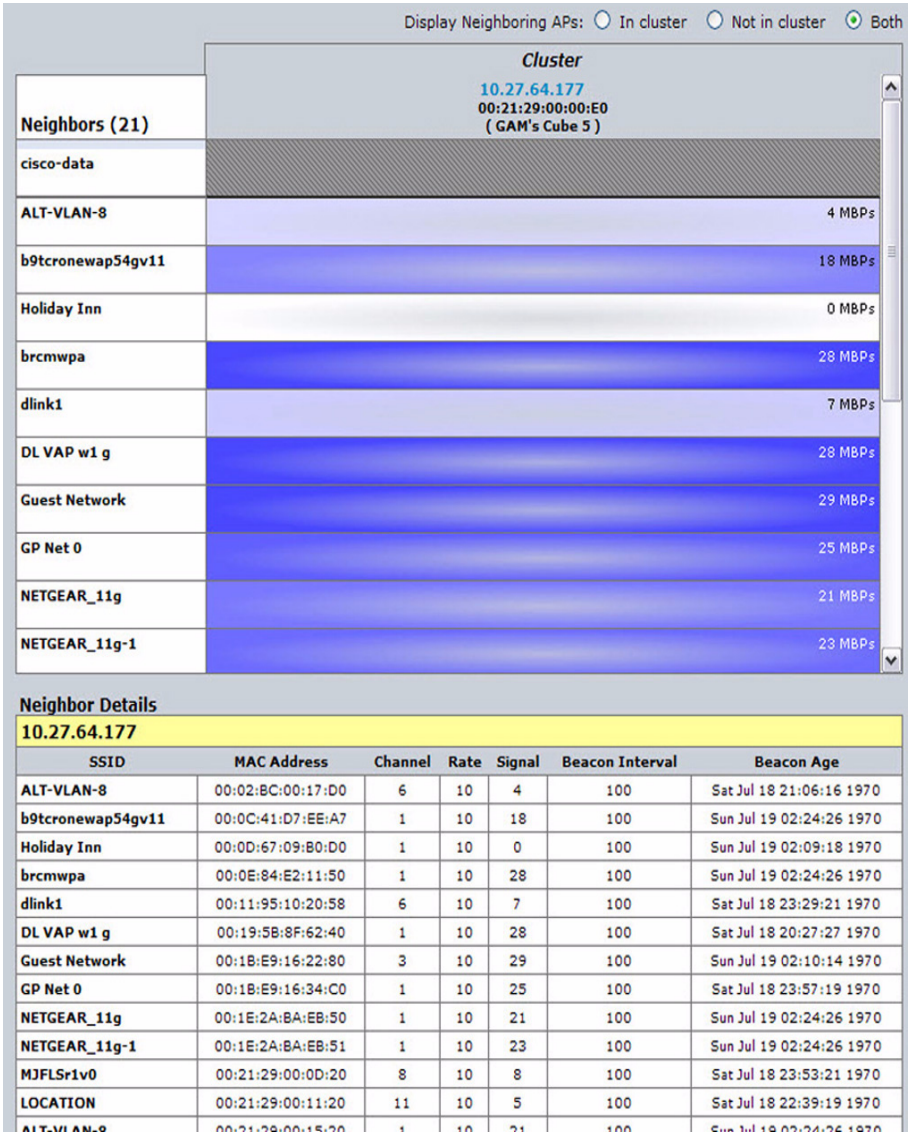
Table 41 Wireless Neighborhood Information

Field	Description
Neighbors	Access points that are neighbors of one or more of the clustered access points are listed in the left column sorted by SSID (network name). An access point detected as a neighbor of a cluster member can also be a cluster member itself. Neighbors that are also cluster members are always shown at the top of the list with a heavy bar above and include a location indicator. The colored bars to the right of each access point in the Neighbors list shows the signal strength for each of the neighbor access points as detected by the cluster member. The IP address is shown at the top of the column. The color of the bar indicates the signal strength: **Dark Blue Bar**—A dark blue bar and a high signal strength number (for example 50) indicates good signal strength detected from the Neighbor seen by the access point with the IP address listed above that column. **Lighter Blue Bar**—A lighter blue bar and a lower signal strength number (for example 20 or lower) indicates medium or weak signal strength from the Neighbor seen by the access point with the IP address listed above that column **White Bar**—A white bar and the number 0 indicates that a neighboring access point that was detected by one of the cluster members cannot be detected by the access point with the IP address listed above that column. **Light Gray Bar**—A light gray bar and no signal strength number indicates a Neighbor that is detected by other cluster members but not by the access point with the IP address listed above that column. **Dark Gray Bar**—A dark gray bar and no signal strength number indicates this is the access point with the IP address listed above that column (since there is no value in showing how well the access point can detect itself).

Viewing Details for a Cluster Member

To view details on a cluster member access point, click on the IP address of a cluster member at the top of the page. Figure 37 shows the Neighbor Details for Radio 1 of the access point with an IP address of 10.27.64.177.

Figure 37 Details for a Cluster Member AP



SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
ALT-VLAN-8	00:02:BC:00:17:D0	6	10	4	100	Sat Jul 18 21:06:16 1970
b9tcronewap54gv11	00:0C:41:D7:EE:A7	1	10	18	100	Sun Jul 19 02:24:26 1970
Holiday Inn	00:0D:67:09:B0:D0	1	10	0	100	Sun Jul 19 02:09:18 1970
brcmwpa	00:0E:84:E2:11:50	1	10	28	100	Sun Jul 19 02:24:26 1970
dlink1	00:11:95:10:20:58	6	10	7	100	Sat Jul 18 23:29:21 1970
DL VAP w1 g	00:19:5B:8F:62:40	1	10	28	100	Sat Jul 18 20:27:27 1970
Guest Network	00:1B:E9:16:22:80	3	10	29	100	Sun Jul 19 02:10:14 1970
GP Net 0	00:1B:E9:16:34:C0	1	10	25	100	Sat Jul 18 23:57:19 1970
NETGEAR_11g	00:1E:2A:BA:EB:50	1	10	21	100	Sun Jul 19 02:24:26 1970
NETGEAR_11g-1	00:1E:2A:BA:EB:51	1	10	23	100	Sun Jul 19 02:24:26 1970
MJFLSr1v0	00:21:29:00:0D:20	8	10	8	100	Sat Jul 18 23:53:21 1970
LOCATION	00:21:29:00:11:20	11	10	5	100	Sat Jul 18 22:39:19 1970

Table 42 describes the parameters of an access point.

Table 42 Cluster Member Details

Field	Description
SSID	The Service Set Identifier (SSID) this access point is on. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. A guest network and an Internal network running on the same access point must have two different network names.
MAC Address	Shows the MAC address of the neighboring access point. A MAC address is a hardware address that uniquely identifies each node of a network.
Channel	Shows the channel on which the access point is broadcasting. The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.
Rate	Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the rates shown in Supported Rates.
Signal	Indicates the strength of the radio signal emitting from this access point measured in decibels (Db).
Beacon Interval	Shows the Beacon interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).
Beacon Age	Shows the date and time of the last beacon received from this access point.

8

Configuration Examples

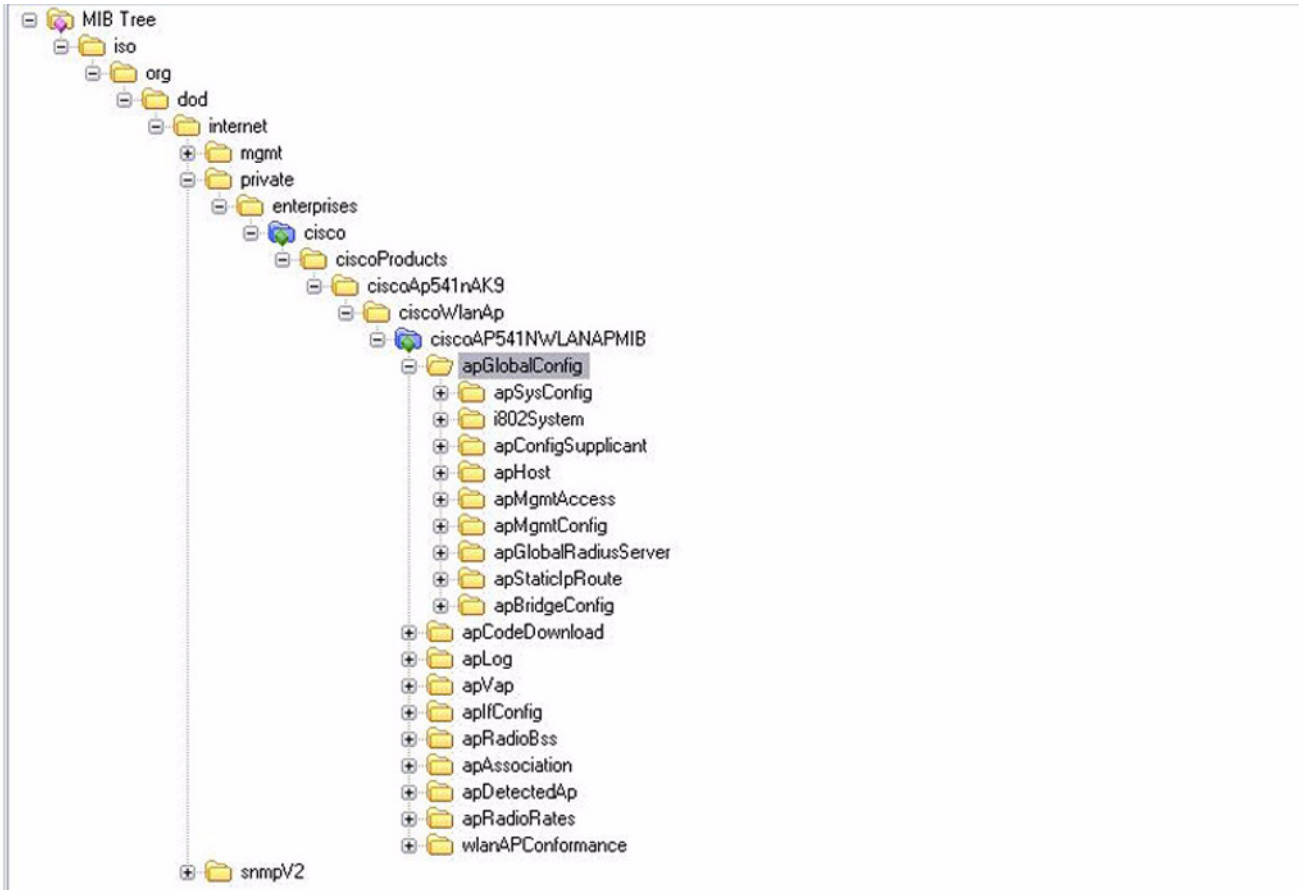
This chapter contains examples of how to configure selected features available on the access point. Each example contains procedures on how to configure the feature by using the *Access Point Configuration Utility*, or SNMP.

This chapter describes how to perform the following procedures:

- **Configuring a VAP**
- **Configuring Wireless Radio Settings**
- **Configuring the Wireless Distribution System**
- **Clustering Access Points**

For all SNMP examples, the objects you use to modify the access point are in a private MIB. The path to the tables that contain the objects is iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).lvl7(6132).lvl7Products(1).fastPath(1).fastPathWLANAP(28), as shown in **Figure 38**.

Figure 38 MIB Tree



Configuring a VAP

This example shows how to configure VAP 3 with the following non-default settings:

- VLAN ID: 3
- SSID: Marketing
- Security: WPA Personal using WPA2 with CCMP (AES)

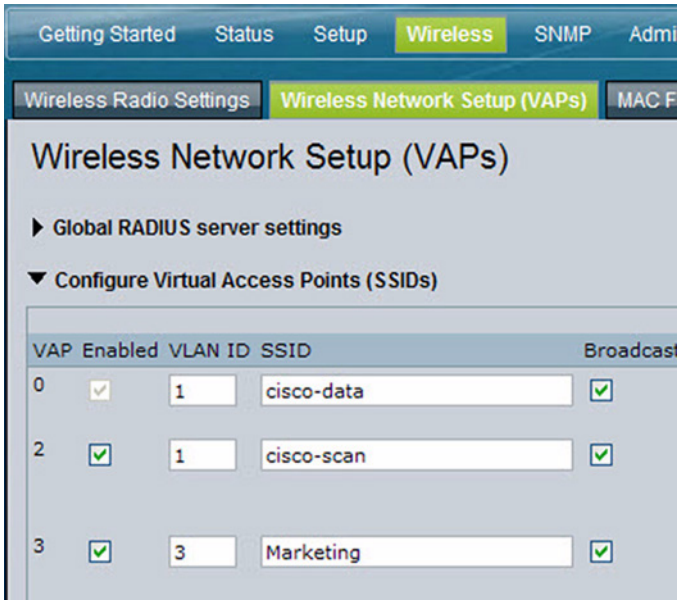
VAP Configuration from the Web Interface

STEP 1 Log onto the access point and navigate to the **Wireless > Wireless Network Setup (VAPs)** page.

STEP 2 In the **Enabled** column for VAP 3, select the check box.

STEP 3 Enter 3 in the VLAN ID column.

STEP 4 In the **SSID** column, delete the existing SSID and type Marketing.



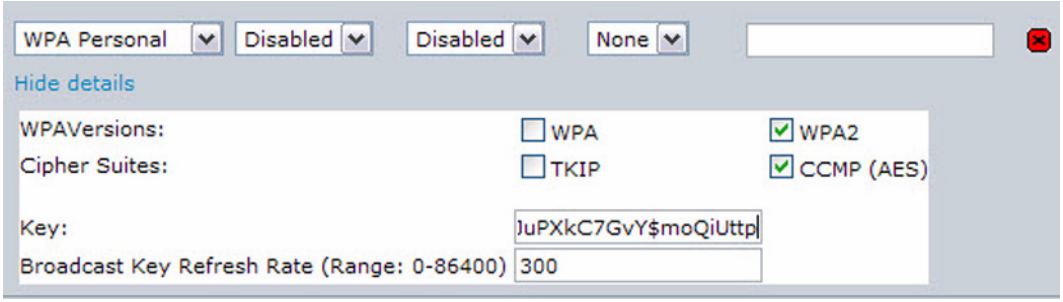
STEP 5 Select **WPA Personal** from the menu in the **Security** column.

The screen refreshes, and additional fields appear.

STEP 6 Select the **WPA2** and **CCMP (AES)** options, and clear the **WPA** and **TKIP** options.

STEP 7 Enter a WPA encryption key in the **Key** field.

The key can be a mix of alphanumeric and special characters. The key is case sensitive and can be between 8 and 63 characters.



STEP 8 Click **Apply** to update the access point with the new settings.

VAP Configuration Using SNMP

STEP 1 Load the FASTPATH-WLAN-ACCESS-POINT-MIB module.

STEP 2 From the MIB tree, navigate to the objects in the apVap table.

STEP 3 Walk the apVapDescription object to view the instance ID for VAP 2 (wlan0vap2).

VAP 2 on wireless Radio 1 is instance 5.

STEP 4 Use the apVapStatus object to set the status of VAP 2 to up (1).

STEP 5 Use the apVapVlanID object to set the VLAN ID of VAP 2 to 2.

STEP 6 Navigate to the objects in the apIfConfig table.

STEP 7 Walk the apIfConfigName object to view the instance ID for VAP 2 (wlan0vap2).

VAP 2 on wireless Radio 1 is instance 7.

STEP 8 Set the value of instance 7 in the apIfConfigSsid object to Marketing.

STEP 9 Set the value of instance 7 in the apIfConfigSecurity object to wpa-personal (3).

STEP 10 Set the value of instance 7 in the apIfConfigWpaPersonalKey object to JuPXkC7GvY$moQiUttp2, which is the WPA pre-shared key.

STEP 11 Navigate to the objects in the apRadioBss > apBssTable table.

STEP 12 Walk the apBssDescr object to view the instance ID for VAP 2.

VAP 2 on wireless Radio 1 is instance 3.

STEP 13 Set the value of instance 3 in the apBssWpaAllowed object to false (2).

STEP 14 Set the value of instance 3 in the apBssWpaCipherTkip object to false (2).

STEP 15 Set the value of instance 3 in the apBssWpaCipherCcmp object to true (1).

Configuring Wireless Radio Settings

This example shows how to configure wireless Radio 1 with the following settings:

- Mode: IEEE 802.11b/g/n
- Channel: 6
- Channel Bandwidth: 40 MHz
- Maximum Stations: 100
- Transmit Power: 75%

Wireless Radio Configuration from the Web Interface

STEP 1 Log onto the access point and navigate to the **Wireless > Advanced Settings** page.

STEP 2 Make sure the number 1 appears in the wireless Radio field and that the status is **On**.

STEP 3 From the **Mode** menu, select 802.11b/g/n.

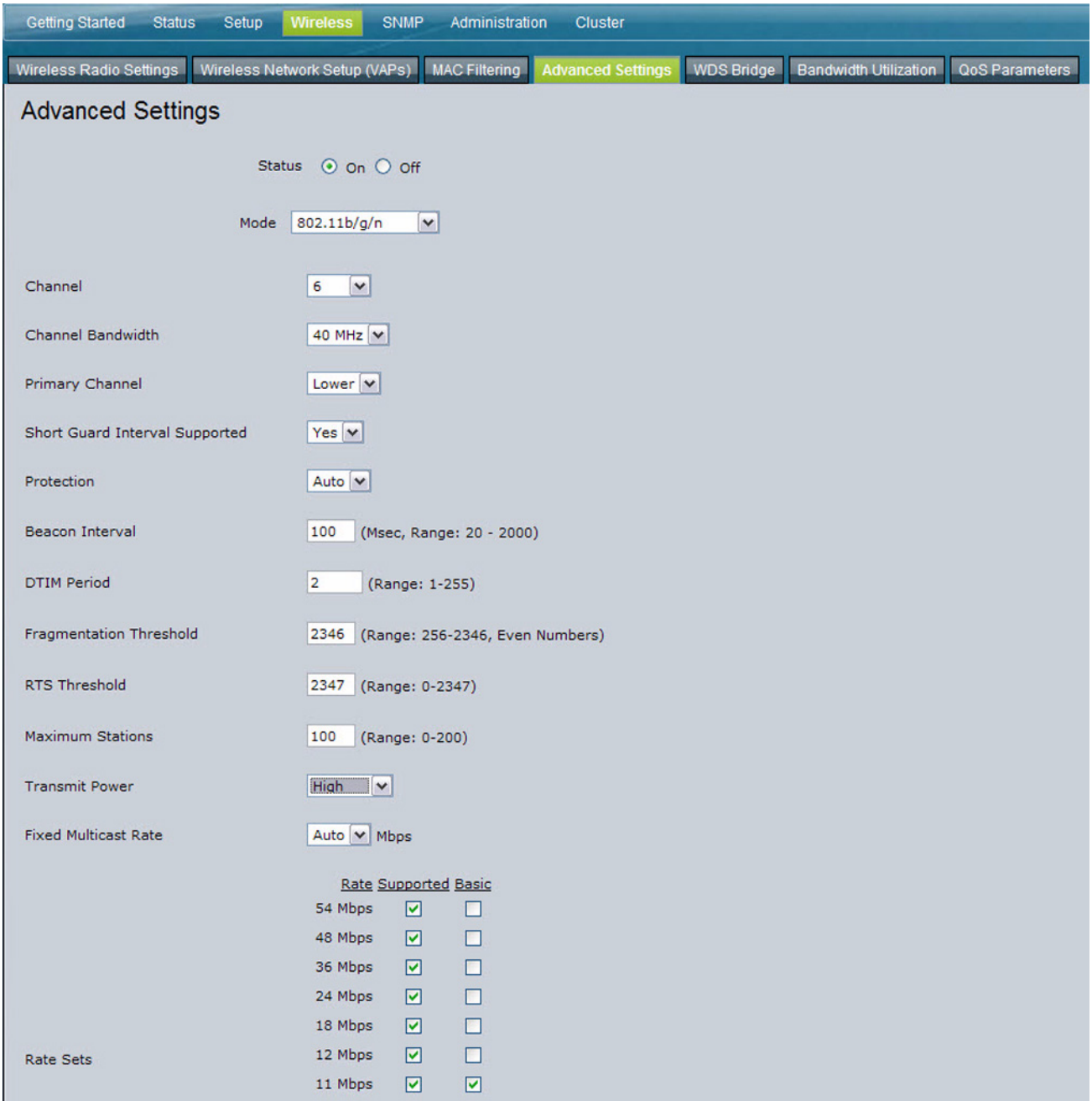
STEP 4 From the **Channel** field, select 6.

STEP 5 From the **Channel Bandwidth** field, select 40 MHz.

STEP 6 In the **Maximum Stations** field, change the value to 100.

STEP 7 In the **Transmit Power** field, change the value to High.

The next window shows the **Advanced Settings** page with the settings specified in this example.



STEP 8 Click **Apply** to update the access point with the new settings.

Wireless Radio Configuration Using SNMP

STEP 1 Load the Cisco specific MIB module.

STEP 2 From the MIB tree, navigate to the objects in the apRadio table (apRadioBss > apRadioTable).

STEP 3 Use the apRadioStatus object to set the status of wireless Radio 1 to up (1).

STEP 4 Use the apRadioMode object to set the wireless Radio 1 mode to IEEE 802.11b/g/n, which is bg-n (4).

STEP 5 Use the apRadioChannelPolicy object to set the channel policy to static (1), which disables the automatic channel assignment.

STEP 6 Use the apRadioStaticChannel object to set the channel to 6.

STEP 7 Use the apRadioChannelBandwith object to set the channel bandwidth for wireless Radio 1 to 40-MHz (2).

STEP 8 Use the apRadioTxPower object to set the transmission power on wireless Radio 1 to 75.

STEP 9 Navigate to the objects in the apBssTable.

STEP 10 Use the apBssMaxStations object to set the value of the maximum allowed stations to 100.

Configuring the Wireless Distribution System

This example shows how to configure a WDS link between two APs. The local access point is MyAP1 and has a MAC address of 00:1B:E9:16:32:40, and the remote access point is MyAP2 with a MAC address of 00:30:AB:00:00:B0.

The WDS link has the following settings, which must be configured on both APs:

- Encryption: WPA (PSK)
- SSID: wds-link
- Key: abcdefghijk

WDS Configuration from the Web Interface

To create a WDS link between a pair of access points **MyAP1** and **MyAP2** use the following steps:

STEP 1 Log onto MyAP1 and navigate to the **Wireless > WDS Bridge** page.

The MAC address for MyAP1 (the access point you are currently viewing) is automatically provided in the Local Address field.

STEP 2 Enter the MAC address for MyAP2 in the Remote Address field.

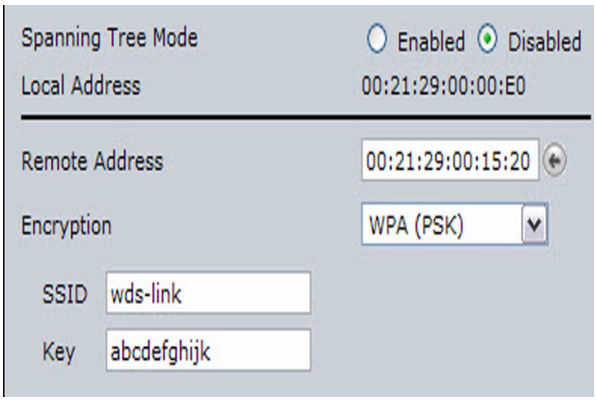
STEP 3

STEP 4 Select **WPA (PSK)** from the Encryption menu.

NOTE The WPA (PSK) option is available only if VAP 0 on wireless Radio 1 uses WPA (PSK) as the security method. If VAP 0 is not set to WPA Personal or WPA Enterprise, you must choose either None (Plain-text) or WEP for WDS link encryption.

STEP 5 Enter `wds-link` in the **SSID** field and `abcdefghijk` in the **Key** field.

STEP 6 Click **Apply** to apply the WDS settings to the access point.



STEP 7 Log onto MyAP2 and repeat steps 2-5 (but be sure to use the MAC address of MyAP1 in the Remote Address field).

NOTE MyAP1 and MyAP2 must be set to the same IEEE 802.11 Mode and be transmitting on the same channel.

WDS Configuration Using SNMP

STEP 1 Load the FASTPATH-WLAN-ACCESS-POINT-MIB module.

STEP 2 From the MIB tree, navigate to the objects in the apIfConfig table.

STEP 3 Walk the apIfConfigName object to view the instance ID for the first WDS link (wlan0wds0).

The first WDS link is instance 1.

STEP 4 Set the value of instance 1 in the apIfConfigRemoteMac object to 00:30:AB:00:00:B0.

In the MG-Soft browser, the format for the MAC address value to set is # 0x00 0x30 0xAB 0x00 0x00 0xB0.

STEP 5 Set the value of instance 1 in the apIfConfigWdsSecPolicy object to WPA Personal (3).

STEP 6 Set the value of instance 1 in the apIfConfigSsid object to wds-link.

STEP 7 Set the value of instance 1 in the apIfConfigWdsWpaPskKey object to abcdefthijk.

Some MIB browsers require that the value be entered in HEX values rather than ASCII values.

STEP 8 Perform the same configuration steps on MyAP2.

Clustering Access Points

This example shows how to configure a cluster with two APs and to enable automatic channel re-assigment.The location of the local access point is Room 214, and the cluster name is MyCluster.

Clustering APs by Using the Web Interface

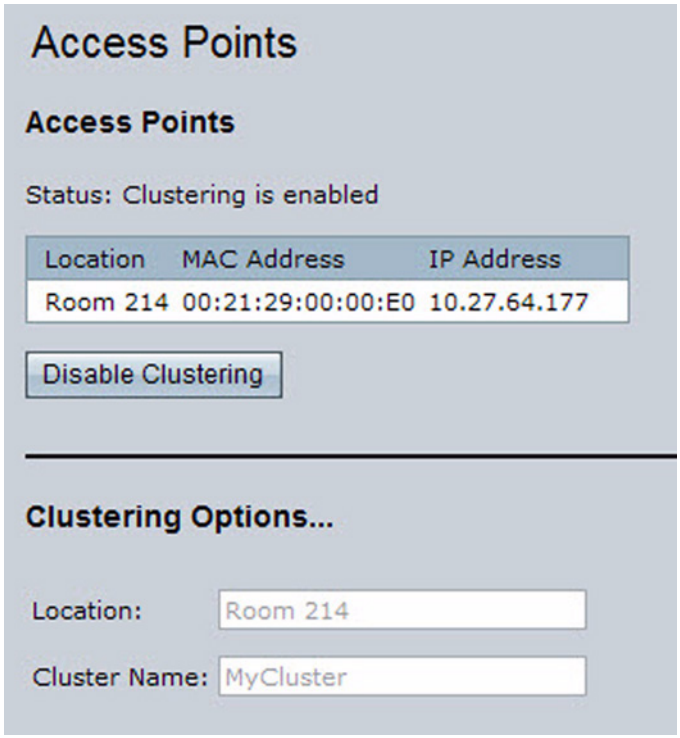
STEP 1 Log onto the access point and navigate to the **Cluster > Access Points** page.

STEP 2 Enter the access point location and the name of the cluster for it to join.

STEP 3 Click **Apply**.

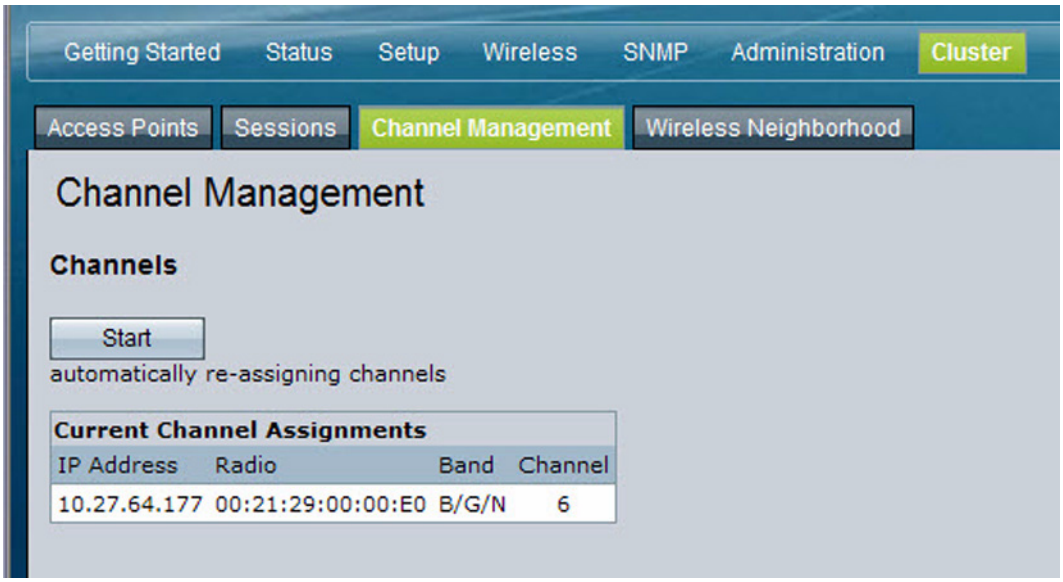
STEP 4 Click **Enable Clustering** to enable the clustering feature.

After you refresh the page, other APs that are on the same bridged segment, have wireless radios in the same operating mode, are enabled for clustering, and have the same cluster name appear in the Access Points table.



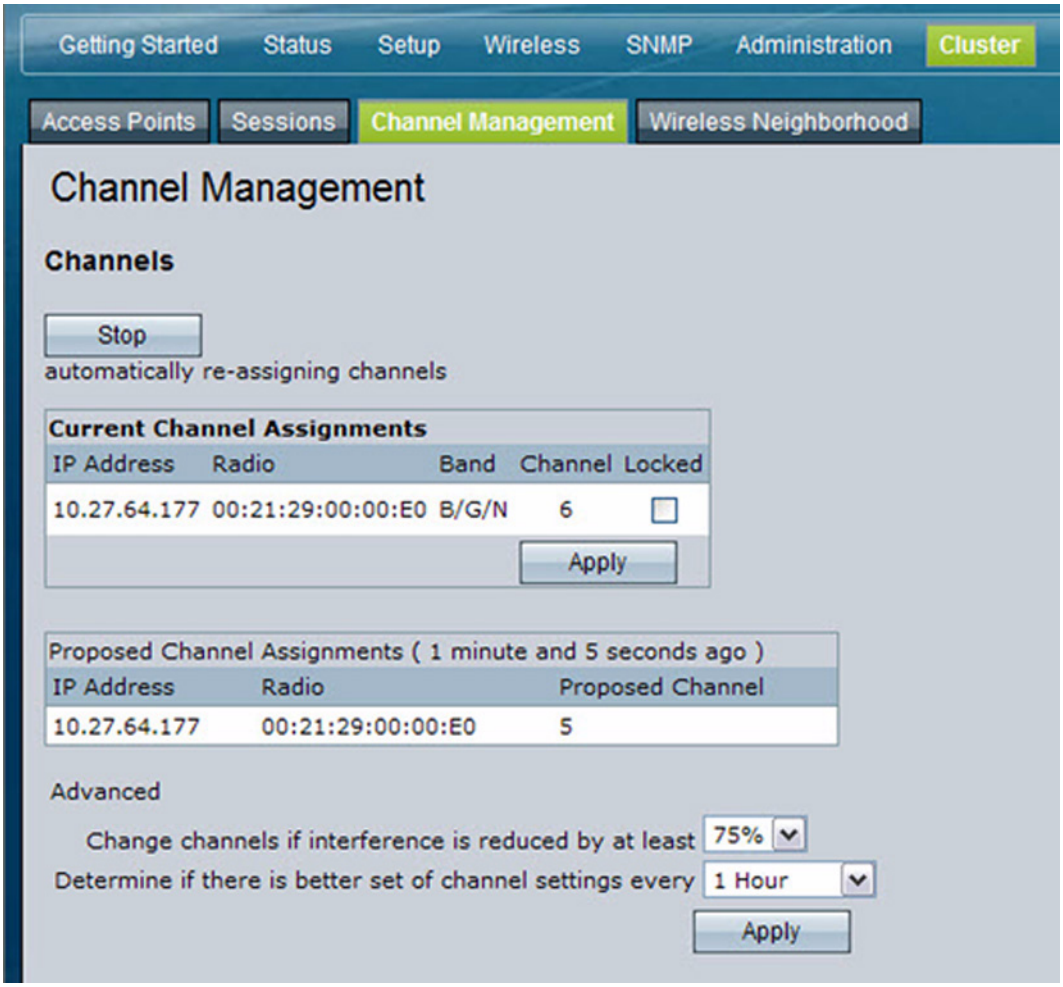
STEP 5 To start the automatic channel assignment feature, go to the **Channel Management** page.

A table on the page displays the current channel assignments.



STEP 6 Click **Start**.

The page refreshes and lists the proposed channel changes for all APs in the cluster. The interval setting in the Advanced section determine how often proposed changes are applied.



Clustering Access Points by Using SNMP

Cluster configuration by using SNMP is not supported.

9

Default Settings

When you first power on an access point, it has the default settings shown in Table 43.

Table 43 UAP Default Settings

Feature	Default
System Information	
User Name	**cisco**
Password	*cisco*
Ethernet Interface Settings	
Connection Type	DHCP
DHCP	Enabled
IP Address	*192.168.10.10* (if no DHCP server is connected)
Subnet Mask	255.255.255.0
DNS Name	None
Management VLAN ID	1
Untagged VLAN ID	1
Radio Settings	
Radio	Off
Radio 1 IEEE 802.11 Mode	802.11b/g/n
802.11b/g/n Channel	Auto
Wireless Radio 1 Channel Bandwidth	20 MHz
802.11a/n Channel	Auto

Table 43 UAP Default Settings (Continued)

Feature	Default
Primary Channel	Lower
Protection	Auto
MAX Wireless Clients	200
Transmit Power	100 percent
Rate Sets Supported (Mbps)	IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 IEEE 802.11b: 11, 5.5, 2, 1 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 IEEE 5-GHz 802.11n: 54, 48, 36, 24, 18, 12, 9, 6 IEEE 2.4 GHz 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1
Rate Sets (Mbps) (Basic/Advertised)	IEEE 802.11a: 24, 12, 6 IEEE 802.11b: 2, 1 IEEE 802.11g: 11, 5.5, 2, 1 EEE 5-GHz 802.11n: 24, 12, 6 IEEE 2.4 GHz 802.11n: 11, 5.5, 2, 1
SSIDs	cisco-data, cisco-voice, cisco-scan
Broadcast/Multicast Rate Limiting	Enabled
Fixed Multicast Rate	Auto
Beacon Interval	100
DTIM Period	2
Fragmentation Threshold	2346
RTS Threshold	2347
Virtual Access Point Settings	
Status	VAP0 is enabled on both radios, all other VAPs disabled

Table 43 UAP Default Settings (Continued)

Feature	Default
VLAN ID	1
Network Name (SSID)	Cisco VAP for VAP0 SSID for all other VAPs is Virtual Access Point *x* where *x* is the VAP number.
Broadcast SSID	Allow
Security (mode)	VAP2 is WPA Personal All others are None (plain text)
Authentication Type	None
RADIUS IP Address	0.0.0.0
RADIUS Key	secret
RADIUS Accounting	Disabled
HTTP Redirect	None
Other Default Settings	
WDS Settings	None
STP	Disabled
MAC Authentication	No stations in list
Load Balancing	Disabled
SNMP	Enabled
RO SNMP Community Name	Public
Managed AP Mode	Disabled
Authentication (802.1X Supplicant)	Disabled
Management ACL	Disabled
HTTP Access	Enabled
HTTPS Access	Enabled
SNMP Agent Port	161
SNMP Set Requests	Disabled
Console Port Access	Enabled

Table 43 UAP Default Settings (Continued)

Feature	Default
Telnet Access	Enabled
SSH Access	Enabled
WMM	Enabled
Network Time Protocol (NTP)	None
Clustering	Stopped
Client QoS Global Admin Mode	Disabled
VAP QoS Mode	Disabled

10

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the AP541N Dual-band Single-radio Access Point.

Product Resources

Resource	Location
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Technical Documentation	http://www.cisco.com/en/US/products/ps10492/index.html
Cisco AP541N Wall Mount Template	http://www.cisco.com/en/US/docs/wireless/access_point/csbap/AP541N/release_notes/78-19205.pdf
Firmware Downloads	www.cisco.com/en/US/products/ps10024/index.html
Customer Support	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Online Technical Support (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Warranty and End User License Agreement	www.cisco.com/go/warranty

Resource	Location
Open Source License Notices	www.cisco.com/go/osln
Regulatory Compliance and Safety Information	www.cisco.com/en/US/products/ps10024/tsd_products_support_series_home.html
Cisco Configuration Assistant	http://www.cisco.com/en/US/products/ps7287/index.html
Cisco Partner Central site for Small Business	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

OL-20285-01