



CHAPTER 5

Using IOS Templates

The WLSE allows you to view, create, copy, edit, and delete IOS configuration templates and apply them to large numbers of devices at a time.



Tip

It is strongly recommended that you *not* use multiple templates to configure the same access point. While you can create multiple templates to configure different groups of access points, it is good practice to use the same template to configure the same access point every time.

The topics covered are:

- [What is a Configuration Template, page 5-1](#)
- [Creating a Template, page 5-2](#)
- [Copying a Template, page 5-3](#)
- [Editing a Template, page 5-3](#)
- [Deleting a Template, page 5-4](#)
- [Importing a Template, page 5-4](#)
- [Exporting a Template, page 5-5](#)
- [Template Choices, page 5-6](#)

Related Topics

- [Using WLSM Templates, page 6-1](#)
- [Using Wizard Templates, page 7-1](#)
- [Managing Configuration Jobs, page 8-7](#)

What is a Configuration Template

You can think of a configuration template as a configuration update file that you can apply to large numbers of devices at a time. This file might contain the update for only one parameter or a complete access point configuration.

IOS-based templates are stored as text files containing IOS commands.

You can use the **Configure > Templates** option to:

- Viewing existing templates—See [Viewing the Existing Templates, page 5-2](#)

- Create a configuration template—See [Creating a Template, page 5-2](#)
- Copy an existing template—See [Copying a Template, page 5-3](#)
- Edit an existing template—See [Editing a Template, page 5-3](#)
- Delete a template—See [Deleting a Template, page 5-4](#).
- Import a template—See [Importing a Template, page 5-4](#)
- Export a template—[Exporting a Template, page 5-5](#)

Viewing the Existing Templates

Use this option to create a configuration template.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select the type of templates you want to display, then click Filter.
- Step 3** The selected template types are displayed in the Existing Templates table.
-

Creating a Template

Use this option to create a configuration template.



Tip

It is strongly recommended that you not use multiple templates to configure the same access point. While you can create multiple templates to configure different groups of access points, it is good practice to use the same template to configure the same access point every time.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** From the list, select **IOS**.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.

- Step 4** Click **New**. The window refreshes with the Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 5** Select the choices in the left pane to create a configuration template. For a description, see [Template Choices, page 5-6](#).
-

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to copy from the Existing Templates table, then click **Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 3** Enter a unique name. See [Naming Guidelines, page B-1](#) for details.
- Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates table.
- Step 5** Click **Edit**. See [Editing a Template, page 5-3](#).
-

Editing a Template

Use this option to edit a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to edit from the Existing Templates table, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Template Choices, page 5-6](#).
-

Deleting a Template

Use this option to delete a configuration template.


Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to delete from the Existing Templates table, then click **Delete**. A window appears asking if you want to delete the template.


Note

You cannot delete a template if it used in a scheduled job.

- Step 3** Click **OK** to delete it.

Importing a Template

Use this option to import a configuration to the WLSE, either from a file or from a device. You can import files from devices that are not managed by the WLSE.

When you import a configuration from an IOS access point, the imported configuration options are displayed in the Custom Values template screen.


Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select **IOS**.
- Step 3** Click **Import**. The Import Template window appears and varies depending upon which type you selected.
- Step 4** Complete the following:

Field	Description
Template Name	If you are importing from a file, enter a new name for the template or leave the entry blank to use the imported template name. If you are importing from a device, you must enter a template name.
Description	Enter a description for the template. Do not click the Enter key at the end of the description; it will generate an error.

Field	Description
From file	Enter the template filename or browse to find the file, then click Import .
From device (IP Address)	Enter a device name or IP address, then click Import .
Non-IP-Identity	Select this option if you do not want to download identity parameters, such as IP address, from the access point. Some parameters are ignored using this type of import. The downloaded configuration parameters are not a full representation of the access point's configuration but an optimal representation.
Full	Select this option to import a full configuration from the access point. This type of import includes the access point's identity parameters, such as sysname, IP address, etc. When using this option, it is recommended you delete all the custom key values from the imported template before applying the template to any device.
Device Credentials	Select Telnet or SSH.
User Name	If the device is not managed by the WLSE, or if the device is managed but the credentials have not been set, enter the username on the access point.
User Password	If the device is not managed by the WLSE, enter the user password on the access point.

Step 5 To import another template, click **Back** and go to [Step 3](#).

Step 6 When you are finished, click **Done**.

Step 7 View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates table.

Exporting a Template

Use this option to export a configuration template to your local drive.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure > Templates**. The Templates dialog box appears.

Step 2 Select a template name from Existing Templates, then click **Export**. The Export Template window appears.

Step 3 From the list, select the template you want to export, then click **Export**. The Export Template to Desktop window appears with the name of the template.

- Step 4** Right-click on the template name, select **Save As**, and enter the location to save the template.
-

Template Choices

When you create or edit an IOS configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See [Naming the Template, page 5-7](#).
2. **Template Categories**



Note Any or all of the template categories can be completed in any order.

- **Basic Settings**—See [Using Basic Settings, page 5-8](#).
 - **Basic Security**—See [Using Basic Security, page 5-13](#).
 - **Voice Express**—See [Configuring Voice Express, page 5-15](#)
 - **Association**—See [Using Association, page 5-16](#).
 - **Network Interfaces**—See [Setting Up Network Interfaces, page 5-19](#).
 - **Security**—See [Defining Security Settings, page 5-38](#).
 - **Services**—See [Defining Services, page 5-69](#).
 - **Event Log**—See [Configuring the Event Log, page 5-100](#).
 - **Wireless Services**—See [Configuring Wireless Services, page 5-96](#).
 - **System Config**—See [System Config, page 5-102](#).
 - **Device Specific**—See [Configuring Device Specific Settings, page 5-104](#)
 - **Custom Values**—See [Configuring Custom Values, page 5-104](#).
3. **Preview**—See [Previewing the Template, page 5-106](#).
 4. **Save**—See [Saving the Template, page 5-106](#).

Naming the Template

This option enables to you to name the template.

Procedure



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Template Name	Enter a name for the template. See Naming Guidelines, page B-1 .
Description	Enter a description of the purpose of the template. See Naming Guidelines, page B-1 . Do not click the Enter key at the end of the description; it will generate an error.

Step 2 Select a template category. For additional information, see [2.Template Categories, page 5-6](#).

Using Basic Settings

Use this option if you need to set up an access point quickly with a simple configuration. This will allow you to enter all the access point’s essential settings for basic operation.

Procedure

Step 1 Select **Basic Settings**. The Basic Settings dialog box displays in the right pane:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-1 Basic Settings

Field	Description
Configuration Server Protocol	Set this entry to match the network’s method of IP address assignment. Select one of the following options: <ul style="list-style-type: none"> • DHCP—Use this setting if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time. • Static IP—Use this setting if your network does has an automatic system for IP address assignment.
Default Gateway	Enter the IP address of your default Internet gateway. The entry 255.255.255.255 indicates no gateway.
Web Server	Select one of the following: Standard (HTTP) or Secure (HTTPS).
SNMP Request Credentials	
SNMPv2c/SNMPv1	<ol style="list-style-type: none"> 1. Select SNMPv2c/SNMPv1. 2. Enter the SNMP community name in the SNMP Community. 3. Re-enter the SNMP community name in the Confirm Community field. 4. Select one of the following SNMP Access options: Read-Only or Read-Write. <p>Note After a template job with the “Update device credentials in WLSE” option enabled and the template with this setting is successfully applied, the SNMP community string is displayed under Devices > Discover > Device Credentials > SNMP Communities.</p>

Table 5-1 Basic Settings (continued)

Field	Description
SNMPv3	<ol style="list-style-type: none"> 1. Select SNMPv3. 2. Enter the SNMPv3 username in the SNMP User Name field. 3. Enter the SNMPv3 password in the SNMP Password and Confirm Password fields. 4. Select MD5 or SHA from the Auth Algorithm drop-down menu. 5. Select Read-Only or Read-Write for SNMP access. <p>Note After a template job with the “Update device credentials in WLSE” option enabled and the template with this setting is successfully applied, the SNMP community string is displayed under Devices > Discover > Device Credentials > SNMP Communities.</p>
SNMPv2c Traps	
Send all traps to this WLSE	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the access point to send traps to this WLSE. (The WLSE’s address is added as an SNMP trap destination.) Enabling this setting allows faster processing of faults. (See Ports Hosted by the WLSE, page C-2 for correct port setting.) • Disable—Use this setting to disallow traps being sent to this WLSE. Using the setting does not disable traps; it removes this WLSE’s address as an SNMP trap destination. <p>Click See Detail for more information.</p>

Table 5-1 Basic Settings (continued)

Field	Description
Radio0-802.11B/G/N	
Role in Radio Network	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Access Point Root—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. • Bridge Root—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Non-Root—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Install Mode—Use this setting to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. Click See detail to see for which device types or versions this setting is valid. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.
Optimize Radio Network for	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. • Range—Use this setting to maximize the access point's range; however, it might reduce throughput. • Default—Use this setting to set the data rates to factory default settings. This option is not supported on the 2.4-GHz, 802.11b radio.
Aironet Extensions	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.

Table 5-1 Basic Settings (continued)

Field	Description
Radio0-802.11A/N Role in Radio Network	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Access Point Root—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. • Bridge Root—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Non-Root—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. <p>Click See detail to see for which device types or versions this setting is valid.</p> <ul style="list-style-type: none"> • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.

Table 5-1 Basic Settings (continued)

Field	Description
Optimize Radio Network for	Select one of the following: <ul style="list-style-type: none"> • Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. • Range—Use this setting to maximize the access point's range; however, it might reduce throughput. • Default—Use this setting to specify the that the access point use settings entered for the Network Interfaces Settings.
Aironet Extensions	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disables load balancing, Message Integrity Check (MIC), and WEP key hashing. Click See detail to see for which device types or versions this setting is valid.

- Step 2** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Using Basic Security

Use this option if you need to set up an access point quickly with a simple security configuration. This will allow you to enter all the access point's essential settings for basic operation.

Procedure

Step 1 Select **Basic Security**. The Basic Security dialog box displays in the right pane:

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-2 Basic Security

Field	Description
SSID Configuration	
Apply to	Select one of the following: <ul style="list-style-type: none"> • Radio B/G/N—Select this option for radio 802.11b/g/n. • Radio A/N—Select this option for radio 802.11a/n.
SSID	Select one of the following: <ul style="list-style-type: none"> • Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. • Select Broadcast SSID in Beacon to allow devices without a specified SSID to associate with this access point. Click for additional information.
VLAN	Select one of the following: <ul style="list-style-type: none"> • No VLAN—Use this setting to indicate there is no VLAN setting. • Enable VLAN ID—Use this setting to indicate there is a VLAN setting, then enter the VLAN identification number. <ul style="list-style-type: none"> – Native VLAN—Select to indicate that this is a Native VLAN. – Bridge-Group—Enter the bridge group. If you do not make an entry the VLAN number will used.
Security	Select one of the following: <ul style="list-style-type: none"> • No Security—Use this setting if you do not want to specify security options. Click for additional information. • Static WEP Key—Use this setting to specify WEP encryption. Click for additional information. <ul style="list-style-type: none"> – 40-bit WEP keys, enter 10 hexadecimal digits (0-9, a-f, or A-F). – 128-bit WEP keys, enter 26 hexadecimal digits (0-9, a-f, or A-F). • EAP Authentication—Use this setting to specify mandatory WEP, encryption open authentication + EAP, network EAP authentication, and no key management, RADIUS server authentication on port 1645. Click for additional information. <ul style="list-style-type: none"> – RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either creating or deleting. – RADIUS Server Secret—Enter the server’s shared secret. • WPA—Use this setting to specify encryption ciphers TKIP, open authentication + EAP, network EAP authentication, mandatory WPA key management, and RADIUS server authentication on port 1645. Click for additional information. <ul style="list-style-type: none"> – RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either creating or deleting. – RADIUS Server Secret—Enter the server’s shared secret.

Step 3 Click **Add** to add the SSID to the table.

To delete an SSID, select it from the table, then click **Delete**.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Voice Express

This option enables to you to configure admission control for voice and video. You can also configure call admission control for SSID and enable the Gratuitous Probe Response feature.

Procedure

Step 1 Select **Voice Express**. The Voice Express dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-3 Voice Express

Field	Description
Voice Express	Select one of the following: <ul style="list-style-type: none"> • Enable—Use the setting to enable the voice express feature. • Disable—Use the setting to disable the voice express feature. Click See detail for information about which default values are populated when you select either enable or disable.
Admission Control for Voice and Video Category 802.11A/N	
Video (User Priority 4-5)	Accept the defaults or enter a value for the following:
Voice (User Priority 6-7)	<ul style="list-style-type: none"> • Max Channel Capacity (%)—Enter the maximum channel capacity allowed. • Admission Control—Select to increase the number of voice calls that an access point can support by relieving congestion of voice packets over the wireless media. <p>Note Admission control should not be enabled if your deployment includes softphone applications. If you are not deploying softphone applications on laptops, then use the default.</p>

Table 5-3 Voice Express (continued)

Field	Description
Gratuitous Probe Response (GPR) 802.11A/N	<p>Accept the default or select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable GPR. The Gratuitous Probe Response feature helps conserve battery power by providing a high rate packet on the order of 10ms. <p>Note If you are not deploying the CN622 handset from Motorola, then GPR should be disabled.</p> <ul style="list-style-type: none"> • Disable—Use this setting to disable this feature. <p>Click See detail for additional information about these settings.</p>
Low Latency Packet Rates 802.11A/N	<p>Accept the defaults, or for each frequency, select one of the following: Nominal Rate, Allowed Rate, or Disable.</p> <p>Click See detail for additional information about these settings.</p>
Traffic Stream Metrics	<ol style="list-style-type: none"> 1. Accept the defaults or select one of the following: <ul style="list-style-type: none"> – Enable—Use this setting to have the access point report aggregated measurements to the WDS. – Disable—Use this setting to disable this feature. <p>Click See detail for additional information about this setting.</p> 2. Select for which radio these settings apply: Radio B/G/N and/or Radio A/N.
Voice for SSID 802.11A/N	<p>Allow or disallow Voice on selected SSIDs.</p> <ul style="list-style-type: none"> • Allow Voice for SSID—Enter the Service Set ID and click >>>. The SSID and the text (Voice Allowed) appears in the selection box on the right. • Disallow Voice for SSID—Enter the Service Set ID and click >>>. The SSID and the text (Voice Disallowed) appears in the selection box on the right. <p>To remove an SSID from the selection box, highlight the SSID and click Delete.</p> <p>Click See detail to see the versions for which this setting is valid and additional information.</p>

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Using Association

Use this option to configure the number of seconds that the access point tracks an inactive device.

Procedure

Step 1 Select **Association**. The Association: Activity Timeout dialog box displays in the right pane:

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-4 Association

Field	Description
Association: Activity Timeout	
These settings determine the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive.	
Device Class <ul style="list-style-type: none"> • Bridge— A device that connects two wired networks together through a wireless network. • Client Station— A device that is connected to an access point or bridge. • Repeater—A device (typically another access point) that forwards data from a client station to another access point. • Workgroup Bridge—A device that provides wireless infrastructure connections for Ethernet-enabled devices. A device connected to a workgroup bridge communicates with the network infrastructure through Cisco access points. • Unknown—A non-Cisco device. 	<ul style="list-style-type: none"> • Default—Specifies the activity timeout value that the access point uses when a device associates and either proposes a zero-refresh rate or does not propose a refresh rate. • Maximum—Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates.

Table 5-4 Association (continued)

Field	Description
Delete Activity Timeout	These settings are used to remove existing timeout settings configured on the access point.
Device Class <ul style="list-style-type: none"> • Bridge— A device that connects two wired networks together through a wireless network. • Client Station— A device that is connected to an access point or bridge. • Repeater—A device (typically another access point) that forwards data from a client station to another access point. • Workgroup Bridge—A device that provides wireless infrastructure connections for Ethernet-enabled devices. A device connected to a workgroup bridge communicates with the network infrastructure through Cisco access points. • Unknown—A non-Cisco device. 	<ul style="list-style-type: none"> • Default—Specifies the activity timeout value that the access point uses when a device associates and either proposes a zero-refresh rate or does not propose a refresh rate. • Maximum—Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Setting Up Network Interfaces

Use this option to configure the device's network interface settings.

Procedure

- Step 1** Select **Network Interfaces**. The menu expands and the Network Interfaces: Fast/Gigabit Ethernet Settings dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- Fast/Gigabit Ethernet—See [Configuring Fast/Gigabit Ethernet Settings, page 5-19](#).
 - Radio-802.11b/g/n—See [Configuring Radio-802.11b/g/n Settings, page 5-20](#).
 - Radio-802.11a/n—See [Configuring Radio-802.11a/n Settings, page 5-29](#)
-

Configuring Fast/Gigabit Ethernet Settings

Use this option to define the Fast/Gigabit Ethernet port settings.

Procedure

- Step 1** Select **Network Interfaces > Fast/Gigabit Ethernet**. The Network Interfaces: Fast/Gigabit Ethernet Settings dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-5 Fast/Gigabit Ethernet Settings

Field	Description
Enable Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable Fast/Gigabit Ethernet. • Disable—Use this setting to disable Fast/Gigabit Ethernet.
Requested Duplex	Select one of the following: <ul style="list-style-type: none"> • Auto—Use this setting to allow the duplex setting to be automatically negotiated between the access point and the hub, switch, or router to which the access point is connected. • Half—Use this setting to allow operation in half-duplex mode. • Full—Use this setting to allow operation in full-duplex mode.
Requested Speed	Select one of the following: <ul style="list-style-type: none"> • Auto—Use this setting to allow the transmission speed to be automatically negotiated between the access point and the hub, switch, or router to which the access point is connected. • 10 Mbps—Use this setting to allow a transmission speed of 10 Mbps. • 100 Mbps—Use this setting to allow a transmission speed of 100 Mbps. • 1000 Mbps—Use this setting to allow a transmission speed of 1000 Mbps. Click See detail to see for which device types or versions this setting is valid.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Radio-802.11b/g/n Settings

Use this option to configure the device's 802.11b, 802.11g, and 802.11n radio.

Procedure

Step 1 Select **Network Interfaces > Radio-802.11b/g/n**. The Network Interfaces: Radio-802.11b/g/n dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-6 Radio-802.11b/g/n Settings

Field	Description
Configure Radio	Select the radio interface type: <ul style="list-style-type: none"> • Radio B • Radio G/N—Click See detail to see for which device types or versions this setting is valid.
Enable Radio	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow the access point to send packets through its radio interface and monitor when other devices use the radio interface to send packets. • Disable—Use this setting to change the administrative state of the radio from up to down.
Role in Radio Network (Fallback mode upon loss of Ethernet connection)	This setting is used to configure a fallback role for the access point. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. <p>Select one of the following:</p> <ul style="list-style-type: none"> • Access Point Root (Fallback to Radio Island)—Use this setting to enable wireless clients to continue to associate even when there is no connection to the wired LAN. • Access Point Root (Fallback to Radio Shutdown)—Use this setting to force the clients to associate to another access point, if one is available, when the radio shuts down because the wired connection is lost. • Access Point Root (Fallback to Repeater)—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band.

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
	<ul style="list-style-type: none"> <li data-bbox="662 317 1458 436">• Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. <li data-bbox="662 457 1458 577">• Bridge Root without Clients—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. <li data-bbox="662 598 1458 657">• Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. <li data-bbox="662 678 1458 764">• Bridge Non-Root without Clients—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. <li data-bbox="662 785 1458 844">• Bridge Non-Root with Clients—Use this setting to specify that the bridge operates as a non-root bridge with clients. <li data-bbox="662 865 1458 951">• Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. <p data-bbox="695 972 1458 1031">Click See detail to see for which device types or versions this setting is valid.</p>

Table 5-6 Radio-802.11b/g/n Settings (continued)


Field	Description
Data Rates	<ul style="list-style-type: none"> • Click one of the following to automatically set the data transmission rates: <ul style="list-style-type: none"> – Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput. – Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. – Default—Use this setting to compromise between range and throughput, providing good range and good throughput. <p>Or</p> <ul style="list-style-type: none"> • Select one of the following to manually set the data transmission rates: <ul style="list-style-type: none"> – Require—Use this setting to enable transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Require. A client must support a required rate before it can associate. – Enable—Use this setting to enable transmission at this rate for unicast packets only. – Disable—Use this setting to not allow transmission at this rate.
Transmitter Power (mW)	<p>Select the power level of the radio transmission.</p> <p>Note Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device.</p> <p>To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.</p> <p> Caution Do not use the 50mW or 10mW setting for Japanese channels.</p> <p>For a list of maximum power levels allowed in each regulatory domain refer to one of the following:</p> <ul style="list-style-type: none"> • URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443 • Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>. <p>Click See detail to see for which device types or versions this setting is valid.</p> <p>Click Power Translation Table mW/dBm to see the mapping values for transmitter power.</p>

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
CCK Transmitter Power (mW)	Use this setting on the 2.4-GHz, 802.11g/n radio to specify Complementary Code Keying (CCK) power levels in milliwatts. CCK modulation is supported by 802.11b/g/n devices. Click See detail to see for which device types or versions this setting is valid.
CCK Transmitter Power (dBm)	Use this setting on the 2.4-GHz, 802.11g/n radio to specify Complementary Code Keying (CCK) power levels in decibels below 1 milliwatt. CCK modulation is supported by 802.11b/g/n devices. Click See detail to see for which device types or versions this setting is valid.
OFDM Transmitter Power (mW)	Use this setting on the 2.4-GHz, 802.11g/n radio to specify Orthogonal Frequency Division Multiplexing (OFDM) power levels in milliwatts. OFDM modulation is supported by 802.11g/n and 802.11a/n devices. Click See detail to see for which device types or versions this setting is valid.
OFDM Transmitter Power (dBm)	Use this setting on the 2.4-GHz, 802.11g/n radio to specify Orthogonal Frequency Division Multiplexing (OFDM) power levels in decibels below 1 milliwatt. OFDM modulation is supported by 802.11g/n and 802.11a/n devices. Click See detail to see for which device types or versions this setting is valid.
Client Power Local	Use this setting to limit the power level on client devices that associate to the access point to the same setting as the AP's configured transmitter power. Note Setting the client's power level to the same as the AP transmitter power provides improved interference control in the WLAN. Note If you disable this option, you should use one of the Limit Client Power fields (see below) to set the client's power level to a specific value. Click See detail to see for which device types or versions this setting is valid.
Limit Client Power (mW)	Use this setting to limit the power level on client devices that associate to the access point in milliwatt. When a client device associates to the access point, the access point sends the maximum power level setting to the client.
Limit Client Power (dBm)	Use this setting to limit the power level on client devices that associate to the access point in decibel. When a client device associates to the access point, the access point sends the maximum power level setting to the client.

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
Default Radio Channel	<p>From the list, select the radio channel you want for a default.</p> <p>If you select Least Congested Frequency, the access point scans for the radio channel that is least busy and selects that channel for use. The device scans at power-up and when the radio settings are changed.</p> <p>Click See detail to verify which channels are applicable in your region.</p>
Least Congested Channel Search	<p>If you want to limit the channels the access point scans when the Default Radio Channel is set for Least Congested Frequency, select one or more channels from the list.</p>
World Mode Multi-Domain Operation	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable—Use this setting to not allow the access point to add channel carrier set information to its beacon. • Legacy—Use this setting to enable Cisco legacy world mode. • Dot11d—Use this setting to enable 802.11d world mode. <p>When you use this setting, you must enter an ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website.</p>
Country Code (use only for Dot11d)	<p>From the list, select the country code, then select either indoor or outdoor.</p>
Radio Preamble	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Short—Use this setting to improve throughput performance; Cisco Aironet's Wireless LAN Adapter supports short preambles. • Long—Use this setting to ensure compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).
Receive Antenna	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.)
Transmit Antenna	
External Antenna Configuration	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to configure the access point or bridge's antenna gain. • Disable—Use this setting to disable this feature.
Antenna Gain (dB)	<p>Enter the desired antenna gain.</p>

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
Aironet Extensions	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing.
Ethernet Encapsulation Transform	Select one of the following: <ul style="list-style-type: none"> • RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. • 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.
Concatenation	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting for packet concatenation on the bridge radio to combine multiple packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Max Length of Concatenation	Use this setting to specify a maximum size, in bytes, for concatenated packets.
Distance (Km)	Enter value between 0 and 99 that determines the length of the radio link propagation delay. Click See detail to see for which device types or versions this setting is valid.
Reliable Multicast to WGB	Select one of the following: <ul style="list-style-type: none"> • Disable—Use this setting to not allow reliable multicast to workgroup bridges. • Enable—Use this setting to allow reliable multicast to workgroup bridges.
Public Secure Packet Forwarding	Note Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting Services > VLAN . Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable use of the protected port for secure mode configuration. (No exchange of unicast, broadcast, or multicast traffic occurs between protected ports.) • Disable—Use this setting to disable the use of the port for secure mode configuration.

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
Mobile Station	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow scanning by a mobile station for a better radio connection, which provides seamless roaming. • Disable—Use this setting to disable the feature.
Mobile Station Scan	Select the channels to use for scanning by a mobile station.
Ignore Mobile Station Neighbors List	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to ignore the neighbors list report for mobile station scanning. This setting will have effect only if the Mobile Station Scan option is configured. • Disable—Use this setting to use the neighbors list report for mobile station scanning.
Beacon privacy guestmode	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable the beacon privacy guest mode. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Short Slot-Time	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable short slot time on the 802.11g/n, 2.4-GHz radio. Short slot time reduces the slot time from 20 microseconds to 9 microseconds, thereby increasing throughput. The access point uses short slot time only when all clients that are associated to the 802.11g/n radio can support short slot time. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 kilomicrosecond.
Max. Data Retries	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
RTS Max. Retries	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.

Table 5-6 Radio-802.11b/g/n Settings (continued)



Field	Description
Fragmentation Threshold	<p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p> <p>Click See detail for the maximum fragmentation threshold value for access points.</p>
RTS Threshold	<p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.</p> <p>Click See detail for the maximum RTS threshold value for access points.</p>
Repeater Parent AP Timeout	<p>Enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list.</p>
Repeater Parent AP MAC1 through MAC 4	<p>Enter the MAC address for the access point to which the repeater should associate.</p> <p>You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list.</p>
Radio-802.11N(2.4GHz and 5GHz)	
Click See detail to see for which radios this setting is valid.	
MCS Rates	<p>Select one or more MCS rates.</p> <p> Note Select at least one data rate before selecting MCS rates.</p>
Channel Width	Select the channel width from the drop-down menu.
Guard Interval	<p>Select one of the following:</p> <p>Any—Use this setting to allow the access point to choose guard interval as short or long based on the associated client capabilities.</p> <p>Long—Use this setting to configure Guard Interval as Long, which is the default setting.</p>

Table 5-6 Radio-802.11b/g/n Settings (continued)

Field	Description
Transmitter Power (dBm)	<p>Select the power level of the bridge's radio transmission.</p> <p>To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.</p> <p>For a list of maximum power levels allowed in each regulatory domain, refer to one of the following:</p> <ul style="list-style-type: none"> http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443 Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.
	<p> Note Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the bridge.</p>

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Radio-802.11a/n Settings

Use this option to configure the device's 802.11a/n radio.

Procedure

Step 1 Select **Network Interfaces > Radio-802.11a/n**. The Network Interfaces: Radio-802.11a/n dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-7 Radio-802.11a/n Settings

Field	Description
Enable Radio	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow the access point to send packets through its 802.11a/n radio interface and monitor when other devices use the 802.11a/n radio interface to send packets. • Disable—Use this setting to change the administrative state of the radio from up to down.
Role in Radio Network (Fallback mode upon loss of Ethernet connection)	This setting is used to configure a fallback role for the access point. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. <p>Select one of the following:</p> <ul style="list-style-type: none"> • Access Point Root (Fallback to Radio Island)—Use this setting to enable wireless clients to continue to associate even when there is no connection to the wired LAN. • Access Point Root (Fallback to Radio Shutdown)—Use this setting to force the clients to associate to another access point, if one is available, when the radio shuts down because the wired connection is lost. • Access Point Root (Fallback to Repeater)—Use this setting for a root access point to become a repeater and associate to a nearby root access point when the wired connection is lost. • Repeater Non-Root—Use this setting if the access point is not connected to the wired LAN. Client data is transferred to the access point selected as the repeater parent. • Scanner Access Point—Select to specify that the access point is a Scanning AP, which is used to guard certain air space from any potential intruders that operate on the same frequency band. • Workgroup Bridge—Use this setting to specify that the device is a workgroup bridge. Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges.

Table 5-7 *Radio-802.11a/n Settings (continued)*

Field	Description
	<ul style="list-style-type: none"> • Bridge Root without Clients—Use this setting to designate one device in each group of bridges as the root bridge. A root bridge can only communicate with non-root bridges and other client devices and cannot associate with another root bridge. • Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. • Bridge Non-Root without Clients—Use this setting to specify that the bridge operates as a non-root bridge and must associate to a root bridge. • Bridge Root with Clients—Use this setting to designate a device as the root bridge with clients. • Install Mode—Select to configure a bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI), which assists in antenna alignment. <p>Click See detail to see for which device types or versions this setting is valid.</p>

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Data Rates	<ul style="list-style-type: none"> • Click one of the following to automatically set the data transmission rates: <ul style="list-style-type: none"> – Best Range—Use this setting to maximize the access point's range; however, it might reduce throughput. – Best Throughput—Use this setting to maximize the data volume handled by the access point; however, it might reduce the access point's range. – Default—Use this setting to compromise between range and throughput, providing good range and good throughput. <p>Or</p> <ul style="list-style-type: none"> • Select one of the following to manually set the data transmission rates: <ul style="list-style-type: none"> – Require—Use this setting to enable transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Require. A client must support a required rate before it can associate. – Enable—Use this setting to enable transmission at this rate for unicast packets only. – Disable—Use this setting to not allow transmission at this rate.
Transmitter Power (mW)	<p>Select the power level of the access point's radio transmission.</p> <p>Note Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device.</p> <p>To reduce interference, limit the range of your access point, or conserve power, select a lower power setting.</p> <p>For a list of maximum power levels allowed in each regulatory domain refer to one of the following:</p> <ul style="list-style-type: none"> • URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_command_reference_chapter09186a0080147d8b.html#87443 • Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Transmitter Power (dBm)	<p>Select the power level of the bridge's radio transmission:</p> <p>Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the bridge.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p> <p>Click Power Translation Table mW/dBm to see the mapping values for transmitter power.</p>

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Client Power Local	<p>Use this setting to limit the power level on client devices that associate to the access point to the same setting as the AP's configured transmitter power.</p> <p>Note Setting the client's power level to the same as the AP transmitter power provides improved interference control in the WLAN.</p> <p>Note If you disable this option, you should use one of the Limit Client Power fields (see below) to set the client's power level to a specific value.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Limit Client Power (mW)	<p>Use this setting to limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Limit Client Power (dBm)	<p>Use this setting to limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Default Radio Channel	<p>From the list, select the radio channel you want for a default.</p> <p>If you select Least Congested Frequency, the access point scans for the radio channel that is least busy and selects that channel for use. The device scans at power-up and when the radio settings are changed.</p> <p>Click See detail for information on valid settings.</p>

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Frequency Band/Channel Selection	<p>The items displayed in this list depend on your default radio channel selection:</p> <ul style="list-style-type: none"> If you select Dynamic Frequency Selection (DFS) from the Default Radio Channel drop-down menu, a list of 4 bands are displayed in this box. <p>If you do not select any band in this box, the following commands are added to the Preview page:</p> <pre>interface Dot11Radio 1 channel dfs dfs band 1 2 3 4 block</pre> <p>If you select one or more bands from the list (for example bands 2 and 4), the following commands are added to the Preview page:</p> <pre>interface Dot11Radio 1 channel dfs dfs band 1 3 block</pre> <p>If you select all the bands in the list, the following commands are added to the Preview page:</p> <pre>interface Dot11Radio 1 channel dfs no dfs band block</pre> <ul style="list-style-type: none"> If you select any other entry from the Default Radio Channel drop-down menu, a list of channels are displayed in this box. Select one or more channels from the list.
World Mode Multi-Domain Operation	<p>Select one of the following:</p> <ul style="list-style-type: none"> Disable—Use this setting to not allow the access point to add channel carrier set information to its beacon. Legacy—Use this setting to enable Cisco legacy world mode. Dot11d—Use this setting to enable 802.11d world mode. <p>When you use this setting, you must enter an ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Country Code (use only for Dot11d)	<p>From the list, select the country code, then select one either Indoor or Outdoor.</p>

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	<ul style="list-style-type: none"> • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) <p>Click See detail to see for which device types or versions this setting is valid.</p>
External Antenna Configuration	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to configure the access point or bridge's antenna gain. • Disable—Use this setting to disable this feature. <p>Click See detail to see for which device types this setting is valid.</p>
Antenna Gain (dB)	Enter the desired antenna gain.
Aironet Extensions	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • Disable—Use this setting to disable load balancing, Message Integrity Check (MIC), and WEP key hashing. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Ethernet Encapsulation Transform	<p>Select one of the following:</p> <ul style="list-style-type: none"> • RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. • 802.1H—Use this setting to provide optimum performance for Cisco Aironet wireless products.
Concatenation	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting for packet concatenation on the bridge radio to combine multiple packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. • Disable—Use this setting to disable this feature. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Max Length of Concatenation	Use this setting to specify a maximum size, in bytes, for concatenated packets.

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Distance (Km)	Enter value between 0 and 99 that determines the length of the radio link propagation delay. Click See detail to see for which device types or versions this setting is valid.
Reliable Multicast to WGB	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow reliable multicast to workgroup bridges. • Disable—Use this setting to not allow reliable multicast to workgroup bridges. Click See detail to see for which device types or versions this setting is valid.
Public Secure Packet Forwarding	Note Use this setting only if no VLAN is configured. If a VLAN is configured, then enable and disable PSPF by selecting Services > VLAN . Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable use of the protected port for secure mode configuration. (No exchange of unicast, broadcast, or multicast traffic occurs between protected ports.) • Disable—Use this setting to disable the use of the port fro secure mode configuration. Click See detail to see for which device types or versions this setting is valid.
Mobile Station	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow scanning by a mobile station for a better radio connection, which provides seamless roaming. • Disable—Use this setting to disable the feature.
Mobile Station Scan	Select the channels to use for scanning by a mobile station.
Ignore Mobile Station Neighbors List	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to ignore the neighbors list report for mobile station scanning. This setting will have effect only if the Mobile Station Scan option is configured. • Disable—Use this setting to use the neighbors list report for mobile station scanning.
Beacon privacy guestmode	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable the beacon privacy guest mode. • Disable—Use this setting to disable this feature. Click See detail to see for which device types or versions this setting is valid.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)

Table 5-7 Radio-802.11a/n Settings (continued)

Field	Description
Data Beacon Rate (DTIM)	<p>Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>If the beacon period is set to 100, its default setting, and the data beacon rate is set to 2, its default setting, then the access point sends a beacon containing a DTIM every 200 kilomicrosecond.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Max. Data Retries	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
RTS Max. Retries	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Fragmentation Threshold	<p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
RTS Threshold	<p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Repeater Parent AP Timeout	<p>Enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Repeater Parent AP MAC1 though MAC 4	<p>Enter the MAC address for the access point to which the repeater should associate.</p> <p>You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list.</p>
Radio-802.11N(5GHz)	
Click See detail to see for which radios this setting is valid.	
MCS Rates	Select one or more MCS rates.
Channel Width	Select the channel width from the drop-down menu.
Guard Interval	Select Any or Long .

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Defining Security Settings

Use this option to configure the device's security settings.

Procedure

- Step 1** Select **Security**. The menu expands and the Security: Admin Access dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- Admin Access—See [Configuring Admin Access Settings, page 5-38](#).
 - SSID 802.11b/g/n—See [Configuring SSID 802.11b/g/n Settings, page 5-40](#).
 - SSID 802.11a/n—See [Configuring SSID 802.11a/n Settings, page 5-46](#).
 - WEP 802.11b/g/n—See [Configuring WEP 802.11b/g/n Settings, page 5-53](#).
 - WEP 802.11a/n—See [Configuring WEP 802.11a/n Settings, page 5-55](#).
 - Server Manager—See [Configuring Server Manager Settings, page 5-59](#).
 - Advanced Security—See [Configuring Advanced Security, page 5-63](#).
 - Local Radius Server—See [Setting Up the Local RADIUS Server, page 5-66](#).
-

Configuring Admin Access Settings

Use this option to add users to the system, remove users from the system, and assign user capabilities.

Procedure

- Step 1** Select **Security > Admin Access**. The Security: Admin Access dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-8 Admin Access Settings

Field	Description
Corporate Server	Select the type of server: RADIUS or TACACS+.
Administrator Authenticated by	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Default Authentication (Global Password)—Use this setting to skip the username and enter only a password. You will need to enter the password in the Default Authentication (Global Password field below). • Local User List Only (Individual Password)—Use this setting to designate the local user list for authentication. You will need to have at least one Read-Write user in the Local User List on the access point or in the Local User List field below. • Authentication Server Only—Use this setting to designate the server for authentication. • Authentication Server if not found in Local List—Use this setting to designate the server for authentication if not in the local list. You will need to have at least one Read-Write user in the Local User List on the access point or in the Local User List field below. • Local List if no response from Authentication Server—Use this setting to designate the local list for authentication if there is no response from the server. • Enable Authentication Server Caching—Use this setting to enable AAA authentication caching. Click See detail to see for which versions this setting is valid.
Default Authentication (Global Password)	
Default Authentication Password	Enter the password to be used as the default.
Confirm Authentication Password	Reenter the password.
Local User List (Individual Passwords)	
User List	<p>Lists the existing users.</p> <p>To delete a username from the list, select it, then click Delete.</p>
Username	Enter the username.
Password	Enter the password
Confirm Password	Reenter the password
Capability Settings	Select one of the settings, then click Add .
Delete Users	
User ID	Enter the user identification, then click >>.
Users to Delete	<p>Lists the users to be deleted.</p> <p>To remove users from the list, click <<</p>

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SSID 802.11b/g/n Settings

Use this option to configure SSID 802.11b, 802.11g, and 802.11n settings.

Procedure

Step 1 Select **Security > SSID 802.11b/g/n**. The Security: SSID Manager 802.11b/g/n dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-9 SSID 802.11b/g/n Settings


Field	Description
SSID List	Lists the currently configured SSIDs. To delete an SSID from the list, select it, then click Delete .
SSID	Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. The SSID is a unique identifier that clients use to associate with the radio.
VLAN	Enter the identification number or the name of the VLAN.
Network ID	Enter the network identification number.
Backup VLANs	To specify up to three backup VLANs, check the Backup VLANs check box and enter the IDs or names of the VLANs in the fields below.  Note The Backup VLANs option is supported only for device versions 12.3(11)JA*, 12.3(8)JEA*, and later releases.

Table 5-9 SSID 802.11b/g/n Settings (continued)

Field	Description
Authentication Methods Accepted	
Open Authentication	<p>Select one of the following from the list:</p> <ul style="list-style-type: none"> • MAC Authentication—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to allow client devices that associate to the access point using 802.11 open authentication to first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • MAC Authentication or EAP—Use this setting to allow client devices that associate to the access point using open authentication to first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • Optional EAP—Use this setting to allow both Open clients and EAP clients to associate and become authenticated with either authentication method.
Shared Authentication	<p>Select one of the following from the list:</p> <ul style="list-style-type: none"> • MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC and EAP authentication.
Network EAP	<p>Select the following from the list:</p> <p>MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.</p>

Table 5-9 SSID 802.11b/g/n Settings (continued)

Field	Description
Server Priorities	
EAP Authentication Servers	Select one of the following: <ul style="list-style-type: none"> • Use Defaults—Use this setting to use the defaults. • Use Server Group—Use this setting to specify a server group then enter the group name. • Customize—Use this setting to create a new server group. • New Group Name—Enter a name for the new group. • Priority—Enter the server IP address or hostname. <ul style="list-style-type: none"> – Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. or <ul style="list-style-type: none"> – Select a name from the list.
MAC Authentication Servers	
Authenticated Key Management	From the list, select one of the following: <ul style="list-style-type: none"> • None—Use this setting to indicate you do not want to use authenticated key management. • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.
CCKM	<p>Note For 802.11b/g/n, you can select both CCKM and WPAv1 or CCKM and WPAv2.</p> <p>Select this option to use Cisco Centralized Key Management (CCKM). Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain services (WDM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDM's cache of credentials reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.</p> <p>Note To enable CCKM for an SSID, you must configure network-EAP authentication.</p>

Table 5-9 SSID 802.11b/g/n Settings (continued)


Field	Description
WPAv1	<p>Note For 802.11b/g/n, you can select both CCKM and WPAv1.</p> <p>Select this option to use version 1 of the Wi-Fi Protected Access (WPAv1). The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point.</p> <p>If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (e.g., EAP-TLS) and generate a Pairwise Master Key.</p> <p>Note To enable WPAv1 for an SSID, you must also enable Open authentication and/or Network EAP. You should also configure TKIP as a Cipher suite for WPAv1.</p>
WPAv2	<p>Note For 802.11b/g/n, you can select both CCKM and WPAv2.</p> <p>Select this option to use version 2 of the Wi-Fi Protected Access (WPAv2).</p> <p>Note To enable WPAv2 for an SSID, you must also enable Open authentication and/or Network EAP. You should also configure TKIP or AES as a Cipher suite for WPAv2.</p>
MFP-Client	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this option to enable Client Management Frame Protection (MFP) on an SSID. Also select whether this option is optional or required from the drop-down menu. • Disable—Use this option to disable Client MFP on a SSID. <p>Click See detail to see for which device types or versions this setting is valid.</p>  <p>Note MFP-Client, protects authenticated clients from spoofed frames by preventing many of the common attacks against WLANs from becoming effective (for example rogue containment).</p>
WPA Pre-shared Key	<p>Enter a key for the access point to support client devices using WPA key management.</p> <p>For versions earlier than 12.2(11)JA, Enter a WEP key. For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits.</p> <p>Select either ASCII or Hexadecimal. If you use hexadecimal, you must enter 64 hexadecimal characters (unencrypted key) to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. Up to 63 ASCII characters are allowed.</p>
EAP Client	
Username (optional)	Enter the username used for EAP authentication when the repeater access point is associating with a parent access point.
Password (optional)	Enter the EAP client password.

Table 5-9 SSID 802.11b/g/n Settings (continued)

Field	Description
Association Limit (optional)	Enter the maximum number of clients that may associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.
Broadcast this SSID in Beacon (BSSID)	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this option to enable BSSID. • Disable—Use this option to disable BSSID.
Multiple Beacon Rate (DTIM)	Enter the rate at which the beacon sends a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. For example, if the beacon period is set at 100, and the data beacon rate is set at 1, then the access point sends a beacon containing a DTIM every 100 Kmsecs. One Kmsec equals 1,024 microseconds.
Accounting	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to indicate whether you want this server to record usage data of clients associating with the access point. • Disable—Use this setting to turn off accounting for your wireless network
Accounting Server Priorities	Select one of the following: <ul style="list-style-type: none"> • Use Defaults—Use this setting to select the defaults. • Use Server Group—Use this setting to specify a server group, then enter the name of the group. • Customize—Use this setting to create a new server group, then enter the name of the group. • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. <ul style="list-style-type: none"> – Acct Port—Enter the accounting port. or <ul style="list-style-type: none"> – Select a name from the list.
Advertise Extended Capabilities of this SSID	Select to enable advertising SSIDL IE information (only extended capabilities) in beacon/probe response. Advertise Wireless Provisioning Services (WPS) Support—Use this option to set WPS flag in the extended capabilities. Advertise the SSID as a Secondary Broadcast SSID—Use this option to send SSID name and capabilities in the SSIDL IE.
Enable IP Redirection on this SSID	Use this setting to redirect all packets sent from client devices associated to the SSID to a specific IP address. This is used primarily on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. <ul style="list-style-type: none"> • IP Address—Enter the IP address. • IP Filter—Enter a filter name or choose from an existing one.

Step 3 Click **Save**.

Step 4 Complete the following to set Beacon Mode/Infrastructure SSID:

Table 5-10 *Setting Beacon Mode/Infrastructure SSID*

Field	Description
Set Infrastructure SSID	<p>Enter the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID.</p> <p>Click Force infrastructure devices to associate only to this SSID if you want to enforce it.</p>
Set Beacon Mode	<ul style="list-style-type: none"> • Single Beacon SSID—Use this option to disable the MBSSID for this interface. Enter the SSID for Guest mode. • Multiple Beacon SSID—Use this option to enable MBSSID for this interface. Guest mode is disabled.

Step 5 Complete the following:

Table 5-11 *Setting MBSSID 802.11b/g/n Global Properties*

Field	Description
Multiple BSSID	<ul style="list-style-type: none"> • Enable—Use this option to enable MBSSID on all the interfaces that support it. • Disable—Use this option to disable MBSSID on all the interfaces that support it.

Step 6 Complete the following to delete an SSID:

Table 5-12 *Deleting SSID 802.11b/g/n*

Field	Description
SSID	Enter the SSID you want to delete, then click >>. The SSID is added to the SSID to Delete list.
Remove this SSID Globally	Select this option to delete the SSID globally.
SSID to Delete	Lists the SSIDs to delete. To remove an SSID from this list, click <<.

Step 7 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SSID 802.11a/n Settings

Use this option to configure SSID 802.11a/n settings.

Procedure

Step 1 Select **Security > SSID 802.11a/n**. The Security: SSID Manager 802.11a/n dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-13 SSID 802.11a/n Settings


Field	Description
SSID List	Lists the currently configured SSIDs. To delete an SSID from the list, select it, then click Delete .
SSID	Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. The SSID is a unique identifier that clients use to associate with the radio. Click See detail to see for which device types or versions this setting is valid.
VLAN	Enter the identification number or the name of the VLAN.
Network ID	Enter the network identification number.
Backup VLANs	To specify up to three backup VLANs, check the Backup VLANs check box and enter the IDs or names of the VLANs in the fields below. Click See detail to see for which device types or versions this setting is valid.  Note The Backup VLANs option is supported only for device versions 12.3(11)JA*, 12.3(8)JEA*, and later releases.
Authentication Methods Accepted	Click See detail to see for which device types or versions this setting is valid.
Open Authentication	Select one of the following from the list: <ul style="list-style-type: none"> • MAC Authentication—Use this setting to specify that client devices that associate to the access point with open authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with open authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to allow client devices that associate to the access point using 802.11 open authentication to first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • MAC Authentication or EAP—Use this setting to allow client devices that associate to the access point using open authentication to first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. • Optional EAP—Use this setting to allow both Open clients and EAP clients to associate and become authenticated with either authentication method.

Table 5-13 SSID 802.11a/n Settings (continued)

Field	Description
Shared Authentication	<p>Select one of the following from the list:</p> <ul style="list-style-type: none"> • MAC Authentication—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC authentication. • EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use EAP authentication. • MAC Authentication and EAP—Use this setting to specify that client devices that associate to the access point with shared authentication, use MAC and EAP authentication.
Network EAP	<p>Select the following from the list:</p> <p>MAC Authentication—Use this setting to specify that client devices that associate to the access point with network EAP authentication, use MAC authentication.</p>
Server Priorities	
EAP Authentication Servers	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Use Defaults—Use this setting to use the defaults. • Use Server Group—Use this setting to specify a server group then enter the group name. • Customize—Use this setting to create a new server group. • New Group Name—Enter a name for the new group. • Priority—Enter the server IP address or hostname. <ul style="list-style-type: none"> – Auth Port—Enter the authentication port. – Acct Port—Enter the accounting port. <p>or</p> <ul style="list-style-type: none"> – Select a name from the list.
MAC Authentication Servers	
<p>Click See detail to see for which device types or versions this setting is valid.</p>	
Authenticated Key Management	
Authenticated Key Management	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting to indicate you do not want to use authenticated key management. • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.

Table 5-13 SSID 802.11a/n Settings (continued)

Field	Description
CCKM	<p>Note To enable CCKM for an SSID, you must configure network-EAP authentication.</p> <p>Note For 802.11a/n, you can select both CCKM and WPAv1 or CCKM and WPAv2.</p> <ol style="list-style-type: none"> 1. Select this option to use Cisco Centralized Key Management (CCKM). Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain services (WDM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDM's cache of credentials reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. 2. From the list, select one of the following: <ul style="list-style-type: none"> • Mandatory—Use this setting to indicate authenticated key management is mandatory. • Optional—Use this setting to indicate authenticated key management is optional.
WPAv1	<p>Note For 802.11a/n, you can select both CCKM and WPAv1.</p> <p>Select this option to use version 1 of the Wi-Fi Protected Access (WPAv1). The WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (e.g., EAP-TLS) and generate a Pairwise Master Key.</p> <p>Note To enable WPAv1 for an SSID, you must also enable Open authentication and/or Network EAP. You should also configure TKIP as a Cipher suite for WPAv1.</p>
WPAv2	<p>Note For 802.11a/n, you can select both CCKM and WPAv2.</p> <p>Select this option to use version 2 of the Wi-Fi Protected Access (WPAv2).</p> <p>Note To enable WPAv2 for an SSID, you must also enable Open authentication and/or Network EAP. You should also configure TKIP or AES as a Cipher suite for WPAv2.</p>

Table 5-13 SSID 802.11a/n Settings (continued)


Field	Description
MFP-Client	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this option to enable Client Management Frame Protection (MFP) on an SSID. Also select whether this option is optional or required from the drop-down menu. • Disable—Use this option to disable Client MFP on a SSID. <p>Click See detail to see for which device types or versions this setting is valid.</p> <p> Note MFP-Client, protects authenticated clients from spoofed frames by preventing many of the common attacks against WLANs from becoming effective (for example rogue containment).</p>
WPA Pre-shared Key	<p>Enter a key for the access point to support client devices using WPA key management.</p> <p>For versions earlier than 12.2(11)JA, Enter a WEP key. For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits.</p> <p>Select either ASCII or Hexadecimal. If you use hexadecimal, you must enter 64 hexadecimal characters (unencrypted key) to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. Up to 63 ASCII characters are allowed.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
EAP Client Username	Enter the username used for EAP authentication when the repeater access point is associating with a parent access point.
Password	Enter the EAP client password.
Association Limit	Enter the maximum number of clients that may associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.
Broadcast this SSID in Beacon (BSSID)	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this option to enable BSSID. • Disable—Use this option to disable BSSID.
Multiple Beacon Rate (DTIM)	<p>Enter the rate at which the beacon sends a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>For example, if the beacon period is set at 100, and the data beacon rate is set at 1, then the access point sends a beacon containing a DTIM every 100 Kmsecs. One Kmsec equals 1,024 microseconds.</p>

Table 5-13 SSID 802.11a/n Settings (continued)

Field	Description
Accounting	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to indicate whether you want this server to record usage data of clients associating with the access point. • Disable—Use this setting to turn off accounting for your wireless network. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Accounting Server Priorities	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Use Defaults—Use this setting to select the defaults. • Use Server Group—Use this setting to specify a server group, then enter the name of the group. • Customize—Use this setting to create a new server group, then enter the name of the group. • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. <ul style="list-style-type: none"> – Acct Port—Enter the accounting port. <p>or</p> <ul style="list-style-type: none"> – Select a name from the list.
Advertise Extended Capabilities of this SSID	<p>Select to enable advertising SSIDL IE information (only extended capabilities) in beacon/probe response.</p> <hr/> <p>Advertise Wireless Provisioning Services (WPS) Support—Use this option to set WPS flag in the extended capabilities.</p> <hr/> <p>Advertise the SSID as a Secondary Broadcast SSID—Use this option to send SSID name and capabilities in the SSIDL IE.</p>
Enable IP Redirection on this SSID	<p>Use this setting to redirect all packets sent from client devices associated to the SSID to a specific IP address. This is used primarily on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address.</p> <ul style="list-style-type: none"> • IP Address—Enter the IP address. • IP Filter—Enter a filter name or choose from an existing one.

Step 3 Click **Save**.

Step 4 Complete the following to set Beacon Mode/Infrastructure SSID:

Table 5-14 Setting Beacon Mode/Infrastructure SSID

Field	Description
Set Infrastructure SSID	Enter the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. Click Force infrastructure devices to associate only to this SSID if you want to enforce it.
Set Beacon Mode	<ul style="list-style-type: none"> Single Beacon SSID—Use this option to disable the MBSSID for this interface. Enter the SSID for Guest mode. Multiple Beacon SSID—Use this option to enable MBSSID for this interface. Guest mode is disabled.

Step 5 Complete the following:

Table 5-15 Setting MBSSID 802.11a/n Global Properties

Field	Description
Multiple Beacon BSSID	<ul style="list-style-type: none"> Enable—Use this option to enable BSSID. Disable—Use this option to disable BSSID.

Step 6 Complete the following to delete an SSID:

Table 5-16 Deleting SSID 802.11a/n

Field	Description
SSID	Enter the SSID you want to delete, then click >>. The SSID is added to the SSID to Delete list.
Remove this SSID Globally	Select this option to delete the SSID globally.
SSID to Delete	Lists the SSIDs to delete. To remove an SSID from this list, click <<.

Step 7 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WEP 802.11b/g/n Settings

Use this option to select authentication types for the access point. The WEP keys allow you to encrypt radio signals sent by the device and decrypt radio signals received by the device.

Procedure

- Step 1** Select **Security > WEP 802.11b/g/n**. The Security: WEP Key Manager 802.11b/g/n dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-17 WEP 802.11b/g/n Settings

Field	Description
Set Encryption Mode and Keys for VLAN	Enter the VLAN for which you want to set the encryption mode and keys. If you enter None, properties are applied globally.
VLAN List	Lists the currently configured VLANs. To remove a VLAN from the list, select it, then click Delete .
Encryption Modes	
None	Select this option if the device communicates only with client devices that are not using WEP.
WEP Encryption	Select this option if you want to use WEP key encryption. From the list, select one of the following: <ul style="list-style-type: none"> Optional—Use this option to allow client devices to communicate with the access point either with or without WEP. Mandatory—Use this option to require client devices to use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate. Select one of the following: <ul style="list-style-type: none"> Cisco Compliant TKIP Features—Use this option to enable Temporal Key Integrity Protocol (TKIP). When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point. Enable MIC—Use this setting if you to enable Message Integrity Check (MIC). When you enable MIC, only MIC-capable client devices can communicate with the access point. Enable Per Packet Keying—Use this option to enable MIC on both the access point and all associated client devices. A few bytes are added to each packet to make the packets tamper-proof.

Table 5-17 WEP 802.11b/g/n Settings (continued)

Field	Description
Cipher	<p>Select this option to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM).</p> <p>Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.</p> <p>From the list, select the one of the cipher suites.</p> <ul style="list-style-type: none"> • WEP 128 bit—Use this option to specify that 128-bit WEP is included in the cipher suite. • WEP 40 bit—Use this option to specify that 40-bit WEP is included in the cipher suite. • TKIP—Temporal key integrity protocol is the most secured cipher suite. • CKIP—Cisco Key Integrity Protocol is Cisco's WEP key permutation technique based on an early algorithm. • CMIC—Cisco Message Integrity Check is Cisco's message integrity check mechanism designed to detect forgeries attracts. • CKIP + CMIC—See description for CKIP and CMIC. • TKIP+WEP 128 bit—See description for TKIP and WEP 128 bit. • TKIP+WEP 40 bit—See description for TKIP and WEP 40 bit. • AES CCMP—Advanced Encryption Standard of symmetric block cipher that encrypts and decrypt data using keys of 128, 192, and 256 bits.
	<ul style="list-style-type: none"> • AES CCMP+TKIP—See description for AES CCMP and TKIP. • AES CCMP+TKIP+WEP 128 bit—See description for AES CCMP, TKIP, and WEP 128 bit. • AES CCMP+TKIP+WEP 40 bit—See description for AES CCMP, TKIP, and WEP 40 bit.
WEP Keys	
Encryption Keys 1 through 4	
Transmit Key	Select to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	<p>Enter the type of encryption key used:</p> <ul style="list-style-type: none"> • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • 40 bit • 128 bit

Table 5-17 WEP 802.11b/g/n Settings (continued)

Field	Description
Broadcast Key Rotation Interval	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Rotation—Use this setting to disable broadcast key rotation. • Enable Rotation with Interval—Use this setting for the access point to provide a dynamic broadcast WEP key and to change it at the selected interval.
WPA Group Key Update	<p>Select the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices.</p> <ul style="list-style-type: none"> • Enable Group Key Update on Membership Termination—Select this setting if clients do not roam frequently among access points. The access point generates and distributes a new group key when any authenticated station disassociates from the access point. This option keeps the group key private to only currently active members. However, it may generate some overhead if clients in your network roam frequently. • Enable Group Key Update on Member's Capability Change—Use this setting, when in WPA migration mode, to improve the security of the key management capable clients when there are no legacy clients associated to the access point. The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates.

Step 3 Click **Save**. The VLAN is added to the list box.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WEP 802.11a/n Settings

Use this option to select authentication types for the access point. The WEP keys allow you to encrypt radio signals sent by the device and decrypt radio signals received by the device.

Procedure

Step 1 Select **Security > WEP 802.11a/n**. The Security: WEP Key Manager 802.11a/n dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-18 WEP 802.11a/n Settings

Field	Description
Set Encryption Mode and Keys for VLAN	Enter the VLAN for which you want to set the encryption mode and keys. If you enter None, properties are applied globally.
VLAN List	Lists the currently configured VLANs. To remove a VLAN from the list, select it, then click Delete .
Encryption Modes	
None	Select this option if the device communicates only with client devices that are not using WEP.
WEP Encryption	Select this option if you want to use WEP key encryption. From the list, select one of the following: <ul style="list-style-type: none"> • Optional—Use this option to allow client devices to communicate with the access point either with or without WEP. • Mandatory—Use this option to require client devices to use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate. Select one of the following: <ul style="list-style-type: none"> • Cisco Compliant TKIP Features—Use this option to enable Temporal Key Integrity Protocol (TKIP). When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point. • Enable MIC—Use this setting if you to enable Message Integrity Check (MIC). When you enable MIC, only MIC-capable client devices can communicate with the access point. • Enable Per Packet Keying—Use this option to enable MIC on both the access point and all associated client devices. A few bytes are added to each packet to make the packets tamper-proof.

Table 5-18 WEP 802.11a/n Settings (continued)

Field	Description
Cipher	<p>Select this option to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM).</p> <p>Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.</p> <p>From the list, select the one of the cipher suites.</p> <ul style="list-style-type: none"> • WEP 128 bit—Use this option to specify that 128-bit WEP is included in the cipher suite. • WEP 40 bit—Use this option to specify that 40-bit WEP is included in the cipher suite. • TKIP—Temporal key integrity protocol is the most secured cipher suite. • CKIP—Cisco Key Integrity Protocol is Cisco's WEP key permutation technique based on an early algorithm. • CMIC—Cisco Message Integrity Check is Cisco's message integrity check mechanism designed to detect forgeries attracts. • CKIP + CMIC—See description for CKIP and CMIC. • TKIP+WEP 128 bit—See description for TKIP and WEP 128 bit. • TKIP+WEP 40 bit—See description for TKIP and WEP 40 bit. • AES CCMP—Advanced Encryption Standard of symmetric block cipher that encrypts and decrypt data using keys of 128, 192, and 256 bits.
	<ul style="list-style-type: none"> • AES CCMP+TKIP—See description for AES CCMP and TKIP. • AES CCMP+TKIP+WEP 128 bit—See description for AES CCMP, TKIP, and WEP 128 bit. • AES CCMP+TKIP+WEP 40 bit—See description for AES CCMP, TKIP, and WEP 40 bit.
WEP Keys	
Encryption Keys 1 through 4	
Transmit Key	Select to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	<p>Enter the type of encryption key used:</p> <ul style="list-style-type: none"> • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • 40 bit • 128 bit

Table 5-18 WEP 802.11a/n Settings (continued)

Field	Description
Broadcast Key Rotation Interval	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Rotation—Use this setting to disable broadcast key rotation. Click See detail to see for which device types or versions this setting is valid. • Enable Rotation with Interval—Use this setting for the access point to provide a dynamic broadcast WEP key and to change it at the selected interval.
WPA Group Key Update	<p>Select the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices.</p> <ul style="list-style-type: none"> • Enable Group Key Update on Membership Termination—Select this setting if clients do not roam frequently among access points. The access point generates and distributes a new group key when any authenticated station disassociates from the access point. This option keeps the group key private to only currently active members. However, it may generate some overhead if clients in your network roam frequently. Click See detail to see for which device types or versions this setting is valid. • Enable Group Key Update on Member's Capability Change—Use this setting, when in WPA migration mode, to improve the security of the key management capable clients when there are no legacy clients associated to the access point. The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates.

Step 3 Click **Save**. The VLAN is added to the list box.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Server Manager Settings

Use this option to enter the authentication settings. The RADIUS server on the your network uses EAP to provide authentication service for wireless client devices.

Procedure

- Step 1** Select **Security > Server Manager**. The Security: Server Manager dialog box appears.
- Step 2** Complete the following to add a server to the list:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-19 Backup Radius Server

Field	Description
Backup Radius Server Click See detail to see for which device types or versions this setting is valid.	Select one of the following: <ul style="list-style-type: none"> • Create—Use this setting to create a backup RADIUS server. • Delete—Use this setting to delete a backup RADIUS server.
Backup Radius Server	Enter the hostname or IP address of the RADIUS server you are either creating or deleting.
Shared Secret	Enter the server's shared secret.
Corporate Servers	
Current Server List	Lists the servers that are currently configured. To remove a server from the list, select it, then click Delete .
RADIUS	Select this option if you are configuring settings for RADIUS.
TACACS+	Select this option if you are configuring settings for TACACS+.
Server	Enter the hostname or IP address for the selected server.
Shared Secret	Enter the shared secret used by your server.
Authentication Port	Enter the port number your server uses for authentication. Enter the port number the server uses for authentication.
Accounting Port	Enter the port number your server uses for accounting.

- Step 3** Click **Save**. The server appears on the list.
- Step 4** To delete a server from the list, select it from the list, then click **Delete**.

Step 5 Complete the following to set default server priorities:

Table 5-20 *Default Server Priority Settings*

Field	Description
EAP Authentication	<ul style="list-style-type: none"> • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port used by the server. • Acct Port—Enter the accounting port used by the server.
MAC Authentication	
Click See detail to see for which device types or versions this setting is valid.	
Accounting	
Click See detail to see for which device types or versions this setting is valid.	
Admin Authentication (RADIUS)	
Admin Authentication (TACACS+)	

Step 6 Complete the following to set global server properties:

Table 5-21 Global Server Properties

Field	Description
Accounting Update Interval	Enter the interval at which the accounting updates should be performed. The accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming.
TACACS+ Server Timeout	Enter the number of seconds the access point should wait before resending the request.
RADIUS Server Timeout	Enter the number of seconds the access point should wait before resending the request.
RADIUS Server Retransmit Retries	Enter the number of seconds the access point should wait before giving up contacting the server.
Dead RADIUS Server List	When a server is found to be unresponsive after numerous retransmissions and time-outs, it is assumed to be dead and is put in a dead server list. Select one of the following: <ul style="list-style-type: none"> • Disable—Use this setting to disable the feature. • Enable; Server remains on list for—Use this setting to enable the feature and to set the length of time for which the server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
RADIUS Calling/Called Station ID Format	Use this setting to indicate the format of the Called Station ID and Calling Station ID. field in the authentication packets sent to the RADIUS server. Select one of the following: <ul style="list-style-type: none"> • Default—Use this setting to implement the Cisco IOS MAC address format. • IETF—Use this setting to implement the standard recommended by the IETF document. • Unformatted— Use this setting to implement the MAC address format used in non-IOS access points.
RADIUS Attributes	
Remove Existing WISPr Location-ID	Select to remove the existing location identification configured on the access point, which is sent with authentication and account requests, and use the ISO and E.164 country codes, and E.164 area code instead.
ISO Country Code	Enter a unique two-letter code. Information about the ISO 3166 country codes can be found at the following URL: http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html

Table 5-21 Global Server Properties (continued)

Field	Description
E.164 Country Code	Enter a three-digit code for special uses. Information about the ISO 3166 country codes can be found at the following URL: http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html .
E.164 Area Code	Enter a three-digit code based on the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) recommendations. Information about ITU-T can be found at the following URL: http://www.itu.int/ITU-T/

Step 7 Complete the following to delete RADIUS servers:

Table 5-22 Deleting Servers and Server Groups

Field	Description
Servers to Delete	Lists the servers to delete. To delete a server from the list, select it, then click Delete .
Delete Server	Enter the server you want to delete, then select either RADIUS or TACACS+.
Authentication Port	Enter the port number your RADIUS/TACACS+ server uses for authentication.
Accounting Port	Enter the port number your RADIUS/TACACS+ server uses for accounting.
From Group	Enter the name of the group from which you want to delete the server.
Delete Server also?	If you want to delete the server from the group and delete the server itself.. Click Add Server to Delete List and the server name is added to the Servers to Delete.

Step 8 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Advanced Security

Use this option to set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication.

When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network. If the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication.

Procedure

Step 1 Select **Security > Advanced Security**. The Security: Advanced Security dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-23 *Advanced Security*

Field	Description
MAC Address Authentication	Click See detail to see for which device types or versions this setting is valid.
MAC Addresses Authenticated by	Select one of the following: <ul style="list-style-type: none"> Local List Only—Use this setting if you want the authentication to be stored on the access point, and enter MAC addresses. Authentication Server Only—Use this setting if you want the authentication to be stored on the server. Authentication Server if not found in Local List—Use this setting if you want to try MAC authentication list first and then automatically try the Authentication server list.
Local MAC Address List	Click See detail to see for which device types or versions this setting is valid.
Local List	The local MAC address list is displayed in this listbox. To delete an entry from the list, select it, then click Delete .
New MAC Address	Enter the MAC address, then click Add . Click Add MAC Address from file to open a window that allows you to browse for a file of MAC addresses, if you have created one. To see an example of a file, click Sample File . After you have located the sample file containing the MAC addresses, click OK .

Table 5-23 *Advanced Security (continued)*

Field	Description
EAP Authentication	
EAP Reauthentication Interval	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Reauthentication—Use this setting to disable reauthentication. • Enable Reauthentication with Interval—Use this setting to enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. • Enable Reauthentication with Interval given by Authentication Server—Use this setting to use the reauthentication period specified by the authentication server.
EAP Client Timeout (optional)	Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails.
Radio-802.11B/G/N TKIP	
TKIP MIC Failure Holdoff Time (Radio-802.11B/G/N)	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Holdoff—Use this setting to disable the TKIP MIC failure holdoff feature. • Enable Holdoff with Interval—Use this setting to enable the TKIP MIC failure hold time. The number of seconds you enter specifies the amount of time the access point blocks all TKIP clients on the interface.
Radio-802.11A/N TKIP	
TKIP MIC Failure Holdoff Time (Radio-802.11A/N)	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Holdoff—Use this setting to disable the TKIP MIC failure holdoff feature. • Enable Holdoff with Interval—Use this setting to enable the TKIP MIC failure hold time. The number of seconds you enter specifies the amount of time the access point blocks all TKIP clients on the interface.
Global Client Properties	
Click See detail to see for which device types or versions this setting is valid.	
Client Holdoff Time	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Disable Holdoff--Use this setting to disable the client holdoff feature. • Enable Holdoff with Interval--Use this setting to specify the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication.

Table 5-23 *Advanced Security (continued)*

Field	Description
Association Access List	
Click See detail to see for which device types or versions this setting is valid.	
Filter client association with MAC address access list	Select one of the following: <ul style="list-style-type: none"> • Enable— Use this setting to enable a MAC address filter for clients who are trying to associate with the access point. • Disable—Use this setting to prevent clients from associating based on their MAC addresses.
Filter	Enter the MAC address filter or select one from the list.

Step 3 Complete the following to delete local MAC addresses:

Click **See detail** to see for which device types or versions this setting is valid.

Table 5-24 *Deleting Local MAC Addresses*

Field	Description
Delete Local MAC Addresses	
Click See detail to see for which device types or versions this setting is valid.	
MAC Address	Enter the address you want to delete, then click >>. The address is added to the MAC Addresses to Delete list.
MAC Addresses to Delete	Lists the MAC dress to delete. To remove an address from the list, select it, then click <<.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Setting Up the Local RADIUS Server

Use this option to configure local server settings.

Procedure

Step 1 Select **Security > Local Radius Server**. The Security: Local Radius Server - General Set-Up dialog box appears.



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 2 Complete the following:

Table 5-25 Local Radius Server

Field	Description
Local Radius Server Authentication Settings	
EAP-FAST	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this option to enable authentication settings for this local Radius server. • Disable—Use this option to disable settings for this local Radius server.
LEAP	
MAC	
Network Access Server	
Click See detail to see for which device types or versions this setting is valid.	
Current Network Access Servers	Lists the network access servers. To remove a server from the list, select it, then click Delete .
Network Access Server	Enter the IP address of the RADIUS server.
Shared Secret	Enter the shared secret text string used between the access point and the RADIUS server.
User Groups	
Current User Group	Lists the user groups. To remove a group from the list, select it, then click Delete .
Group Name	Enter a name for the a new group.
Session Timeout	Use this setting to specify the maximum number of seconds of service to be provided to the user before the session terminates.
Number of Failed Authentications	Enter the number of times a user assigned to this group can provide an incorrect password; when the user fails this number of authentication attempts, the access point locks out the user. This setting helps prevent or delay password “dictionary” attacks.

Table 5-25 Local Radius Server (continued)

Field	Description
Lockout	Select one of the following: <ul style="list-style-type: none"> • Infinite—Use this setting to manually unlock any locked-out users. • Interval—Use this setting to specify the length of time that the access point locks out a user before the user can reattempt authentication.
VLAN ID	Enter the identification number of the VLAN.
SSID	Enter the SSID (any alphanumeric, case-sensitive string, from 1 to 32 characters long), then click Add .
SSID List	Lists all the SSIDs. To delete an SSID from the list, select it, then click Delete .
Individual User	
Current User List	Lists the current usernames. To remove a user from the list, select it, then click Delete .
Username	Enter the username.
Password	Enter the password, then select Text or NT Hash.
Confirm Password	Reenter the password.
Group Name	From the list, select the group name or None if the user does not belong to any group. MAC Authentication Only—Select to enable. Click Save to add the name to the current user list.
PAC Encryption Keys—Before a client can authenticate with an access point that is functioning as local RADIUS server, it needs a provision called PAC (Protected Access Credential).	
Primary Key	Enter a key to use for encryption or select Generate Random to have the system generate an encryption key.
Secondary Key	Enter a secondary key to use for encryption or click Copy from Primary .
PAC Content	
Authority Info	Enter information describing the authority information.
Authority ID	Enter an authority identification number for the access server.
Automatic PAC Provisioning—Use this setting when the client is auto-provision capable and is issued a PAC.	
Current User Group	Lists the current user groups.
User Group Name	Enter a user group name.
PAC Expiration	Enter the amount of time for which the issued PAC is valid.
PAC Grace Period	Enter the amount of time for a grace period after the PAC has expired. (The PAC can be used after it has expired as long as it is within the configured grace period.)
Out-of-Band PAC Generation—Use this setting when the client, using an IP address, accesses a machine in which PAC is stored.	

Table 5-25 Local Radius Server (continued)

Field	Description
Current User List	Lists the current usernames for out-of-band PAC generation.
User Name	Enter the user name.
TFTP File Server	Enter the IP address of the server in which PAC is stored.
PAC File Name	Enter the file name that contains the PAC information.
PAC Encryption Password	Enter the password to use to encrypt the PAC information.
PAC Expiration	Enter the time after which PAC becomes invalid, then click Generate PAC .
Delete Servers, Groups, and Users	
Server	Enter the server you want to delete, then click Add . The server name is added to the Servers to Delete list.
Servers to Delete	Select the server to delete from the list, then click Delete .
Group	Enter the group you want to delete, then click Add . The group name is added to the Groups to Delete list.
Groups to Delete	Select the group to delete from the list, then click Delete .
User	Enter the user you want to delete, then click Add . The user name is added to the Servers to Delete list.
Users to Delete	Select the user to delete from the list, then click Delete .
Delete PAC Encryption Keys, PAC Content	
Primary Key	Select an option to remove it.
Secondary Key	
Authority ID	
Authority Info	

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Defining Services

Use this option to configure various system features and support services on the device.

Procedure

- Step 1** Select **Services**. The menu expands and the Security: Telnet/SSH dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- Telnet/SSH—See [Configuring Telnet/SSH, page 5-69](#).
 - Hot Standby—See [Configuring Hot Standby, page 5-71](#).
 - CDP—See [Configuring CDP, page 5-72](#).
 - DNS—See [Configuring DNS, page 5-73](#).
 - MAC address filters—See [Configuring MAC Address Filters, page 5-74](#).
 - IP filters—See [Configuring IP Filters, page 5-76](#).
 - Ethertype filters—See [Configuring Ethertype Filters, page 5-79](#).
 - HTTP—See [Configuring HTTP, page 5-81](#).
 - QoS policies—See [Configuring QoS Policies, page 5-82](#).
 - QoS radio 802.11b/g/n—See [Configuring QoS Radio 802.11b/g, page 5-86](#).
 - QoS radio 802.11a/n—See [Configuring QoS Radio 802.11a/n, page 5-87](#).
 - SNMP—See [Configuring SNMP, page 5-87](#).
 - SNTP—See [Configuring SNTP, page 5-90](#).
 - VLAN—See [Configuring VLAN, page 5-91](#).
 - ARP Cache—See [Configuring ARP Cache, page 5-93](#).
 - STP—See [Configuring STP, page 5-94](#).
 - Packet Handle 802.11a/n—[Configuring Packet Handling 802.11a/n, page 5-96](#).

Configuring Telnet/SSH

Use this option to configure the access point to work through Telnet or SSH.

Procedure

- Step 1** Select **Services > Telnet/SSH**. The Services: Telnet/SSH dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-26 Telnet/SSH

Field	Description
Telnet	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to disable Telnet access to the management system.
Terminal Type	Select one of the following: <ul style="list-style-type: none"> • Teletype—Use this setting if your terminal emulator does not support ANSI. • ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.
Columns	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters. <p>Note For versions 12.3(8)JA and later, the default number of lines is reduced from 16 to 5. Therefore, this option generates a configuration for lines 0 to 4. To enable additional lines, use the Custom Values option to configure them.</p>
Secure Shell Configuration	
Secure Shell	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable secure shell. <p>Note You must enter values in the System Name and Domain Name fields to enable SSH. If you do not enter an RSA key size, it will default to 768.</p> <ul style="list-style-type: none"> • Disable—Use this setting to disable secure shell. • Modify—Use this setting to modify secure shell.
System Name	Enter a system name for your access point.
Domain Name	Enter a domain name for your access point.
RSA Key Size	Enter the additional bits used for authentication. <p>Note For SSH, you must enter a key size or it will remain disabled.</p>
Authentication Timeout	Enter the timeout in seconds, not to exceed 120 seconds for the length of time for authentication to take place.
Authentication Retries	Enter the number of authentication retries.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Hot Standby

Use this option to configure an access point for hot standby mode. Hot standby mode designates an access point as a backup for another access point.

The standby access point is placed near the access point it monitors, and is configured exactly the same as the monitored access point.

The standby access point associates with the monitored access point as a client and queries the monitored access point regularly through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Procedure

Step 1 Select **Services > Hot Standby**. The Services: Hot Standby dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-27 Hot Standby

Field	Description
Hot Standby Mode	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable hot standby mode on the access point. • Disable—Use this setting to disable hot standby mode on the access point. • Modify—Use this setting to modify the hot standby mode. Click See detail to see for which device types or versions this setting is valid.
MAC Address for the Monitored 802.11B/G/N Radio	Enter the MAC address of the access point to be monitored.
MAC Address for the Monitored 802.11A/N Radio	

Table 5-27 Hot Standby (continued)

Field	Description
Polling Interval	Enter the number of seconds between queries that the access point sends to the monitored access point's radio and Ethernet ports.
Timeout for Each Polling	Enter the number of seconds the access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.
Shutdown Primary Radios on Failover	Select one of the following: Yes—Use this setting to shut down the primary radios on failover. No—Use this setting to not shut down the primary radios on failover.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring CDP

Use this option to enable, disable, or adjust the access point's CDP settings.

Procedure

Step 1 Select **Services > CDP**. The Services: CDP-Cisco Discovery Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-28 CDP Settings

Field	Description
Cisco Discovery Protocol (CDP)	Select one of the following: <ul style="list-style-type: none"> • Enabled—Use this setting to enable CDP on the access point. • Disabled—Use this setting to disable CDP on the access point.
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packets Sent Every	Enter the number of seconds between each CDP packet the access point sends. This value should always be less than the packet hold time.

Table 5-28 CDP Settings (continued)

Field	Description
Individual Port Enable	
Ethernet	Select one of the following: <ul style="list-style-type: none"> Enabled—Use this option to enable CDP on the Ethernet port. Disabled—Use this option to disable CDP on the Ethernet port.
Radio-802.11B/G/N	Select one of the following: <ul style="list-style-type: none"> Enabled—Use this option to enable CDP on the radio port. Disabled—Use this option to disable CDP on the radio port.
Radio-802.11A/N	Select one of the following: <ul style="list-style-type: none"> Enabled—Use this option to enable CDP on the radio port. Disabled—Use this option to disable CDP on the radio port.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring DNS

Use this option to configure the access point to work with your network's Domain Name System (DNS) server.

Procedure

Step 1 Select **Services > DNS**. The Services: DNS-Domain Name Service dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-29 DNS Settings

Field	Description
Domain Name System (DNS)	Select one of the following: <ul style="list-style-type: none"> Enabled—Use this setting if your network uses DNS. Disabled—Use this setting if you network does not use DNS.
Domain Name (optional)	Enter the domain name.

Table 5-29 DNS Settings (continued)

Field	Description
Name Server IP Addresses	Enter the IP addresses of up to three domain name servers on your network.
Delete Name Servers	
Server	Enter the server you want to delete, then click >>. The server name is added to the Servers to Delete list.
Servers to Delete	Select the server to delete, then click <<.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring MAC Address Filters

Use this option to configure MAC address filters.

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.

Procedure

Step 1 Select **Services > MAC address filters**. The Services: Filters - MAC Address Filters dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-30 MAC Address Filters

Field	Description
Create and Apply	Select this option to create and apply MAC address filters.
Create Only	Select this option to create MAC address filters, but not apply them.
Apply Only	Select this option to apply the MAC address filters.
Filters List	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete Filter .

Table 5-30 *MAC Address Filters (continued)*

Field	Description
Filter Index	<p>Enter a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.</p> <p>ACLs applied from the WLSE have a cumulative effect on the device. If you want to modify the ACLs, delete the existing ACL using a template and then regenerate it using the WLSE. This way you are guaranteed that the ACL is applied in the correct order.</p> <p>For example, If an ACL has the following lines:</p> <pre>access-list 700 permit 0040.1111.1111 0000.0000.0000 access-list 700 permit 0040.2222.2222 0000.0000.0000 access-list 700 deny 0.0.0 ffff.ffff.ffff</pre> <p>and you would like to add the following at the beginning of the list:</p> <pre>access-list 700 permit 0040.3333.3333 0000.0000.0000</pre> <p>Then you need to delete the ACL and reapply it. Otherwise, the line you added will show up at the end of the list, not at the beginning where you intended it.</p>
Add MAC Address	Enter the MAC address.
Mask	Enter the subnet mask.
Action	<p>From the list, select one of the following actions:</p> <ul style="list-style-type: none"> • Forward—Use this setting to forward the MAC addresses. • Block—Use this setting to block the MAC addresses.
Load MAC Address	<p>Click to open a window that allows you to browse for a file of MAC addresses, if you have created one. To see an example of a file, click Sample File.</p> <p>After you have located the sample file containing the MAC addresses, click OK.</p>
VLAN ID	<p>Enter the VLAN identification number then click >>.</p> <p>To remove a VLAN ID from the list, select it, then click <<.</p>
Bridge-Group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.
Apply Filter to	
Fast/Gigabit Ethernet	Select one of the following:
Radio0-802.11B/G/N	<ul style="list-style-type: none"> • Incoming—Use this option to apply the filter to the incoming packets.
Radio0-802.11A/N	<ul style="list-style-type: none"> • Outgoing—Use this option to apply the filter to the outgoing packets. <p>Click AddFilter.</p>

Table 5-30 MAC Address Filters (continued)

Field	Description
Default Action	Select one of the following: <ul style="list-style-type: none"> Block All Forward All then click Update . The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select Block as the action for all of them, you must choose Forward All as the filter's default action.
Filters Classes	Lists MAC addresses. To remove the MAC address from the Filters Classes list, select it, then click Delete .
Delete Filters	
Filters	To delete a filter, select it from the list, then click Delete .
Filter Index	Enter the filter index number.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To delete a VLAN ID from the list, click <<.
Bridge-Group	Enter a valid bridge group number.
Remove Filter from	
Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> Incoming—Use this option to remove the filter from the incoming packets. Outgoing—Use this option to remove the filter from the outgoing packets. Click AddFilter .
Radio0-802.11B/G/N	
Radio0-802.11A/N	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring IP Filters

Use this option to create IP filters that prevent or allow the use of IP address(es), IP protocols, and TCP/UDP ports through the access point's Ethernet and radio ports.



Note

The WLSE applies IP filters before contacting a device. This means that the WLSE will not discover devices excluded from IP filters.



Note Discovery and switch port tracing will use IP filters to restrict access to excluded device.



Note To exclude a device with multiple IP addresses, you should list all of its IP addresses in the filter as excluded.

Procedure

Step 1 Select **Services > IP filters**. The Services: Filters - IP Filters dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-31 IP Filters

Field	Description
Create and Apply	Select this option to create and apply IP address filters.
Create Only	Select this option to create IP address filters, but not apply them.
Apply Only	Select this option to apply the IP address filters.
Filter Name List	List the currently configured filters. To delete a filter from the list, select it, then click Delete Filter .
Filter Name	Enter a name for the filter.
Default Action	From the list, select one of the following: <ul style="list-style-type: none"> Block All—Use this setting to block all IP addresses. Forward All—Use this setting to forward all IP addresses. then click Update .
IP Address	
Destination Address	Enter the IP address that you want to filter.
Mask	Enter the mask for the destination IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example). If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.

Table 5-31 IP Filters (continued)

Field	Description
Source Address	Enter the IP address you want to filter.
Mask	Enter the mask for the source IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example). The method for entering the mask depends on the release. Entering 255.255.255.255 as the mask causes the access point to accept any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.
Action	From the list, select one of the following: <ul style="list-style-type: none"> • Forward —Use this setting to forward the IP address. • Block —Use this setting to block the IP address. Click Add .
IP Protocol	
IP Protocol	Do one of the following: <ul style="list-style-type: none"> • Click the existing protocol list, then select a protocol. • Click Custom, then enter a custom protocol.
Action	From the list, select one of the following: <ul style="list-style-type: none"> • Forward —Use this setting to forward the IP protocol. • Block —Use this setting to block the IP protocol. Click Add .
UDP/TCP Port	
TCP Port	Do one of the following: <ul style="list-style-type: none"> • Click the TCP Port list, then select one port from the list. • Click Custom, then enter a custom port.
Action	From the list, select one of the following: <ul style="list-style-type: none"> • Forward —Use this setting to forward the TCP port. • Block —Use this setting to block the IP TCP port. Click Add .
UDP Port	Do one of the following: <ul style="list-style-type: none"> • Click the UDP Port list, then select one port from the list. • Click Custom, then enter a custom port.
Action	From the list, select one of the following: <ul style="list-style-type: none"> • Forward —Use this setting to forward the UDP port. • Block —Use this setting to block the IP UDP port. Click Add .
VLAN ID	Enter the VLAN identification number then click >>. To remove a VLAN ID from the list, select it, then click <<.

Table 5-31 IP Filters (continued)

Field	Description
Apply Filter to	
Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> • Incoming—Use this option to apply the filter to the incoming packets. • Outgoing—Use this option to apply the filter to the outgoing packets. Click Apply .
Radio0-802.11B/G/N	
Radio0-802.11A/N	
Filters Classes	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete .
Delete Filters	
Filters	To delete a filter from the list, select it from the list, then click Delete .
Filter Name	Enter the filter name.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To remove a VLAN ID from the list, click <<.
VLAN List	Lists the VLANS.
Remove Filter from	
Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> • Incoming—Use this option to remove the filter from the incoming packets. • Outgoing—Use this option to remove the filter from the outgoing packets. Click AddFilter .
Radio0-802.11B/G/N	
Radio0-802.11A/N	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).



Note

After you save a filter, the WLSE will perform a check for the filters on the devices currently in the system and then list all devices that conflict with the filter rules. You can use the **Delete** button to delete these devices. If you decide to continue without deleting these devices, other WLSE modules will still poll the devices besides discovery and switch port tracing.

Configuring Ethertype Filters

Use this option to configure Ethertype filters to prevent or allow the use of specific L3 protocols through the access point's Ethernet and radio ports.

Procedure

Step 1 Select **Services > Ethertype Filters**. The Services: Filters - Ethertype Filters dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-32 Ethertype Filters

Field	Description
Create and Apply	Select this option to create and apply Ethertype filters.
Create Only	Select this option to create Ethertype filters, but not apply them.
Apply Only	Select this option to apply the Ethertype filters.
Filters List	Lists the currently configured filters. To remove a filter from the list, select it, then click Delete Filter .
Filter Index	Enter a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.
Add EtherType	Enter an Ethertype number.
Mask	Enter the mask for the Ethertype.
Action	From the list, select one of the following: <ul style="list-style-type: none"> • Forward —Use this setting to forward the traffic. • Block —Use this setting to block the traffic.
VLAN ID	Enter the VLAN identification number then click >>. To remove a VLAN ID from the list, select it, then click <<.
Bridge-Group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.
Apply Filter to	
Fast/Gigabit Ethernet	Select one of the following:
Radio0-802.11B/G/N	• Incoming—Use this option to apply the filter to the incoming packets.
Radio0-802.11A/N	• Outgoing—Use this option to apply the filter to the outgoing packets. Click Apply .
Default Action	From the list, select one of the following: <ul style="list-style-type: none"> • Block All—Use this setting to block all. • Forward All—Use this setting to forward all. then click Update .
Filters Classes	Lists the currently configured filters. To delete a filter from the list, select it, then click Delete .
Delete Filters	

Table 5-32 *Ethertype Filters (continued)*

Field	Description
Filters	To delete a filter from the list, select it from the list, then click Delete .
Filter Index	Enter the filter index.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list. To delete a VLAN ID from the list, click <<
Bridge-Group	Enter a valid bridge group number.
Remove Filter	
Fast/Gigabit Ethernet	Select one of the following:
Radio0-802.11B/G/N	<ul style="list-style-type: none"> • Incoming—Use this option to remove the filter from the incoming packets. • Outgoing—Use this option to remove the filter from the outgoing packets.
Radio0-802.11A/N	
Click AddFilter .	

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring HTTP

Use this option to configure HTTP settings for the access point.

Procedure

- Step 1** Select **Services > HTTP**. The Services: HTTP-Web Server dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-33 HTTP

Field	Description
Web-based Configuration Management	Select one of the following: <ul style="list-style-type: none"> • Enable Standard (HTTP) Browsing—Use this setting to allow web-based browsing to the management system. • Enable Secure (HTTPS) Browsing—Use this setting to allow secure web-based browsing to the management system. • Disable Web-based Management—Use this setting to disallow web-based browsing to the management system.
HTTP Port	Enter the port through which the access point provides web access.
HTTPS Port	Enter the port through which the access point provides secure web access.
Default Help Root URL	Enter the URL where the device can locate help files.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Policies

Use this option to configure quality of service policies.

If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.

Procedure

Step 1 Select **Services > QoS Policies**. The Services: QoS Policies dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** in the upper right side of the screen removes all the entries you have made so far and returns you to the Template Name page.

Clicking **Clear** in the lower right side of the screen only removes entries you have made on this page.

Clicking **Reset** clears the entries you have made on the page and restores the defaults, if any were set.

Table 5-34 QoS Policies

Field	Description
Create and Apply	Select this option to create and apply QoS policies.
Create Only	Select this option to create QoS policies., but not apply them.
Apply Only	Select this option to apply the QoS policies.
QoS Element for Wireless Phones	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to specify that wireless phone clients' traffic has a higher priority than the rest of the clients. • Disable—Use this setting to disable this feature. • Dot11e—Select to enable for.11e. <p>Click See detail to see for which device types or versions this setting is valid.</p>
IGMP Snooping Helper	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable Internet Group Membership Protocol (IGMP) snooping. When this feature is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams. • Disable—Use this setting to disable this feature. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Map Ethernet Packets with CoS 5 to CoS 6 (AVVID Priority Mapping)	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting if your network is based on the Cisco AVVID specification. This setting will prioritize voice packets coming with priority 5 (video). • No—Use this setting if your network is not based on the Cisco AVVID specification. <p>Click See detail to see for which device types or versions this setting is valid.</p>
WiFi Multimedia	<p>Click See detail to see for which device types or versions this setting is valid.</p> <p>For each radio interface select one the following:</p> <ul style="list-style-type: none"> • Enable—Select this option to enable WME support. • Disable—Select this option to disable the feature.
Policy List	<p>Lists the names of the existing policies.</p> <p>To remove a name from the list, select it, then click Delete Policy.</p>
Policy Name	Enter a name for the policy.
Classifications	<p>Lists the classifications assigned to that policy.</p> <p>To delete a classification from the list, select it, then click Delete.</p>

Table 5-34 QoS Policies (continued)

Field	Description
Match Classifications	
Precedence	If the packets that you need to prioritize contain IP precedence information select an IP precedence classification from the list.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets of the type that you selected from the Precedence list, then click Add .
IP DSCP	If the packets that you need to prioritize contain IP DSCP information, select an IP DSCP classification from the list or create a new one.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets of the type that you selected from the IP DSCP list, then click Add .
IP Protocol 119	If you need to prioritize the packets from Spectralink on your wireless LAN, select the class of service the access point will apply to the phone packets, then click Add . Click See detail to see for which device types or versions this setting is valid.
Apply Class of Service	
Filter	If you need to assign a priority to filtered packets, from the list, select the filter to include in the policy or create a new one.
Apply Class of Service	From the list, select the class of service that the access point will apply to packets that match the filter that you selected or entered, then click Add .
Default Classification for Packets on the VLAN	If you want to set a default classification for all packets on a VLAN, select the class of service that the access point will apply to packets on a VLAN, then click Add .
Class based traffic policing (click See detail to see for which device versions are supported)	
Match any	<ol style="list-style-type: none"> For the Match any field, select one the following: <ul style="list-style-type: none"> Enable—XYZ. Disable—XYZ. Enter the average rate for class-based traffic policing and select an action from the Conform action drop-down menu. Enter the normal burst rate for class-based traffic policing and select an action from the Exceed action drop-down menu. Enter the maximum burst rate for class-based traffic policing and select an action from the Conform action drop-down menu. Click Add to add the policy to the Classifications list.
Average Rate	
Normal Burst Rate	
Maximum Burst Rate	
VLAN ID	
VLAN ID List	To delete a VLAN ID from the list, click <<.

Table 5-34 QoS Policies (continued)

Field	Description
Apply Policy to	
Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> Incoming—Use this option to apply the filter to the incoming packets. Outgoing—Use this option to apply the filter to the outgoing packets. Click ApplyPolicy .
Radio0-802.11B/G/N	
Radio0-802.11A/N	
Remove Policy from Interface/VLANs	
Policy List	To delete a policy from the list, select it from the list, then click Delete .
Policy Name	Enter the name of the policy.
VLAN ID	Enter the VLAN identification number, then click >> to add it to the list.
VLAN ID List	To delete a VLAN ID from the list, click <<.
Remove Policy from	
Fast/Gigabit Ethernet	Select one of the following: <ul style="list-style-type: none"> Incoming—Use this option to remove the filter from the incoming packets. Outgoing—Use this option to remove the filter from the outgoing packets. Click AddPolicy .
Radio0-802.11B/G/N	
Radio0-802.11A/N	
Remove Policy Map and Class Map	
Policy List	Lists the policies. Select the policy to remove from the list, then click Delete .
Policy Name	Enter the policy name, then click Add Policy . The name appears in the Policy List.
Class Name	Enter the class name. Click >> to add it to the Class Name List
Class Name List	Click << to remove the class name from the list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Radio 802.11b/g

Use this option to define traffic class QoS policies. The access point uses the radio traffic class definitions to calculate backoff times for each packet.

Procedure

Step 1 Select **Services > QoS Radio 802.11b/g/n**. The Services: QoS Policies 11b/g/n - Traffic Class Definition dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-35 QoS Radio 802.11b/g/n Traffic Class Definition

Field	Description
802.11e 4 Level QoS	Select QoS for version 12.3(2)JA and above.
802.11e 4 Level QoS with WMM	Select QoS with Wi-Fi multimedia for version 12.3(2)JA and above.
Background	Enter values for AP and Client for the following access categories: <ul style="list-style-type: none"> • Min Contention Window—Enter the minimum contention window value. The access point computes Contention Window values. • Max Contention Window—Enter the maximum contention window value. The access point computes Contention Window values. • Fixed Slot Time—Enter a value for a fixed slot time. • Admission Control—Not applicable for this release. Used for 802.11e 4 Level QoS with WMM to specify that admission control is mandatory for this class. • Transmit Opportunity—Not applicable for this release. Used for 802.11e 4 Level QoS with WMM to specify the value in microseconds during which transmitters that are qualified to transmit through the normal back-off procedure are allowed to send a set of pending packets during the configured transmit opportunity.
Best Effort	
Video	
Voice	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring QoS Radio 802.11a/n

Use this option to define traffic class QoS policies. The access point uses the radio traffic class definitions to calculate backoff times for each packet.

Procedure

Step 1 Select **Services > QoS Radio 802.11a/n**. The Services: QoS Policies 11a/n- Access Category Definition dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-36 QoS Radio 802.11a/n Traffic Class Definition

Field	Description
Background	Enter a Local and a Cell value for each access category, or set the values automatically by clicking Optimized Voice for optimized voice values or WFA Default for Wireless Fidelity Alliance (WFA) default values. Note Only Local values for Max Contention Window, Min Contention Window, Fixed Slot Time, and Transmit Opportunity will be applied to devices with versions earlier than 12.3(8)JA. To clear the table of values, click Clear .
Best Effort	
Video	
Voice	
Admission Control	Select this option to specify that admission control is mandatory for this class. Note Admission control should not be enabled if your deployment includes softphone applications. If you are not deploying softphone applications on laptops, then use the default.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SNMP

Use this option to configure settings for notifications to be sent to an SNMP server.

This option also enables you to send SNMP traps to this WLSE. Enabling this option allows faster fault processing of policies because the access point is reporting directly to the WLSE instead of the WLSE periodically polling the access point. For additional information, see [Setting RF Port Status Threshold, page 3-34](#) and [Setting RF Port AdminStatus Threshold, page 3-35](#).

Procedure

Step 1 Select **Services > SNMP**. The Services: SNMP- Simple Network Management Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-37 **SNMP**

Field	Description
Simple Network Management Protocol (SNMP)	Select one of the following: <ul style="list-style-type: none"> • Enabled—Use this setting to allow event notifications to be sent to an SNMP server. • Disabled—Use this setting to disallow event notifications to be sent to an SNMP server.
System Name	Enter the name of the access point. The name in this field is reported to your SNMP's management station as the name of the device when you use SNMP to communicate with the access point.
System Location	Enter a description of the access point's physical location, such as the building or room in which it is installed.
System Contact	Enter the name the system administrator responsible for the access point.

Table 5-37 SNMP (continued)

Field	Description
SNMP Request Credentials	
Current Community Strings	<p>Lists the current community strings.</p> <p>To delete an entry from the list, select it, then click Delete.</p> <p>To edit an entry, select it.</p>
Edit Community Strings	<ul style="list-style-type: none"> SNMP Community—The SNMP Community value for the selected community string displays. SNMP community strings authenticate access to MIB objects and function as embedded passwords. Object Identifier —The Object Identifier value for the selected community string displays. Enter a new object identifier for the community string. The object identifier limits the scope of the SNMP MIB object that the user can access through the community string. <p>For for example, if you enter <code>iso</code> as the Object Identifier value for the public string, then only users using the public string can access the OID that is represented by the SNMP variable name <code>iso</code>, including all the variables that come under this variable starting at this point. (This is the MIB family view to which the community has access.)</p> <ul style="list-style-type: none"> Select Read-Only or Read-Write.
SNMP Traps	
Send all traps to this WLSE	<p>Select one of the following:</p> <ul style="list-style-type: none"> Enable—Use this setting to enable the access point to send traps to this WLSE. (The WLSE's address is added as an SNMP trap destination.) Enabling this setting allows faster processing of faults. <p>(See Ports Hosted by the WLSE, page C-2 for correct port setting.)</p> <ul style="list-style-type: none"> Disable—Use this setting to disallow traps being sent to this WLSE. <p>Using the setting does not disable traps; it removes this WLSE's address as an SNMP trap destination.</p>
SNMP Trap Destination	<ol style="list-style-type: none"> Enter the IP address or the host name of the server running the SNMP Management software. Select one of the following: <ul style="list-style-type: none"> Enable All Trap Notifications—Use this setting to enable all traps. Enable Specific Traps—Use this setting to select one or more of the displayed trap types. <p>Click See detail to see for which device types or versions the particular settings are valid.</p> Click Save. <p>Click See Detail for more information.</p>
Delete Communities and SNMP Trap Destinations	
Community	Enter the community to delete, then click >>.
Communities to Delete	<p>Lists the communities to be deleted.</p> <p>To delete a community, select it, then click <<.</p>

Table 5-37 *SNMP (continued)*

Field	Description
SNMP Trap	Enter the IP address or the host name of the server to delete.
Communities	Enter the community associated with the SNMP trap, then click >>.
Destinations to Delete	Lists the SNMP trap destinations to be deleted. To delete a destination, select it, then click <<.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).



Note The WLSE's address appears as "%thiswlse%" in the displayed IOS commands. This is because the address is not known until the template is applied to an access point.

- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring SNTP

This option allows you to configure the date and time on using SNTP (Simple Network Time Protocol).

Procedure

Step 1 Select **Services > SNTP**. The Services: NTP - Network Time Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-38 *SNTP*

Field	Description
SNTP Server	Click See detail for information about NTP support.
Simple Network Time Protocol (SNTP)	Select one of the following: <ul style="list-style-type: none"> • Enabled—Use this setting to use of NTP. • Disabled—Use this setting to disallow the use NTP.
Time Server	Enter the server's IP address.
Time Settings	
GMT Offset	From the list, select one of the options.

Table 5-38 *SNTP (continued)*

Field	Description
Use Daylight Savings Time	Select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to use daylight savings time. • No—Use this setting if you are not going to use daylight savings time.
Manually Set Date	Use this setting to manually set the date.
Manually Set Time	Use this setting to manually set the time.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring VLAN

Using this option, you can configure VLANs on the access point.

Procedure

Step 1 Select **Services > VLAN**. The Services: VLAN dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-39 *VLAN*

Field	Description
Global VLAN Properties	
Set Native VLAN	From the list, select a VLAN for the default.
Assigned VLANs	
Current VLAN List	Lists the current VLANs. To delete a VLAN from the list, select it, then click Delete .
Create VLAN	
VLAN ID	Enter a VLAN ID.
VLAN Name	Enter a name for the VLAN.

Table 5-39 VLAN (continued)


Field	Description
Bridge-Group	<p>Enter the bridge group number.</p> <ul style="list-style-type: none"> If the VLAN ID you entered is less than 255, and you do not enter a value in this field, then the same number for the bridge group is automatically assigned. If the VLAN ID you entered is 255 or greater you will need to know what bridge group numbers are unused on the access point and enter one of them. <p>When a VLAN is created directly on the access point, the access point dynamically assigns a bridge group to the VLAN. So, if you create a VLAN ID of 123, then the bridge group is 123.</p> <p>If the VLAN is larger than 255, the access point starts at 255 and decrements the count until it gets to an unused bridge group number. So, if you create a VLAN ID of 500, the access point assigns a bridge group of 255 if that number is unused. If it is used, it will then try 254, and so on until it finds an unused number for the bridge group.</p>
Enable Public Secure Packet Forwarding	<p>Select to enable public secure packet forwarding (PSPF).</p> <p>With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.</p> <p>Click See detail to see for which device types or versions this setting is valid.</p>
Associate SSIDs with VLAN Name	<p>Select to enable association of the VLAN name with the SSID.</p>
Enable Nonroot-bridge Client-VLAN	<p>Check this check box to enable multiple VLAN support for bridges. This option is applicable for any device configured as “Non-root bridge.”</p> <p>Click See detail for more information.</p>
Radio0-802.11B/G/N SSID	<p>Select the appropriate radio, if desired, and enter its SSID. This setting is not enforced.</p>
Radio0-802.11A/N SSID	<p>For Radio0-802.11A/N, click See detail to see for which device types or versions this setting is valid.</p>
Backup VLANs	<p>To specify up to three backup VLANs, check the Backup VLANs check box and enter the IDs or names of the VLANs in the fields below.</p> <p> Note The Backup VLANs option is supported only for device versions 12.3(11)JA*, 12.3(8)JEA*, and later releases.</p>
STP	<p>Select one of the following:</p> <ul style="list-style-type: none"> Enable—Use this setting to enable Spanning Tree Protocol (bridges only). Disable—Use this setting to disable the feature. <p>then click Add.</p>

Table 5-39 VLAN (continued)

Field	Description
Workgroup Bridge Ethernet Client VLAN	
Add	Click to configure a client VLAN when the workgroup bridge's clients are on a non-native VLAN, then enter the VLAN ID.
Delete	Click to delete the client, then enter the VLAN ID.
Delete VLANs	
VLANs to Delete	Lists the VLANs to delete. To delete VLAN from the list, select it, then click Delete .
VLAN ID	Enter the identification number of the VLAN you want to add to the VLANs to Delete list.
VLAN Name	Enter the VLAN name.
Associate SSIDs with VLAN Name	Select to associate the SSIDs with the VLAN name.
Disable Nonroot-bridge Client-VLAN	Check this check box to disable multiple VLAN support for bridges. This option is applicable for any device configured as "Non-root bridge." Click See detail for more information.
Radio0-802.11B/G/N Radio1-802.11A/N	Select the appropriate radio.
SSID	Enter the SSID, then click Add . The VLAN appears in the VLANs to Delete list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring ARP Cache

Address resolution protocol (ARP) is used to find the MAC address that corresponds to a particular IP address. Using this option, the access point remembers the IP addresses of its clients and will not send ARP requests to them.

This feature helps improve performance because it reduces traffic load over the wireless link. If all client IP address are not known, the access point drops the ARP request, and caching is prevented.

Procedure

Step 1 Select **Services > ARP Cache**. The Services: Client ARP Caching dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-40 **ARP Cache**

Field	Description
Client ARP Caching	Select one of the following: <ul style="list-style-type: none"> • Enabled—Use this setting to allow ARP caching. • Disabled—Use this setting to disable the feature. Click See detail to see for which device types or versions this setting is valid.
Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known	Select when all client IP address are not known, so that the access point forwards the ARP request to all its clients, and caching is prevented

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring STP

This option enables to you to configure spanning tree protocol.

Procedure

Step 1 Select **Services > STP**. The Spanning Tree Protocol dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-41 STP

Field	Description
STP Properties	
Click See detail to see for which device types or versions this setting is valid.	
Per VLAN Spanning Tree List	Lists the current STPs. To remove an STP from the list, select it, then click Delete .
VLAN ID	Enter the VLAN identification number.
Bridge Group	Enter the name of the bridge group.
Root Configuration	
Priority	Enter the spanning tree priority (STP) for the bridge. STP uses the bridge priority to select the spanning tree root. The lower the priority, the more likely it is that the bridge will become the spanning tree root.
Max Age	Enter the interval that the bridge waits to hear BPDUs from the spanning tree root. If the bridge does not hear bridge protocol data units (BPDUs) from the spanning tree root within this specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.
Hello Time	Enter the interval between hello bridge protocol data units (BPDUs).
Forward Delay	Enter the forward delay interval on the bridge.
Port Configuration	These settings apply to individual ports on the bridge. Use these settings to adjust the status of individual ports i.e. Ethernet or Radio port on the bridge.
Ethernet	Complete the following:
Root Radio 802.11B/G/N	<ul style="list-style-type: none"> • Path Cost—Use this setting to specify the relative efficiency of the port's network link. A port with a high path cost is less likely to become a bridge's root port. • Priority—Use this setting to influence whether STP designates a port as a root port. A port with a low priority setting is more likely to become a root port.
Root Radio 802.11A/N	
Spanning Tree without VLAN	
STP for Radio 802.11B/G/N	Select one of the following: Enable or Disable.
STP for Radio 802.11A/N	Select one of the following: Enable or Disable.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Packet Handling 802.11a/n

Use this option to define packet retry policies.

Procedure

- Step 1** Select **Services > Packet Handling 802.11a/n**. The Stream-Packet Handling Radio 802.11a/n dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-42 Packet Handling 802.11a/n

Field	Description
General Packet Handling	Click See detail to see the versions for which this setting is valid.
Packet Handling per User Priority:	
User Priority	Lists the Class of Service (COS) for which you can set packet handling and maximum number of retries before the packet is discarded.
Packet Handling	Select one of the following: <ul style="list-style-type: none"> • None—Use this setting to disable packet handling. • Reliable—Use this setting to disable the max-retry option of packets. • Low Latency—Use this setting to enable the max-retry option of packets.
Max Retries for Packet Discard	This option specifies the packet retries before dropping a packet if the first fail-threshold not reached. It is disabled if Packet Handling is set to None. For Reliable and Low Latency packet handling settings, accept the default or specify a different number of maximum retries.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Wireless Services

This option provides context control to the nodes by maintaining a cache of all client contexts within a given subnet.

Procedure

-
- Step 1** Select **Wireless Services**. The menu expands and the Wireless Services: AP dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- AP Configuration—See [Configuring the AP, page 5-97](#).
 - WDS—See [Configuring WDS, page 5-98](#).
-

Configuring the AP

Use this option to configure the access point to interact with wireless services.

Procedure

-
- Step 1** Select **Wireless Services > AP Configuration**. The Wireless Services: AP dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-43 AP Configuration

Field	Description
Use Wizard Configuration	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to employ the configuration defined with the Deployment Wizard. The fields on this page are grayed out when this setting is selected. • Disable—Use this setting to disable the Deployment Wizard configuration, and to use this page to configure the AP.
Participate in SWAN Infrastructure	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting indicate that the access point is participating in the Cisco Structured Wireless Aware Network (SWAN). • Disable—Use this setting to indicate that the access point is not participating in SWAN. Click See detail to see for which device types or versions this setting is valid.
WDS Discovery	Select one of the following: <ul style="list-style-type: none"> • Auto Discovery—Use this setting to search for any WDS access point. • Specified Discovery—Use this setting to search for a particular WDS access point, then enter the IP address for that access point.

Table 5-43 AP Configuration (continued)

Field	Description
Username	Enter a username.
Password	Enter a password.
Confirm Password	Reenter the password.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring WDS

Use this option to configure wireless domain services and to set its priority.

Procedure

Step 1 Select **Wireless Services > WDS**. The Wireless Services: WDS - Wireless Domain Services - Settings dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-44 WDS Settings

Field	Description
Use Wizard Configuration	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to employ the configuration defined with the Deployment Wizard. The fields on this page are grayed out when this setting is selected. • Disable—Use this setting to disable the Deployment Wizard configuration, and to use this page to configure WDS.

Table 5-44 WDS Settings (continued)

Field	Description
Global Properties	
Click See detail to see for which device types or versions this setting is valid.	
Use this AP as Wireless Domain Services	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the access point to provide Wireless Domain Services. • Disable—Use this setting to disable the access point from providing Wireless Domain Services. • Modify—Use this setting to modify the Wireless Domain Services on the access point.
Use this AP Only for Wireless Domain Services	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the access point to provide only Wireless Domain Services. • Disable—Use this setting to disable the access point from providing only Wireless Domain Services. <p>Click See Detail for more information.</p> <p>If you enable this option, you should add the following commands to the Custom Values page (see Configuring Custom Values, page 5-104) to make the access point work in WDS-only mode:</p> <pre>write erase reload</pre>
Wireless Domain Services Priority	<p>Enter a number between 1 and 255 to indicate the priority.</p> <p>The priority is structured so that a WDS will not replace an active WDS with the same priority value, even it has a higher node ID.</p>
Wireless Network Manager Address	Enter the access point's IP address or hostname.
Use Local MAC List for Client Authentication	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to use the local MAC address list for authentication. • Disable—Use this setting to disable the local MAC address list for authentication.
Server Groups	
Server Group List	<p>Lists the configured servers.</p> <p>To delete a server from the list, select it, then click Delete.</p>
Server Group Name	<p>Enter the name of the server group then complete the following:</p> <ul style="list-style-type: none"> • Priority—Enter the server IP address or hostname. • Auth Port—Enter the authentication port. • Acct Port—Enter the accounting port. <p>or</p> <ul style="list-style-type: none"> • Select a name from the list.

Table 5-44 WDS Settings (continued)

Field	Description
Use Group for	Select one of the following: <ul style="list-style-type: none"> Infrastructure Authentication—Use this setting to initiate infrastructure authentication by sending a path initialization request message to its WDS, which acts as the IN authenticator. Client Authentication—Use this setting to provide client authentication services, then under Authentication Settings, select one of the types of client authentication.
SSID	Enter the SSID or leave blank to apply to all SSIDs, then click >> to add to the SSID List. Click Save .
SSID List	Lists the current SSIDs. To remove an SSID from the list, select it, then click <<.
Delete Server Group	
Server Group Name	Enter the server group to delete.
Server Group List to Delete	Lists the server groups to delete. To remove a group from the list, select it, then click <<.
Use Group For	Select one of the following: <ul style="list-style-type: none"> Infrastructure Authentication—Use this setting to initiate infrastructure authentication by sending a path initialization request message to its WDS, which acts as the IN authenticator. Client Authentication—Use this setting to provide client authentication services. Select the type of client authentication. Then, click >> to add to the Server Group List to Delete.

Step 3 Click **Save**. The server is added to the Authentication Server List.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring the Event Log

This option enables you to customize the display of access point events.

Procedure

-
- Step 1** Select **Event Log**. The menu expands and the Event Log: Configuration Options dialog box displays in the right pane.
- Step 2** Select one of the following from the menu:
- Configuration Options—See [Setting Configuration Options, page 5-101](#).
 - Notification Options—See [Setting Notification Options, page 5-102](#).
-

Setting Configuration Options**Procedure**

-
- Step 1** Select **Event Log > Configuration Options**. The Event Log: Configuration Options dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-45 Configuration Options

Field	Description
Disposition of Events (by Severity Level)	
Emergency	Check one or more of the following for each of the events:
Alert	
Critical	
Error	
Warning	
Notification	
Information	
Debugging	
Time Stamp Format for Future Events	Select one of the following: <ul style="list-style-type: none"> • System Uptime—Use this setting to use the system uptime in the timestamp. • Global Standard Time—Use this setting to use the global standard time in the timestamp. • Local Time—Use this setting to use the local time in the timestamp.
Event Log Size	Enter the maximum size of the event log.
History Table Size	Enter the maximum number of messages in the history table.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Setting Notification Options

Procedure

- Step 1** Select **Event Log > Notification Options**. The Event Log: Notification Options dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-46 Notification Options

Field	Description
Events Generate Syslog Messages	Select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow events to generate syslog messages. • Disable—Use this setting to disable the feature.
Syslog Server Hostname or IP Address	Enter the hostname or IP address of the syslog server.
Syslog Facility	From the list, select the syslog facility.
Delete Syslog Server	
Server Hostname or IP Address to remove	Enter the Syslog server hostname or IP address to be deleted.

- Step 3** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).

System Config

This option allows you to do two different things: reload a device and negotiate power settings.

Reload Settings

Before you reload, you can choose either to save the configuration to NVRAM or not to save the configuration to NVRAM.

**Note**

If custom commands have been configured, they will be applied before a Reload command; the Reload command is always applied last.

Power Option Settings

These settings allow the access point to negotiate its power settings when it powers on. It negotiates the power settings as follows:

- If the access point is powered from an AC adaptor, no configuration is necessary.
- If the access point is connected to an inline switch that supports power negotiation, the access point will negotiate its power settings with the switch.
- If the access point is powered from a 15W inline switch that does not support power negotiation, “Pre-standard Compatibility Mode” is required.
- If the access point is powered from a 6W inline switch, a power injector is required. The “Power Injector” is required with a MAC address that matches the one on the Ethernet port where the injector is connected.
- If the access point is powered from a non-Cisco 802.3(af) switch, no additional configuration is required.
- If the access point is unable to verify a 15W inline power source, then the access point will stay in a low power state.

Procedure

Step 1 Select **System Config**. The System Config dialog box appears.

Step 2 Complete the following:

**Note**

Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Table 5-47 System Config

Field	Description
System Config	
Reload Device	Select one of the following: <ul style="list-style-type: none"> • Without Writing NVRAM—Select this option to write the configuration to NVRAM. • With Writing NVRAM—Select this option if you do not want the configuration written to NVRAM. Click See detail for caution.

Table 5-47 System Config (continued)

Field	Description
Power Settings	
Power Settings	<p>Select one of the following:</p> <ul style="list-style-type: none"> Power Negotiation—Use this setting to allow a device to negotiate inline power with the switch. Pre-standard Compatibility—Use this setting if the access point is powered from a 15W inline switch that does not support power negotiation. <p>Click See detail to see for which device types or versions this setting is valid.</p>
Power Injector	<p>Select one of the following:</p> <ul style="list-style-type: none"> Enable installed on Port with MAC Address—Use this setting if the access point is powered from a 6W inline switch and requires a power injector. that matches the one on the Ethernet port where the injector is connected. Disable—Use this setting to disable the use of the power injector.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
- **Save** to save the template. See [Saving the Template, page 5-106](#).
- Another template category to configure more options. See [2.Template Categories, page 5-6](#).

Configuring Device Specific Settings

This option enables you to create a template with specific settings. Unlike other template options, these commands are not validated when the template is saved.

For information on importing, exporting, and viewing device settings, see [Managing Device Specific Configurations, page 8-46](#).

Procedure

Step 1 Select **Device Specific**. The Device Specific Settings dialog box appears.

Step 2 Select **Enable Device Specific Settings for this Template** to use the settings specified in the CSV file.

Configuring Custom Values



Note

This option should be used only by advanced users.

This option enables you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu.

Important Notes

- Any custom values you configure are applied to the device only after all the other template configurations have been applied.
- Custom values are not validated. However, if a configuration contains a combination of custom values and values entered using the templates, the values entered using the templates are validated; only the values entered with the custom configuration are not.
- If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.
- If you use the `username` command with the password encryption option (i.e 7), for example:

```
username Cisco1 privilege 15 password 7 062506324F4158
```

then after applying the command through the config job, the credentials will not be updated in the WLSE. The WLSE cannot decrypt the IOS-encrypted password.

Procedure

Step 1 Select **Configure > Templates > Custom Values**. The Custom IOS Values dialog box appears.



Note Clicking **Clear** removes all the entries you have made so far and returns you to the Template Name page. Clicking **Reset** clears only the entries you have made on that page and restores the defaults, if any were set.

Step 2 Enter the IOS commands.



Note Do not use either the `exit` or `end` commands

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 5-106](#).
 - **Save** to save the template. See [Saving the Template, page 5-106](#).
 - Another template category to configure more options. See [2.Template Categories, page 5-6](#).
-

Previewing the Template

Procedure

-
- Step 1** Click **Preview**. A Command Preview window displays the configuration choices you have made to the template.
- (See [In What Order are the Template Configurations Applied to the Devices?](#), page 8-8 for information about the order in which the template choices are applied.)
- Step 2** Click **Save**. See [Saving the Template](#), page 5-106.
-



Note

The Preview page displays the command for the 802.11B/G/N(2.4GHz) radio interface as `interface Dot11Radio 0` and the command for the 802.11B/G/N(2.4GHz) radio interface as `interface Dot11Radio 1`.

Saving the Template

When you save a template, the WLSE first validates the template and displays the valid Device Type, Interface, and the corresponding Device Version(s) for that template.

An access point with an 802.11G radio, supports different commands from a similar access point with an 802.11B radio. The same is true for a 1310 wireless bridge in bridge mode versus a 1310 wireless bridge in access point mode or in a workgroup bridge mode.

If the Interface column displays G/A, it means that the template is applicable to an access point with A and G radio. If the Interface column displays B/A, it means that the template is applicable to an access point with a and b radio.

Similarly, if the Device Type column displays BR1310, it means that the configuration template is applicable to a 1310 wireless bridge which is in bridge mode. If the Device Type column displays an AP1310, it means the template is applicable to a 1310 wireless bridge in access point mode.

Procedure

-
- Step 1** Click **Save** in the left pane to complete creating a template. The Save dialog box appears in the right pane.
- Step 2** Click **Save** to create the template.
- Step 3** Do one of the following:
- Click **Yes** if you want to save the template then schedule a configuration job.
The window refreshes to the Job Creation window and a job is automatically created for you using the template name and a random number. See [Selecting Devices](#), page 8-14.
 - Click **No** if you want to save the template only.
 - Click **Cancel** to cancel the operation and then display the previous screen.
-