



Using Non-IOS Templates



Note

Non-IOS templates are used only with the WLSE, not the WLSE Express.

The WLSE allows you to create, modify, and delete non-IOS configuration templates.

The topics covered in this section are:

- [What is a Configuration Template?, page 6-2](#)
- [Viewing the Existing Templates, page 6-2](#)
- [Creating a Template, page 6-3](#)
- [Copying a Template, page 6-3](#)
- [Editing a Template, page 6-4](#)
- [Converting a Template, page 6-5](#)
- [Importing a Template, page 6-6](#)
- [Deleting a Template, page 6-6](#)
- [Exporting a Template, page 6-8](#)
- [Template Choices, page 6-9](#)

Related Topics

- [Using IOS Templates, page 5-1](#)
- [Using WLSM Templates, page 7-1](#)
- [Managing Configuration Jobs, page 9-8](#)

What is a Configuration Template?

You can think of a configuration template as a configuration update file for an access point. This file might contain the update for only one parameter or a complete access point configuration.

Templates for non-IOS access points are stored internally as files in the `.ini` format that is understood by the access points. You can use the **Configure > Templates** option to:

- Create a configuration template (see [Creating a Template, page 6-3](#)).
- Import templates directly from devices and export them to files (see [Exporting a Template, page 6-8](#)).
- Convert non-IOS templates to IOS-based templates (see [Converting a Template, page 6-5](#)).

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.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
 - Step 2** Select **non-IOS** depending upon the type of template you want to create.
 - 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 6-9](#).
-

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 6-4](#).
-

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 6-9](#).
-

Converting a Template

Use this option to convert a non-IOS configuration template to an IOS template. You cannot convert an IOS template to a non-IOS 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 non-IOS template you want to convert from the Existing Templates table, then click **Convert**.

A dialog box appears with the following fields:

Field	Description
Name	Enter a name for the converted template.
Description	Enter a description for the template.
Converted Configuration	Displays the non-IOS configurations that have been converted to IOS.
Commands Not Converted	<p>Displays the non-IOS configurations that were not converted to IOS.</p> <p>These commands are not converted for one of two reasons:</p> <p>There is no equivalent command for IOS.</p> <p>The command conversion is not supported by the conversion tool.</p>

- Step 3** To save the template, click **Save**.
- The Templates window displays and the new name appears in the Existing Templates table.

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 a non-IOS access point, the configuration options are displayed in their corresponding template screens. However, if the imported configuration options do not have corresponding template screens, they 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 Non-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	<p>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.</p> <p>If you are importing from a device, you must enter a template name.</p>
Description	<p>Enter a description for the template.</p> <p>Do not click the Enter key at the end of the description; it will generate an error.</p>
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	<p>Select this option if you do not want to download identity parameters, such as IP address, from the access point.</p> <p>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.</p>

Field	Description
Full	<p>Select this option to import a full configuration from the access point.</p> <p>This type of import includes the access point's identity parameters, such as sysname, IP address, etc.</p> <p>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.</p>
Device Credentials	
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 a non-IOS configuration template, the following choices appear in the left pane of the Templates window:



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.

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

1. **Template Name**—See [Naming the Template](#), page 6-10.
2. **Template Categories**



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

- **Basic Settings**—See [Using Basic Settings](#), page 6-11.
- **Association**—See [Setting Up Association](#), page 6-16.
- **Ethernet**—See [Configuring the Ethernet Port](#), page 6-59.
- **11b Radio**—See [Configuring the 11b Radio](#), page 6-66.
- **11a Radio**—See [Configuring the 11a Radio](#), page 6-85.

- **Security**—See [Defining the Security Settings](#), page 6-117.
 - **Services**—See [Configuring Services](#), page 6-129.
 - **Events**—See [Configuring Events](#), page 6-154.
 - **Custom Values**—See [Configuring Custom Values](#), page 6-160.
3. **Preview**—See [Previewing the Template](#), page 6-161.
 4. **Save**—See [Saving the Template](#), page 6-162.

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 [Template Categories](#), page 6-9.

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 6-1 Basic Settings

Field	Description
Reboot Device	From the list, select Yes if you want to allow device reboots.
SysName	Enter a system name. The system name appears in the titles of the management system pages and in the access point's Association Table page. This is not an essential setting, but it helps identify the access point on your network.
SysLocation	Enter the system's location. This is not an essential setting, but it helps identify the access point on your network.
SysContact	Enter a contact name. This is not an essential setting but it helps identify the person responsible for the access point on your network.

Table 6-1 Basic Settings (continued)

Field	Description
Configuration Server Protocol	<p>Set this entry to match the network's method of IP address assignment.</p> <p>From the list, select one of the following options:</p> <ul style="list-style-type: none"> • None-Static IP—Use this if your network does not have an automatic system for IP address assignment. • BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses. • DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time.
Default Subnet Mask	<p>Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN.</p> <p>If DHCP or BOOTP is not enabled, this field is the subnet mask.</p> <p>If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.</p>
Default Gateway	<p>Enter the IP address of your default Internet gateway.</p> <p>The entry 255.255.255.255 indicates no gateway.</p>

Table 6-1 Basic Settings (continued)

Field	Description
Radio Service Set ID (SSID)	<p data-bbox="733 293 1170 350">Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p data-bbox="733 370 1231 553">The SSID is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity and provides access to VLANs by wireless client devices.</p> <p data-bbox="733 573 1157 630">Several access points on a network or subnetwork can share an SSID.</p>

Table 6-1 Basic Settings (continued)

Field	Description
Role in Network	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Access Point—Use this setting if the access point is connected to the wired LAN. • Repeater—Use this setting for access points not connected to the wired LAN. • Survey Client—Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate and the bridge's STP function is disabled. • Root Bridge—Use this setting to set a bridge as the root bridge. (One bridge in each group of bridges must be set as the root bridge.) The root bridge cannot associate with another root bridge. • Non-Root Bridge w/ Client—Use this setting for non-root bridges that accept associations from client devices and for bridges acting as repeaters. A non-root bridge will only associate to another bridge (root or non-root). • Non-Root Bridge w/o Client—Use this setting for non-root bridges that should not accept associations from client devices. A non-root bridge (without clients) can connect to a wired LAN and only associates to another bridge (root or non-root).

Table 6-1 Basic Settings (continued)

Field	Description
Ensure Compatibility with 1Mb/sec Clients	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to operate at a maximum speed of one megabit per second. • Disable—Use this setting if you do not want devices to operate at a maximum speed of one megabit per second.
Ensure Compatibility with 2Mb/sec Clients	From the list, select one of the following: <ul style="list-style-type: none"> • Enable— Use this setting to operate at a maximum speed of two megabits per second. • Disable—Use this setting if you do not want devices to operate at a maximum speed of two megabits per second.
Ensure Compatibility with non-Aironet 802.11	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to automatically configure the device to be compatible with other Cisco devices on your wireless LAN. • Disable—Use this setting to not automatically configure the device to be compatible with other Cisco devices on your wireless LAN.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Up Association

Use this option to set up spanning tree protocol (STP) on bridges and to set up filtering to control the flow of data through the access point.

Procedure

- Step 1** Select **Association**. The menu expands and the Association dialog box displays in the right pane.
- Step 2** Select one of the following from the Association menu:
- Spanning Tree—See [Defining Spanning Tree Protocol, page 6-17](#).
 - Address Filters—See [Defining Address Filters, page 6-19](#).
 - Ethertype Filters—See [Defining Ethertype Filters, page 6-22](#).
 - IP Protocol Filters—See [Defining IP Protocol Filters, page 6-26](#).
 - IP Port Filters—See [Defining IP Port Filters, page 6-30](#).
 - Policy Groups—See [Configuring Policy Groups, page 6-34](#).
 - VLANs—See [Configuring VLANs, page 6-36](#).
 - Quality of Service—See [Configuring Quality of Service, page 6-42](#).
 - Service Sets—See [Configuring Service Sets, page 6-43](#).
 - Primary Service Set—See [Configuring Primary Service Set, page 6-48](#).
 - Advanced—See [Defining Advanced Associations, page 6-51](#).
 - Port Assignments—See [Configuring Port Assignments, page 6-57](#).
 - DSCP to CoS—See [Configuring DSCP to CoS, page 6-58](#).
-

Defining Spanning Tree Protocol

This option is used for only bridges.

Procedure

- Step 1** Select **Association > Spanning Tree**. The Association: Spanning Tree Protocol dialog box appears.
- Step 2** Click **See detail** for information on which bridges this configuration is valid.
- Step 3** 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 6-2 *Spanning Tree Protocol Settings*

Field	Description
Spanning Tree Protocol (STP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable STP on the bridge. • Disable—If you do not want STP enabled the bridge.
Always Unblock Ethernet when STP is disabled	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to maintain a bridge link when STP is disabled. • No—Use this setting to not maintain a bridge link when STP is disabled. Click See detail to see for which versions this setting is valid.

Table 6-2 Spanning Tree Protocol Settings (continued)

Field	Description
Root Configuration	
Priority (0-65535)	<p>Enter a number to influence which bridge is designated the root bridge in the spanning tree.</p> <p>When bridges have the same priority setting, STP uses the MAC addresses as a tiebreaker.</p> <p>The bridge with the lowest priority setting is likely to be designated the root bridge in the tree.</p>
Max Age (6-40 Seconds)	<p>Enter the number of seconds to define how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt.</p> <p>For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BPDU from the root bridge in the spanning tree within 20 seconds.</p>
Hello Time (1-10 Seconds)	<p>Enter the number of seconds to define how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same.</p>
Forward Delay (4-30 Seconds)	<p>Enter the number of seconds to define how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree.</p>
Port Configuration	
Path Cost (1-65535)	<p>Enter a number to indicates the relative efficiency of a port's network link.</p> <p>A port with a high path cost is less likely to become a bridge's root port.</p>

Table 6-2 Spanning Tree Protocol Settings (continued)

Field	Description
Priority (0-255)	Enter a number to influence whether STP designates a port as a bridge's root port. A port with a low priority setting is more likely to become a bridge's root port.
Enable	From the list, select one of the following for each port configured: <ul style="list-style-type: none"> • Enable—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.) • Disable—Use this setting to indicate that the port does not participate in STP.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Defining Address Filters

Using this option, you can:

- Create a MAC address filter
- Remove a MAC address filter

Procedure

Step 1 Select **Association > Address Filters**. The Association: Address Filters dialog box appears.

Step 2 To add or delete a new MAC address filter complete the following fields:



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 6-3 Address Filters Settings

Field	Description
New Destination MAC Address	<ol style="list-style-type: none"> Enter a destination MAC address by entering the address in one of the following ways: <ul style="list-style-type: none"> With colons separating the character pairs (00:40:96:12:34:56, for example). Without any intervening characters (004096123456, for example). Select one of the following: <ul style="list-style-type: none"> Allowed—Use this setting to pass traffic to the MAC address. Disallowed—Use this setting to discard traffic to the MAC address. Client Disallowed—Use this setting to block traffic from clients that do not have a specific MAC address. Click >> to add it to the Current MAC Address Filters list.
Current MAC Address Filters (Add)	<p>Lists the current MAC address filters.</p> <p>To remove a filter from the list, select it, then click <<.</p>

Table 6-3 Address Filters Settings (continued)

Field	Description
Delete MAC Address	Enter the MAC address to delete, then click >> to add it to the Current MAC Address Filters list.
Current MAC Address Filters (Delete)	Lists the current MAC address filters to delete. To remove a filter from the list, select it, then click <<.
Lookup MAC address on Authentication Server if not in an Existing Filter List?	Click one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to allow looking up a MAC address on the authentication server. • No—Use this setting to disallow looking up a MAC address.
Is MAC Authentication alone sufficient for a client to be fully authenticated?	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to specify that client devices that associate to the access point using 802.11 open authentication, first attempt MAC authentication. • No—Use this setting to specify that MAC authentication alone is not sufficient. Click See detail to see for which 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 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Defining Ethertype Filters

Procedure

-
- Step 1** Select **Association > Ethertype Filters**. The Association: Ethertype Filters dialog box appears.
- Step 2** Using this option:
- Create new filters—See [Creating New Ethertype Filters, page 6-22](#).
 - Create Special Cases—See [Creating Special Cases, page 6-24](#).
-

Creating New Ethertype Filters

Procedure

-
- Step 1** To create and enable protocol filters for the access point's Ethernet port, enter the following:



Note For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com.

Table 6-4 *Creating New Ethertype Filters Settings*

Field	Description
New Ethertype Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page B-1 .

Table 6-4 *Creating New Ethertype Filters Settings (continued)*

Field	Description
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click >>. The new name is added to the Current Ethertype Filters list.

Step 3 To delete an Ethertype filter 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 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Creating Special Cases

Procedure

- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 6-5 *Ethertype Filter Special Cases Settings*

Field	Description
New Special Cases	
Ethertype	Enter the Ethertype filter name.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Default—Use the disposition you set for the Ethertype filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 6-5 Ethertype Filter Special Cases Settings (continued)

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network’s most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the access point’s buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the access point’s buffer before they are discarded.
Alert	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • No—Use this setting to not send an alert to the event log.

Step 3 Click >>. The new name is added to the Special Cases list.

Step 4 To remove a name from the Special Cases list, select it, then click <<.

- Step 5** Select one of the following:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining IP Protocol Filters

Procedure

- Step 1** Select **Association > IP Protocol Filters**. The Association: IP Protocol Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New IP Protocol Filters, page 6-26](#).
 - Create Special Cases—See [Creating Special Cases, page 6-28](#).
-

Creating New IP Protocol Filters

Procedure

- Step 1** To create and enable IP protocol filters, enter the following:



Note For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com.

Table 6-6 IP Protocol Filter Settings

Field	Description
New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page B-1 .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click >>. The new name is added to the Current Protocol Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Creating Special Cases

Procedure

-
- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 6-7 *IP Protocol Filters Special Cases Settings*

Field	Description
New Special Cases	
Protocol	Enter the IP protocol name.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Default—Use the disposition you set for the protocol filter. • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.

Table 6-7 IP Protocol Filters Special Cases Settings (continued)

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • No—Use this setting to not send an alert to the event log.

- Step 3** Click >>. The new name is added to the list box.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining IP Port Filters

Procedure

- Step 1** Select **Association > IP Port Filters**. The Association: IP Port Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New Port Filters, page 6-31](#).
 - Create Special Cases—See [Creating Special Cases, page 6-32](#).
-

Creating New Port Filters



Note For a list of protocols, refer to Appendix B, Protocol Filter Lists in the *Cisco Aironet Access Point Software Configuration Guide*. The guide can be found on Cisco.com.

Procedure

Step 1 To create and enable port filters, enter the following:

Table 6-8 IP Port Filter Settings

Field	Description
New Port Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page B-1 .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Default Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click >>. The new name is added to the Current Port Filters list.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Creating Special Cases

Procedure

- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 6-9 IP Port Filters Special Cases Settings

Field	Description
New Special Cases	
Port	Enter the IP Port filter name.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Default—Use the disposition you set for the port filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 6-9 IP Port Filters Special Cases Settings (continued)

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
Unicast	Enter the number of milliseconds unicast packets should stay in the buffer before they are discarded.
Multicast	Enter the number of milliseconds multicast packets should stay in the buffer before they are discarded.
Alert	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • No—Use this setting to not send an alert to the event log.

- Step 3** Click >>. The new name is added to the Special Cases list.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Policy Groups

Policy groups are used to configure access parameters to a logical group of stations in a consistent manner from a single place. For example, protocol filters can be applied to frames for a selected group of stations.

Procedure

- Step 1** Select **Association > Policy Group**. The Association: Policy Group dialog box appears.

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



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** Using this option you can:
- Add a policy group—See [Adding a New Policy Group, page 6-35](#).
 - Delete an exiting Policy Group From a Device—See [Deleting an Existing Policy Group from a Device, page 6-36](#).
-

Adding a New Policy Group

Procedure

Step 1 To add a new policy group, enter the following:

Table 6-10 New Policy Group Settings

Field	Description
Group ID	Enter an identification number for the policy group.
Group Name	Enter a name for the policy group, then click >>.
Policy Groups to Add.	Lists the policy groups to be added. To remove a group from the list, click <<.
Ethertype	
Receive	Enter the ID of a defined Ether type filter, or select one of the filters you created using Association > Ether type Filters .
Transmit	Enter the ID of a defined Ether type filter, or select one of the filters you created using Association > Ether type Filters .
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .

- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Deleting an Existing Policy Group from a Device

Procedure

- Step 1** Enter the group identification number in the **Group ID** text box, then click >> to add it to the Policy Groups to Delete list.
- To remove a group from the list, click <<.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring VLANs

Access points and bridges in a VLAN network, which are running specific software versions, can provide a wireless VLAN trunk link between two wired segments of the network.

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

Procedure

Step 1 Select **Association > VLANs**. The Association: VLAN 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 Click **See detail** to see for which versions this option is valid.

Step 3 Enter the following information:

Table 6-11 VLAN Configuration

Field	Description
VLAN (802.1Q) Tagging	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> Enabled—Use this setting to allow IEEE 802.1Q protocol tagging on VLAN packets. <p>The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies.</p> <ul style="list-style-type: none"> Disabled—Use this setting to not allow tagging.
Native VLAN ID	<p>Enter identification number of the access point's native VLAN.</p> <p>Note This setting must agree with the native VLAN ID setting on the switch.</p>
Single VLAN ID which allows unencrypted packets	<p>Enter an identification number to allow unencrypted packets. An entry with a value of 0 (zero requires the use of encryption.)</p>
Optionally allow Encrypted Packets on unencrypted VLAN	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> Yes—Use this setting to allow point-to-point encryption. No—Use this setting to not allow point-to-point encryption.

- Step 4** Using this option you can:
- Add a new VLAN—See [Adding a New VLAN](#), page 6-38.
 - Delete an exiting VLAN from a Device—See [Deleting an Existing VLAN](#), page 6-41.
-

Adding a New VLAN

Procedure

- Step 1** To add a new VLAN, enter the following:

Table 6-12 New VLAN Settings

Field	Description
VLAN ID	Enter the identification number of the VLAN. Note This setting must match the setting on the switch.
VLAN Name	Enter the a unique name for the VLAN configured on the access point.
VLAN Enable	From the list, select one of the following: <ul style="list-style-type: none"> • Enabled—Use this setting to enable the VLAN. • Disabled—Use this setting to disable the VLAN.

Table 6-12 New VLAN Settings (continued)

Field	Description
Default Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Default—Use this setting for normal LAN traffic. • Excellent Effort—Use this setting for the network’s most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Default Policy Group	Enter the default policy group number, or select one you created using Association > Policy Groups .
Enhanced MIC verify WEP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting if you do not want Message Integrity Check (MIC) enabled. • MMH—Use this setting if you want MIC enabled to protect WEP keys. <p>Note When you enable MIC, only MIC-capable client devices can communicate with the access point.</p>

Table 6-12 New VLAN Settings (continued)

Field	Description
Temp Key Integrity Protocol	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> None—Use this setting if you do not want to enable the temporal key integrity protocol (TKIP), or WEP key hashing. Cisco—Use this setting to enable TKIP. <p>Note 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.</p>
WEP Key Rotation Interval	<p>Use this setting to enable or disable broadcast key rotation.</p> <ul style="list-style-type: none"> To enable it, enter the rotation interval in seconds. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. <p>Note When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5) cannot use the access point when you enable broadcast key rotation.</p> <ul style="list-style-type: none"> To disable it, enter 0 (zero).
Alert?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> Yes—Use this setting if you are not adding an encrypted VLAN. No—Use this setting if you are adding an encrypted VLAN.
WEP Keys 1 through 4	Enter the encryption keys used: 40 bit or 128 bit hexadecimal digits.
Size	For each WEP key, select one of the following: Not set, 40 bit, or 128 bit.

- Step 2** Click >> to add the VLAN to the VLANs to Add list.
- Step 3** To make sure the VLAN ID you want to create does not already exist, click **Update**.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Deleting an Existing VLAN

Procedure

- Step 1** Enter the VLAN identification number in the **VLAN ID** text box, then click >> to add it to the VLANs to Delete list.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Quality of Service

This option is used to configure the access point's Quality of Service feature.

Procedure

- Step 1** Select **Association > Quality of Service**. The Association: Quality of Service 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** Click **See detail** to see for which versions this option is valid.
- Step 3** Enter the following information:

Table 6-13 Quality of Service Settings

Field	Description
Generate QBBS Element	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to enable support for basic 802.11 Quality of Service. • No—Use this setting to disable support for basic 802.11 Quality of Service.
User Symbol Extensions	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting enables support for Symbol Voice over IP (VoIP phones). • No—Use this setting to disable support for Symbol VoIP phones.

Table 6-13 Quality of Service Settings (continued)

Field	Description
Send IGMP General Query	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication. • No—Use this setting to not allow the access point to send an IGMP General Query.
Background (spare)	From the CWmin and CWmax lists, select the minimum and maximum contention window values for each traffic category.
Best Effort (default)	
Excellent Effort	
Controlled Load	
Interactive Video	
Interactive Voice	
Network Control	

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Service Sets

This option allows you to define service sets.

Procedure

Step 1 Select **Association > Service Sets**. The Association: Service Sets 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 Click **See detail** to see for which versions this option is valid.

Step 3 Enter the following information:

Table 6-14 Service Set Settings

Field	Description
Device	
SSID for use by Infrastructure Stations (such as Repeaters)	Enter the SSID to be used by repeaters and workgroup bridges to associate to the access point. This SSID should be mapped to the native VLAN ID in order to facilitate communications between infrastructure devices and a non-root access point or bridge.
Disallow Infrastructure Stations on any other SSID	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—This setting prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID. • No—This setting does not prevent repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID.

Step 4 Using this option you can:

- Add a new Service Set—See [Adding a New Service Set, page 6-45](#).
- Delete an exiting Service Set from a device—See [Deleting an Existing Service Set, page 6-48](#).

Adding a New Service Set

Procedure

Step 1 To add a new Service set, enter the following:

Table 6-15 New Service Set Settings

Field	Description
SSID Index	Enter an identification number from 1-32 digits for the SSID.
SSID Name	Enter the SSID name.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.
Proxy Mobile IP Enabled	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—This setting allows proxy mobile IP use by all stations associated to this access point. • No—This setting does not allow proxy mobile IP use.
Default VLAN ID	Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using Association >VLANs .
Default Policy Group	Enter the identification number of a defined policy group, or select one of the policy groups you created using Association > Policy Groups .
Service Sets To Add	Lists the added service sets. To remove a service set from the list, click <<.
Accept Authentication Type	

Table 6-15 New Service Set Settings (continued)

Field	Description
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.

Table 6-15 New Service Set Settings (continued)

Field	Description
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open	From the list, select one of the following:
Shared	<ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Network-EAP	

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Deleting an Existing Service Set

Procedure

-
- Step 1** Enter the Service Set number in the **Service Set ID** text box, then click >> to add it to the Service Sets to Delete list.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Primary Service Set

This option allows you to set a default VLAN for the primary SSID on an access point.

Procedure

-
- Step 1** Select **Association > Primary Service Set**. The 11a Radio: Primary Service Set dialog box appears.
- Step 2** Complete the following:

Table 6-16 Primary Service Set

Field	Description
Service Set Name	Enter the SSID name.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.

Table 6-16 Primary Service Set (continued)

Field	Description
Proxy Mobile IP Enabled	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—This setting allows proxy mobile IP use by all stations associated to this access point. • No—This setting does not allow proxy mobile IP use.
Default VLAN ID	<p>Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using Association > VLANs.</p>
Default Policy Group	<p>Enter the identification number of a defined policy group, or select one of the policy groups you created using Association > Policy Groups.</p>
Accept Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.

Table 6-16 Primary Service Set (continued)

Field	Description
Network-EAP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Shared	
Network-EAP	

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining Advanced Associations

Use this option to control the total number of devices an access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive.

Procedure

- Step 1** Select **Association > Advanced**. The Association: Advanced dialog box appears.
- Step 2** To define advanced associations, enter 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 6-17 Advanced Association Settings

Field	Description
Alert Severity Level	<p>From the list select one of the following:</p> <ul style="list-style-type: none"> • <code>systemFatal</code>—Indicates an event that prevents operation of the port or device. • <code>protocolFatal</code>—Indicates an event that prevents operation of the port or device • <code>portFatal</code>—Indicates an event that prevents operation of the port or device • <code>systemAlert</code>—Indicates that you need to take action to correct the condition. • <code>protocolAlert</code>—Indicates that you need to take action to correct the condition. • <code>portAlert</code>—Indicates that you need to take action to correct the condition. • <code>externalAlert</code>—Indicates that you need to take action to correct the condition.

Table 6-17 Advanced Association Settings (continued)

Field	Description
	<ul style="list-style-type: none"> • systemWarning—Indicates that an error or failure may have occurred. • protocolWarning—Indicates that an error or failure may have occurred. • portWarning—Indicates that an error or failure may have occurred. • externalWarning—Indicates that an error or failure may have occurred. • systemInfo--Notification that some sort of event has occurred. • protocolInfo--Notification that some sort of event has occurred. • portInfo--Notification that some sort of event has occurred. • externalInfo--Notification that some sort of event has occurred
Max Bytes Stored Per Alert Packet	<p>Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled.</p> <p>If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.</p>
Max Fwd Table Entries	<p>Note Changing this setting may cause the access point to reboot.</p> <p>From the list, select one of the settings to designate the maximum number of devices that can appear in the Association Table.</p>

Table 6-17 Advanced Association Settings (continued)

Field	Description
Rogue AP alert timeout (minutes)	<p>Enter the amount of time in minutes the access point transmits an alert message. (When an access point detects a rogue access point, it sends an alert message to the system log.) When the timeout is reached, the access point stops sending the alert message.</p> <p>Click See detail to see for which versions this option is valid.</p>
Enable RFC 1493 802.1D Stats In MIB	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the storage of detailed RFC 1493 802.1D statistics in access point memory. • Disable—Use this setting to disable the storage of detailed RFC 1493 802.1D statistics in access point memory. When you disable extended statistics you conserve memory, and the access point can include more devices in the Association Table. <p>Click See detail to see for which versions this option is valid.</p>
Enable Extended Stats in MIB	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the storage of detailed statistics in the device's memory. • Disable—Use this setting to disable the storage of detailed statistics in the device's memory. <p>When you disable extended statistics you conserve memory, and the device can include more devices in the Association Table.</p>

Table 6-17 Advanced Association Settings (continued)

Field	Description
Map Multicast Entries to Broadcast Entry	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to make the access point more virus-resistant by mapping all multicast MAC addresses into the Broadcast address. • Disable—Use this setting to disable this feature. <p>Click See detail to see for which versions this setting is valid.</p>
Enable PSPF	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable Publicly Secure Packet Forwarding, which ensures that 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. • Disable—Use this setting to disable Publicly Secure Packet Forwarding. <p>Click See detail to see for which versions this option is valid.</p>

Table 6-17 Advanced Association Settings (continued)

Field	Description
Unknown Class Timeout	Enter 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. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.
Multicast Addresses Timeout	
Infrastructure Hosts Timeout	
Client Stations Timeout	
Repeaters Timeout	
Access Points Timeout	
Across Bridge Hosts Timeout	
Non-Root Bridges Timeout	
Root Bridges Timeout	

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Port Assignments

When you assign specific ports, your network topology remains constant even when devices reboot.

Procedure

Step 1 Select **Association > Port Assignments**. The Association: Port Assignments dialog box appears.

Step 2 To define port assignments, enter 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 6-18 Port Assignments Settings

Field	Description
ifIndex	Lists the port's designator in the Standard MIB-II (RFC1213)-MIB.my interface index.
dot1dBasePort	Lists the port's designator in the Bridge MIB (RFC1493); BRIDGE-MIB.my interface index.
AID	Lists the port's 802.11 radio drivers association identifier.
Station	Enter the MAC address of the device to which you want to assign the port.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring DSCP to CoS

This option is use to statically map Differentiated Services Code-Point (DSCP) values to corresponding Class of Service (CoS) values.

Procedure

- Step 1** Select **Association > DSCP to CoS**. The Association: DSCP to CoS Conversion 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** Click **See detail** to see for which versions this option is valid.
- Step 3** For each DSCP, enter the CoS conversion.
- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring the Ethernet Port

Use this option to configure the device's Ethernet port.

Procedure

- Step 1** Select **Ethernet**. The menu expands and the Ethernet dialog box displays in the right pane.
- Step 2** Select one of the following from the Ethernet menu:



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.

- Identification—See [Identifying the Ethernet Port](#), page 6-59.
 - Filters—See [Setting Up Ethernet Filters](#), page 6-61.
 - Hardware—See [Setting Up Hardware](#), page 6-62.
 - Advanced—See [Defining the Ethernet Advanced Settings](#), page 6-64.
-

Identifying the Ethernet Port

Use this option to define basic identity information for the Ethernet port.

Procedure

- Step 1** Select **Ethernet > Identification**. The Ethernet: Identification dialog box displays in the right pane.
- Step 2** Enter the following information to identify the port:

Table 6-19 Ethernet Port Settings

Field	Description
Primary Port	From the list, select one of the following: <ul style="list-style-type: none"> • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.
Adopt Primary Port Identity	<p>Note Changing this setting may cause the access point to reboot.</p> From the list, select one of the following: <ul style="list-style-type: none"> • yes—This adopts the primary port settings (MAC and IP addresses for the Ethernet port). • no—This uses different MAC and IP addresses for the Ethernet port.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Setting Up Ethernet Filters

Use this option to define filters for the Ethernet port, the IP Protocol, and the IP Port.

Procedure

- Step 1** Select **Ethernet > Filters**. The Ethernet: Filters 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 6-20 Ethernet Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .

Table 6-20 Ethernet Filters Settings (continued)

Field	Description
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Up Hardware

This option allows you to select the hardware settings used by the access point's Ethernet port.

Procedure

Step 1 Select **Ethernet > Hardware**. The Ethernet: Hardware 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.

Step 2 Click **See detail** to see for which versions this option is valid.

Step 3 Complete the following:

Table 6-21 Ethernet Hardware Settings

Field	Description
Loss of Backbone Connectivity # of Secs (1-1000)	Enter the number of seconds the system must detect loss of backbone connectivity (i.e. loss of Ethernet link and no active trunk available on any of the radios) before taking the specified by Loss of Backbone Connectivity Action.
Loss of Backbone Connectivity Action	From the list, select one of the following: <ul style="list-style-type: none"> • No action • Switch to repeater mode • Shut the radio off • Restrict to SSID
Loss of Backbone Connectivity SSID	Enter an SSID index required if the Loss of Backbone Connectivity Action is set to Restrict to SSID, or select the SSID from the list.

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the Ethernet Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

- Step 1** Select **Ethernet > Advanced**. The Ethernet: Advanced 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 6-22 Ethernet Advanced Settings

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> • up—Enables the Ethernet port for normal operation. • down—Disables the device’s Ethernet port.
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.

Table 6-22 Ethernet Advanced Settings (continued)

Field	Description
Default Multicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under Association > Address Filters. • disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under Association > Address Filters.
Maximum Multicast Packets/Second	<p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>
Default Unicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under Association > Address Filters. • disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under Association > Address Filters.

Table 6-22 Ethernet Advanced Settings (continued)

Field	Description
Always Unblock Ethernet when STP is disabled	<p>From the list, select one of the following:</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to maintain a bridge link when STP is disabled • No—Use this setting to not maintain a bridge link when STP is disabled. <p>Click See detail to see for which versions this option is valid.</p>
Optimize Ethernet for	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Performance—Allows faster packet forwarding. • Statistics Collection—Allows better statistics collection. <p>Click See detail to see for which versions this option is valid.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring the 11b Radio

Use this option to configure the device's 11b radio.

Procedure

- Step 1** Select **11b Radio**. The menu expands and the Radio dialog box displays in the right pane.
- Step 2** Select one of the following from the Radio menu:



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.

- Identification—See [Identifying the 11b Radio Port, page 6-67](#).
 - Filters—See [Setting Up 11b Radio Filters, page 6-70](#).
 - Hardware—See [Defining the 11b Radio Hardware Settings, page 6-71](#).
 - Advanced—See [Defining the 11b Radio Advanced Settings, page 6-76](#).
 - Searched Channels—See [Defining the 11b Radio Searched Channels Settings, page 6-82](#).
-

Identifying the 11b Radio Port

Use this option to define basic identity information for the port.



Note Changing this setting may cause the access point to reboot.

Procedure

- Step 1** Select **11b Radio > Identification**. The 11b Radio: Identification dialog box displays in the right pane.
- Step 2** Enter the following information to identify the port:



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 6-23 11b Radio Identification Settings

Field	Description
Primary Port	<p>From the list, select one of the following:</p> <p>Note If the primary port was set using Ethernet > Identification, the selected value is displayed.</p> <ul style="list-style-type: none"> • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.

Table 6-23 11b Radio Identification Settings (continued)

Field	Description
Adopt Primary Port Identity	<p>Note Changing this setting may cause the access point to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.
LEAP User Name	<p>Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server.</p> <p>Click See detail to see for which versions this option is valid.</p>
LEAP Password	<p>Enter the LEAP password.</p> <p>Click See detail to see for which versions this option is valid.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Up 11b Radio Filters

Procedure

- Step 1** Select **11b Radio > Filters**. The 11b Radio Filters 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 6-24 11b Radio Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .

Table 6-24 11b Radio Filters Settings (continued)

Field	Description
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Defining the 11b Radio Hardware Settings

Procedure

Step 1 Select **11b Radio > Hardware**. The 11b Radio: Hardware 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 6-25 11b Radio Hardware Settings

Field	Description
Service Set ID (SSID)	<p>Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>Several access points on a network or sub-network can share an SSID.</p>
Allow “Broadcast” SSID to Associate	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point. <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p>
Enable “World Mode” multi-domain operation?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows the access point to add channel carrier set information to its beacon. <p>Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.</p> <ul style="list-style-type: none"> • no—Does not allow the access point to add channel carrier set information to its beacon.

Table 6-25 11b Radio Hardware Settings (continued)

Field	Description
Data Rates (Mb/sec)	
1.0	<p>From the list, select one of the following for each of the four rates in megabits per second:</p> <ul style="list-style-type: none"> • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
2.0	
5.5	
11.0	
Transmit Power	<p>From the list, select one of the following milliwatt settings: 1, 5, 20, 30, 50, 100.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p> <p>Click See detail to see for which versions this option is valid.</p>
Fragmentation Threshold (256-2338)	<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>
RTS Threshold (0-2339)	<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>

Table 6-25 11b Radio Hardware Settings (continued)

Field	Description
Maximum RTS Retries (1-128)	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Max. Data Retries (1-128)	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
Beacon Period (Kusec)	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)
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 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.</p>
Default Radio Channel	<p>From the list, select the radio channel you want for a default. Each channel covers 22 MHz.</p> <p>The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz.</p>
Search for less-congested Radio Channel?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.

Table 6-25 11b Radio Hardware Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	<ul style="list-style-type: none"> <li data-bbox="744 337 1231 526">• 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.) Use this setting for both receive and transmit. <li data-bbox="744 620 1231 808">• 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.) Use this setting for both receive and transmit. <li data-bbox="744 902 1231 1091">• 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. Use this setting for both receive and transmit.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11b Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

- Step 1** Select **11b Radio > Advanced**. The 11b Radio: Advanced 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 6-26 11b Radio Advance Settings

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> • up— Enables the Radio port for normal operation. • down—Disables the device's Radio port.

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under Association > Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under Association > Address Filters.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.
Maximum Number of Associations	Enter the maximum number of wireless networking devices that are allowed to associate to the access point. If you enter 0 it means that the maximum possible number of associations is allowed. Click See detail to see for which versions this option is valid.

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Use Aironet Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does not enable the features listed above.
Classify Workgroup Bridges as network infrastructure	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less. • no—Use this setting to allow more than 20 workgroup bridges to associate to the access point. <p>Click See detail to see for which versions this option is valid.</p>
User Symbol Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to enable the following features: load balancing, message integrity check (MIC), temporal key integrity protocol (TKIP). • no—Use this setting to disable use of Cisco Aironet 802.11 extensions. <p>Click See detail to see for which versions this option is valid.</p>
Ethernet encapsulation transform	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Enhanced MIC verification for WEP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks. <p>Click See detail to see for which versions this setting is valid.</p>
Temporal Key Integrity Protocol	<p>From the list, select the following:</p> <ul style="list-style-type: none"> • None—Does not enable WEP key hashing. • Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. <p>Click See detail to see for which versions this option is valid.</p>
Broadcast WEP Key rotation interval (sec)	<p>Enter a rotation interval in seconds.</p> <ul style="list-style-type: none"> • If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. • If you enter 0, you disable broadcast WEP key rotation. <p>Click See detail to see for which versions this option is valid.</p>

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Default Unicast Address Filter	
Open	From the list, select one of the following: <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. Select Disallowed for each authentication type that also uses MAC-based authentication.
Shared	
Network-EAP	
Specified Access Point 1	If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate.
Specified Access Point 2	
Specified Access Point 3	
Specified Access Point 4	
Radio Modulation	With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points. From the list, select one of the following: <ul style="list-style-type: none"> • Standard—This setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association. • MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Radio Preamble	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Long—Ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). • Short—Cisco Aironet’s Wireless LAN Adapter supports short preambles; it improves throughput performance.
Bridge Spacing (km)	<p>Enter a value from 0 to 40 kilometers to specify the distance from a root bridge to non-root bridges with which it communicates. Note that you do not need to adjust this setting on non-root bridges.</p> <p>The Bridge Spacing setting adjusts the bridge's timeout values to account for the time required for radio signals to travel from bridge to bridge. If more than one non-root bridge communicates with the root bridge, enter the distance from the root bridge to the non-root bridge that is farthest away.</p> <p>Click See detail to see for which versions this option is valid.</p>

Table 6-26 11b Radio Advance Settings (continued)

Field	Description
Non-Root Mobility	<p>This setting applies mainly to repeater access points that you intend to use in a roaming environment.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Stationary—Use this setting to specify that the radio firmware not aggressively scan for a better root association, which makes the association more stable but does not allow the access point to roam. • Mobile—Use this setting to specify that the radio firmware aggressively scan for a better root association, which allows the access point to roam throughout the wireless network. <p>Click See detail to see for which versions this setting is valid.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Defining the 11b Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

**Note**

Not all channels are available for all geographic domains.

Procedure

-
- Step 1** Select **11b Radio > Searched Channels**. The 11b Radio: Searched Channels dialog box displays in the right pane.
- Step 2** Click **See details** to see for which versions this option is valid.
- Step 3** 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 6-27 11b Radio Searched Channels Settings

Field	Description
Channel Number	Lists the available channels by number.
Frequency (mHz)	<p>Lists the channel frequency.</p> <p>For a list of channel frequency, 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#2450296 • Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.
Search?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring the 11a Radio

Use this option to configure the device's 11a radio.

Procedure

- Step 1** Select **11a Radio**. The menu expands and the 11a Radio dialog box displays in the right pane.
- Step 2** Click **See details** to see for which versions this option is valid.
- Step 3** Select one of the following from the Radio menu:



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.

- Identification—See [Identifying the 11a Radio Port](#), page 6-86.
 - Filters—See [Setting Up 11a Radio Filters](#), page 6-88.
 - Hardware—See [Defining the 11a Radio Hardware Settings](#), page 6-90.
 - Advanced—See [Defining the 11a Radio Advanced Settings](#), page 6-95.
 - Searched Channels—See [Defining the 11a Radio Searched Channels Settings](#), page 6-102.
 - Data Encryption—See [Defining the 11a Radio Data Encryption Settings](#), page 6-104.
 - Module Service Sets—See [Defining the 11a Radio Module Service Sets](#), page 6-108.
 - Primary Service Set—See [Defining the 11a Radio Primary Service Set](#), page 6-112.
 - Module QoS—See [Configuring 11a Radio QoS](#), page 6-115.
-

Identifying the 11a Radio Port

Use this option to define basic identity information for the Ethernet port.

**Note**

Changing this setting may cause the access point to reboot.

Procedure

-
- Step 1** Select **11a Radio > Identification**. The 11a Radio: Identification dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.
- Step 3** Enter the following information to identify the port:

**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 6-28 11a Radio Identification Settings

Field	Description
Primary Port	<p>From the list, select one of the following:</p> <p>Note If the primary port was set using Ethernet > Identification, the selected value is displayed.</p> <ul style="list-style-type: none"> • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.
Adopt Primary Port Identity	<p>Note This setting may cause the device to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port. <p>Click See detail to see for which versions this setting is valid.</p>

Table 6-28 11a Radio Identification Settings (continued)

Field	Description
LEAP User Name	Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server. Click See detail to see for which versions this option is valid.
LEAP Password	Enter the LEAP password. Click See detail to see for which versions this option is valid.

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Up 11a Radio Filters

Procedure

- Step 1** Select **11a Radio > Filters**. The 11a Radio Filters dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.

Step 3 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 6-29 11a Radio Filters Settings

Field	Description
Ethernet	
Receive	Enter the ID of a defined Ethernet filter, or select one of the filters you created using Association > Ethernet Filters .
Transmit	Enter the ID of a defined Ethernet filter, or select one of the filters you created using Association > Ethernet Filters .
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11a Radio Hardware Settings

Procedure

- Step 1** Select **11a Radio > Hardware**. The 11a Radio: Hardware dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this option is valid.
- Step 3** 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 6-30 11a Radio Hardware Settings

Field	Description
Service Set ID (SSID)	<p>Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 1 to 32 characters long.</p> <p>Several access points on a network or sub-network can share an SSID.</p>
Allow “Broadcast” SSID to Associate	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point) to associate with to associate with the access point. <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p>
Data Rates (Mb/sec)	
6.0	<p>From the list, select one of the following for each of the four rates in megabits per second:</p> <ul style="list-style-type: none"> • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
9.0	
12.0	
18.0	
24.0	
36.0	
48.0	
54.0	

Table 6-30 11a Radio Hardware Settings (continued)

Field	Description
Transmit Power	<p>From the list, select one of the following milliwatt settings: 5, 10, 20, 40.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p>
Fragmentation Threshold (256-2338)	<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>
RTS Threshold (0-2339)	<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>
Maximum RTS Retries (1-128)	<p>Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.</p>
Max. Data Retires (1-128)	<p>Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.</p>
Beacon Period (Kusec)	<p>Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)</p>

Table 6-30 11a Radio Hardware 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 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 Kmsecs. (One Kmsec equals 1,024 microseconds.)</p>
Default Radio Channel	<p>From the list, select the radio channel you want for a default.</p>
Search for less-congested Radio Channel?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.

Table 6-30 11a Radio Hardware Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	<ul style="list-style-type: none"> <li data-bbox="744 337 1231 521">• 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.) Use this setting for both receive and transmit. <li data-bbox="744 618 1231 802">• 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.) Use this setting for both receive and transmit. <li data-bbox="744 899 1231 1083">• 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. Use this setting for both receive and transmit.

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11a Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

- Step 1** Select **11a Radio > Advanced**. The 11a Radio: Advanced dialog box displays in the right pane.
- Click **See detail** to see for which versions this setting is valid.
- 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 6-31 11a Radio Advanced Settings

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> • up—Enables the Radio port for normal operation. • down—Disables the device’s Radio port.

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under Association > Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under Association > Address Filters.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Radio Cell Role	<p>From the list, enter one of the following:</p> <ul style="list-style-type: none"> • Client/Non-Root—use this setting for diagnostics or site surveys, such as when you need to test and access point by having it communicate with another access point or bridge without accepting associations from client devices. • Repeater/Non-Root—Use this setting for access points that are not connected to a wired LAN and which transfer data between another access point or repeater. • Access Point/Root—Use this setting if the access point is connected to a wired LAN.
Maximum Number of Associations	<p>Enter the maximum number of wireless networking devices that are allowed to associate to the access point.</p> <p>If you enter 0 it means that the maximum possible number of associations is allowed.</p>
Use Aironet Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does no enable the features listed above.
Classify Workgroup Bridges as network infrastructure	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less. • no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Ethernet encapsulation transform	From the list, select one of the following: <ul style="list-style-type: none"> • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.
Enhanced MIC verification for WEP	From the list, select one of the following: <ul style="list-style-type: none"> • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks.
Temporal Key Integrity Protocol	From the list, select the following: <ul style="list-style-type: none"> • None—Does not enable WEP key hashing. • Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key.
Broadcast WEP Key rotation interval (sec)	Enter a rotation interval in seconds. <ul style="list-style-type: none"> • If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. • If you enter 0, you disable broadcast WEP key rotation.
Accept Authentication Type	

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Shared	
Network-EAP	

Table 6-31 11a Radio Advanced Settings (continued)

Field	Description
Specified Access Point 1	If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate.
Specified Access Point 2	
Specified Access Point 3	
Specified Access Point 4	
Non-Root Mobility	With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.
	<p>This setting applies mainly to repeater access points that you intend to use in a roaming environment.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Stationary—Use this setting to specify that the radio firmware not aggressively scan for a better root association, which makes the association more stable but does not allow the access point to roam. • Mobile—Use this setting to specify that the radio firmware aggressively scan for a better root association, which allows the access point to roam throughout the wireless network. <p>Click See detail to see for which versions this setting is valid.</p>

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11a Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.



Note

Not all channels are available for all geographic domains.

Procedure

- Step 1** Select **11a Radio > Searched Channels**. The 11a Radio: Searched Channels dialog box displays in the right pane.

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

- 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 6-32 11a Radio Searched Channels Settings

Field	Description
Channel Number	Lists the available channels by number.
Frequency (mHz)	<p>Lists the channel frequency.</p> <p>For a list of channel frequency, 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#2450296 • Cisco IOS Commands for Access in the <i>Cisco Aironet 1200 Series Access Point Command Reference</i>.
Search?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11a Radio Data Encryption Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

- Step 1** Select **11a Radio > Data Encryption**. The 11a Radio: Data Encryption dialog box displays in the right pane.
- Step 2** Click **See detail** to see for which versions this setting is valid.

Step 3 Complete the following:

Table 6-33 11a Radio Data Encryption Settings

Field	Description
Data Encryption by Stations	<p>From the list, select the encryption type:</p> <ul style="list-style-type: none"> • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.
Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.

Table 6-33 11a Radio Data Encryption Settings (continued)

Field	Description
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—This setting enables the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—This setting does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network EAP	<p>From the list, select one of the following:</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.

Table 6-33 11a Radio Data Encryption Settings (continued)

Field	Description
Shared	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	
Transmit Key	Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	Enter the type of encryption key used: <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	From the list, select one of the following: <ul style="list-style-type: none"> • 40 bit • 128 bit • Not set

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Defining the 11a Radio Module Service Sets

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and to select that channel for use.

Procedure

Step 1 Select **11a Radio > Module Service Sets**. The 11a Radio: Module Service Sets dialog box displays in the right pane.

Step 2 Click **See detail** to see which versions this option is valid for.



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 3 Using this option you can:

- Add a new Service Set—See [Adding a New Service Set, page 6-109](#).
 - Delete an exiting Service Set from a device—See [Deleting an Existing Service Sets, page 6-112](#).
-

Adding a New Service Set

Procedure

Step 1 To add a new module service set, enter the following:

Table 6-34 *New Module Service Sets*

Field	Description
Device	
SSID for use by Infrastructure Stations (such as Repeaters)	Enter an identification number for the client radio SSID.
Disallow Infrastructure Stations on any other SSID	From the list, select one of the following: Yes—Use this option to disallow infrastructure stations on any other SSID. No—Use this option to allow infrastructure stations on any other SSID.
Add New Service Set	
Service Set ID (1-32)	Enter an identification for the SSID.
Service Set Name	Enter the SSID.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.
Proxy Mobile IP Enabled	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—This setting allows proxy mobile IP use by all stations associated to this access point. • No—This setting does not allow proxy mobile IP use.
Default VLAN ID	Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using Association >VLANs .

Table 6-34 New Module Service Sets (continued)

Field	Description
Default Policy Group	Enter the identification number of a defined policy group, or select one of the policy groups you created using Association > Policy Groups .
Accept Authentication Type	
Open	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.

Table 6-34 New Module Service Sets (continued)

Field	Description
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Shared	
Network-EAP	

Step 2 Click **Add** to add the Service Set to the Service Sets to Add list.

Step 3 To delete a group from the list, select the name, then click **Delete**.

- Step 4** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Deleting an Existing Service Sets

Procedure

- Step 1** Enter the Service Set number in the **Service Set ID** text box, then click **Add** to add it to the Service Sets to Delete list.
- Step 2** To delete an identification number from the list, select it, then click **Delete**.
- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Defining the 11a Radio Primary Service Set

Use this option to set a default VLAN for the primary SSID on an access point.

Procedure

- Step 1** Select **11a Radio > Primary Service Set**. The 11a Radio: Primary Service Set 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.

- Step 2** Enter the following information:

Table 6-35 Primary Service Set

Field	Description
Service Set Name	Enter the name.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.
Proxy Mobile IP Enabled	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—This setting allows proxy mobile IP use by all stations associated to this access point. • No—This setting does not allow proxy mobile IP use.
Default VLAN ID	Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using Association > VLANs .
Default Policy Group	Enter the identification number of a defined policy group, or select one of the policy groups you created using Association > Policy Groups .

Table 6-35 Primary Service Set (continued)

Field	Description
Accept Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.

Table 6-35 Primary Service Set (continued)

Field	Description
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open	From the list, select one of the following:
Shared	<ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Network-EAP	

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring 11a Radio QoS

Use this option to define traffic class QoS policies.

Procedure

Step 1 Select **11a Radio > Module QoS**. The 11a Radio: Quality of Service dialog box appears.

Click **See detail** to see which versions this option is valid for.

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 6-36 11a Radio QoS

Field	Description
Generate QBBS Element	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to enable support for basic 802.11 Quality of Service. • No—Use this setting to disable support for basic 802.11 Quality of Service.
User Symbol Extensions	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting enables support for Symbol Voice over IP (VoIP phones). • No—Use this setting to disable support for Symbol VoIP phones.
Send IGMP General Query	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication. • No—Use this setting to not allow the access point to send an IGMP General Query.

Table 6-36 11a Radio QoS (continued)

Field	Description
Background (spare)	<ul style="list-style-type: none"> Min Contention Window—Enter the minimum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.
Best Effort (default)	
Excellent Effort	<ul style="list-style-type: none"> Max Contention Window—Enter the maximum contention window value. The value listed is to the power of 2. The access point computes Contention Window values.
Controlled Load	
Interactive Video	
Interactive Voice	<ul style="list-style-type: none"> Fixed Slot Time—Enter a value for a fixed slot time.
Network Control	

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Choices, page 6-9](#).

Defining the Security Settings

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

Procedure

- Step 1** Select **Security**. The menu expands and the Security dialog box displays in the right pane.
- Step 2** Select one of the following from the Security menu:



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.

- Local Admin Access—See [Setting Local Admin Access, page 6-118](#).
 - Local AP/Client Security—See [Setting Local AP/Client Security, page 6-122](#).
 - Authentication Server Security—See [Setting Authentication Server Security, page 6-125](#).
-

Setting Local Admin Access

Use this option to enable or disable local admin access.

Procedure

- Step 1** Select **Security > Local Admin Access**. The Security: Local 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 6-37 Local Admin Access Settings

Field	Description
Local Admin Authentication	From the list, select one of the following: <ul style="list-style-type: none">• Enable—Use this setting to enable local admin authentication.• Disable—Use this setting to disable local admin authentication.
Allow read-only browsing without login	From the list, select one of the following: <ul style="list-style-type: none">• Yes—Use this setting to allow read-only browsing.• No—Use this setting to disallow read-only browsing.

Step 3 Using this option you can:

- Add Users—See [Adding Users, page 6-120](#).
- Delete Users—See [Deleting Users, page 6-121](#).

Adding Users

Procedure

Step 1 To add a new user, enter the following:

Field	Description
Add Users	Click See user details for information about existing user IDs. See Understanding the User Details Window, page 6-121 for information about the table.
User Identifier	Enter an identification number for the user. Use the table in the User Details window to help assign a number. If you use an existing identifier number, you will modify the current setting. Tip If you want to set the same user name on all access points and do not know which user ID's may already be in use, enter a very high value (2000).
User Name	Enter the name for the user.
User Password	Enter a password for the user.
Confirm User Password	Reenter the password.
Capabilities	Select the capabilities you want to allow the user.

Step 2 Click >> to add the users to the Users to Add list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Deleting Users

Procedure

-
- Step 1** Click **See detail** to see which versions this option is valid for.
Click **See user details** for information about existing user IDs. See [Understanding the User Details Window, page 6-121](#) for information about the table.
- Step 2** Enter the user's identification number in the **User Identifier** text box, then click >> to add it to the Users to Delete list.
- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Understanding the User Details Window

When you click **see user details**, a window appears with the following table:

Field	Description
Device Name	The device name.
IP Address	The IP address of the device.
User Identifier	The currently assigned user identifier.
Username	The user name.
Timestamp	The time and date in which the information was collected from the access point.

Setting Local AP/Client Security

Use this option to set up the local access point and client security.

Procedure

Step 1 Select **Security > Local AP/Client Security**. The Security: Local AP/Client 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 6-38 Local AP/Client Security Settings

Field	Description
Data Encryption by Stations	<p>From the list, select the encryption type:</p> <ul style="list-style-type: none"> • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.

Table 6-38 Local AP/Client Security Settings (continued)

Field	Description
Authentication Type	
Open	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared Key	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.

Table 6-38 Local AP/Client Security Settings (continued)

Field	Description
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	
Transmit Key	Click 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"> • Not set • 40 bit • 128 bit

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Authentication Server Security

Use this option to set up authentication server security.

**Note**

Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Security > Authentication Server**. The Security: Authentication 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 6-39 Authentication Server Settings

Field	Description
802.1X Protocol Version (For EAP Authentication)	<p>Note This setting may cause the device to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting. • Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier. • Draft 10—Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later. <p>Click See detail for information on which version this setting is valid</p>
Primary Server Reattempt Period (Min)	<p>Enter the amount of time a before another attempt is made if the server is not responding.</p> <p>Click See detail for information on which version this setting is valid.</p>

Table 6-39 Authentication Server Settings (continued)

Field	Description
Send Service Type Attribute Login Only	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting so that the service type attribute for access requests is Login. • No—Use this setting so that the service type attribute for reauthentication requests is Authentication Only.
Server Name/IP	Enter the name or IP address of the server.
Server Type	From the list, select the type of server. Click See detail for information on which version this setting is valid
Port	Enter the port number your server uses for authentication.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Retran Int (sec)	Enter the number of seconds the access point should wait before retransmitting. Click See detail for information on which version this setting is valid.
Max Retran	Enter the number of times the access point should attempt to contact the server before giving up. Click See detail for information on which version this setting is valid.

Table 6-39 Authentication Server Settings (continued)

Field	Description
EAP Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this server for EAP authentication. <p>In this type of authentication, the access point relays authentication messages between the server and the authenticating client device.</p> <ul style="list-style-type: none"> • No—Do not use this server for EAP authentication. <p>Click See detail for information on which version this setting is valid.</p>
MAC Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this server for MAC-based authentication. <p>This allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point.</p> <ul style="list-style-type: none"> • No—Do not use this server for MAC-based authentication. <p>Click See detail for information on which version this setting is valid.</p>

Table 6-39 Authentication Server Settings (continued)

Field	Description
User Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to allow user authentication. • No—Use this setting to disallow user authentication. <p>Click See detail for information on which version this setting is valid.</p>
MIP Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this setting to authenticate proxy Mobile IP configured clients. • No—Use this setting to disallow authentication of proxy Mobile IP configured clients. <p>Click See detail for information on which version this setting is valid.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring 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 Services dialog box displays in the right pane.
- Step 2** Select one of the following from the Services menu:
- Start-Up—See [Configuring Start-Up Settings](#), page 6-130.
 - Console/Telnet—See [Configuring Console/Telnet Settings](#), page 6-134.
 - Hot Standby—See [Configuring Hot Standby Settings](#), page 6-136.
 - Routing—See [Configuring Routing Settings](#), page 6-137.
 - CDP—See [Configuring CDP Settings](#), page 6-139.
 - DNS—See [Configuring DNS Settings](#), page 6-140.
 - FTP—See [Configuring FTP Settings](#), page 6-141.
 - HTTP—See [Configuring HTTP Settings](#), page 6-142.
 - SNMP—See [Configuring SNMP Settings](#), page 6-144.
 - SNTP—See [Configuring SNTP Settings](#), page 6-145.
 - Accounting—See [Configuring Accounting Settings](#), page 6-146.
 - ProxyMobile IP Setup—See [Setting Up Proxy Mobile IP](#), page 6-150.
 - ProxyMobile SA Bind—See [Configuring Proxy Mobile SA Bindings](#), page 6-152.
-

Configuring Start-Up Settings

Use this option to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

Procedure

Step 1 Select **Services > Start-Up**. The Services: Start-Up 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 6-40 Start-Up Settings

Field	Description
Configuration Server Protocol	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting if your network does not have an automatic system for IP address assignment. • BOOTP—Use this setting if IP addresses are hard-coded based on MAC addresses. • DHCP—Use this setting if IP addresses are “leased” for predetermined periods of time.
Use prior Config Server settings if no server responds?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to have the access point save the boot server's most recent response. • no—Use this setting to not use the most recent response.

Table 6-40 Start-Up Settings (continued)

Field	Description
Read “.ini” file from file server?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • always—Use this setting for the access point to always load configuration settings from an .ini file on the server. • never—Use this setting for the access point to never load configuration settings from an.ini file on the server. • if specified by server—Use this setting for the access point to load configuration settings from an.ini file on the server if the server’s DHCP or BOOTP response specifies that an.ini file is available.
BOOTP Server Timeout (sec’s)	Enter the length of time the access point waits to receive a response from a single BOOTP server.
DHCP Multiple-Offer Timeout (sec’s)	Enter the length of time the access point waits to receive a response when there are multiple DHCP servers.
DHCP Requested Lease Duration (min’s)	Enter the length of time the access point requests for an IP address lease from your DHCP server.
DHCP Minimum Lease Duration (min’s)	Enter the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period.
DHCP Client Identifier Type	<p>From the list, select one of the client identifier types.</p> <p>Click See detail to see for which versions this setting is valid.</p>

Table 6-40 Start-Up Settings (continued)

Field	Description
DHCP Client Identifier Value	<p>Use this setting to include a unique identifier in the access point's DHCP request packet.</p> <ul style="list-style-type: none"> • If you select Other-Non Hardware from the DHCP Client Identifier Type list, you can enter up to 255 alphanumeric characters. • If you select any other option from the DHCP Client Identifier Type list, you can enter up to 12 hexadecimal characters (numbers 0 through 9, and the letters A through F). <p>Click See detail to see for which versions this setting is valid.</p>
DHCP Class Identifier	<p>Enter the access point's group name.</p> <p>The DHCP server uses the group name to determine the response to send to the access point.</p>

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Console/Telnet Settings

Use this option to configure the access point to work with a terminal emulator or through Telnet.

Procedure

- Step 1** Select **Services > Console/Telnet**. The Services: Console/Telnet 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 6-41 Console/Telnet Settings

Field	Description
Baud Rate	Enter a rate from 110 to 115,200, expressed in bits per second. The rate you enter is dependent on the capability of the computer you use to open the access point management system.

Table 6-41 Console/Telnet Settings (continued)

Field	Description
Parity	From the list, select one of the following: <ul style="list-style-type: none"> • None—Use this setting to use no parity bit. • Even—Use this setting to make the total number of bits even. • Odd—Use this setting to make the total number of bits odd.
Data Bits	From the list, select one of the data bit settings.
Stop Bits	From the list, select one of the stop bit settings.
Flow Control	From the list, select one of the following: <ul style="list-style-type: none"> • None—Use this setting to indicate no flow control is used. • SW Xonn/Xoff—Use this setting to indicate the method information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device.
Terminal Type	From the list, 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 (64-132)	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines (16-50)	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters.

Table 6-41 Console/Telnet Settings (continued)

Field	Description
Telnet	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to prevent Telnet access to the management system.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Hot Standby Settings

Use this option to configure a standby access point as a client device associated to a monitored access point.

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 6-42 Hot Standby Settings

Field	Description
Hot Standby Mode	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow hot standby mode. • Disable—Use this setting to disable hot standby mode.
Service Set ID (SSID)	Enter the monitored access point's SSID.
MAC Address for the Monitored AP	Enter the monitored access point's MAC address.
Polling Frequency (1-30)	Enter the number of seconds between each query the standby access point sends to the monitored access point.
Timeout for Each Polling (1-600)	Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Routing Settings

Use this option to configure the access point to communicate with the IP network routing system.

Procedure

Step 1 Select **Services > Routing**. The Services: Routing 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 6-43 Routing Settings

Field	Description
Default Gateway	Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.
New Network Route	
Destination Network	Enter the IP address of the destination network.
Gateway	Enter the IP address of the gateway used to reach the destination network.
Subnet Mask	Enter the subnet mask associated with the destination network.

Step 3 Click >> to add an additional network route for the access point.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring CDP Settings

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

Procedure

Step 1 Select **Services > CDP**. The Services: CDP 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 6-44 CDP Settings

Field	Description
Cisco Discovery Protocol (CDP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable CDP. • Disable—Use this setting to disable CDP.
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packet 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.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring DNS Settings

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 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 6-45 DNS Settings

Field	Description
Domain Name System (DNS)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this option if your network DNS. • Disable—Use this option if you network does not use DNS.
Default Domain	Enter the name of your network's IP domain. Your entry might look like this: mycompany.com

Table 6-45 DNS Settings (continued)

Field	Description
Domain Name Servers	Enter the IP addresses of up to three domain name servers on your network.
Domain Suffix	Enter the portion of the full domain name that you would like omitted from access point displays.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring FTP Settings

Use this option to configure File Transfer Protocol settings for the access point. All non-browser file transfers are governed by these settings.

Procedure

Step 1 Select **Services > FTP**. The Services: FTP 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 6-46 FTP Settings

Field	Description
File Transfer Protocol (FTP)	From the list select one of the protocols.
Default File Server	Enter the IP address or DNS name of the file server where the access point should look for FTP files.
FTP Directory	Enter the file server directory that contains the firmware image files.
FTP User Name	Enter the username assigned to your FTP server. You do not need to enter a name in this field if you selected TFTP.
FTP User Password	Enter the password associated with the file server's username. You do not need to enter a password in this field if you selected TFTP.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring HTTP Settings

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

Procedure

Step 1 Select **Services > HTTP** The Services: HTTP 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 6-47 HTTP Settings

Field	Description
Allow Non-Console Browsing	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow browsing to the management system. • Disable—Use this setting to make the management system accessible only through the console and Telnet interfaces.
HTTP Port	Enter the port through which the access point provides web access.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring SNMP Settings

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

Procedure

Step 1 Select **Services > SNMP**. The Services: SNMP 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 6-48 *SNMP Settings*

Field	Description
Simple Network Management Protocol (SNMP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow event notifications to be sent to an SNMP server. • Disable—Use this setting to not allow event notifications to be sent to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.
SysName	Enter the system name.
SysLocation	Enter the system location.
SysContact	Enter the system contact.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring SNTP Settings

Use this option to configure time server settings.

Procedure

Step 1 Select **Services > SNTP**. The Services: SNTP 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 6-49 SNTP Settings

Field	Description
Simple Network Time Protocol (SNTP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting if your network uses Simple Network Time Protocol. • Disable—Use this setting if your network does not use Simple Network Time Protocol.
Default Time Server	Enter enter the server's IP address.

Table 6-49 *SNTP Settings (continued)*

Field	Description
GMT Offset (hr)	From the list, select the time zone in which the access point operates.
Use Daylight Savings Time	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to have the access point automatically adjust to Daylight Savings Time. • Disable—Use this setting to not have the access point automatically adjust to Daylight Savings Time.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Accounting Settings

Use this option to configure settings that enable you to send network accounting information about wireless client devices to a RADIUS server on your network.

Procedure

- Step 1** Select **Services > Accounting**. The Services: Accounting dialog box appears. Click **See detail** to see for which versions this setting is valid.
- 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 6-50 Accounting Settings

Field	Description
Enable accounting	From the list, select one of the following: <ul style="list-style-type: none"> enable—Use this setting to turn on accounting for your wireless network. disable—Use this setting to turn off accounting for your wireless network
Enable delaying to report STOP	From the list, select one of the following: <ul style="list-style-type: none"> enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate. disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.

Table 6-50 Accounting Settings (continued)

Field	Description
Minimum delay time to report STOP (sec)	Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point.
Server Name/IP	Enter the name or IP address of the server to which the access point sends accounting data.
Server Type	Select RADIUS from the list. (Additional types may be added in future software releases.)
Port	Enter the communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Retran (sec)	Enter the amount of time to wait before retransmitting.
Max Retran	Enter the maximum number of times to attempt retransmissions. Click See detail for information on which version this setting is valid.

Table 6-50 Accounting Settings (continued)

Field	Description
Enable Update	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> enable—Use this setting to allow accounting update messages for wireless clients. <p>With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point.</p> <ul style="list-style-type: none"> disable—Use this setting to not allow accounting update messages. <p>With updates disabled, the access point sends only accounting start and accounting stop messages to the server.</p>
Update Delay (sec)	<p>Enter the update interval in seconds.</p> <p>If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.</p>
EAP Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> Yes—Use this server for EAP authentication. <p>In this type of authentication, the access point relays authentication messages between the server and the authenticating client device.</p> <ul style="list-style-type: none"> No—Do not use this server for EAP authentication.

Table 6-50 Accounting Settings (continued)

Field	Description
Non-EAP Auth.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this server for non-EAP authentication. • No—Do not use this server for non-EAP authentication.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Setting Up Proxy Mobile IP

Use this option to enable the access points to work in conjunction with Mobile IP configured on your network routers.

Procedure

Step 1 Select **Services > ProxyMobileIP Setup**. The Services: Proxy Mobile IP Setup 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 6-51 Proxy Mobile IP Setup

Field	Description
Enable Proxy Mobile IP	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this setting to enable proxy mobile IP. • No—Use this setting to disable proxy mobile IP.
Authoritative IP 1 through 3	Enter the IP address of the authoritative access point. Proxy Mobile IP must be enabled on the wireless SSID. Since multiple SSIDs may exist on the access point and not all SSIDs may have to accommodate mobile clients, you must enable proxy Mobile IP per SSID. The authoritative access point is used to communicate with new access points to update subnet map records and send the new access points a new and complete subnet mapping table.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Proxy Mobile SA Bindings

Use this option to identify the clients that are able to establish contact with a foreign agent in another network segment or network other than the client's home network.

Procedure

- Step 1** Select **Services > ProxyMobile SA Bind.** The Services: Proxy Mobile SA Bindings 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 6-52 Proxy Mobile SA Bindings

Field	Description
IP Address Range - Start	Enter the beginning IP address of the range in which client devices must reside in order to be valid.
IP Address Range - End	Enter the ending IP address of the range in which the client devices must reside in order to be valid.

Table 6-52 Proxy Mobile SA Bindings (continued)

Field	Description
Group SPI	<p>Enter the security parameter index of the IP address range entered in the IP Address Range - Start and End fields.</p> <p>The SPI is a 32-bit number (8 hexadecimal digits) assigned to the initiator of the security association request by the receiving IPSec endpoint. On receiving a packet, the destination address, protocol, and SPI are used to determine the security association.</p> <p>The security association allows the node to authenticate or decrypt the packet according to the security policy configured for that security association.</p>
Group Key	<p>Enter an authentication key that the group specified in the security association uses to access a foreign agent.</p> <p>The group key is a 128-bit key entered as 32 hexadecimal digits (0-9, a-f, or A-F).</p> <p>To add to the current SA Bindings, click >>.</p>
Current SA Bindings	<p>Lists previously configured security association bindings.</p> <p>To remove a binding from the list, select it, then click <<.</p>
Delete Existing SA Binding from Device	
SA Binding ID	<p>Enter the identification number of the SA binding to delete, then click >>.</p>
SA Bindings To Delete	<p>Lists the SA bindings to be deleted.</p>

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Events

This option enables to you to customize the display of access point events (alerts, warnings, and normal activity).

Procedure

- Step 1** Select **Events**. The menu expands and the Events dialog box displays in the right pane.
- Step 2** Select one of the following from the Events menu:



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.

- Event Handling—See [Configuring Event Handling, page 6-154](#).
 - Event Notifications—See [Configuring Event Notification, page 6-158](#).
-

Configuring Event Handling

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information.

Procedure

Step 1 Select **Events > Event Handling**. The Events: Event Handling 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 6-53 Event Handling Settings

Field	Description
System Fatal	From the list, select one of the following: <ul style="list-style-type: none"> • Count—Use this option to tally the total events occurring in this category without any form of notification or display. • Display Console—Use this option to provide a read-only display of the event but not record it. • Record—Use this option to make a record of the event in the log and provide a read-only display of the event. • Notify—Use this option to makes a record of the event in the log, display the event, and tell the access point to notify someone of the occurrence.
Protocol Fatal	
Network Port Fatal	
System Alert	
Protocol Alert	
Network Port Alert	
External Alert	
System Warning	
Protocol Warning	
Network Port Warning	
External Warning	
System Information	
Protocol Information	
Network Port Information	
External Information	

Table 6-53 Event Handling Settings (continued)

Field	Description
Handle Alerts as Severity Level	<p data-bbox="736 289 1197 318">From the list, select one of the following:</p> <ul data-bbox="744 337 1231 1143" style="list-style-type: none"> <li data-bbox="744 337 1193 423">• <code>systemFatal</code>—Indicates an event that prevents operation of the device as a whole. <li data-bbox="744 443 1231 565">• <code>protocolFatal</code>—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP. <li data-bbox="744 584 1193 670">• <code>portFatal</code>—Indicates an event that prevents operation of the Ethernet or radio network interface. <li data-bbox="744 690 1231 781">• <code>systemAlert</code>—Indicates that you need to take action to correct a condition on the device as a whole. <li data-bbox="744 800 1231 922">• <code>protocolAlert</code>—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP. <li data-bbox="744 941 1231 1032">• <code>portAlert</code>—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface. <li data-bbox="744 1052 1231 1143">• <code>externalAlert</code>—Indicates that you need to take action to correct the condition on a device on the network.

Table 6-53 Event Handling Settings (continued)

Field	Description
	<ul style="list-style-type: none"> • <code>systemWarning</code>—Indicates that an error or failure may have occurred on the device as a whole. • <code>protocolWarning</code>—Indicates that an error or failure may have occurred on a specific communications protocol in use, such as HTTP or IP. • <code>portWarning</code>—Indicates that an error or failure may have occurred on an Ethernet or radio network interface. • <code>externalWarning</code>—Indicates that an error or failure may have occurred on a device. • <code>systemInfo</code>—Notification that some sort of event has occurred on a device. • <code>protocolInfo</code>—Notification that some sort of event has occurred on a communications protocol in use, such as HTTP or IP. • <code>portInfo</code>—Notification that some sort of event has occurred on an Ethernet or radio network interface. • <code>externalInfo</code>—Notification that some sort of event has occurred on a device.

Table 6-53 Event Handling Settings (continued)

Field	Description
Maximum Number of Bytes Stored per Alert Packet (0- 2312)	Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.
Maximum Memory Reserved for Detailed Event Trace Buffer (bytes) (0-8388608)	Note Changing this setting may cause the access point to reboot. Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Configuring Event Notification

Use this option to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

Procedure

Step 1 Select **Events > Event Notification**. The Events: Event Notification 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 6-54 *Events > Event Notification Settings*

Field	Description
Should Notify-Disposition Events generate SNMP Traps?	From the list, select one of the of the following: <ul style="list-style-type: none"> • Yes—Use this option to send event notifications to an SNMP server. • No—Use this option if you do not want to send notifications to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.
Should Notify-Disposition Events generate Syslog Messages?	From the list, select one of the of the following: <ul style="list-style-type: none"> • Yes—Use this option to send event notifications to a Syslog server. • No—Use this option if you do not want to send notifications to a Syslog server.
Syslog Destination Address	Enter the IP address or the host name of the server running Syslog.
Syslog Facility Number	Enter the Syslog Facility number for the notifications.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
 - **Save** to save the template. See [Saving the Template, page 6-162](#).
 - Another template category to configure more options. See [Template Categories, page 6-9](#).
-

Configuring Custom Values

This option enables to 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.



Note

This option should be used only by advanced users who have a good understanding of the MIB variables they are setting.

Templates with custom key values are not validated.

Procedure

- Step 1** Select **Configure > Templates > Custom Values**. The Custom 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** Complete the following:



Note

You must enter the exact syntax for the setting to work properly.

Field	Description
Key	Enter a valid MIB key.
Value	Enter a valid MIB value.

Step 3 Click >> to add the custom value to the list.



Note 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.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. See [Previewing the Template, page 6-161](#).
- **Save** to save the template. See [Saving the Template, page 6-162](#).
- Another template category to configure more options. See [Template Categories, page 6-9](#).

Previewing the Template

Procedure

Step 1 Click **Preview**. A Command Preview window displays the configuration choices you have made to the template.

Step 2 Click **Save**. See [Saving the Template, page 6-162](#).

Saving the Template

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 9-37](#).
 - Click **No** if you want to save the template only.
 - Click **Cancel** to cancel the operation and then display the previous screen.
-

