



CHAPTER 8

Configuring Mobility Groups

This chapter describes mobility groups and explains how to configure them on Cisco NCS. It contains the following sections:

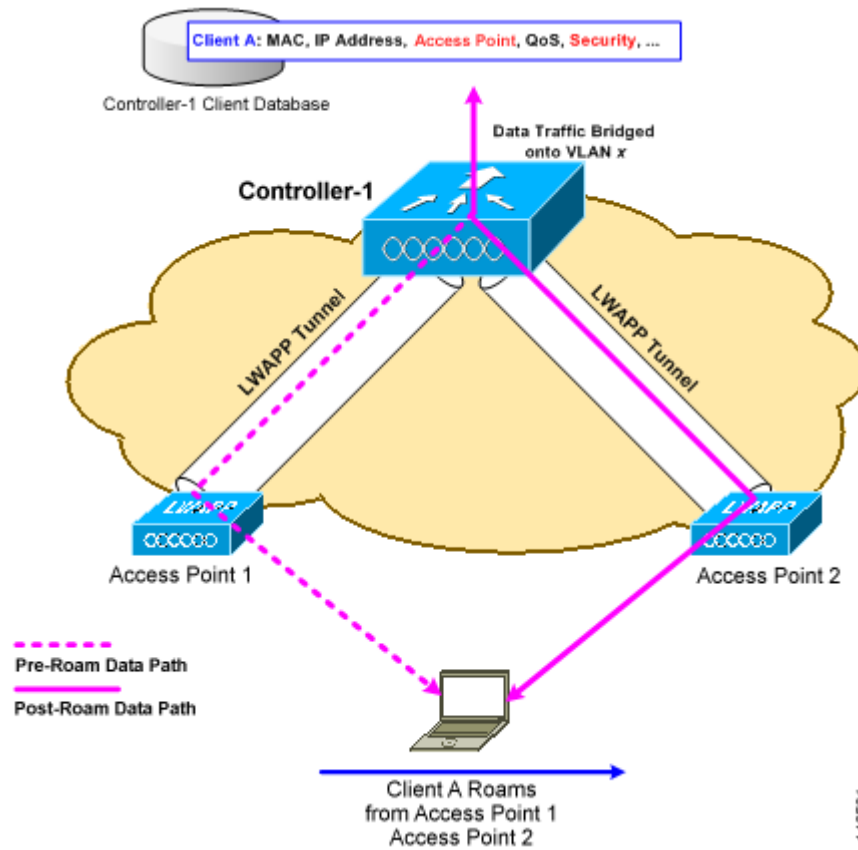
- [Information About Mobility, page 8-1](#)
- [Symmetric Tunneling, page 8-5](#)
- [Overview of Mobility Groups, page 8-5](#)
- [Configuring Mobility Groups, page 8-8](#)
- [Mobility Anchors, page 8-12](#)
- [Configuring Multiple Country Codes, page 8-14](#)
- [Configuring Controller Config Groups, page 8-16](#)
- [Reporting Config Groups, page 8-22](#)
- [Downloading Software, page 8-22](#)

Information About Mobility

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client. [Figure 8-1](#) illustrates a wireless client roaming from one access point to another when both access points are joined to the same controller.

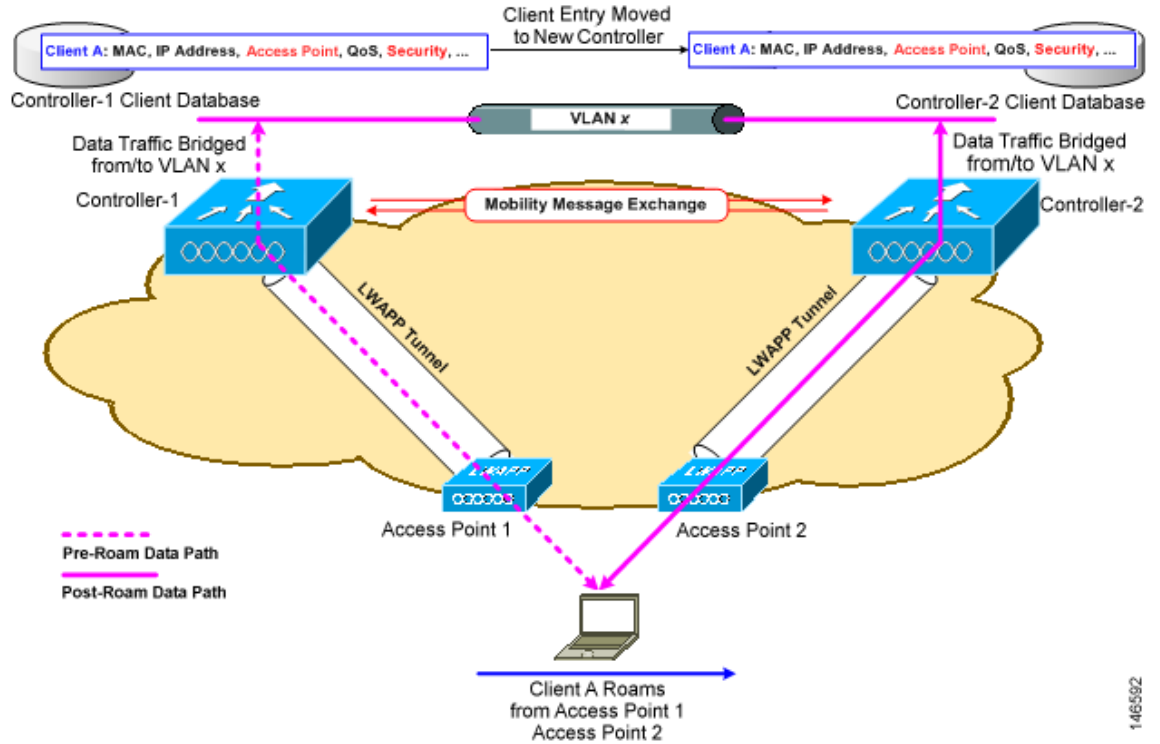
Figure 8-1 Intra-Controller Roaming



When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. The process also varies based on whether the controllers are operating on the same subnet. Figure 8-2 illustrates *inter-controller roaming*, which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.

Figure 8-2 Inter-Controller Roaming



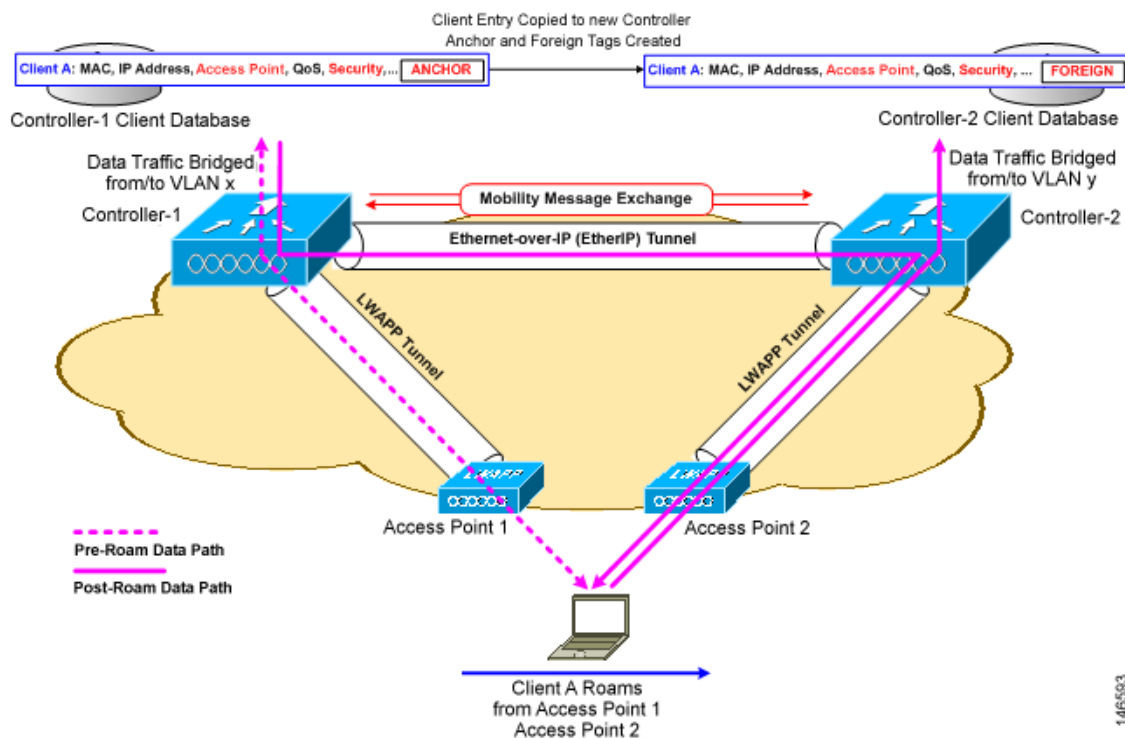
When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

**Note**

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.

Figure 8-3 illustrates *inter-subnet roaming*, which occurs when the wireless LAN interfaces of a controller are on different IP subnets.

Figure 8-3 Inter-Subnet Roaming



Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

Note

Currently, multicast traffic cannot be passed during inter-subnet roaming. In other words, avoid designing an inter-subnet network for Spectralink phones that need to send multicast traffic while using push to talk.

Note

Both inter-controller roaming and inter-subnet roaming require the controllers to be in the same mobility group. See the next two sections for a description of mobility groups and instructions for configuring them.

Symmetric Tunneling

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. You enable or disable symmetric tunneling by choosing **Configure > Controller** and then **System > General** from the left sidebar menu.



Note All controllers in a mobility group should have the same symmetric tunneling mode.



Note For symmetric tunneling to take effect, a reboot is required.

With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

See the [“Configuring Controller Templates” section on page 11-4](#) for instructions on configuring this feature within a template.

Overview of Mobility Groups

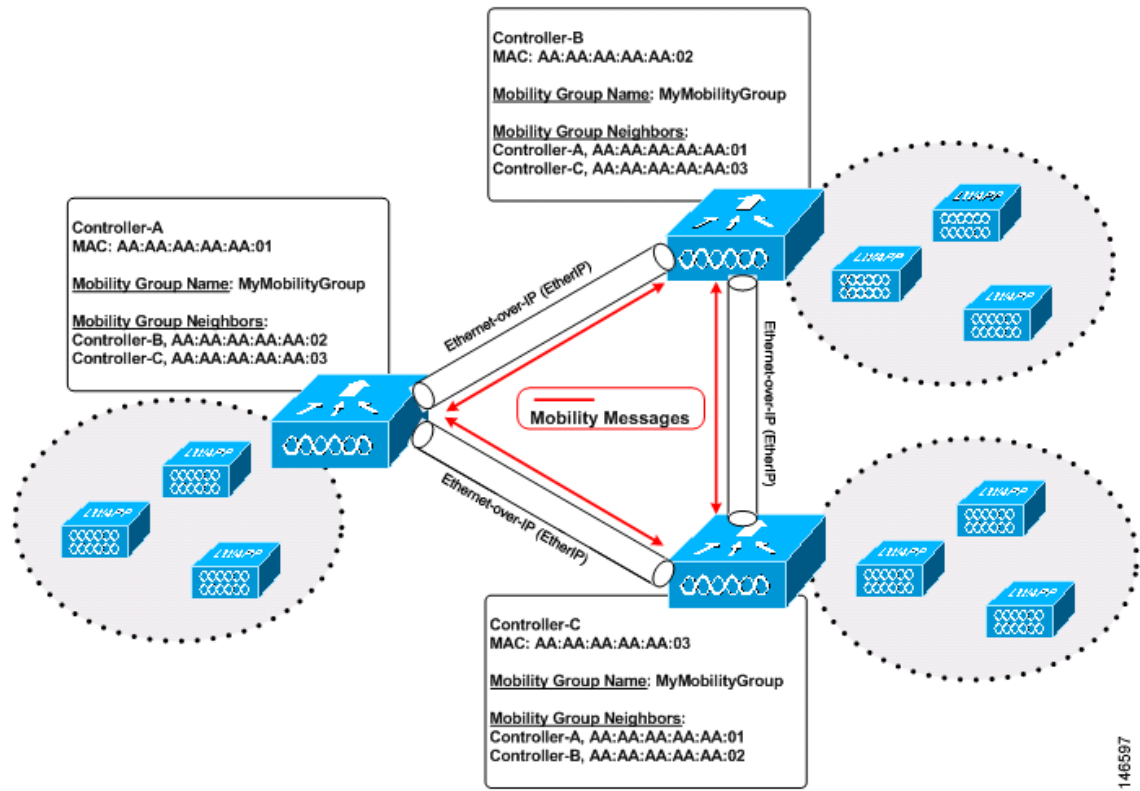
A set of controllers can be configured as a *mobility group* to allow seamless client roaming within a group of controllers. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.



Note Clients do not roam across mobility groups.

[Figure 8-4](#) shows an example of a mobility group.

Figure 8-4 A Single Mobility Group



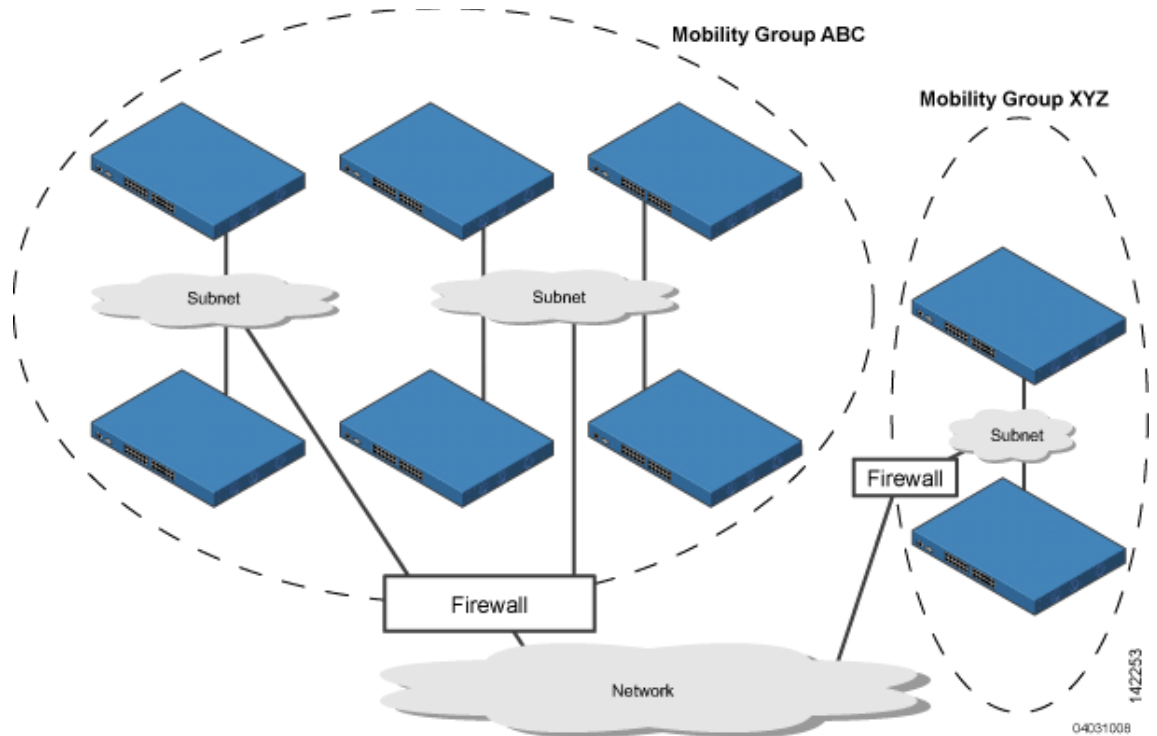
As shown in [Figure 8-4](#), each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points ($24 * 100 = 2400$ access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points ($12 * 25 + 12 * 50 = 300 + 600 = 900$ access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. [Figure 8-5](#) shows the results of creating distinct mobility group names for two groups of controllers.

Figure 8-5 Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

**Note**

Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

When to Include Controllers in a Mobility Group

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Messaging among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In NCS and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list
The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In NCS and controller software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in controller software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.
- Sending Mobile Announce messages using multicast instead of unicast
In NCS and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, PMK Update, AP List Update, and IDS Shun) are meant for all members in the group. In NCS and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, We recommend that it be enabled or disabled on all group members.

Configuring Mobility Groups

This section provides instructions for configuring mobility groups.



Note

You can also configure mobility groups using the controller. See the *Cisco Wireless LAN Controller Configuration Guide* for instructions.

Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same LWAPP transport mode (Layer 2 or Layer 3).



Note

You can verify and, if necessary, change the LWAPP transport mode in the System > General page.

- IP connectivity must exist between the management interfaces of all devices.



Note

You can verify IP connectivity by pinging the controllers.

- All controllers must be configured with the same mobility group name.



Note

For the Cisco WiSM, both controllers should be configured with the same mobility group name for seamless routing among 300 access points.

- All devices must be configured with the same virtual interface IP address.

**Note**

If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming might appear to work, but the hand-off does not complete, and the client loses connectivity for a period of time.

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you configure all controllers with the MAC address and IP address of all the other mobility group members.

**Note**

You can find the MAC and IP addresses of the other controllers to be included in the mobility group in the **Configure > Controllers** page.

To add each WLC controller into mobility groups and configure them, follow these steps:

- Step 1** Choose **Configure > Controllers** (see [Figure 8-6](#)).

Figure 8-6 *Configure > Controllers*

IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Life Cycle State	Reachability Status	Audit Status
9.1.192.50	COMMON-5500-2	5500		7.0.116.0	ram	Device is managed and synchronized	Reachable	Not Available
9.1.96.40	ATN2106	WLC2106		7.0.116.0	pdmm	Device is managed and synchronized	Reachable	Not Available
9.1.72.40	RK4402	4400		7.0.116.0	Ramesh	Device is managed and synchronized	Reachable	Not Available
9.1.120.11	RB5500	5500		7.0.116.0	ra	Device is managed and synchronized	Reachable	Not Available
9.1.189.40	COMMON-4400-3	4400		7.0.114.107	ram	Device is managed and synchronized	Reachable	Not Available
9.1.122.11	RB2100	WLC2106		7.0.116.0	auto2100	Device is managed and synchronized	Reachable	Not Available
9.1.73.50	RK5508	5500		7.0.116.0	TEST_GROUP	Device is managed and synchronized	Reachable	Not Available
9.1.104.40	SR4404	4400		7.0.116.0	w	Device is managed and synchronized	Reachable	Not Available
9.1.121.11	RB4400	4400		7.0.116.0	RamarB	Device is managed and synchronized	Reachable	Not Available
9.1.105.40	SR5508	5500		7.0.98.0	test_group	Device is managed and synchronized	Reachable	Not Available

This page shows the list of all the controllers you added in Step 1. The mobility group names and the IP address of each controller that is currently a member of the mobility group is listed.

- Step 2** Choose the first controller by clicking the WLC IP address. You then access the controller templates interface for the controller you are managing.
- Step 3** Choose **System > Mobility Groups** from the left sidebar menu. The existing Mobility Group members are listed in the page (see [Figure 8-7](#)).

Figure 8-7 Existing Mobility Groups

The screenshot shows the Cisco Prime Network Control System interface. The left sidebar contains a navigation menu with 'Mobility Groups' selected. The main content area displays a table of existing mobility groups. The table has the following columns: Controller Name, Member MAC Address, Member IP Address, Multicast Address, and Group Name. There is one entry in the table: COMMON-5500-2, 68:ef:bd:8e:5c:00, 9.1.192.50, 0.0.0.0, and (Local). The interface also shows a search bar and navigation controls at the top.

- Step 4** You see a list of available controllers. From the Select a command drop-down list in the upper right-hand corner, choose **Add Group Members** and then click **Go**.
- Step 5** If no controllers were found to add to the mobility group, you can add the members manually by clicking the “To add members manually to the Mobility Group click here” link. The Mobility Group Member page appears (see Figure 8-8).

Figure 8-8 Mobility Group Member Page

The screenshot shows the Cisco Prime Network Control System interface for the 'Mobility Groups Details' page. The page title is 'Mobility Groups Details' and the breadcrumb is 'Configure > Controllers > 9.1.192.50 > System > Mobility Groups > Mobility Groups Details'. The main content area shows a form for adding a member to the mobility group. The form has the following fields: Member MAC Address (68:ef:bd:8e:5c:00), Member IP Address (209.165.200.224), Multicast Address (0.0.0.0), and Group Name (Group1). There are 'Save' and 'Cancel' buttons at the bottom of the form. The interface also shows a search bar and navigation controls at the top.

- Step 6** In the Member MAC Address text box, enter the MAC address of the controller to be added.
- Step 7** In the Member IP Address text box, enter the management interface IP address of the controller to be added.



Note If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the management interface IP address of the controller. Otherwise, mobility fails among controllers in the mobility group.

- Step 8** Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The group address of the local mobility member must be the same as the group address of the local controller.
- Step 9** In the Group Name text box, enter the name of the mobility group.
- Step 10** Click **Save**.
- Step 11** Repeat the Steps 1 through 9 for the remaining WLC devices.

Setting the Mobility Scalability Parameters

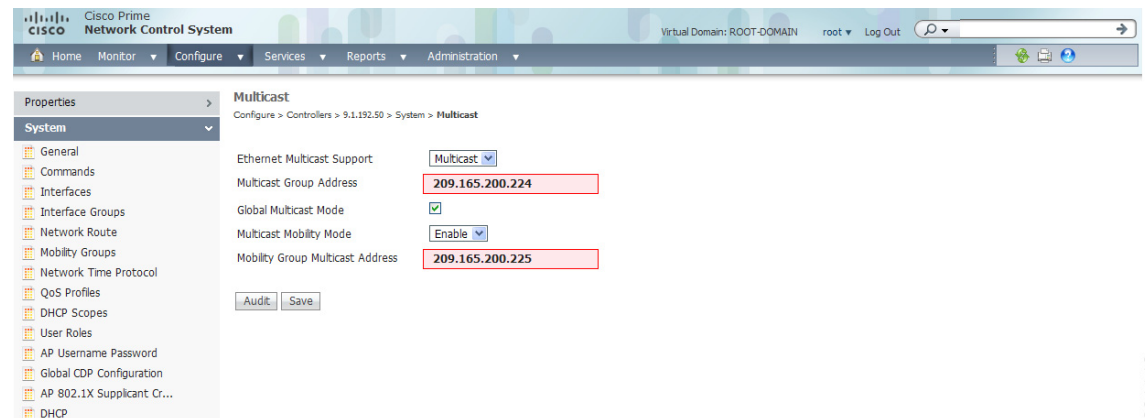
To set the mobility message parameters, follow these steps:



Note You must complete the steps in the “[Configuring Mobility Groups](#)” section on page 8-8 prior to setting the mobility scalability parameters.

- Step 1** Choose **Configure > Controllers**.
- Step 2** Choose an IP address of a controller whose software version is 5.0 or later.
- Step 3** Choose **System > Multicast** from the left sidebar menu. The Multicast page appears (see [Figure 8-9](#)).

Figure 8-9 Multicast Page



- Step 4** From the Ethernet Multicast Support drop-down list, specify if you want to disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members. Otherwise, you can choose **Multicast** or **Unicast** from the drop-down list.
- Step 5** If you chose multicast in Step 4, you must enter the group IP address at the Multicast Group Address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group, but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.
- Step 6** Select the **Global Multicast Mode** check box to make the multicast mode available globally.
- Step 7** Select the **Enable IGMP Snooping** check box to enable IGMP snooping.

291113

Step 8 Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 9 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 10 Select the **Multicast Direct** check box to enable videos to be streamed over a wireless network.

Step 11 Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

- a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client
- b. URL—A web address reported to the client
- c. Email—An e-mail address reported to the client
- d. Phone—A telephone number reported to the client
- e. Note—A note reported to the client



Note All media streams on a controller share this configuration.

Step 12 Click **Save**.

Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

**Note**

A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controller can have a 4100 series controller or a 4400 series controller as its anchor.

**Note**

The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Configuring Mobility Anchors

To create a new mobility anchor for a WLAN, follow these steps:

- Step 1** Choose **Configure > Controllers**.
- Step 2** Choose a controller by clicking an IP address.
- Step 3** Choose **WLANs > WLAN Configuration** from the left sidebar menu.
- Step 4** Select the check box of the desired WLAN ID URL (see [Figure 8-10](#)).

Figure 8-10 WLAN Page

WLAN ID	Profile_Name	SSID	WLAN/Guest/Remote LAN	Security Policies	Status	Task List
<input type="checkbox"/> 1	ram	ram	WLAN	[WPA2] [Auth(802.1X)]	Enabled	N/A

- Step 5** After choosing a WLAN ID, a tabbed page appears (see [Figure 8-11](#)). Click the **Advanced** tab.

Figure 8-11 Advanced Page

The screenshot shows the 'New Controller Template' configuration page in the Cisco Prime Network Control System. The 'Advanced' tab is selected, displaying various configuration options. The left sidebar shows a navigation menu with categories like System, WLANs, H-REAP, Security, 802.11, 802.11a/n, 802.11b/g/n, Mesh, Management, CLI, and Location. The main content area is divided into sections: General, Security, QoS, and Advanced. The Advanced section includes settings for H-REAP Local Switching, H-REAP Local Auth, Diagnostic Channel, Aronet IE, IPv6, Session Timeout, Coverage Hole Detection, Override Interface ACL, Peer to Peer Blocking, Client Exclusion, Timeout Value, Media Session Snooping, Passive Client, DTIM Period, DHCP, Management Frame Protection (MFP), Load Balancing and Band Select, and NAC. The DTIM Period section shows values for 802.11a/n (1-255) and 802.11b/g/n (1-255) both set to 1 ms. The DHCP section has checkboxes for DHCP Server (Override) and DHCP Address Assignment (Required). The MFP section has checkboxes for MFP Signature Generation (Enable) and MFP Client Protection (Enabled). The Load Balancing and Band Select section has checkboxes for Client Load Balancing (Enable) and Client Band Select (Enable). The NAC section has a dropdown for NAC State set to None. At the bottom, there are 'Save' and 'Cancel' buttons.

291115

- Step 6** Click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears.
- Step 7** Select the **IP address** check box of the controller to be designated a mobility anchor, and click **Save**.
- Step 8** Repeat [Step 6](#) and [Step 7](#) to set any other controllers as anchors for this WLAN.
- Step 9** Configure the same set of anchor controllers on every controller in the mobility group.

Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.



Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose **Configure > Controllers**, select the desired controller you want to disable, choose **802.11a/n** or **802.11b/g/n** from the left sidebar menu, and then choose **Parameters**. The Network Status is the first check box.



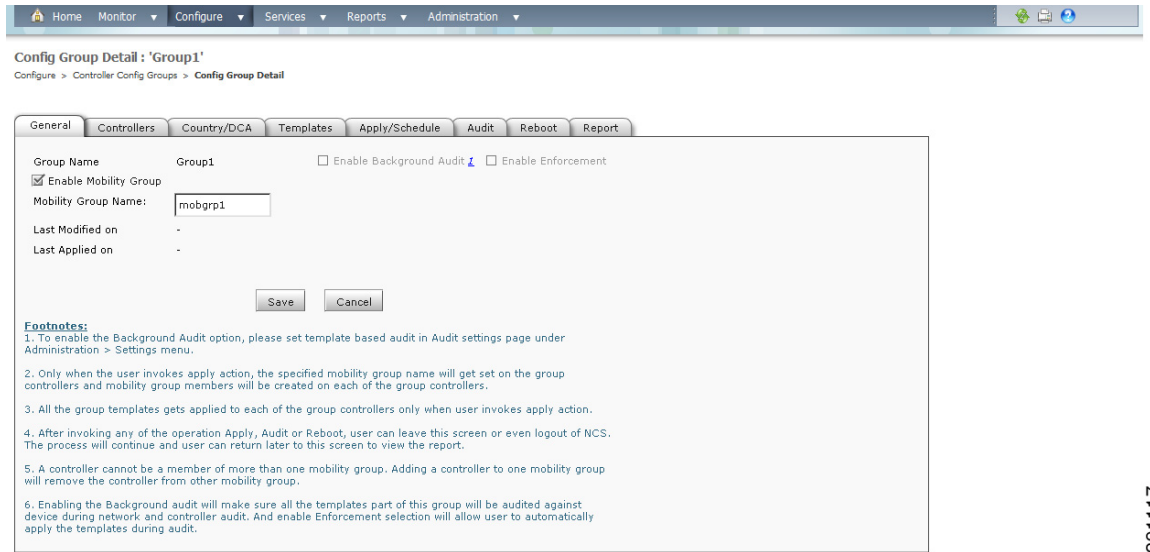
Note To configure multiple country codes outside of a mobility group, see the [“Configuring Security Parameters”](#) section on page 9-85.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

- Step 1** Choose **Configure > Controller Config Groups**.

- Step 2** Choose **Add Config Groups** from the Select a command drop-down list, and click **Go**.
- Step 3** Create a config group by entering the group name and mobility group name.
- Step 4** Click **Save**. The Config Groups page appears (see [Figure 8-12](#)).

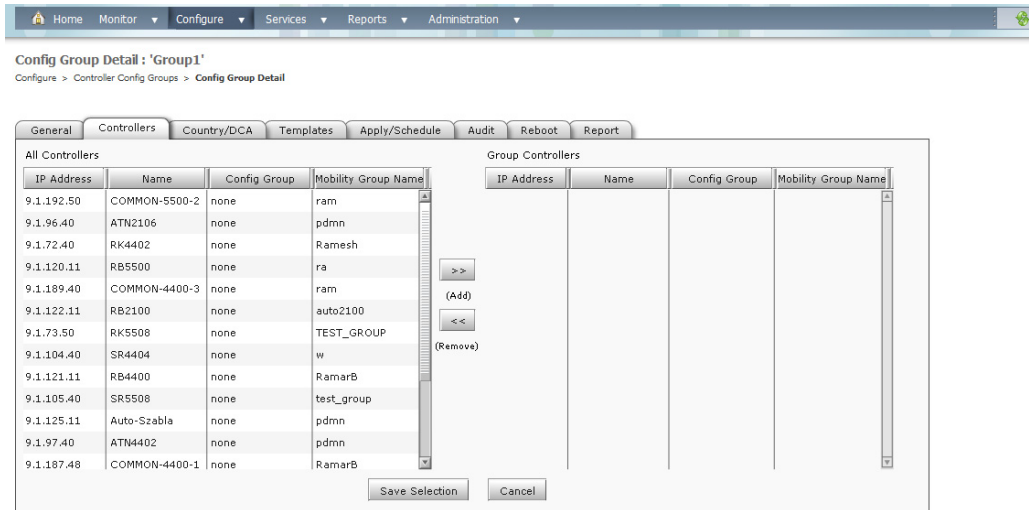
Figure 8-12 Config Groups Page



291117

- Step 5** Click the **Controllers** tab. The Controllers page appears (see [Figure 8-13](#)).

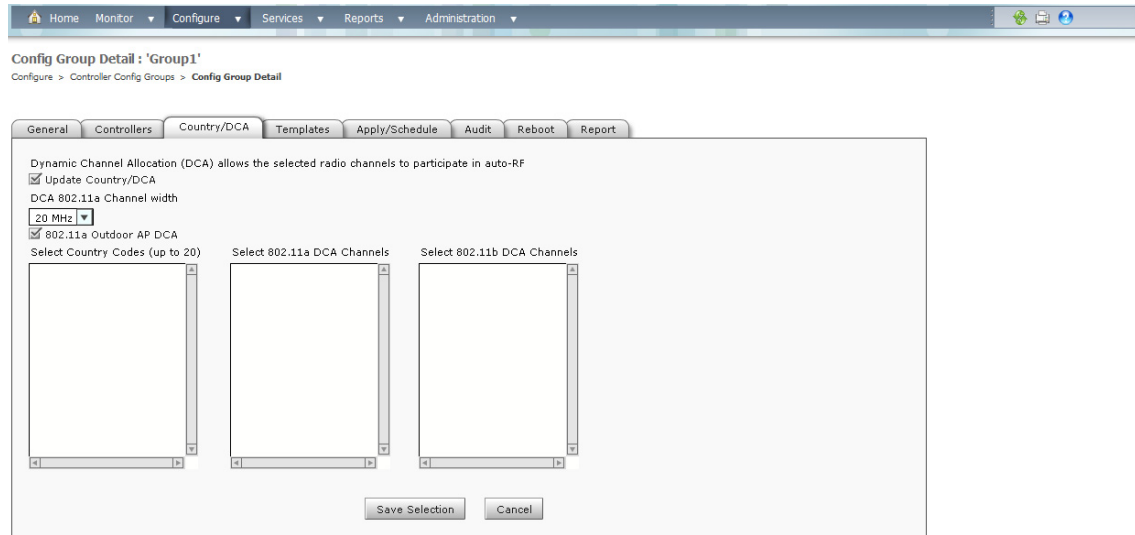
Figure 8-13 Controllers Tab



291118

- Step 6** Highlight the controllers you want to add, and click **Add**. The controller is added to the Group Controllers page.
- Step 7** Click the **Country/DCA** tab. The Country/DCA page appears (see [Figure 8-14](#)). Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Figure 8-14 Country/DCA Tab



291119

- Step 8** Select the **Update Country/DCA** check box to display a list of countries from which to choose.
- Step 9** Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection**.



Note A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Configuring Controller Config Groups

By creating a config group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected config groups.



Note A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

For information about applying templates to either individual controllers or controllers in selected Config Groups, see the [“Using Templates” section on page 11-1](#).

By choosing Configure > Controller Config Groups, you can view a summary of all config groups in the NCS database. When you choose Add Config Groups from the Select a command drop-down list, the page displays a table with the following columns:

- Group Name: Name of the config group.

- Templates: Number of templates applied to config group.

Adding New Group

To add a config group, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**.
- Step 2** From the Select a command drop-down list, choose **Add Config Group**, and click **Go**. The Add New Group page appears.
- Step 3** Enter the new config group name. It must be unique across all groups. If Enable Background Audit is selected, the network and controller audits occur for this config group. If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.



Note If the Enable Background Audit option is chosen, the network and controller audit is performed on this config group.

- Step 4** Other templates created in NCS can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:
- Select and add later: Click to add a template at a later time.
 - Copy templates from a controller: Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.



Note The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.



- Step 5** Click **Save**. The Config Groups page appears (see [Figure 8-15](#)).

Figure 8-15 *Config Groups Page*



Configuring Config Groups


To configure a config group, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column. The Config Group page shown in [Figure 8-15](#) appears.
- Step 2** Click the **General** tab. The following options for the config group appear:
- Group Name: Name of the config group
 - Enable Background Audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
 - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.
-
-  **Note** The audit and enforcement of the config group template happens when the selected audit mode is *Template based audit*.
-
- Enable Mobility Group—If selected, the mobility group name is pushed to all controllers in the group.
 - Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here.
-
-  **Note** A controller can be part of multiple config groups.
-
- Last Modified On: Date and time config group was last modified.
 - Last Applied On: Date and time last changes were applied.
- Step 3** You must click the **Apply/Schedule** tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.
- Step 4** Click **Save**.
-

Adding or Removing Controllers from a Config Group

To add or remove controllers from a config group, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
- Step 2** Click the **Controllers** tab. The columns in the table display the IP address of the controller, the config group name the controller belongs to, and the mobility group name of the controller.
- Step 3** Click to highlight the row of the controller you want to add to the group.
- Step 4** Click **Add**.

 **Note** If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click **Remove**.

- Step 5** You must click the **Apply/Schedule** tab, and click **Apply** to add or remove the controllers to the config groups.
- Step 6** Click **Save Selection**.
-

Adding or Removing Templates from the Config Group

To add or remove templates from the config group, follow these steps:

- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
- Step 2** Click the **Templates** tab. The Remaining Templates table displays the item number of all available templates, the template name, and the type and use of the template.
- Step 3** Click to highlight the row of the template you want to add to the group.
- Step 4** Click **Add** to move the highlighted template to the Group Templates column.



Note If you want to remove a template from the group, highlight the template in the Remaining Templates box, and click **Remove**.

- Step 5** You must click the **Apply/Schedule** tab, and click **Apply** to add or remove the templates to the config groups.
- Step 6** Click **Save Selection**.

Applying or Scheduling Config Groups



Note The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all the controllers in a config group, follow these steps:

- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
- Step 2** Click the **Apply/Schedule** tab to access this page.
- Step 3** Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this page or log out of NCS. The process continues, and you can return later to this page to view a report.



Note Do not perform any other config group functions during the apply provisioning.

A report is generated and appears in the Recent Apply Report page. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.



Note If you want to print the report as shown on the page, you must choose landscape page orientation.

- Step 4** Enter a starting date in the text box or use the calendar icon to choose a start date.
 - Step 5** Choose the starting time using the hours and minutes drop-down lists.
 - Step 6** Click **Schedule** to start the provisioning at the scheduled time.
-

Auditing Config Groups

The Config Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this screen or log out of NCS. The process continues, and you can return to this page later to view a report.

**Note**

Do not perform any other config group functions during the audit verification.

To perform a config group audit, follow these steps:

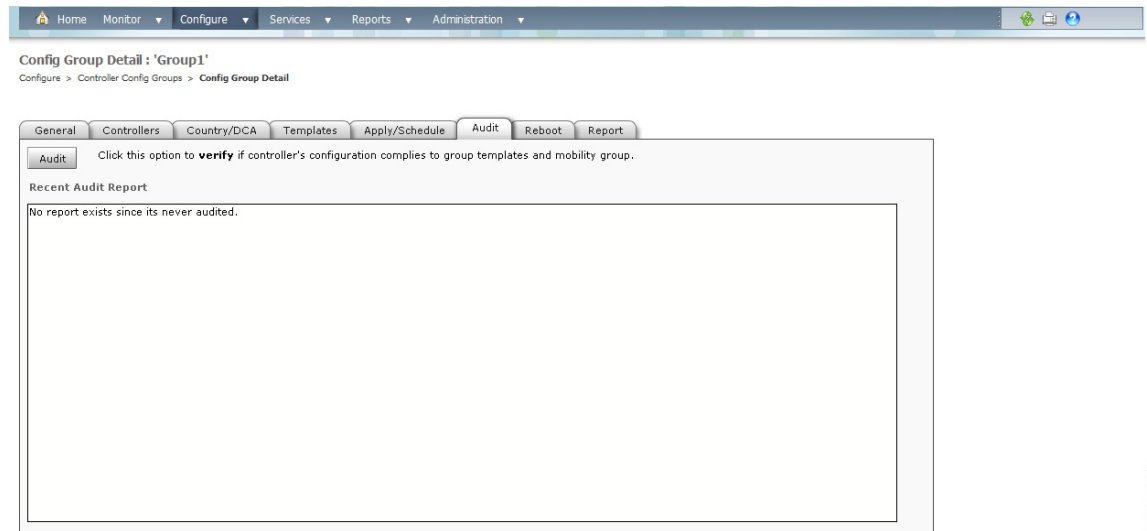
- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
- Step 2** Click the **Audit** tab to access this page.
- Step 3** Click to highlight a controller from the Controllers tab, choose >> (**Add**), and **Save Selection**.
- Step 4** Click to highlight a template from the Templates tab, choose >> (**Add**), and **Save Selection**.
- Step 5** Click **Audit** to begin the auditing process (see [Figure 8-16](#)).

A report is generated and the current configuration on each controller is compared with that in the config group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

**Note**

This audit does not enforce the NCS configuration to the device. It only identifies the discrepancies.

Figure 8-16 Config Groups Audit Tab



001101

- Step 6** Click **Details** to view the Controller Audit Report details.
- Step 7** Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in NCS, and its value in the controller.



Note Click **Retain NCS Value** to push all attributes in the Attribute Differences page to the device.

- Step 8** Click **Close** to return to the Controller Audit Report page.

Rebooting Config Groups

To reboot a config group, follow these steps:

- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
- Step 2** Click the **Reboot** tab.
- Step 3** Select the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.
- Step 4** Click **Reboot** to reboot all controllers in the config group at the same time. During the reboot, you can leave this page or logout of NCS. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If NCS is unable to reboot the controller, a failure is shown.



Note If you want to print the report as shown on the page, you must choose landscape page orientation.

Reporting Config Groups

To display all recently applied reports under a specified group name, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.
 - Step 2** Click the **Report** tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:
 - Apply Status—Indicates success, partial success, failure, or not initiated.
 - Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
 - Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
 - Details—Click **Details** to view the individual failures and associated error messages.
 - Step 3** If you want to view the scheduled task reports, click the **click here** link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Config Group menu where you can view reports of the scheduled config groups.
-

Downloading Software

To download software to all controllers in the selected groups after you have a config group established, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**.
 - Step 2** Select the check box to choose one or more config groups names on the Config Groups page.
 - Step 3** Choose **Download Software** from the Select a command drop-down list, and click **Go**.
 - Step 4** The Download Software to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.
 - Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
 - Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
 - Step 7** The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds **_custom.sgi** as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.
 - Step 8** Click **OK**.
-

Downloading IDS Signatures

To download Intrusion Detection System (IDS) signature files from your config group to a local TFTP server, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**.
 - Step 2** Select the check box to choose one or more config groups on the Config Groups page.
 - Step 3** Choose **Download IDS Signatures** from the Select a command drop-down list, and click **Go**.
 - Step 4** The Download IDS Signatures to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.
 - Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
 - Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
 - Step 7** The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds **_custom.sgi** as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.
 - Step 8** Click **OK**.
-

Downloading Customized WebAuth

To download customized web authentication, follow these steps:

-
- Step 1** Choose **Configure > Controller Config Groups**.
 - Step 2** Select the check box to choose one or more config groups on the Config Groups page.
 - Step 3** Choose **Download Customized WebAuth** from the Select a command drop-down list, and click **Go**.
 - Step 4** The Download Customized Web Auth Bundle to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed.
 - Step 5** Choose **local machine** from the File is Located On field.
-

