CHAPTER 14

Working with Device Configurations

Cisco Prime Infrastructure archives device configurations and provides information such as the date of last configuration change, status of the configuration jobs, and allows you to compare current and previous configurations. Prime Infrastructure also allows you to roll back to a previously saved configuration in the archive if a configuration deployment fails.

Configuration Archives

Prime Infrastructure attempts to collect and archive the following device configuration files:

- Startup configuration
- Running configuration
- VLAN configuration, if configured

A configuration archive is created if there is a change between the last archived configuration and the current configuration only. You can specify how Prime Infrastructure archives the configurations:

- On demand—You can have Prime Infrastructure collect the configurations of selected devices by choosing **Operate > Configuration Archives**.
- Scheduled—You can schedule when Prime Infrastructure collects the configurations of selected devices and specify recurring collections by choosing **Operate > Configuration Archives**, then clicking **Schedule Archive**.
- During inventory—You can have Prime Infrastructure collect device configurations during the inventory collection process. See Changing Prime Infrastructure Device Configuration Settings for more information.
- Based on Syslogs— If device is configured to send syslogs, when there is any device configuration change, Prime Infrastructure collects and stores the configuration.

Changing Prime Infrastructure Device Configuration Settings

By default, Prime Infrastructure has the following configuration settings:

- Does not back up the running configuration before pushing configuration changes to a device.
- Does not attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails
- When pushing CLI to a device, uses 5 thread pools.

To change the default configuration settings:

Step 1 Choose **Administration > System Settings**, then click **Configuration**.

- Click **Backup Running Configuration** to have Prime Infrastructure back up the running configuration before pushing configuration changes to a device.
- Click **Rollback Configuration** to have Prime Infrastructure attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails.

Step 2 Click **Save**.

Comparing Current and Previous Device Configurations

To compare a current device configuration with a previous version:

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Click the expand icon for the device whose configuration you want to view. Then click the expand icon again to view the specific configuration version that you want to compare.

Step 3 Under the Compare With column, choose the configuration for which you want to compare the configuration you selected in the previous step.

The color key at the bottom of the report shows the differences between the configurations.

Overview of Device Configurations

You can change a device's configuration in two ways:

- **Operate > Device Work Center**—Use the Device Work Center to change the configuration of a single device. See Changing a Single Device Configuration.
- **Design > Configuration Template**—To change the configuration of more than one device and apply a common set of changes, use a configuration template to make the changes.

  Prime Infrastructure provides the following default configuration templates:

  - CLI templates—CLI templates are user-defined and created based on your own parameters. CLI templates allow you to select the elements in the configurations. Prime Infrastructure provides variables which you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See Creating CLI Configuration Templates.
  - Feature and technology templates—Feature templates are configurations that are specific to a feature or technology in a device's configuration. See Creating Features and Technologies Templates.
  - Composite templates—Composite templates are two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See Creating Composite Templates.

Changing a Single Device Configuration

Step 1 Choose **Operate > Device Work Center**, then click a device name.

The device details appear in the lower part of the page.

Step 2 Click the **Configuration** tab.

The Feature Selector displays the values, organized into features, for the device you selected.

Step 3 Select the feature that you want to change, then make the necessary changes.

Step 4 Click **Save** to save your configuration changes in the Prime Infrastructure database. (To view the status of the configuration change, choose **Administration > Jobs Dashboard**.)

Adding a Wireless LAN Controller

The Cisco Unified Wireless Network (CUWN) solution is based on Wireless LAN Controllers running Airespace Operating System. The wireless LAN controller models include 2100, 2500, 4400, WiSM/WiSM2 (6500 service module), 5500, 7500, 8500. In this solution, access points tunnel the wireless traffic to the controllers through CAPWAP.

The Cisco Unified Access (UA) Wireless Solution is new architecture that provides a converged model where you can manage your wired and wireless network configurations in the same place. This solution includes the 3850 series switch with integrated wireless support. The solution also includes the 5760 series wireless controller, which can act as an aggregation point for many 3850 switches. This platform is based on IOS-XE, so the command structure is similar to other IOS products. In this solution, the wireless traffic can terminate directly on the 3850 switch, so that it can be treated in a similar mode to a wired connection on the switch.

Step 1 Choose **Operate > Device Work Center**.

Step 2 Click **Add**. The Add Device page appears.

Step 3 In the Add Device page, enter the necessary parameters.

Step 4 Click **Add**.

Changing Wireless LAN Controller Configuration Settings

Step 1 Choose **Operate > Device Work Center**.

Step 2 Expand Device Type, and then click **Wireless Controller**.

Step 3 Select the controller that you want to change. The Device Work Center contains configuration functions at the bottom of the page. For details, see the Device Work Center.

Step 4 Click the **Configure** tab, then make the necessary changes.

Step 5 Click **Save**.

Rebooting Controllers

Step 1 Choose **Operate > Device Work Center**.

Step 2 Expand Device Type, and then click **Wireless Controller**.

Step 3 Select the check box(es) of the applicable controller(s).

Step 4 From the Reboot drop-down list, choose **Reboot Controllers**.

Note Save the current controller configuration prior to rebooting.

Step 5 Select the Reboot Controller options that must be applied.

- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
- Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

Note Options are disabled unless the Reboot APs check box is selected.

Step 6 Click **OK** to reboot the controller with the optional configuration selected.

Configuration Rollbacks

You can change the configuration on a device with a configuration stored in Prime Infrastructure. You can select multiple archived versions or a single archived version to which you want to "rollback."

During the configuration rollback process, the configuration is converted into a set of commands which are them executed sequentially on the device.

When rolling back a configuration file you can specify the following options:

- The type of configuration file to which to rollback, for example running or startup configuration
- Whether to sync the running and startup configurations after rolling back the running configuration
- If rolling back a startup configuration only, specify to reboot the device so that startup configuration becomes the running configuration
- Before rolling back the configuration, specify whether to create new archived versions

Rolling Back Device Configuration Versions

You can use Prime Infrastructure to rollback a device's configuration to a previous version of the configuration.

To roll back a configuration change.

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Click the expand icon for the device whose configuration you want to roll back.

Step 3 Click the specific configuration version that you want to roll back, then click **Schedule Rollback**.

Step 4 Specify the rollback and scheduling options.

Step 5 Click **Submit**.

Deleting Device Configurations

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives a configuration change event

You cannot delete configuration versions, but older configuration versions are replaced by newer configuration versions.

To change the number of configurations that Prime Infrastructure retains:

Step 1 Choose **Administration > System Settings**, then click **Configuration Archive**.

Step 2 Enter a new value in the Number of Versions field. To archive an unlimited number of configuration versions, uncheck the **Number of version to retain** and **Number of days to retain** check boxes.

Step 3 Click **Save**.

Configuring Redundancy on Controllers

The term Redundancy in the Prime Infrastructure refers to the high availability (HA) framework in Cisco WLC. Redundancy in wireless networks allows you to reduce the downtime of the networks. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the controller in the Active state through a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing ordered unique device identifier (UDI). A controller with redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.

Note The stateful switchover of clients is not supported, which means that all clients, with the exception of clients on locally switched WLANs on access points in FlexConnect mode, are deauthenticated and forced to reassociate with the new controller in the Active state.

Prerequisites and Limitations for Redundancy

Before configuring Redundancy, you must consider the following prerequisites and limitations:

- The Redundancy is supported only on the 5500, 7500, 8500, and WiSM2 controllers.
- The primary and secondary controllers must be of the same hardware model.
- The primary and secondary controllers must be running the same Controller software release.
- The IP addresses of the Management, Redundancy Management, and Peer Redundancy Management interfaces must be in the same subnet.
- The service port IP address and route information is maintained for each device.
- If the Redundancy is enabled on a controller, the Prime Infrastructure or any other device cannot manage the standby controller.
- You cannot enable the Redundancy on a controller, if the controller is added to the Prime Infrastructure through the service port. You must delete the controller and add it through the management interface to enable the Redundancy on that controller.
- When there is an audit mismatch between a controller and the Prime Infrastructure, you must not restore the Redundancy parameters from the Prime Infrastructure on to the controller. However, you can refresh the Redundancy Parameters in the Prime Infrastructure.
- Before you enable the Redundancy, you must download the certificates for each device.
- Configuration is downloaded from the network to the active controller, and then the details are transferred to the standby controller through the Redundancy interface.
- When an old active controller pairs up with the new active controller, the control is not transferred back to the old active controller and it becomes the standby controller for the new active controller.

Configuring Redundancy Interfaces

There are two Redundancy interfaces—redundancy-management interface and redundancy-port interface. The redundancy-management interface is a local physical management interface that shares the subnet mask, gateway, and VLAN ID from the management interface. You must configure only the IP address for the redundancy management interface to enable Redundancy on the primary and secondary controllers. The IP address for the redundancy-port interface is auto-generated and it is used internally.

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the controller that you have chosen as the primary controller. The details of the device appear on the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **System > Interfaces**. The Interfaces list page appears.

Step 6 Click the **redundancy-management** interface. The redundancy-management interface details page appears.

Step 7 In the IP Address field, enter an IP address that belongs to the management interface subnet.

Step 8 Click **Save**.

Note You can also configure the IP address of the Redundancy Management in the Global Configuration details page. Choose **Operate > Device Work Center> Device Type > Wireless Controller >** *Controller* **> Configuration > Redundancy > Global Configuration** to access the Global Configuration details page.

Configuring Redundancy on a Primary Controller

To configure redundancy on a primary or active controller:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.

Step 6 You must configure the following parameters before you enable the Redundancy Mode for the primary controller:

- Redundancy-Management IP—The IP address of the local physical management interface, which you had configured in the redundancy-management interface details page is displayed. You can also modify the IP address.
- Peer Redundancy-Management IP—Enter the IP address of the peer redundancy management interface.
- Redundant Unit—Choose **Primary**.
- Mobility MAC Address—Enter the virtual MAC address for the Redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.

Step 7 Click **Save**. The Enabled check box for the Redundancy Mode becomes available for editing.

Step 8 Select the **Enabled** check box for the Redundancy Mode to enable the Redundancy on the primary controller.

Note After you enable the Redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address.

Note You cannot configure this controller during the Redundancy pair-up process.

Step 9 Click **Save**. The configuration is saved and the system reboots.

Configuring Redundancy on a Secondary Controller

To configure Redundancy on a secondary or standby controller:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the controller that you have chosen as a secondary controller. The details of the controller appear on the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration Details page appears.

Step 6 You must configure the following parameters before you enable the Redundancy Mode for the secondary controller:

- Redundancy-Management IP—Enter the IP address of the local physical management interface. This IP address must be the same as the IP address of the peer redundancy management interface of the primary controller.
- Peer Redundancy-Management IP—Enter the IP address of the peer physical management interface. This IP address must be the same as the IP address of the local physical management interface of the primary controller.
- Redundant Unit—Choose **Secondary**.
- Mobility MAC Address—Enter the virtual MAC address of the Redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.

Step 7 Click **Save**. The Enabled check box for the Redundancy Mode becomes available for editing.

Step 8 Select the **Enabled** check box for the Redundancy Mode to enable the Redundancy on the secondary controller.

Note After you enable the Redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address.

Note You cannot configure the primary controller during the Redundancy pair-up process.

Step 9 Click **Save**. The configuration is saved and the system reboots.

Monitoring and Troubleshooting the Redundancy States

After the Redundancy mode is enabled on the primary and secondary controllers, the system reboots. The Redundancy state for both the controllers becomes Enabled in the Wireless Controller Members list page. The following traps are triggered:

- RF_SWITCHOVER_ACTIVITY—This trap is triggered when the standby controller becomes the new active controller. For more information about this trap, see the "RF_SWITCHOVER_ACTIVITY" section on page 14-9.
- RF_PROGRESSION_NOTIFY—This trap is triggered by the primary or active controller when the peer state changes from 'Disabled' to 'StandbyCold', and then to 'StandbyHot'. For more information about this trap, see the "RF_PROGRESSION_NOTIFY" section on page 14-9.
- RF_HA_SUP_FAILURE_EVENT—This trap is triggered when the redundancy fails because of a discrepancy between the active and the standby controllers. For more information about this trap, see the "RF_HA_SUP_FAILURE_EVENT" section on page 14-10.

You can view the Redundancy state details such as the local and peer state, unit, IP addresses of the redundancy management, peer redundancy management, redundancy port, peer redundancy port, and peer service port of the paired controller. Choose **Operate > Device Work Center > Device Type > Wireless Controller >** *Controller* **> Device Details > Redundancy > Redundancy States** to view these details.

RF_SWITCHOVER_ACTIVITY

MIB Name	ciscoRFSwactNoti
Alarm Condition	Switch over activity triggered
Prime Infrastructure Message	Switch Over Activity triggered. Controller *IP addr*
Symptoms	This notification is sent by the active controller when the switch over activity is triggered
Severity	Critical
Category	Controller
Probable Causes	When the primary controller crashes or reboots, the switch over occurs and the secondary controller becomes active
Recommended Actions	None

RF_PROGRESSION_NOTIFY

MIB Name	ciscoRFProgressionNotif
Alarm Condition	Peer state of the active controller change

Prime Infrastructure Message	1. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* and peer state 'Disabled' 2. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* and peer state 'StandbyCold' 3. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* and peer state 'StandbyHot'
Symptoms	This notification is sent by the active controller when the peer state changes from 'Disabled' to 'StandbyCold', and then to 'StandbyHot'
Severity	Critical
Category	Controller
Probable Causes	1. 'Disabled'—The Redundancy is enabled on the primary controller and it is disabled in the secondary controller 2. 'StandbyCold'—The Redundancy is enabled on the secondary controller and the configuration synchronization is in progress between the primary and the secondary controllers 3. 'StandbyHot'—The Redundancy pair up process is completed
Recommended Actions	None.

RF_HA_SUP_FAILURE_EVENT

MIB Name	ciscoRFSupHAFailureEvent
Alarm Condition	Triggered when the Redundancy fails
Prime Infrastructure Message	Redundancy Failure Event trap triggered by controller *IP addr* for the reason '{1}'
Symptoms	This notification is sent when the Redundancy fails due to the discrepancy between the active and the standby controllers
Severity	Major
Category	Controller
Probable Causes	None
Recommended Actions	None

Running Redundancy Status Background Tasks

Sometimes, when the peer state changes from 'StandbyCold' to 'StandbyHot', the Redundancy traps are missed by the Prime Infrastructure. As a result, the Redundancy pair-up process cannot be completed. To fix this issue, you must run the Redundancy Status background task manually.

To run the Redundancy Status background task:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In the Other Background Tasks area, select the **Redundancy Status** background task.

Step 3 From the Select a command drop-down list, choose **Execute Now**.

Step 4 Click **Go**.

When traps are missed by the Prime Infrastructure, you must run this background task to complete the following:

- Remove the standby controller from the Prime Infrastructure.
- Swap the network route table entries with the peer network route table entries.
- Update the Redundancy state information and system inventory information.

Once the Redundancy pair-up process is completed, the Redundancy state for the active controller becomes Paired and the standby controller is removed from the Prime Infrastructure.

Configuring Peer Service Port IP and Subnet Mask

You can configure a peer service port IP address and a subnet mask only when the state of the peer controller is in 'StandbyHot'. Ensure that DHCP is disabled on local service port before you configure the peer service port IP address.

To configure the peer service port IP and subnet mask:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the primary or active controller. The details of the controller appear in the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.

Step 6 In the Peer Service Port IP field, enter the IP address of the peer service port.

Step 7 In the Peer Service Netmask IP field, enter the IP address of the peer service subnet mask.

Step 8 Click **Save**.

Adding a Peer Network Route

You can add a peer network route on an active controller only when the state of the peer controller is in 'StandbyHot'. A new network route table is maintained. When the standby controller becomes active, the entries of the network route table swaps with the entries of the peer network route table.

To add a peer network route:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Peer Network Route**.

Step 6 From the Select a command drop down list, choose **Add Peer Network Route**.

Step 7 Click **Go**. The Peer Network Route Details page appears.

Step 8 Configure the required fields.

Step 9 Click **Save**. The peer network route is added.

Administration Commands for Redundancy

When the standby controller is in the 'StandbyHot' state and the Redundancy pair-up process is completed, you can reset the standby controller using the **Reset Standby** command. Also, you can upload files from the standby controller to the active controller using the **Upload File from Standby Controller** command. Choose **Operate > Device Work Center > Device Type > Wireless Controller > *Controller* > Device Details > Redundancy > Redundancy Commands** to access these commands.

Disabling Redundancy on Controllers

To disable redundancy on a controller:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the controller for which you want to disable the redundancy. The details of the controller appear in the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.

Step 6 Unselect the **Enabled** check box for the Redundancy Mode to disable the Redundancy on the selected controller.

Step 7 Click **Save**. The configuration is saved and the system reboots.

When you disable redundancy on the controller, both active and standby controllers reboot. You must refresh the configuration from the device to remove any audit mismatches in the Redundancy parameters. The active controller becomes a standalone controller and the standby controller reboots with all of the ports disabled.