Work With Wireless Mobility

- What Is Mobility?, on page 1
- What is WLAN Hierarchical Mobility, on page 2
- View Mobility Domains Using the Mobility Work Center, on page 2
- Create a Mobility Domain from a Group of Controllers, on page 3
- What are Mobility Anchors, on page 5
- What is a Spectrum Expert, on page 7
- Use Cisco Adaptive wIPS Profiles for Threat Protection in Mobility Networks, on page 8

What Is 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. To allow more flexible roaming and to minimize the need for tunnel encapsulation of traffic, Prime Infrastructure provides a robust mobility architecture that distributes mobility functionality across the network devices.

The following are the key elements of the mobility architecture:

- Mobility Controller (MC)—The MC (for example, Cisco 5700 Series Wireless Controller) is responsible for one or more MAs or switch peer groups, handling roaming within its span of control, and transiting traffic between MAs and/or MCs when co-located with MTE.
- Mobility Agent (MA)—The MA (for example, Catalyst 3650 or Catalyst 3850 Switch) resides in the access switch or edge switch that the WAP is directly connected to, and terminates at the CAPWAP tunnel for communications with the WAP.
- Mobility Oracle (MO)—The MO is a top-level control entity responsible for connecting multiple MCs or mobility subdomains in deployments of the largest scale, to enable roaming across very large physical areas.
- Mobility Domain—A roaming domain: a mobile user may roam across all of the devices in this domain (the set of WAPs and all of the control entities associated with it). This typically includes MAs and MCs, and may include a MO (to join multiple subdomains).
- Mobility Sub-Domain—The set of WAPs and associated MAs and one MC, representing a portion of a larger mobility domain (where a MO serves to coordinate roaming between multiple sub-domains).
- Switch Peer Group (SPG)—A group of switches (acting as MAs). An SPG establishes a full mesh of mobility tunnels among the group members to support efficient roaming across the WAPs associated

with the switches in the group. An SPG is also intended to limit the scope of interactions between switches during handoffs. An SPG is configured by the Mobility Controller, and every switch in the switch peer group has the same view of the membership. The switches in an SPG might be interconnected by a set of direct tunnels. When a station roams from one switch to another within the same switch peer group, if the point of presence stays at the original or anchor switch, the traffic can be directly tunneled back to the anchor switch without involving the MTE. This direct tunneling mechanism is a data path optimization and is optional.

- Mobility Group—A mobility group is a set of MCs (and their associated MAs / switch peer groups)
- Mobility Tunnel Endpoint—The Mobility Tunnel Endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant. If the VLAN or subnet of the roamed client is available at the MTE, the MTE could become the point of presence; otherwise it merely functions as a tunnel switching entity that connects the roamed client to access switch or MTE that is the point of presence.

Related Topics

View Mobility Domains Using the Mobility Work Center, on page 2
Create a Mobility Domain from a Group of Controllers, on page 3

What is WLAN Hierarchical Mobility

Hierarchical Mobility is referred to as New Mobility in the wireless LAN controller configuration. Cisco Prime Infrastructure 2.0 supports the new mobility functionality for Cisco 5508 and WiSM2 platforms that run Cisco WLC 7.6.

The key features of the New Mobility functionality in Prime Infrastructure are:

- Mobility Work Center discovers Cisco 5508 and WiSM 2 platforms that run Cisco WLC 7.6 and provide necessary operations related to building hierarchical mobility architecture that involves two device types (Cisco 5508 and WiSM2) and Cisco 3650//3850 deployed as Mobility Agent.
- When deploying the hierarchical mobility architecture, the wireless features such as WLAN, VLAN, security, guest anchor can be configured on Cisco 5508 and WiSM2 using the LifeCycle view.
- Deploying the flat mobility architecture on Cisco 5508 and WiSM2 would be supported only in classic view and entire wireless configuration would be left as it is in classic and LifeCycle view.
- As in Prime Infrastructure 2.0, the IOS based devices 3850 and 5760 continue to be configured using CLI templates for some of the wireless features such as creating VLAN interfaces.

For more information about the new mobility functionality, see the Hierarchical Mobility (New Mobility) section in the Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.112.0.

View Mobility Domains Using the Mobility Work Center

The Mobility Work Center is available by choosing **Services** > **Mobility Services** > **Mobility Domains**.

The following information is displayed:

- Device Name—Name of the MC.
- Management IP—Management IP address of the MC.
- Wireless Interface IP—IP address on the MC which is used for mobility protocol.
- Mobility Group—Name of the mobility group the MC belongs to.
- Mobility Role—Shows administrative and operational mobility mode. If Admin and Operational values are different, the device needs reboot for the administrative mode to be effective. It shows MO in addition to mobility mode if Mobility Oracle is enabled on it.

In this page, you can perform the following tasks:

- Create Mobility Domain.
- Create Switch Peer Group—To create switch peer groups in MC.
- Change Mobility Role—To change the controllers from MA to MC.
- Delete Domain—Deletes only the domain; it does not delete the controllers from Prime Infrastructure.
- Delete Members—To remove selected MCs from a selected domain.
- Set as Mobility Oracle—To enable MO on a selected MC, if the MC must act as the MO for the entire domain. There can be only one MO per domain. Only Cisco 5760 series controllers support the MO feature.
- Add members to switch peer group—To add members to switch peer group.
- Delete members from switch peer group—To delete members from switch peer group.

Note By default, the Mobility Work Center page displays all of the mobility domains configured in the managed network. To see a list of mobility devices, choose **All Mobility Devices** from the left sidebar.

Related Topics

What Is Mobility?, on page 1
Create a Mobility Domain from a Group of Controllers, on page 3

Create a Mobility Domain from a Group of Controllers

A mobility domain is a collection of controllers that have all been configured with each other's IP addresses, allowing clients to roam between the controllers in the mobility domain.

The Mobility Work Center displays all mobility domains configured in the managed network using Prime Infrastructure.

When a node is selected from the left sidebar, the right pane shows more details. When a domain node is selected from the left sidebar, the right pane displays the MCs in the domain.

To create a mobility domain:

Step 1 Choose **Services** > **Mobility Services** > **Mobility Domains**.

Step 2 Click on the left sidebar menu.

Step 3 Enter a name for the mobility domain for the set of MCs that you want to group together.

If a selected MC exists in another domain, it is removed from that domain and added to the new domain.

Step 4 Select mobility domain member devices.

A device can belong to one domain or SPG only.

Step 5 Click **Apply**.

Create a Mobility Switch Peer Group from a Group of Switches

An MC can have switch peer groups (SPGs), and a switch peer group can have MAs. The MAs in a managed network are listed on the Switch Peer Group page. If you create a switch peer group when you already have one, MAs are moved from the old switch peer group to the new one, and the MC wireless interface IP address is set on all of the MAs.

To create a switch peer group, follow these steps:

Step 1 Choose **Services** > **Mobility Services** > **Mobility Domains**.

Step 2 Choose an MC from the left sidebar.

Step 3 Click **Create Switch Peer Group**.

Step 4 Enter a name for the switch peer group that will contain the set of MAs that you want to group together on the selected MC.

If a selected MA exists in another switch peer group, it is removed from that group and added to the new group. You can create multiple switch peer groups on an MC.

Step 5 Select mobility agents.

A device can belong to one domain or SPG only.

Step 6 Click **Apply**.

The SPG that you created appears in the left sidebar. You can navigate to it to see the mobility agents on the selected switch peer group.

Change a Device's Mobility Role

By default, Cisco 3850 controllers act as MAs. These controllers can be converted to MCs if MCs are needed in the network.

To change a mobility role:

Step 1 Choose **Services** > **Mobility Services** > **Mobility Domains**.

Step 2 Choose **All Mobility Devices**.

Step 3 Select a device and the role that you want to change to:

- Change Role To Mobility Controller—Enables the mobility controller feature on the selected controller.
- Change Role To Mobility Agent—Enables the Mobility Agent feature on the selected controller. When you do this, the MC feature is disabled.
- Converting MAs to MCs (and vice versa) is limited to 3850 devices. For a changed role to take effect, you must reboot the device.
- Assign Mobility Group—Allows you to enter new mobility group name for the selected device.

Step 4 Click **Apply**.

What are 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.

Configure a Mobility Guest Anchor Controller for a WLAN

The guest anchor controller is a controller dedicated to guest traffic, and is located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN.

Note The Cisco 5760 controller can be a guest anchor whereas the Catalyst 3850 switch cannot be a guest anchor but it can be a foreign controller.

You can configure a guest controller as a mobility anchor for a WLAN for load balancing.

Before You Begin

- Ensure that wireless devices are set up in Prime Infrastructure. For more information about setting up wireless devices, see *Configuring Wireless Features*.
- Ensure that the wireless devices that you want to configure as mobility anchors for a WLAN are in the same mobility domain.

To configure a guest anchor controller for a WLAN:

SUMMARY STEPS

1. Choose **Inventory > Device Management > Network Devices**.
2. In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.
3. Select the controller that you want to designate as a guest mobility anchor. The details of the device appear in the lower part of the page.
4. Click the **Configuration** tab.
5. From the left sidebar menu, choose **WLANs > WLAN Configuration**. The WLAN Configuration page appears.
6. Select the URL of the desired WLAN ID. A tabbed page appears.
7. Click the **Advanced** tab, and then click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears.
8. Select the **IP address** check box of the controller to be designated a mobility anchor, and click **Save**.

DETAILED STEPS

Step 1 Choose **Inventory > Device Management > Network Devices**.

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

Step 3 Select the controller that you want to designate as a guest mobility anchor. The details of the device appear in the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **WLANs > WLAN Configuration**. The WLAN Configuration page appears.

Note If you are in the Classic view, choose **Configure** > **Controllers** > *Ctrl IP addr* > WLANs > WLAN Configuration to access the WLAN Configuration page.

Step 6 Select the URL of the desired WLAN ID. A tabbed page appears.

Step 7 Click the **Advanced** tab, and then click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears.

Note You can also access the Mobility Anchors page from the WLAN Configuration page. Select the check box of the desired WLAN ID. From the Select a command drop-down list, choose **Mobility Anchors**, and then click **Go**. The Mobility Anchors page appears.

Step 8 Select the **IP address** check box of the controller to be designated a mobility anchor, and click **Save**.

What is a Spectrum Expert

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose **Services > Mobility Services > Spectrum Experts**. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to Prime Infrastructure. The status appears as reachable or unreachable.

See *Mobility Services* section in Cisco Prime Infrastructure Reference Guide for the Descriptions of fields in the Spectrum Expert page.

Configure a Mobility Spectrum Expert to Collect Interferer Data

To add a Spectrum Expert, follow these steps:

SUMMARY STEPS

1. Choose **Services > Mobility Services > Spectrum Experts**.
2. From the Select a command drop-down list, choose **Add Spectrum Expert**. This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing **Add Spectrum Expert** from the Select a command drop-down list.
3. Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

DETAILED STEPS

Step 1 Choose **Services > Mobility Services > Spectrum Experts**.

Step 2 From the Select a command drop-down list, choose **Add Spectrum Expert**. This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing **Add Spectrum Expert** from the Select a command drop-down list.

Step 3 Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to Prime Infrastructure.

See *Mobility Services* section in Cisco Prime Infrastructure Reference Guide for more information.

Use Cisco Adaptive wIPS Profiles for Threat Protection in Mobility Networks

Prime Infrastructure provides several predefined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Predefined profiles include:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

The **wIPS Profiles > Profile List** page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles. The Profile List provides the following information for each profile:

- **Profile Name**—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

Hover your mouse cursor over the profile name to view the Profile ID and version.

- **MSE(s) Applied To**—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- **Controller(s) Applied To**—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

To create a wIPS profile, follow these steps:

SUMMARY STEPS

1. Choose **Services > Mobility Services > wIPS Profiles**.
2. From the **Select a command** drop-down list, choose **Add Profile**, then click **Go**.
3. Enter a profile name in the Profile Name text box of the Profile Parameters page.
4. Select the applicable predefined profile, or choose **Default** from the drop-down list.
5. Choose **Save > Next**.
6. To edit and delete current groups or add a new group:
7. To determine which policies are included in the current profile, choose **Profile Configuration**. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. Using this page, you can:
8. When the profile configuration is complete, select **Next** to proceed to the MSE/Controller(s) page.

9. In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click **Apply** to apply the current profile to the selected mobility services engine/controller(s).

DETAILED STEPS

Step 1 Choose **Services > Mobility Services > wIPS Profiles**.

Step 2 From the **Select a command** drop-down list, choose **Add Profile**, then click **Go**.

Step 3 Enter a profile name in the Profile Name text box of the Profile Parameters page.

Step 4 Select the applicable predefined profile, or choose **Default** from the drop-down list.

Step 5 Choose **Save > Next**.

When you select **Save**, the profile is saved to the Prime Infrastructure database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.

Step 6 To edit and delete current groups or add a new group:

a) From the **Select a command** drop-down list on the SSID Group List page, choose **Add Group** or **Add Groups from Global List**, then click **Go**.

b) Enter the group name and one or more SSID groups, then click **Save**.

Step 7 To determine which policies are included in the current profile, choose **Profile Configuration**. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. Using this page, you can:

- Enable or disable an entire branch or an individual policy by selecting or unselecting the check box for the applicable branch or policy.

By default, all policies are selected.

- Click an individual policy to display the policy description. Use the Policy Rules page add, edit, delete, and reorder the current policy rule settings.

Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

Note If the profile is already applied to a controller, it cannot be deleted.

- Configure the following settings:
  - Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues. Threshold options vary based on the selected policy.
  - When the threshold is reached for a policy, an alarm is triggered. Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page; choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.
  - Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
  - Notification—Indicates the type of notification associated with the threshold.
  - ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

Note Only selected groups trigger the policy.

Step 8 When the profile configuration is complete, select **Next** to proceed to the MSE/Controller(s) page.

Step 9 In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click **Apply** to apply the current profile to the selected mobility services engine/controller(s).

You can also apply a profile directly from the profile list. From the Profile List page, select the profile that you want to apply and click **Apply Profile** from the **Select a command** drop-down list. Then click **Go** to access the Apply Profile page.