Mobility

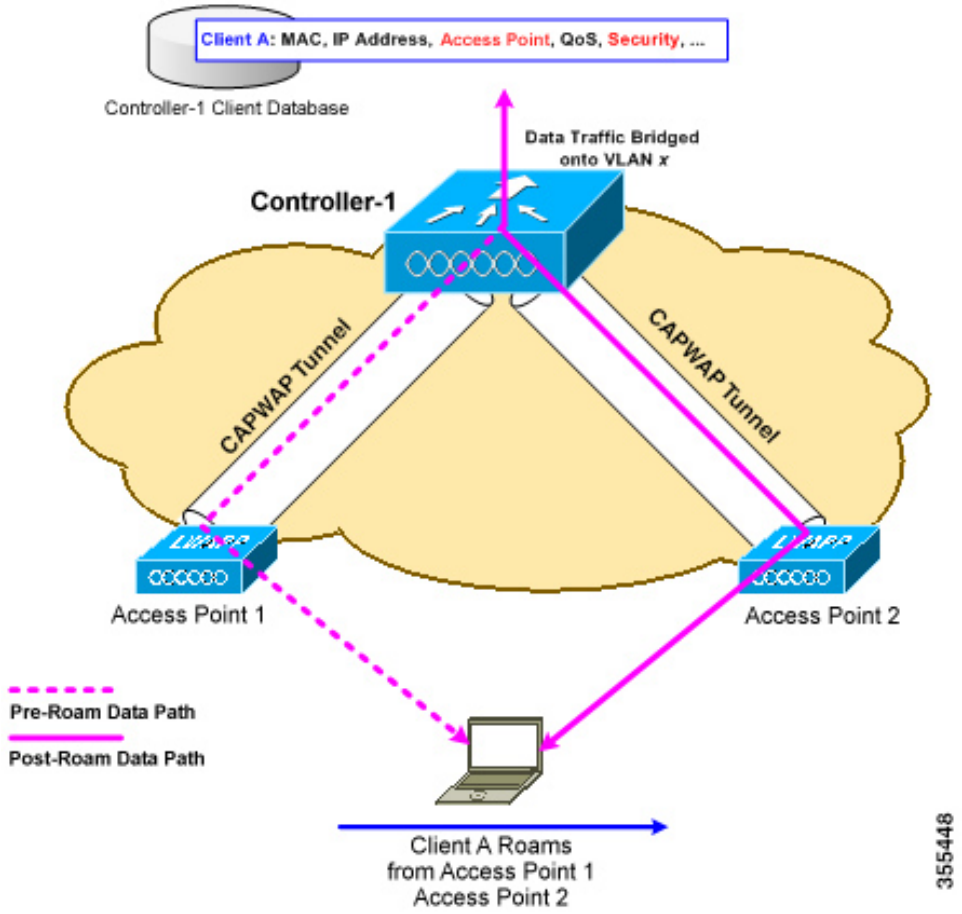
Introduction to Mobility

Mobility or roaming is a wireless LAN client's ability to maintain its association seamlessly from one access point to another access point 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 access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The controller uses this information to forward frames and manage traffic to and from a wireless client.

Figure 1: Intracontroller Roaming

This figure shows a wireless client that roams from one access point to another access point when both access points are joined to the same controller.

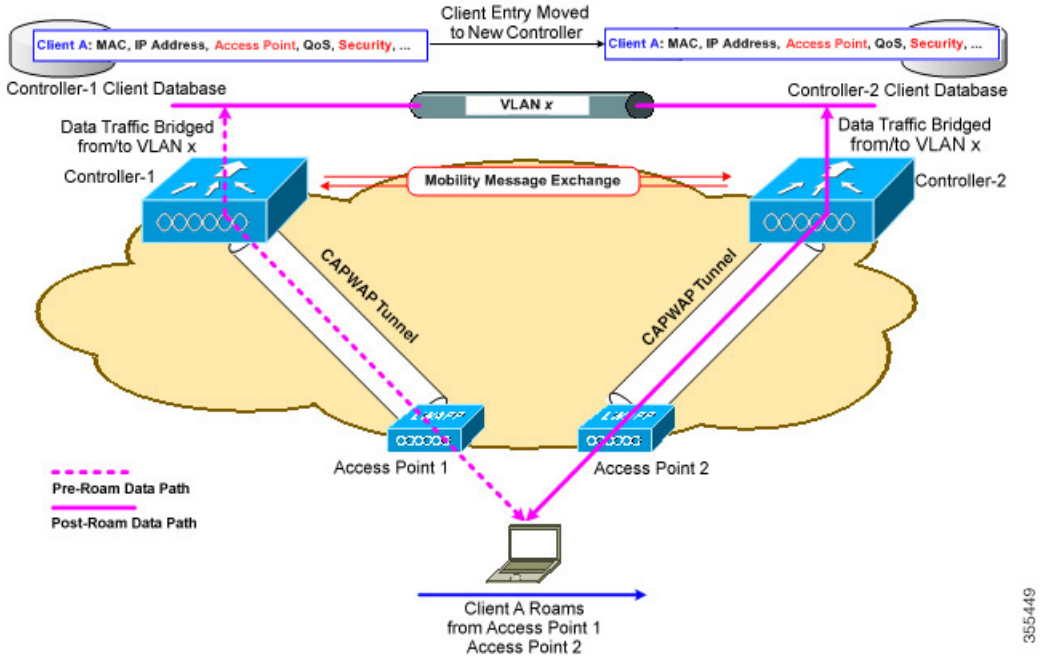


When a wireless client moves its association from one access point to another access point, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

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. It also varies based on whether the controllers are operating on the same subnet.

Figure 2: Intercontroller Roaming

This figure shows intercontroller roaming, which occurs when the wireless LAN interfaces of controllers are on the same IP subnet.



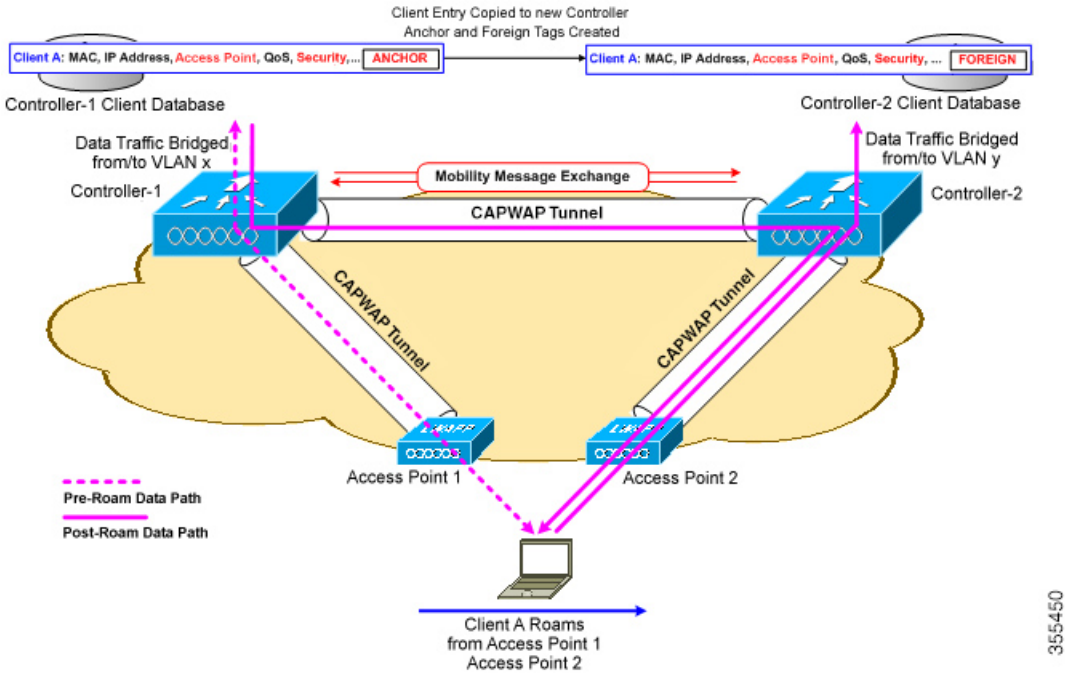
When a client joins an access point associated with a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database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

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

Important Intersubnet Roaming is not supported for SDA.

Figure 3: Intersubnet Roaming

This figure shows intersubnet roaming, which occurs when the wireless LAN interfaces of controllers are on different IP subnets.



Intersubnet roaming is similar to intercontroller roaming in that, controllers exchange mobility messages on the client roam. 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 transparent to the wireless client, and the client maintains its original IP address.

In intersubnet roaming, WLANs on both anchor and foreign controllers should have the same network access privileges, and no source-based routing or source-based firewalls in place. Otherwise, the clients may have network connectivity issues after the handoff.

In a static anchor setup using controllers and a RADIUS server, if AAA override is enabled to dynamically assign VLAN and QoS, the foreign controller updates the anchor controller with the right VLAN after a Layer 2 authentication (802.1x). For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.

Note The Cisco Catalyst 9800 Series Wireless Controller mobility tunnel is a CAPWAP tunnel with control path (UDP 16666) and data path (UDP 16667). The control path is DTLS encrypted by default. Data path DTLS can be enabled when you add the mobility peer.

SDA Roaming

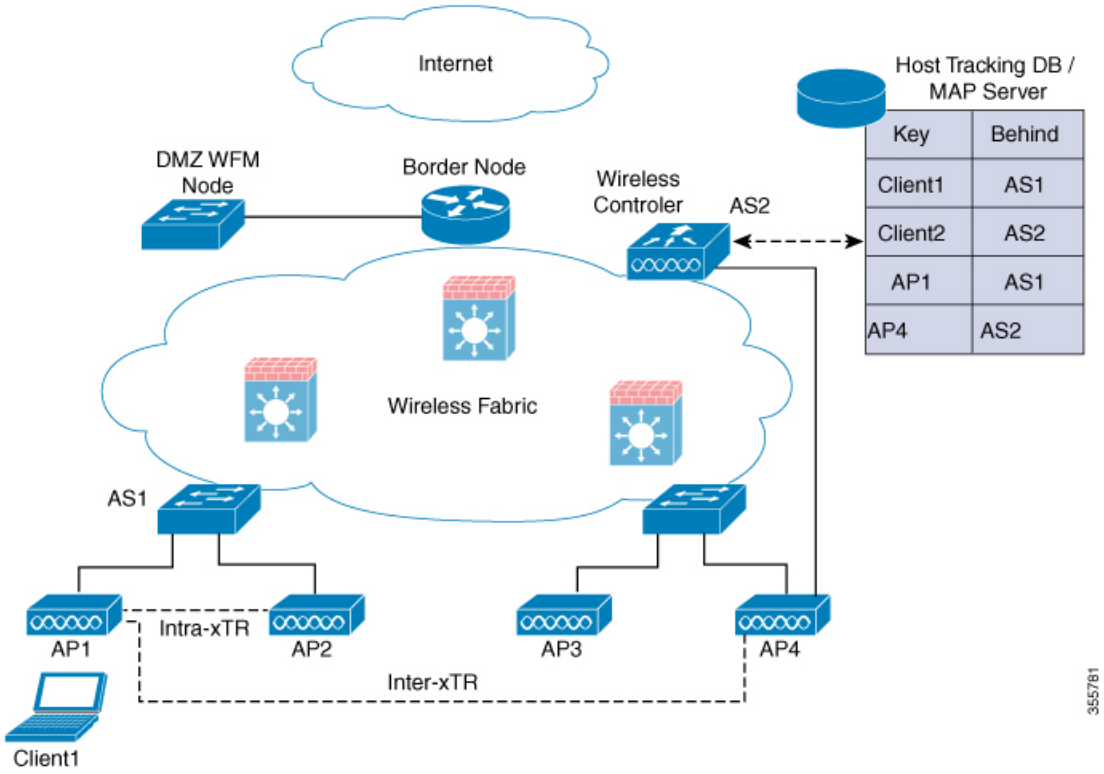
SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point.

Figure 4: SDA Roaming

This figure shows inter-xTR and intra-xTR roaming, which occurs when the client moves from one access point to another access point on the same switch or to a different switch in a Fabric topology.



Definitions of Mobility-related Terms

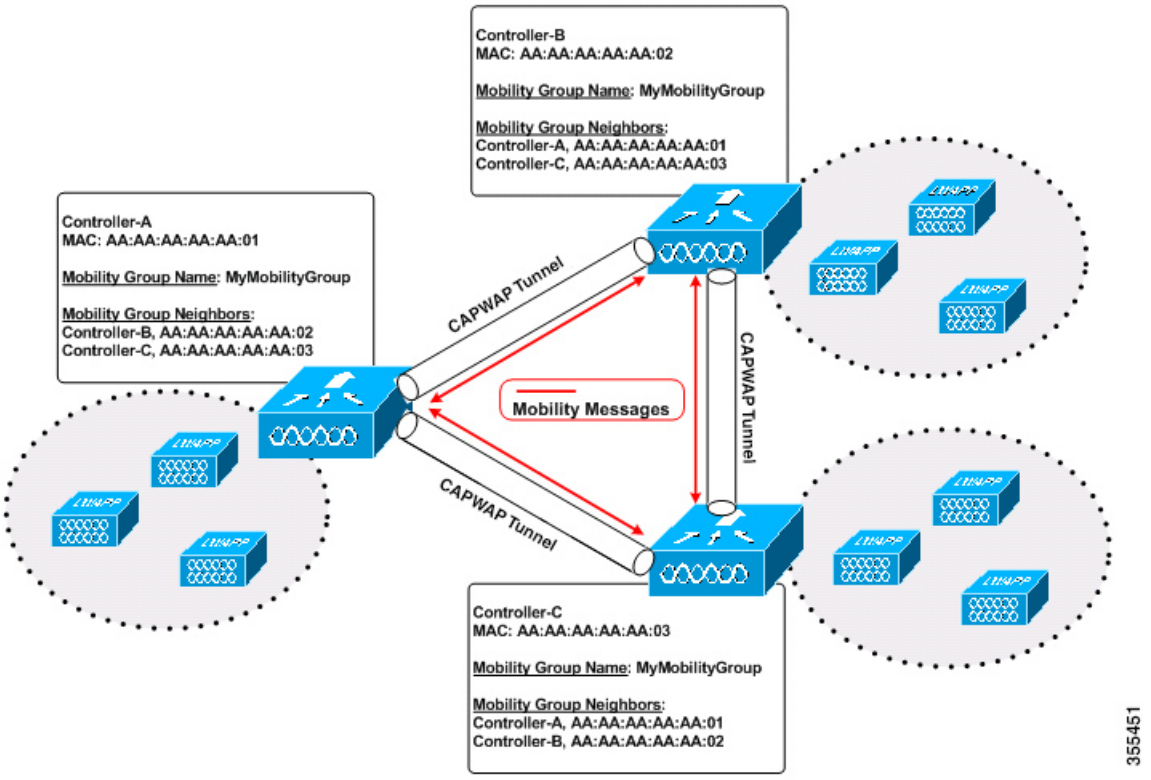
- Point of Attachment—A station's point of attachment is where its data path is initially processed upon entry into the network.
- Point of Presence—A station's point of presence is the place in the network where the station is being advertised.
- Station—A user's device that connects to and requests service from a network.

Mobility Groups

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when intercontroller or intersubnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support intercontroller wireless LAN roaming and controller redundancy.

Note While moving an AP from one controller to another (when both controllers are mobility peers), a client associated to controller-1 before the move might stay there even after the move. This is due to a timeout period on controller-1, where the client entry is maintained (for the purposes of roaming/re-association scenarios). To avoid the client being anchored in controller-1, remove the mobility peer configuration of the controller.

Figure 5: Example of a Single Mobility Group



As shown in the figure above, 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 (or multicast message if mobility multicast is configured) 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.

Guidelines and Restrictions

The following AireOS and Cisco Catalyst 9800 Series Wireless Controller platforms are supported for SDA Inter-Controller Mobility (AireOS controller–to-Cisco Catalyst 9800 Series Wireless Controller):

- **AireOS**
  - Cisco 3504
  - Cisco 5520
  - Cisco 8540
- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-80 Wireless Controller
  - Cisco Catalyst 9800-40 Wireless Controller
  - Cisco Catalyst 9800-L Wireless Controller

The following controller platforms are supported for SDA Inter-Controller Mobility:

- **Catalyst Switches**
  - Cisco 9300
- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-40 Wireless Controller

- Ensure that the data DTLS configuration on the Cisco Catalyst 9800 Series Wireless Controller and AireOS are the same, as configuration mismatch is not supported on the Cisco Catalyst 9800 Series Wireless Controller and it causes the mobility data path to go down.
- In intercontroller roaming scenarios, policy profiles having different VLANs is supported as a Layer 3 roaming.
- In AireOS controller, L3 override is not supported in guest VLAN. Hence, the client does not trigger DHCP Discovery on the new VLAN automatically.
- Policy profile name and client VLAN under policy profile can be different across the controllers with the same WLAN profile mapped.
- In intracontroller roaming scenarios, client roaming is supported between same policy profiles, with WLAN mapped.
- If a client roams in web authentication state, the client is considered as a new client on another controller instead of being identified as a mobile client.
- Controllers that are mobility peers must use the same DHCP server to have an updated client mobility move count on intra-VLAN.

- Data DTLS and SSC hash key must be same for mobility tunnels between members.
- Mobility move count is updated under client detail only during inter-controller roaming. Intra-controller roaming can be verified under client stats and mobility history.
- Anchor VLAN in Cisco Catalyst 9800 Series Wireless Controller is represented as Access VLAN on the Cisco AireOS controller.
- When clients are roaming, their mobility role is shown as *Unknown*. This is because the roaming clients are in *IP learn* state, and in such a scenario, there are many client additions to the new instance and deletions in the old instance.
- In inter-controller roaming between 9800 and 9800/AireOS, client roaming is not supported, whenever there is a WLAN profile mismatch.
- Only IPv4 tunnel is supported between Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS controller.
- Ensure that you configure the mobility MAC address using the **wireless mobility mac-address** command for High-Availability to work.
- If Anchor and Foreign controllers are put in the same Layer 2 network, it creates a loop topology (one path is Layer 3 mobility tunnel between Anchor and Foreign, another path is Layer 2 wired connection between Anchor and Foreign). In this topology, MAC_CONFLICT warning message can be seen on both the Anchor and Foreign controllers. This MAC_CONFLICT warning message is printed once every minute. However, it doesn't have any functionality and performance impact. As a best practice, do not use management VLAN as client VLAN.
-
- If the current AP has 5-GHz slot2 radio on L2 and L3 mobility 5-GHz slot2, the WLAN BSSID is only added to the 11k or 11v neighbor information. As a result, the AP does not have the information of radio properties of the APs belonging to the other controllers. Hence, it can be assumed that the radio properties of the APs belonging to the other controllers are similar to that of the current AP. If the current AP does not have slot2, the other APs cannot be added as a neighbor. In such a scenario, the validation fails and does not add this radio to the neighbor list.
- We recommend that you use the default keepalive count and interval values to reduce convergence time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.
- A new client may take up to 3 seconds to join the network when the mobility tunnel is UP and mobility peers are configured. This is because the system sends three mobile messages (one second apart) to find out whether the client is already part of the network.

Configuring Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility**.
The **Wireless Mobility** page is displayed on which you can perform global configuration and peer configuration.

Step 2 In the **Global Configuration** section, perform the following tasks:

a) Enter a name for the mobility group.
b) Enter the multicast IP address for the mobility group.
c) In the **Keep Alive Interval** field, specify the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
d) Specify the **Mobility Keep Alive Count** amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds.
e) Enter the DSCP value for the mobility group.
f) Enter the mobility MAC address.
g) Click **Apply**.

Step 3 In the **Peer Configuration** tab, perform the following tasks:

a) In the **Mobility Peer Configuration** section, click **Add**.
b) In the **Add Mobility Peer** window that is displayed, enter the MAC address and IP address for the mobility peer. .
c) Enter the mobility group to which you want to add the mobility peer.
d) Select the required status for **Data Link Encryption**.
e) Specify the **SSC Hash** as required.

   SSC hash is required if the peer is a Cisco Catalyst 9800-CL Wireless Controller, which uses self-signed certificate and hence SSC hash is used as an additional validation. SSC hash is not required if peer is an appliance, which will have manufacturing installed certificates (MIC) or device certificates burned in the hardware.

f) Click **Save & Apply to Device**.
g) In the **Non-Local Mobility Group Multicast Configuration** section, click **Add**.
h) Enter the mobility group name.
i) Enter the multicast IP address for the mobility group.
j) Click **Save**.

Configuring Mobility (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Device(config)# wireless mobility group name Mygroup`	Creates a mobility group named **Mygroup**.
Step 2	**wireless mobility mac-address** *mac-addr* **Example:** `Device(config)# wireless mobility mac-address 00:0d:ed:dd:25:82`	Configures the MAC address to be used in mobility messages.

	Command or Action	Purpose
Step 3	**wireless mobility dscp** *value-0-to-63* **Example:** `Device(config)# wireless mobility dscp 10`	(Optional) Configures mobility intercontroller DSCP value.
Step 4	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Device(config)# wireless mobility group keepalive interval 5`	(Optional) Configures the interval between two keepalives sent to a mobility member. Valid range is between 1 and 30 seconds. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.
Step 5	**wireless mobility group keepalive count** *count* **Example:** `Device(config)# wireless mobility group keepalive count 3`	(Optional) Configures the keepalive retries before a member status is termed DOWN.

Step 6	Use the options given below to configure IPv4 or IPv6.
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name* **data-link-encryption**
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 group scalemobility`
		Adds a peer IPv4 or IPv6 address to a specific group.
		To remove the peer from the local group, use the **no** form of this command.

Step 7	**wireless mobility multicast** {**ipv4** | **ipv6** } *ip-address* or **wireless mobility group multicast-address** *group-name* {**ipv4** | **ipv6** } *ip-address*
	Example:
	`Device(config)# wireless mobility multicast ipv4 224.0.0.4`
	Example:
	`Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5`
		(Optional) Configures a multicast IPv4 or IPv6 address for a local mobility group or a nonlocal mobility group.
		Note **Mobility Multicast**—The controller sends a multicast message instead of a unicast message to all the members in the mobility local group or a nonlocal group when a client joins or roams.
		Configures the multicast IPv4 address as 224.0.0.4 for a local mobility group.

	Command or Action	Purpose
		Configures the multicast IPv4 address as 224.0.0.5 for a nonlocal mobility group.

Configuring Inter-Release Controller Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility** > **Global Configuration**.

Step 2 Enter the **Mobility Group Name**, **Multicast IPv4 Address**, **Multicast IPv6 Address**, **Keep Alive Interval (sec)**, **Mobility Keep Alive Count**, **Mobility DSCP Value** and **Mobility MAC Address**.

Step 3 Click **Apply**.

Configuring Inter-Release Controller Mobility

Inter-Release Controller Mobility (IRCM) is a set of features and functionality that enable interworking between controllers running different software releases. IRCM enables seamless mobility and wireless services across controllers running Cisco AireOS and Cisco IOS (for example, Cisco 8540 WLC to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access or termination.

Note To configure IRCM for different combination of AireOS and Catalyst 9800 controllers, see the Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide.

Follow the procedure described to configure mobility peers on the controller:

Before you begin

The Inter-Release Controller Mobility (IRCM) feature is supported by the following Cisco Wireless Controllers.

- For IRCM deployment, we recommended that you configure:
  - Both Cisco AireOS and Cisco Catalyst 9800 Series Controllers as static RF leaders to avoid RF grouping between them.
  - Configure the same RF network name on both the controllers.
- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.
- Supports the following Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software:
  - Cisco 3504 Wireless Controllers

- Cisco 5508 Wireless Controllers
- Cisco 5520 Wireless Controllers
- Cisco 8510 Wireless Controllers
- Cisco 8540 Wireless Controllers

- By design, Cisco Catalyst 9800 Wireless Controllers does not have the Primary Mode configuration exposed that is to be sent in the Discovery Response. The controller always sends the Discovery Response with the Primary Mode enabled.
- Supported Cisco AireOS Wireless Controllers running AireOS 8.8.111.0 and later. The following controllers are supported:
  - Cisco 3504 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8540 Wireless Controllers

Note If the peer Cisco Catalyst 9800 Series Wireless Controller is virtual, configure the hash using command:

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

Optionally enable data tunnel encryption using command:

```
config mobility group member data-dtls 00:0c:29:a8:d5:77
enable/disable
```

The hash configure above can be obtained by running the following command on the Cisco Catalyst 9800 Series Wireless Controller:

```
show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 3f93a86cee2039e9c3aada1822ad74b89fea30c1
Private key Info : Available
```

- The IRCM feature is not supported on the following Cisco AireOS Wireless Controllers:
  - Cisco 2504 Wireless Controllers
  - Cisco Flex 7510 Wireless Controllers
  - Cisco WiSM 2

- IPv6 is not supported for SDA IRCM for fabric client roaming. IPv6 is supported for IRCM for non-fabric client roaming.
- Ensure that you use AireOS controller that supports Encrypted Mobility feature.
- AVC is not supported for IRCM.
- In mixed deployments (Catalyst 9800 and AireOS Controllers), the WLAN profile name and the policy profile name must be the same. This is due to AireOS not knowing about the policy profile and therefore only sends or receives the WLAN name as both the policy profile and WLAN profile.
- Mobility group multicast is not supported because AireOS does not support mobility multicast in encrypted mobility.
- There could be instances where the total number of clients count shown may be more than those supported on the roaming scale. This inconsistency is observed when the client roaming rate is very high, as the system requires time to update the records. Here, the clients presented on multiple WNCds for a very short time are counted more than once. We recommend that you provide sufficient time for the process to obtain a consistent data before using one of the following methods: show CLIs, WebUI, Cisco Catalyst Center, or SNMP.
- Link Local bridging is not supported. Ensure that you disable it also on the peer AireOS controller.
- IRCM is not supported in FlexConnect and FlexConnect+Bridge modes.

The following client features support IPv6 client mobility between AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller: Accounting, L3 Security (Webauth), Policy (ACL and QoS), IP address assignment and learning through SLAAC and DHCPv6, IPv6 Source Guard, multiple IPv6 address learning, IPv6 multicast, and SISF IPv6 features (RA Guard, RA Throttling, DHCPv6 Guard, and ND Suppress).ß

The following IPv6 features are not supported on Cisco Catalyst 9800 Series Wireless Controller:

- Configurable IPv6 timers
- RA Guard enabled on AP
- Global IPv6 disable

Note

- IPv6 CWA is not supported for both AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller.
- Only eight IPv6 addresses are supported per client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Use the options given below to configure IPv4 or IPv6.	Adds a peer IPv4 or IPv6 address to a specific group.

	Command or Action	Purpose

	• **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip* **group** *group-name***data-link-encryption**
	• **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 group scalemobility`
		To remove the peer from the local group, use the **no** form of this command.

Step 3	**wireless mobility group name** *group-name* **Example:** `Device(config#) wireless mobility group name test-group`	Adds a name for the local group. The default local group name is "default".
Step 4	**wireless mobility mac-address** *mac-address* **Example:** `Device(config#) wireless mobility mac-address 000d.bd5e.9f00`	(Optional) Configures the MAC address to be used in mobility messages.
Step 5	**wireless mobility group member ip** *peer-ip* **Example:** `Device(config#) wireless mobility group member ip 9.12.32.15`	Adds a peer in the local group. To remove the peer from the local group, use the **no** form of this command.
Step 6	**wireless mobility dscp** *dscp-value* **Example:** `Device(config#) wireless mobility dscp 52`	(Optional) Configures DSCP. The default value is 48.
Step 7	**wireless mobility group keepalive count** *count* **Example:** `Device(config#) wireless mobility group keepalive count 10`	Configures the mobility control and data path keepalive count. The default value is 3.
Step 8	**wireless mobility group keepalive interval** *interval* **Example:** `Device(config#) wireless mobility group keepalive interval 30`	Configures the mobility control and data path keepalive interval. The default value is 10. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.

Verifying Mobility

To display the summary of the mobility manager, use the following command:

```
Device# show wireless mobility summary
```

To display mobility peer information, use the following command:

```
Device# show wireless mobility peer ip 10.0.0.8
```

To display the list of access points known to the mobility group, use the following command:

```
Device# show wireless mobility ap-list
```

To display statistics for the mobility manager, use the following command:

To display mobility information of the client, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 detail
```

To display roaming history of the active client in the subdomain, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

To display client-specific statistics for the mobility manager, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 stats mobility
```

To verify whether intercontroller roam is successful, use the following commands:

- **show wireless client mac** *mac-address* **detail**: (on the roamed-to Controller) Displays the roam type as L2 and the roam count is incremented by 1.
- **show wireless client summary** : (on the roamed-from controller) The client entry will not be there in the output.

Verifying SDA Mobility

To verify whether intracontroller, intra-xTR roam is successful, use the following commands:

- **show wireless client summary**: Displays the new AP if the client has roamed across the APs on the same xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the same RLOC as before the roam.

To verify whether intracontroller, inter-xTR roam is successful, use the following commands:

- **show wireless fabric client summary**: Displays the new AP if the client has roamed across the APs on a different xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the RLOC of the new xTR to which the client has roamed to.

To check client status before and after intracontroller roaming, perform the following steps:

1. Check if client is on the old AP, using **show wireless client summary** command on the controller.
2. Check whether the client MAC is listed against the old AP, using **show mac addr dyn** command on the xTR1.
3. Check whether the client IP is registered from current xTR1, and client MAC is registered from both current xTR1, and WLC1, using **show lisp site detail** command on the MAP server.
4. After the intra-WLC roam, check whether the client is on the new AP, using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR1.
5. After the Inter-xTR Roam (old and new APs on different xTRs), check whether the client is on the new AP (connected to the new xTR2), using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR2.
6. Check whether the client is registered from the new xTR2, using the **show lisp site detail** command on the MAP server.

Verifying Roaming on MAP Server for SDA

To verify roaming information for SDA, use the following commands:

Run the following command on the MAP server, before and after the roam, to check whether the client IP is registered from current xTR, and client MAC is registered from both current xTR, and WLC.

```
Device# show lisp site detail
```