Configuring Inter Release Controller Mobility in Wireless Deployments supporting AireOS and Catalyst 9800 Controllers

First Published: 2022-03-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 1

Overview of IRCM

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible.

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different wireless LAN controllers (WLC or also referred to as controllers) that run on different software and controllers (for example, Cisco 8540 Wireless LAN Controller to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access.

While there can be several deployment models that use IRCM within the enterprise, this document specifically covers the IRCM support for interoperability between Catalyst 9800 and Cisco AireOS wireless controllers for the following use cases:

- Customers with existing Cisco AireOS controllers in their networks and adding Catalyst 9800 wireless controllers also known as brownfield deployment.
- Customers with Cisco AireOS controllers deployed as guest anchor and additional Catalyst 9800 wireless controllers added.

Mobility Concepts

As we start to configure mobility, it is important to understand the following concepts.

Key players /Network elements

- Controllers - A Wireless LAN (WLAN) controller manages wireless network access points that allow wireless devices to connect to the network.
- Access points—These devices provide access to the wireless network. Access Points (AP)s are placed in strategic locations to minimize interference.
- Client devices—These include laptops, workstations, IP phones, PDAs, and manufacturing devices that access the WLAN through the access points.

Network settings

VLAN - A logical network to which wireless clients are assigned. It is imperative to declare the VLAN before any configuration can start for roaming or otherwise.

Wireless network parameters

- WLANs and SSIDs - WLAN is a network that allows devices to connect and communicate wirelessly. You can configure WLANs with different Service Set Identifier (SSID)s or with the same SSID. An SSID is the name of the specific wireless network that you want the controller to access.
- Tags & Profiles - On Catalyst 9800 controllers, tags are used to control the features that are available for each Access Point(AP). Tags are assigned to every AP and inside every tag, you can find all the settings that were applied to the AP.
- Policy Tag - On 9800 WLCs, a Policy Tag is the link between a WLAN Profile [Service Set Identifier (SSID)] and a Policy Profile.
  - Policy Profile has details about the Virtual Local Area Network (VLAN) ID, type of traffic -central or local switching, Mobility Anchors, Quality of Service (QoS), timers, and other settings.
  - WLAN Profile has details related to SSID name, WLAN ID, security type for the WLAN, advanced protocols like 802.11k and other settings.

Types of roaming in IRCM

- Intercontroller Roaming Layer 2 - A Layer 2 intercontroller roam occurs when the client traffic is bridged to the same IP subnet (and thus the same VLAN) through the LAN interfaces on both WLCs.
- Intercontroller Roaming Layer 3 - Layer 3 intercontroller roaming occurs when the client associates to an AP on a different WLC and the traffic is bridged to a different subnet.

  In case of roaming between AireOS and Catalyst 9800, it is always a Layer 3 roam, even when both the controllers are on the same VLAN ID.

Mobility Definitions and Controller Roles

- Mobility Groups: A set of controllers in a network can be configured as a mobility group, which allows them to dynamically share important information among them, including the context and state of client devices, and controller loading information.
- Local controller: The controller provides both AP association and IP point of presence, which is where the client enters the wired network
- Anchor controller: The controller provides the IP point of presence only and is always paired with a foreign controller.

  In guest access using guest anchor scenario, anchor refers to one or more controllers deployed in the enterprise DMZ that are used to perform guest mobility tunnel termination, web redirection, and user authentication.
- Foreign controller: The controller provides the AP association only and is always paired with an anchor controller.

  In guest access using guest anchor scenario, foreign refers to the one or more controllers deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility tunnel.
- Export Anchor controller: This controller role is relevant in case of a L3 roam for a client, where the controller provides the IP point of presence only and is always paired with an export foreign controller. This is seen with symmetric mobility tunneling and auto-anchoring. Packets for the client are forwarded via a mobility tunnel to the foreign controller for delivery to the client. The anchor controller provides proxy ARP for the client and is the relay to the DHCP server for the client. DHCP packets for the client are forwarded directly to the client via mobility tunnel to the Export Foreign controller.

- Export Foreign controller: This controller role is relevant in case of a L3 roam for a client, when the controller provides the AP association only and is always paired with an export anchor controller. This is seen with symmetric mobility tunneling and auto-anchoring. Packets from the client are forwarded via mobility tunnel to the anchor controller, where they are de-encapsulated and delivered directly to the network. All packets, including ARP and DHCP packets, are sent within the mobility tunnel.
- Auto Anchor: In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a WLAN. You can use this feature to restrict a WLAN to a single subnet, regardless of a client’s entry point into the network. Clients can access a guest WLAN throughout an enterprise but still be restricted to a specific subnet.

Types of Tunnel

- Secure - The Catalyst 9800 controllers or the 9800 and AireOS (IRCM image) controllers use Control tunnel 16666 for Mobility Control messages and Data tunnel 16667 for Mobility Data Messages . The control tunnel is always encrypted and data tunnel can be encrypted with DTLS or can be in clear text. This secure link is called Secure Mobility Tunnel.
- EOIP - Controllers (AireOS to AireOS or AireOS (IRCM image) to AireOS (old)) within a mobility group communicate among themselves over a well-known UDP port 16666, and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. This is an unencrytpted connection.

CHAPTER 2

Supported Platforms

The Inter-Release Controller Mobility (IRCM) feature is supported on the following Cisco Wireless Controllers. For the latest compatible versions refer to https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.
- Supported Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software. The following controllers are supported:
  - Cisco 3504 Wireless Controllers
  - Cisco 5508 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8510 Wireless Controllers
  - Cisco 8540 Wireless Controllers
- 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

CHAPTER 3

IRCM Best Practices

Cisco supports roaming between controllers running different Cisco IOS XE software versions, but in general, it is advisable to use equal code across the controllers in the same mobility group to ensure consistent behavior across the devices.

- Mobility group connectivity- Ensure that IP connectivity exists between the management interfaces of all controllers. If a controller in the mobility group is permanently down (for replacement, testing, etc.), it is recommended that you remove it from the mobility configuration of all peers.
- Seamless and fast roaming- The mobility group name acts as a discriminator to indicate which controllers share a common cache for fast roaming information (Cisco Centralized Key Management, 802.11r, Proactive Key Caching [PKC], or OKC). It is important to ensure that, if fast roaming is needed between controllers, they share the same mobility group name.
- Mobility group size - Do not create unnecessarily large mobility groups. A mobility group should contain only controllers that have APs in the area where a client can physically roam—for example, all controllers with APs in a building. If you have a scenario in which several buildings are separated, they should be broken into several mobility groups. This saves memory and CPU, as controllers do not need to keep large lists of valid clients, rogues, and APs inside the group, which would not interact anyway. The C9800 wireless controller, like AireOS, supports a maximum of 24 members in a single mobility group.
- Inter-controller Layer 2 versus Layer 3 roaming- On the Catalyst 9800, inter-controller Layer 2 roaming occurs when the client VLAN ID associated to the SSID, is the same on both controllers. 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 transparent to the user.

  Inter-controller Layer 3 roaming occurs when the client VLANs associated to the SSID are different on each controller. Layer 3 roaming is similar to Layer 2 roaming in that the 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.

  On the Catalyst 9800 Wireless Controller, the decision for Layer 2 versus Layer 3 roaming is independent of the client subnet mapped to the client VLAN; only the VLAN ID matters in deciding the type of roam. This is because Catalyst 9800 doesn’t require a L3 interface to be configured for each client VLAN. If an inter-controller Layer 2 roaming is desired, then it’s user’s responsibility to make sure that the network is configured so that the same IP subnet is associated to the same VLAN on both wireless controllers.

Note This is different from AireOS, where Layer 2 roaming happens if the client VLAN and the associated subnet are the same on both wireless controllers.

Note In case of roaming between AireOS and Catalyst 9800, it is always a Layer 3 roam, even when both the controllers are on the same VLAN ID.

- Reduce the need for inter-controller roaming- When implementing AP distribution across controllers in the same mobility group, try to ensure that all access points in the same RF space belong to a single controller. This will reduce the number of intercontroller roams required. A “salt and pepper” scenario (in which APs from different controllers cover the same RF space) is supported, but it is a more expensive process in terms of CPU and protocol exchanges compared to having a single controller per RF space.
- We recommend that you map the WLANs to different VLANs when you are trying to promote IRCM between Catalyst 9800 and AireOS controllers. Ensure that the clients are all DHCP enabled, so that the clients can join the different VLAN/subnet associated to the same SSID.

CHAPTER 4

Restrictions for IRCM

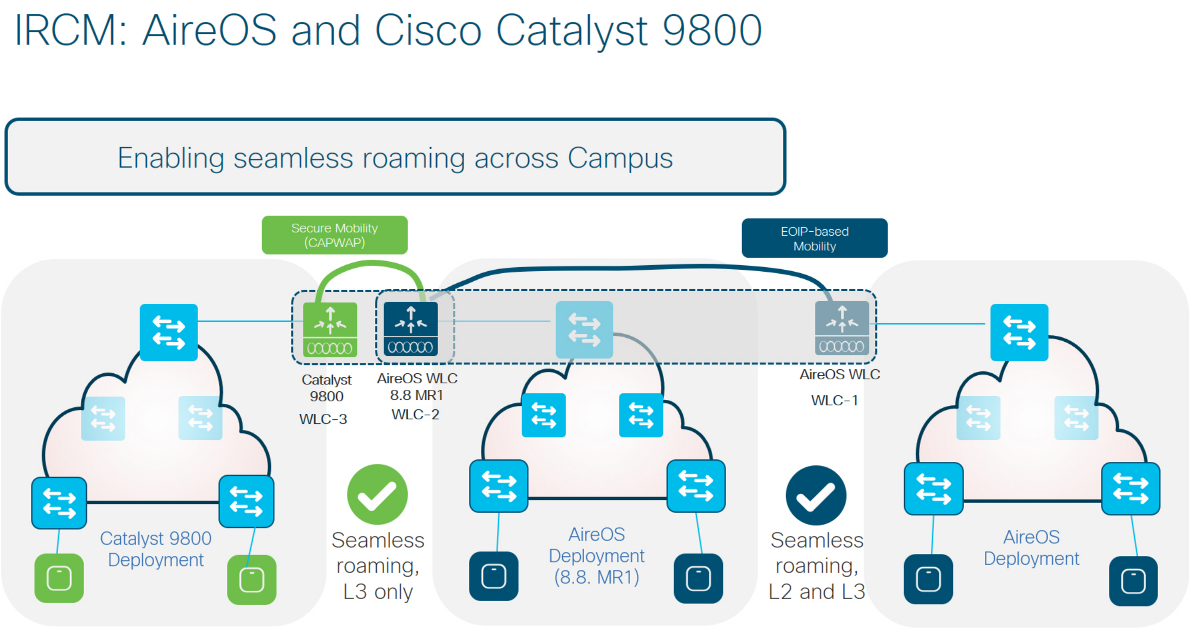
Consider the following before configuring IRCM.

- IPv6 is not supported for SDA IRCM for fabric client roaming. IPv6 is supported for IRCM for non-fabric client roaming.
- IRCM is not supported in FlexConnect and FlexConnect+Bridge modes.
- Link Local bridging is not supported. Ensure that you disable it also on the peer Cisco AireOS controller.
- IPv6 Central Web Authentication (CWA) is not supported for IRCM with Cisco AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller.
- Only eight IPv6 addresses are supported per client.

CHAPTER 5

IRCM Support for Brownfield Deployments within Enterprise

The brownfield deployment use case shows how to expand an existing network within the enterprise with Cisco Catalyst 9800 controllers to provide seamless mobility for clients roaming between Access Points(AP) attached to the different controller versions.


IRCM: AireOS and Cisco Catalyst 9800
Enabling seamless roaming across Campus
Secure Mobility (CAPWAP)
EOIP-based Mobility
Catalyst 9800
WLC-3
AireOS WLC 8.8 MR1
WLC-2
AireOS WLC
WLC-1
Catalyst 9800 Deployment
Seamless roaming, L3 only
AireOS Deployment (8.8. MR1)
Seamless roaming, L2 and L3
AireOS Deployment

This deployment model uses three controllers running different code versions.

- WLC-1–Any AireOS controller running software version 8.2 / 8.3 / 8.5.
- WLC-2–AireOS 5520/8540 or 3504 controllers running software version 8.8.111 and above. WLC can also be a 5508/8510 controller running 8.5 based IRCM supported image.
- WLC-3–Any Catalyst 9800 wireless controller.

In this setup, WLC-1 can only pair up with controllers that can do EOIP. WLC-3 can only pair up with controllers that can do Secure Mobility. WLC-2 running 8.8.111 and above can do either EOIP or Secure mobility on a per peer basis (same for 8.5 based IRCM supported image if you have an older controller like 5508 and 8510).

Seamless client roaming between WLC-1 and WLC-2 is permitted and both L2 and L3 roaming are possible. Seamless client roaming between WLC-2 and WLC-3 will be permitted but will be L3 roaming only.

CHAPTER 6

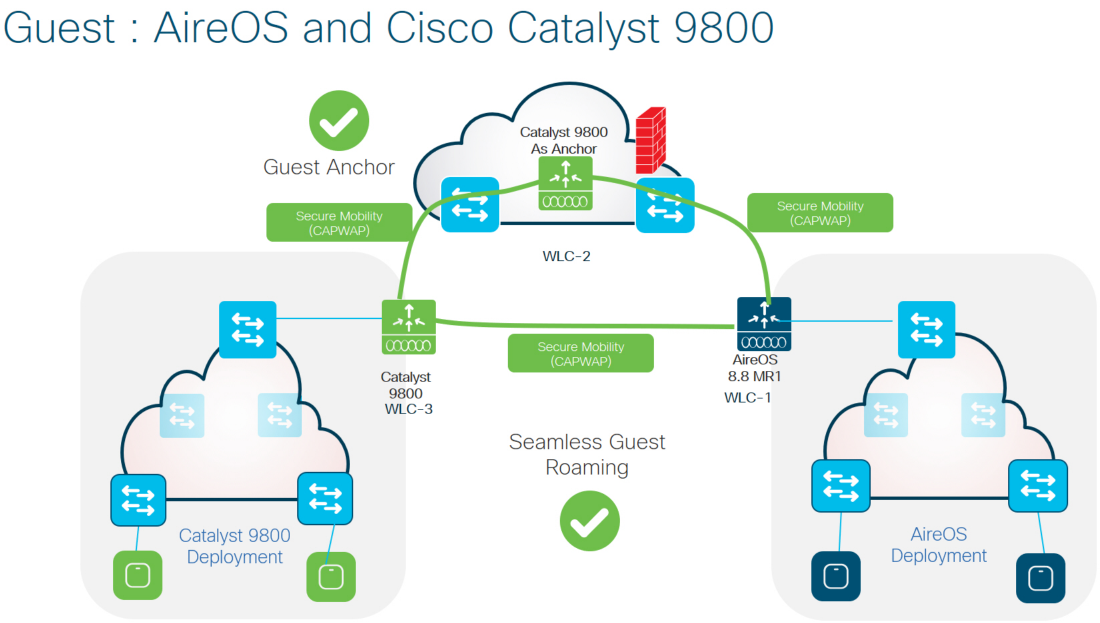
IRCM Support for Brownfield Guest Access using Guest Anchor

The Wireless Guest Access model using guest anchor, addresses the need to provide internet access to guests in a secure and accountable manner. The implementation of a wireless guest network uses the enterprise's existing wireless and wired infrastructure to the maximum extent. While there can be many different deployments for guest access, this document focuses on a solution using two controllers - a Guest Foreign and a Guest Anchor that provides an easy solution to segment guest traffic to a centralised location (DMZ). You can map a provisioned guest WLAN to one or more (anchor) controllers using a tunnel. This allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ.

We will discuss only two possible scenarios described below.

- IRCM support between Catalyst 9800 as Guest Anchor and Catalyst 9800 and AireOS as Foreign Controller, on page 14
- IRCM support between AireOS Controller as Guest Anchor and Catalyst 9800 / AireOS as Foreign Controller, on page 15

IRCM support between Catalyst 9800 as Guest Anchor and Catalyst 9800 and AireOS as Foreign Controller



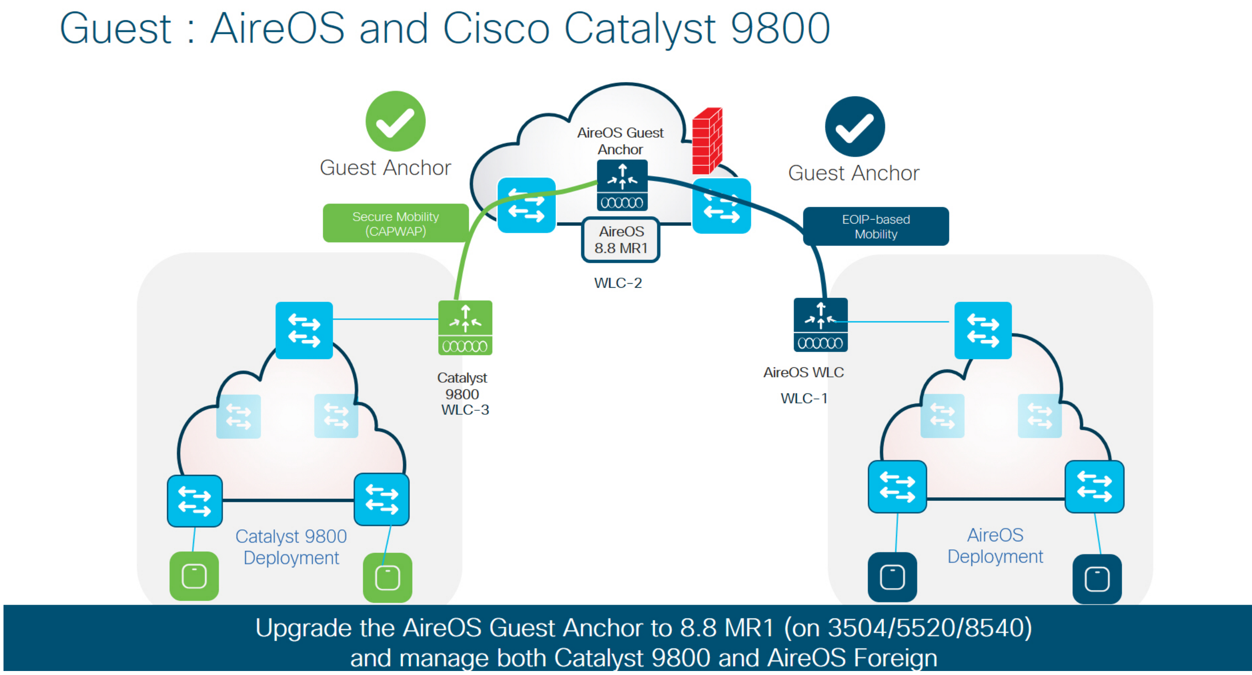
In the above setup, the following controllers are at work.

- WLC-3–Any Catalyst 9800 wireless controller.
- WLC-2–Any Catalyst 9800 wireless controller.
- WLC-1–AireOS 5520/8540 or 3504 controllers running 8.8.111 and above. WLC can also be a 5508/8510 controller running 8.5 based IRCM supported image.

Here all the controllers can participate in secure mobility and will have a tunnel established with the peers . WLC2 here can act a guest anchor for both WLC1 and WLC3.

This setup also support the guest roaming between WLC1 (AireOS) and WLC3 (Catalyst 9800).

IRCM support between AireOS Controller as Guest Anchor and Catalyst 9800 / AireOS as Foreign Controller


Guest : AireOS and Cisco Catalyst 9800

Upgrade the AireOS Guest Anchor to 8.8 MR1 (on 3504/5520/8540) and manage both Catalyst 9800 and AireOS Foreign

In the above setup, the following controllers are at work.

- WLC-3–Any Catalyst 9800 controller.
- WLC-2–AireOS 5520/8540 or 3504 controllers running 8.8.111 and above. WLC can also be a 5508/8510 controller running 8.5 based IRCM supported image.
- WLC-1–Any AireOS controller running 8.2 / 8.3 / 8.5.

Here, WLC-1 can pair up with WLC-2 using EOIP tunnel and WLC-2 can be paired up with WLC-3 through Secure Mobility tunnel. But WLC-1 cannot pair up with WLC-3.

CHAPTER 7

Configure Enterprise Mobility Using the CLI

The Brownfield deployment model assumes that the existing topology has a mix of Cisco AireOS 8.8.111 (or 8.5-based IRCM Image) and Cisco AireOS 8.2/8.3/8.5 controllers and that one or more Catalyst 9800 controllers are being deployed to replace the older AireOS controllers within the enterprise.

Note that the document assumes that you already have an understanding of the preliminary tasks required to set up your topology. However as a brief refresher, the following task list provides you with a checklist to ensure that your configurations are complete before you proceed to configure mobility groups to promote mobility for the wireless clients

Table 1: Preliminary Tasks

Have you completed?	Configurations
1	Configure VLAN, on page 18
2	Configure WLAN, on page 19

Table 2: Mobility specific configurations

Step	Task
1	Ensure Identical Parameter Configuration on Peer Controllers , on page 23
2	Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility, on page 24

Once the above configurations are completed, the following types of roaming are possible between the controllers.

Note The following table is only illustrative of the possible combinations. Depending on the size of the enterprise, clients might roam between two-node or three- node setups. Accordingly, their roam might also be classified as Layer 2 or Layer 3 intercontroller roam with the client roaming between different vlans that are not discussed in detail.

Table 3:

Type of Roaming	Between	Associated VLAN Configuration
Layer 3	Catalyst 9800 and AireOS controllers 8.8.111 (or 8.5-based IRCM Image)	Controllers are on different VLAN ID or same VLAN ID.
	Catalyst 9800 and Catalyst 9800	Controllers are on different VLAN ID.
Layer 2	Two Catalyst 9800 controllers	Controllers are on same VLAN ID
Layer 2	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and AireOS controller 8.2/8.3/8.5	Controllers are on same VLAN ID and same subnet
Layer 3	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and Catalyst AireOS controller 8.2/8.3/8.5	Controllers are on different VLAN ID.

Depending on your requirement, follow the steps below to set up the controllers to enable roaming across the enterprise.

Most of the preliminary steps discussed below, are from the perspective of deploying Catalyst 9800 controllers to your existing setup. If you need help with deploying AireOS controllers with IRCM image, refer to the respective AireOS documents.

- Configure VLAN, on page 18
- Configure WLAN, on page 19
- Create or Modify a Policy Profile, on page 20
- Create or Modify a Policy Tag, on page 22
- Ensure Identical Parameter Configuration on Peer Controllers , on page 23
- Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility, on page 24
- Configure Mobility Groups on Cisco AireOS (IRCM image) Controllers for Secure Mobility , on page 27

Configure VLAN

A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application without regard to the physical locations of the users. Before you start any configuration, you need to add the VLANs to which wireless clients will be assigned.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **vlan** *vlan-id*

Example:

```
Device(config)#vlan 20
```

Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.

Note The available VLAN ID range for this command is 1 to 4094.

Step 4 **name** *vlan-name*

Example:

```
Device(config-vlan)#name test20
```

(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.

Step 5 **exit**

Example:

```
Device(config-vlan)# exit
```

Returns to privileged EXEC mode.

Step 6 **show vlan** {**name** *vlan-name* | **id** *vlan-id*}

Example:

```
Device# show vlan name test20 id 20
```

Verifies your entries.

What to do next

Configure WLAN and associated settings.

Configure WLAN

WLAN is a network that allows devices to connect and communicate wirelessly.

Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability. You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wlan** *profile-name wlan-id* [*ssid*]

Example:

```
Device(config)#wlan IRCM1014_WLAN_OPENAUTH1 34 IRCM1014_WLAN_OPENAUTH1
```

Specifies the WLAN name and ID:

- For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters.
- For the *wlan-id*, enter the WLAN ID. The range is from 1 to 4096.
- For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.

Note

- You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID.
- By default, the WLAN is disabled.

Step 4 **end**

Example:

```
Device(config)#end
```

Returns to privileged EXEC mode.

What to do next

Create or Modify a Policy Profile, on page 20

Create or Modify a Policy Profile

Policy profile contains the policy to be associated with the WLAN. It specifies the settings for client VLAN, Authentication, Authorization, and Accounting (AAA), Access Control Lists (ACLs), session and idle timeout settings and several other parameters.

Before you begin

Ensure you have created the VLANs for assigning the wireless clients.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *new-policy-profile*

Example:

```
Device(config)#wireless profile policy mypolicyprofile
```

Creates a WLAN policy profile/modifies a policy profile.

- For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters.

Step 4 **vlan** *vlan-name*

Example:

```
Device(config-wireless-policy)#vlan test20
```

Enters the profile policy mode and assigns the profile policy to the VLAN.

Step 5 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Restarts the WLAN.

Step 6 **exit**

Example:

```
Device(config-vlan)# exit
```

Returns to privileged EXEC mode.

What to do next

Create or Modify a Policy Tag, on page 22

Create or Modify a Policy Tag

A policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.

You can either create a new policy tag or use the default policy tag. The default policy tag automatically maps any SSID with a WLAN ID between 1 to 16 to the default policy profile. It cannot be modified nor deleted. If you have a WLAN with ID 17 or higher, the default policy tag cannot be used.

Before you begin

- Ensure you have configured a WLAN.
- Ensure you have configured a WLAN policy profile.

Step 1 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 2 **wireless tag policy** *policy-tag-name*

Example:

```
Device(config)#wireless tag policy mobility_policy_tag
```

Configures a policy tag and enters policy tag configuration mode.

Step 3 **wlan** *wlan-name* **policy** *profile-policy-name*

Example:

```
Device(config-policy-tag)#wlan mywlan policy mypolicyprofile
```

Maps the WLAN policy profile to a WLAN profile.

Step 4 **end**

Example:

```
Device(config-policy-tag)# end
```

Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

What to do next

Configure mobility groups and before doing so, Ensure Identical Parameter Configuration on Peer Controllers , on page 23.

Ensure Identical Parameter Configuration on Peer Controllers

For any anchoring or mobility event, the WLAN/policy profile configurations such as details in the security policy values on each controller must match. Before you proceed to configure mobility groups, setup tunnels and configure anchors, ensure that the following parameters are correctly configured on the peer controllers. Use the following checklist to make a note of the configurations on each controller.

Table 4: Checklist for parameter configuration on different controllers

Parameter	On 9800 controllers	On AireOS controllers
Network Settings - VLAN	Go to **Configuration** > **Layer 2** > **VLAN** > **VLAN** and check the VLAN.	Go to **Controller** > **Interface** > **Edit** and check the VLAN.
WLAN Settings		
Security Settings	Go to **Configuration** > **Tags & Profiles** > **WLANs**. Select the **WLAN** and in the **Edit WLAN** window, ensure the parameter settings in the **Security** tab match the settings of the similar parameters on the peer AireOS controllers.	Go to **Controller** > **WLAN** > **WLAN**. Select **WLANEdit WLAN IDSecurity** tab, match the settings of the similar parameters on the peer 9800 controllers.
Layer 2		
Layer 2 Security Mode - MAC Filtering	Y	Y
Layer 2 Security Mode - WPA2/WPA3 Encryption	Y	Y
Layer 2 Security Mode - Auth Key Management	Y	Y
Layer 3		
Web Policy	Y	Y
WLAN Policy Profile **Note** This is available only on Cisco 9800 controllers. Corresponding settings on the Cisco AireOS is available on the WLAN ID.	Go to **Configuration** > **Tags & Profiles** > **Policy**. Select the **Policy Profile** and in the **Edit Policy Profile** window, ensure the parameter settings in the **Advanced** tab match the settings of the similar parameters on the peer AireOS controllers.	

Parameter	On 9800 controllers	On AireOS controllers
		Go to **Controller** > **WLAN** > **WLAN**. Select the **WLAN ID** and in the **WLANs > Edit WLAN IDAdvanced** tab, match the settings of the similar parameters on the peer 9800 controllers.
IPv4 DHCP Required	Y	Y
DHCP Server IP Address	Y	Y
WLAN IPv4 ACL	Y	Y
WLAN IPv6 ACL	Y	Y
QOS	Y	Y
Timeout	Y	Y
KeepAlive	Y	Y
Web Auth Parameter Map The following settings are applicable only for 9800-CL.		
Virtual IPv4 Address		
Virtual IPv6 Address		

Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility

A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These controllers can dynamically share context and state of client devices, controller load information, and can also forward data traffic among them, which enables inter-controller wireless LAN roam and controller redundancy.

Each controller in a mobility group is configured with a list of the other members of the mobility group. Each controller device builds a neighbor relationship with every other member of the group.

The configuration comprises of the following tasks:

This configuration is required when you are setting up Catalyst 9800 and Cisco AireOS (IRCM image) as mobility peers. The configuration consists of:

1. Collecting the peer mobility information, in this case the AireOS controller.
2. Adding the peer controller information into the 9800 controller.

Note that you will need to add this information for all the controllers that are part of the mobility group.

Before you begin

- 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 will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- Each controller must be manually configured with the MAC address and IP address of all the other mobility group members.
- Ensure that there is IP connectivity between the management interfaces of all controller devices; verify by pinging between them.
- The controllers need unrestricted access through any firewalls or access control lists (ACL) to use UDP port 16666 (unencrypted) or UDP port 16667 (encrypted) for message exchange between them.
- All controllers must be configured with the same mobility group name for seamless roaming; the mobility group name is case-sensitive.
- If High Availability (HA) is configured in Catalyst 9800 controller, you will need to manually set the wireless mobility mac address.

Before you start to configure the peers:

- Log in to the AireOS (IRCM image) controller and collect the AireOS mobility information. Gather the Mobility Group Name and Mobility MAC Address by entering the **show mobility summary** exec command.

```
Device >show mobility summary

Mobility Protocol Port.......................... 16666
Default Mobility Domain......................... test
Multicast Mode ................................. Disabled
Mobility Domain ID for 802.11r.................. 0x6ef9
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Members Configured............... 2
Mobility Control Message DSCP Value............. 48

Controllers configured in the Mobility Group

 MAC Address        IP Address         Group Name                 Multicast IP
                             Status
00:59:dc:c3:d0:00  172.16.0.5             test                        0.0.0.0
                               Up
```

- Ensure that you have already created a mobility group on the Catalyst 9800 controller and have set up the global configurations of the group that includes the Mobility MAC Address, IP Address, Keep Alive Interval, Keep Alive Count and the DSCP Value.

On the 9800 controller, follow the steps to setup the tunnel between the peer controllers:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 Use the options given below to configure IPv4 or IPv6.

- **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name* **data-link-encryption**
- **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **public-ip** *public-ip-address* **group** *group-name*

Example:

```
Device(config#)wireless mobility group member mac-address 00:59:dc:c3:d0:00
ip 172.16.0.5 group test data-link-encryption
```

```
Device(config#)wireless mobility mac-address 001E.BD0C.5AFF
ip fd09:9:2:49::55 group test
```

Adds the peer AireOS controller IPv4 or IPv6 address to a specific group.

On the 9800 controller, control plane encryption is always enabled. When you are pairing it with an AireOS controller ensure that Secure Mobility is enabled on the AireOS controller. Check the corresponding configuration on AireOS controller (step 1 of #unique_18. This ensures that the CAPWAP protocol is used for the mobility tunnel and that encryption is always on for the control plane traffic.

(Optional) You can choose to have data link encryption enabled. However if you enable it on 9800, you will need to enable it on AireOS using **config mobility group member data-dtls** *mac-address of Catalyst 9800* enable. Data link encyption ensures that data packets sent between the peer controllers and access points are encrypted. Use the no form of the command to disable encrypted data exchange.

To remove the peer from the local group, use the **no** form of this command.

Step 4 **exit**

Example:

```
Device#exit
```

Returns to the configuration mode.

Step 5 **end**

Example:

```
Device(config)#end
```

Exits the global configuration mode and returns to privileged EXEC mode.

What to do next

Configure the Catalyst 9800 peer controller details on the AireOS (IRCM image) controller.

Configure Mobility Groups on Cisco AireOS (IRCM image) Controllers for Secure Mobility

This configuration is required on the AireOS(IRCM image) controller after you have configured this AireOS controller as a peer on the Catalyst 9800 controller. Including both these controllers as part of the mobility group sets them up as mobility peers.

Before you begin

Before you start to configure the peers, log in to the Catalyst 9800 controller and gather the Mobility Group Name and Mobility MAC Address by entering the **show wireless mobility summary** exec command.

```
Device#show wireless mobility summary

Mobility Summary

Wireless Management VLAN: 2601
Wireless Management IP Address: 9.12.32.10
Mobility Control Message DSCP Value: 10
Mobility Keepalive Interval/Count: 5/3
Mobility Group Name: test
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001E.BD0C.5AFF
```

If you are adding a 9800-CL as a mobility peer, collect the hash value from the 9800 controller

```
Device#show wireless management trustpoint

Trustpoint Name  : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 99459418731eb69f234058da4ebb10fddc9f939c
Private key Info : Available
FIPS suitability : Not Applicable
```

With the above information handy, log in to the AireOS(IRCM image) controller and follow the steps below to setup the tunnel between the peer controllers:

Step 1 **config mobility group member add** *peer-mac-addr peer-ip-addr group-name* **encrypt { enable | disable}**

Example:

```
Device >config mobility group member add mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test encrypt
 enable
```

Adds the peer 9800 controller to a mobility group with the peer's mac address and ip address. Configures a secure communication to the mobility group, by identifying itself with a group name.

Step 2 **config mobility group member data-dtls** *peer-mac-addr* **{ enable | disable}**

Example:

```
Device >config mobility group member data-dtls 001E.BD0C.5AFF { enable | disable}
```

(Optional) Configures the peer controller data traffic encryption. If you enable it on the 9800 controller, you will need to enable it on AireOS.

Step 3 **config mobility group member hash** *peer-ip-addr 40-digit-ssc-hash-key*

Example:

```
Device >config mobility group member hash ip 9.10.17.47 99459418731eb69f234058da4ebb10fddc9f939c
```

Configure the SSC hash of the Cisco Catalyst 9800 Series Wireless Controllers. SSC hash is needed only for peers that do not use a MIC certificate. For example: Cisco Catalyst 9800-CL Wireless Controllers. You should have got the hash information earlier.

Step 4 **show mobility summary encryption**

Example:

```
Device >show mobility summary encryption

Mobility Number of Mobility members configure.... 6
 MAC Address        IP Address                                       Group Name
    Secure           Data Encryption  Status
 001E.BD0C.5AFF     9.12.32.10                                       test
Enabled          Enabled         Control and Data Path Down
 00:35:1a:10:2f:93  9.11.42.109                                      test
N/A              N/A             Up
 00:59:dc:c3:0a:80  9.11.41.108                                      test
Disabled         N/A             Up
 11:11:11:11:11:11  4.5.6.7                                          test
Enabled          Enabled         Control and Data Path Down
 11:22:33:33:44:55  1.1.1.1                                          test
Enabled          Enabled         Control and Data Path Down
 f0:1e:e6:8a:2d:ff  9.10.17.47                                       test
Enabled          Disabled        Control and Data Path Down
```

Displays the peer to peer mobility encryption status.

Step 5 **show mobility summary**

Example:

```
Device >show mobility summary

Mobility Protocol Port........................... 16666
Default Mobility Domain.......................... mobility
Multicast Mode .................................. Disabled
Mobility Domain ID for 802.11r................... 0xd596
Mobility Keepalive Interval...................... 10
Mobility Keepalive Count......................... 3
Mobility Group Members Configured................ 6
Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group
 MAC Address        IP Address                                       Group Name
    Multicast IP                                     Status
 001E.BD0C.5AFF     9.12.32.10                                       test
 0.0.0.0                                          Control and Data Path Down
 00:35:1a:10:2f:93  2009:9:11:40::109                                test
 ::                                               Up
 00:35:1a:10:2f:93  9.11.42.109                                      test
 0.0.0.0                                          Up
 00:59:dc:c3:0a:80  9.11.41.108                                      test
 0.0.0.0                                          Up
 11:11:11:11:11:11  4.5.6.7                                          test
 0.0.0.0                                          Control and Data Path Down
 11:22:33:33:44:55  1.1.1.1                                          test
 0.0.0.0                                          Control and Data Path Down
```

```
f0:1e:e6:8a:2d:ff  9.10.17.47                                    test
0.0.0.0                                   Control and Data Path Down
```

What to do next

Verify the configuration on the 9800 controller

```
Device#show wireless mobility summary

Mobility Summary

Wireless Management VLAN: 2601
Wireless Management IP Address: 172.16.0.5
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: test
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 00:59:dc:c3:d0:00

Controllers configured in the Mobility Domain:

 IP                Public Ip         Group Name                      Multicast IPv4
Multicast IPv6                                 Status                           PMTU
------------------------------------------------------------------------------------------
172.16.0.21       N/A               test                            0.0.0.0           ::
                                           N/A                             N/A
172.16.0.5        172.16.0.5        test                            0.0.0.0           ::
                                           Up                             1385
```

Verify the status of the client for L2 roam in case the client roams:

- from a Catalyst 9800 controller to another Catalyst 9800 controller on the same VLAN
- between two AireoS controllers with IRCM image on the same VLAN.

The following example depicts a L2 roam between two AireOS (IRCM image) controllers.

```
Device >show client summary

Number of Clients............................... 1

Number of PMIPV6 Clients........................ 0

Number of EoGRE Clients......................... 0

                                                                GLAN/
                                                                RLAN/
MAC Address       AP Name                      Slot Status        WLAN  Auth Protocol
      Port Wired Tunnel  Role
----------------- ----------------------------- ---- ------------- ----- ----
---------------- ---- ----- ------- ----------------
60:38:e0:0b:01:1a APA0B4.3969.ADA6              1   Associated     1    Yes   802.11n(5
GHz)   1    No    No      Local
```

Show the details of a particular client:

```
Device >show client detail 60:38:e0:0b:01:1a
Client MAC Address............................. 60:38:e0:0b:01:1a
Client Username ................................ N/A
Client Webauth Username ......................... N/A
Hostname: .......................................
Device Type: .................................... Unclassified
AP MAC Address................................... c4:b2:39:2a:f5:c0
AP Name.......................................... APA0B4.3969.ADA6
AP radio slot Id................................. 1
Client State..................................... Associated
User Authenticated by ........................... None
Client User Group................................
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 1
Wireless LAN Network Name (SSID)................. IRCM1014_WLAN_OPENAUTH1
Wireless LAN Profile Name........................ IRCM1014_WLAN_OPENAUTH1
WLAN Profile check for roaming................... Disabled
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 14 secs
BSSID............................................ c4:b2:39:2a:f5:cf
Channel.......................................... 100
IP Address....................................... 10.14.115.197
Gateway Address.................................. 10.14.115.1

--More-- or (q)uit
Netmask.......................................... 255.255.255.0
IPv6 Address..................................... fe80::6238:e0ff:fe0b:11a
Association Id................................... 1
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Client IPSK-TAG.................................. N/A
Status Code...................................... 0
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
QoS Level........................................ Silver
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
Burst Real Time data Rate........................ 0
Avg Uplink data Rate............................. 0
Burst Uplink data Rate........................... 0
Avg Uplink Real time data Rate................... 0
Burst Uplink Real Time data Rate................. 0
802.1P Priority Tag.............................. disabled
Security Group Tag............................... Unknown(0)
KTS CAC Capability............................... No
Qos Map Capability............................... No
WMM Support...................................... Enabled

--More-- or (q)uit
  APSD ACs......................................  BK  BE  VI  VO
Supported Rates.................................. 6.0,9.0,12.0,18.0,24.0,36.0,
  ............................................... 48.0,54.0
Mobility State................................... Local
Mobility Move Count.............................. 0
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Pre-auth IPv4 ACL Name........................... none
Pre-auth IPv4 ACL Applied Status................. Unavailable
Pre-auth IPv6 ACL Name........................... none
Pre-auth IPv6 ACL Applied Status................. Unavailable
Pre-auth Flex IPv4 ACL Name...................... none
Pre-auth Flex IPv4 ACL Applied Status............ Unavailable
Pre-auth Flex IPv6 ACL Name...................... none
Pre-auth Flex IPv6 ACL Applied Status............ Unavailable
Pre-auth redirect URL............................ none
Audit Session ID................................. 0a0e750a000000796166331d
```

```
AAA Role Type.................................... none
Acct Interim Interval............................ 0
Local Policy Applied............................. none
IPv4 ACL Name.................................... none
AAA FlexConnect ACL Applied Status............... Unavailable
IPv4 ACL Applied Status.......................... Unavailable

--More-- or (q)uit
IPv6 ACL Name.................................... none
IPv6 ACL Applied Status.......................... Unavailable
Post-auth Flex IPv6 ACL Name..................... none
Post-auth Flex IPv6 ACL Applied Status........... Unavailable
Layer2 ACL Name.................................. none
Layer2 ACL Applied Status........................ Unavailable
URL ACL Name..................................... none
URL ACL Applied Status........................... Unavailable
Client Type...................................... SimpleIP
mDNS Status...................................... Disabled
mDNS Profile Name................................ none
No. of mDNS Services Advertised.................. 0
Policy Type...................................... N/A
Encryption Cipher................................ None
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... Unknown
Interface........................................ vlan0115
VLAN............................................. 115
Quarantine VLAN.................................. 0
Access VLAN...................................... 115
Local Bridging VLAN.............................. 115
Client Capabilities:

--More-- or (q)uit
      Radio Capability........................... 802.11n
      CF Pollable................................ Not implemented
      CF Poll Request............................ Not implemented
      Short Preamble............................. Not implemented
      PBCC....................................... Not implemented
      Channel Agility............................ Not implemented
      Listen Interval............................ 10
      Fast BSS Transition........................ Not implemented
      11v BSS Transition......................... Not implemented
Non-Operable Channels............................ None
Non-Prefer Channels.............................. None
Client Wifi Direct Capabilities:
      WFD capable................................ No
      Manged WFD capable......................... No
      Cross Connection Capable................... No
      Support Concurrent Operation............... No
Fast BSS Transition Details:
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0
Assisted Roaming Prediction List details:



--More-- or (q)uit
 Client Dhcp Required:     False
Allowed (URL)IP Addresses
-------------------------

AVC Profile Name: ............................... none
OpenDns Profile Name: ........................... none
```

```
Fastlane Client: ................................ No
Max DSCP: ....................................... 0
Nas Identifier: ................................. Kukri1
Fabric Statistics
--------------------
Client Statistics:
      Number of Bytes Received................... 0
      Number of Bytes Sent....................... 0
      Total Number of Bytes Sent................. 0
      Total Number of Bytes Recv................. 0
      Number of Bytes Sent (last 90s)............ 0
      Number of Bytes Recv (last 90s)............ 0
      Number of Packets Received................. 0
      Number of Packets Sent..................... 0
      Number of Interim-Update Sent.............. 0
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0

--More-- or (q)uit
      Number of EAP Request Msg Timeouts......... 0
      Number of EAP Request Msg Failures......... 0
      Number of EAP Key Msg Timeouts............. 0
      Number of EAP Key Msg Failures............. 0
      Number of Data Retries..................... 0
      Number of RTS Retries...................... 0
      Number of Duplicate Received Packets....... 0
      Number of Decrypt Failed Packets........... 0
      Number of Mic Failured Packets............. 0
      Number of Mic Missing Packets.............. 0
      Number of RA Packets Dropped............... 0
      Number of Policy Errors.................... 0
      Radio Signal Strength Indicator............ -30 dBm
      Signal to Noise Ratio...................... 65 dB
      Client Detected as Inactive................ Yes
Client RBACL Statistics:
      Number of RBACL Allowed Packets............ 0
      Number of RBACL Denied Packets............. 0
Client Rate Limiting Statistics:
      Number of Data Packets Received............ 0
      Number of Data Rx Packets Dropped.......... 0
      Number of Data Bytes Received.............. 0
      Number of Data Rx Bytes Dropped............ 0

--More-- or (q)uit
      Number of Realtime Packets Received........ 0
      Number of Realtime Rx Packets Dropped...... 0
      Number of Realtime Bytes Received.......... 0
      Number of Realtime Rx Bytes Dropped........ 0
      Number of Data Packets Sent................ 0
      Number of Data Tx Packets Dropped.......... 0
      Number of Data Bytes Sent.................. 0
      Number of Data Tx Bytes Dropped............ 0
      Number of Realtime Packets Sent............ 0
      Number of Realtime Tx Packets Dropped...... 0
      Number of Realtime Bytes Sent.............. 0
      Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
      AP00A2.8900.3660(slot 1)
        antenna0: 77 secs ago.................... -30 dBm
        antenna1: 77 secs ago.................... -30 dBm
      APA0B4.3969.ADA6(slot 0)
        antenna0: 1772 secs ago.................. -27 dBm
        antenna1: 1772 secs ago.................. -27 dBm
      APA0B4.3969.ADA6(slot 1)
```

```
        antenna0: 2 secs ago.................... -26 dBm
        antenna1: 2 secs ago.................... -26 dBm


--More-- or (q)uit
DHCP Server IP Address: ...................... 10.14.115.1
 Discover-offer time: 1597

 Request-ack time: 2134
```

Verify the status of the client for L3 roam, in case the client roams:

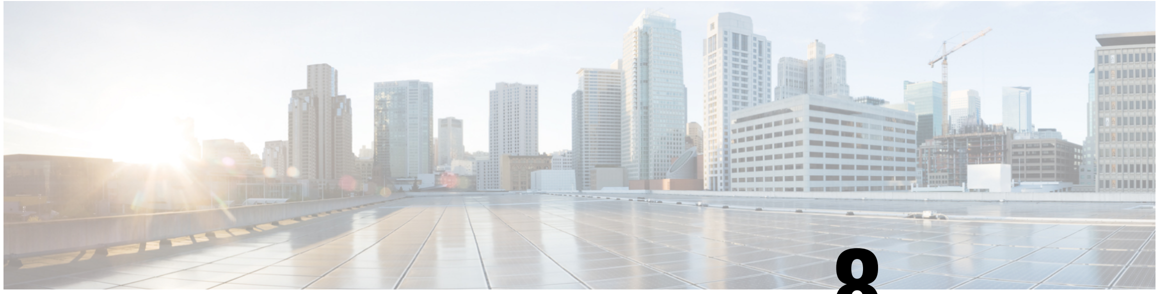
- from a Catalyst 9800 controller to another Catalyst controller on a different VLAN
- from one AireoS controllers (with IRCM image) to another AireOS controller on different VLANs.
- from a Catalyst 9800 controller to an AireOS controller or vice versa.

The following example depicts a client roaming from an AireOS controller to a 9800 controller.

```
Device>show wireless client summary
Number of Clients: 1

MAC Address    AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
6038.e00b.011a AP687D.B45C.1300                               WLAN 1    Run
11n(5)   None       Foreign

Number of Excluded Clients: 0
```

Show the details of a particular client:

```
Device>show wireless client mac-address 6038.e00b.011a detail

Client MAC Address : 6038.e00b.011a
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.14.115.197
Client IPv6 Addresses : fe80::6238:e0ff:fe0b:11a
Client Username: N/A
AP MAC Address : 687d.b45e.e2e0
AP Name: AP687D.B45C.1300
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: IRCM1014_WLAN_OPENAUTH1
Wireless LAN Network Name (SSID): IRCM1014_WLAN_OPENAUTH1
BSSID : 687d.b45e.e2ef
Connected For : 21 seconds
Protocol : 802.11n - 5 GHz
Channel : 149
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1710 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m14
Supported Rates : 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Anchor IP Address           : 10.14.117.10
  Point of Attachment         : 0x90000006
  Point of Presence           : 0xA0000002
  AuthC status                : False
  Move Count                  : 1
  Mobility Role               : Foreign
  Mobility Roam Type          : L3
  Mobility Complete Timestamp : 10/12/2021 18:21:18 PDT
Client Join Time:
  Join Time Of Client : 10/12/2021 18:21:18 PDT
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 21 seconds
Policy Type : N/A
Encryption Cipher : None
Transition Disable Bitmap : 0x00
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 116
Multicast VLAN : 0
Anchor VLAN : 115
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000006
  IIF ID             : 0x90000006
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 0a0e750a000000796166331d
  Acct Session ID  : 0x00000000
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_default-policy-profile_local (priority 254)
    VLAN             : 116
    Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name        : VLAN0116
    VLAN             : 116
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 0
  Number of Bytes Sent to Client : 0
  Number of Packets Received from Client : 0
  Number of Packets Sent to Client : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -25 dBm
  Signal to Noise Ratio : 79 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
  AP58AC.78DC.F830 (slot 1)
   antenna 0: 10 s ago ........ -32  dBm
   antenna 1: 10 s ago ........ -32  dBm
  AP687D.B45C.1300 (slot 1)
   antenna 0: 10 s ago ........ -20  dBm
   antenna 1: 10 s ago ........ -20  dBm
EoGRE : No/Simple client
Max Client Protocol Capability: 802.11n
WiFi to Cellular Steering : Not implemented
Cellular Capability : N/A
Advanced Scheduling Requests Details:
  Apple Specific Requests(ASR) Capabilities/Statistics:
    Regular ASR support: DISABLED
```



CHAPTER 8

Configure Enterprise Mobility using the GUI

The Brownfield deployment model assumes that the existing topology has a mix of Cisco AireOS 8.8.111 (or 8.5-based IRCM Image) and Cisco AireOS 8.2/8.3/8.5 controllers and that one or more Catalyst 9800 controllers are being deployed to replace the older AireOS controllers within the enterprise.

Note that the document assumes that you already have an understanding of the preliminary tasks required to set up your topology. However as a brief refresher, the following task list provides you with a checklist to ensure that your configurations are complete before you proceed to configure mobility groups to promote mobility for the wireless clients

Table 5: Preliminary Tasks

Have you completed?	Configurations
1	Configure VLAN, on page 38
2	Configure WLAN and Associated Settings, on page 39

Table 6: Mobility specific configurations

Step	Task
1	Ensure Identical Parameter Configuration on Peer Controllers , on page 23
2	Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility, on page 40

Once the above configurations are completed, the following types of roaming are possible between the controllers.

Note The following table is only illustrative of the possible combinations. Depending on the size of the enterprise, clients might roam between two-node or three- node setups. Accordingly, their roam might also be classified as Layer 2 or Layer 3 intercontroller roam with the client roaming between different vlans that are not discussed in detail.

Table 7:

Type of Roaming	Between	Associated VLAN Configuration
Layer 3	Catalyst 9800 and AireOS controllers 8.8.111 (or 8.5-based IRCM Image)	Controllers are on different VLAN ID or same VLAN ID.
	Catalyst 9800 and Catalyst 9800	Controllers are on different VLAN ID.
Layer 2	Two Catalyst 9800 controllers	Controllers are on same VLAN ID
Layer 2	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and AireOS controller 8.2/8.3/8.5	Controllers are on same VLAN ID and same subnet
Layer 3	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and Catalyst AireOS controller 8.2/8.3/8.5	Controllers are on different VLAN ID.

Depending on your requirement, follow the steps below to set up the controllers to enable roaming across the enterprise.

Most of the preliminary steps discussed below, are from the perspective of deploying Catalyst 9800 controllers to your existing setup. If you need help with deploying AireOS controllers with IRCM image, refer to the respective AireOS documents.

- Configure VLAN, on page 38
- Configure WLAN and Associated Settings, on page 39
- Configure Mobility Groups between Peer Controllers Using the GUI, on page 39
- Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility, on page 40

Configure VLAN

A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application without regard to the physical locations of the users. Before you start any configuration, you need to add the VLANs to which wireless clients will be assigned.

Step 1 Navigate to **Configuration** > **Layer2** > **VLAN** > **VLAN**

Click on the **Add** button to add a VLAN.

Step 2 Enter the details (VLAN ID and VLAN Name)

Repeat the steps to configure multiple VLANs for e.g. VLAN ID is **vlan 20** and VLAN name as **test 20**Alternatively, create a range of VLANs by entering a VLAN ID range. Note that the available VLAN ID range is 1 to 4094 and the recommended length for the VLAN Name is less than 20 characters.

Step 3 Click **Apply to Device**.

What to do next

Verify the VLAN/Interface Configuration on the GUI. The configured VLANs are listed on the page.

Configure WLAN and Associated Settings

WLAN is a network that allows devices to connect and communicate wirelessly.

Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability. You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.

Step 1 Navigate to **Configuration** > **Wireless** > **WLANs** and click on the **Add** button to add a WLAN.

Step 2 Enter all the needed information (SSID name, security type and so on) and once done, click **Save &Apply to Device**. In this example the SSID name is `IRCM1014_WLAN_OPENAUTH1`.

Step 3 Navigate to **Configuration** > **Tags & Profiles** > **Policy**. Select the name of a pre-existing policy or click **+Add** to create a new policy. Enable the policy, set the needed VLAN and any other parameter you want to customize and click **Save & Apply to Device** .

Step 4 Next, create or modify a Policy Tag. To do so, go to **Configuration** > **Tags & Profiles** > **Tags** > **Policy**. Select a pre-existing policy tag or click **+ Add** to add a new one.

Step 5 Inside the Policy Tag, click **+ Add** . From the drop-down list select the **WLAN Profile** name you want to add to the Policy Tag and to which you want to link it. To complete the task, click **Save & Apply to Device** .

Step 6 Repeat the above for all the WLANs that you want to add. Click **Save & Apply to Device**once the task is complete.

What to do next

Ensure Identical Parameter Configuration on Peer Controllers , on page 23 and Configure Mobility Groups between Peer Controllers Using the GUI, on page 39.

Configure Mobility Groups between Peer Controllers Using the GUI

A Mobility Group is a group of Wireless LAN Controllers (WLCs or controllers) in a network with the same Mobility Group name. These controllers can dynamically share context and state of client devices, controller load information, and can also forward data traffic among them, which enables inter-controller wireless LAN roam and controller redundancy.

Each controller in a mobility group is configured with a list of the other members of the mobility group. Each controller device builds a neighbor relationship with every other member of the group.

The configuration comprises of the following tasks:

Table 8:

Step	Task
1	Create a mobility group on Catalyst 9800 and on the AireOS 8.8.111 (or 8.5-based IRCM Image) controller.
2	Configure peer information on Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) controller and set up tunnel between them.
3	Verify the tunnel.

Before you begin:

- 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 will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- Each controller must be manually configured with the MAC address and IP address of all the other mobility group members.
- Ensure that there is IP connectivity between the management interfaces of all controller devices; verify by pinging between them.
- The controllers need unrestricted access through any firewalls or access control lists (ACL) to use UDP port 16666 (unencrypted) or UDP port 16667 (encrypted) for message exchange between them.
- All controllers must be configured with the same mobility group name; the mobility group name is case-sensitive.
- All controllers must be configured to use the same virtual interface IP address.

Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility

This configuration is required when you are creating a mobility group and setting up Catalyst 9800 and Cisco AireOS (IRCM image) as mobility peers.

Follow the steps to setup the tunnel between the peer controllers:

Step 1 Configure Mobility Group on the Catalyst 9800 controller. To do so, on the Catalyst 9800's GUI , go to **Configuration** > **Mobility** and in the **Global Configuration** tab, perform the following tasks:

a) Enter a name for the mobility group.
b) Enter the multicast IP address for the mobility group.
c) n 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) (Optional) Enter the DSCP value for the mobility group.

f) Enter the mobility MAC address.

g) (Optional) Enable the **DTLS High Cipher Only** button to advertise higher cipher suites during DTLS handshakes. This is disabled, by default.

h) Click **Apply**.

Step 2 Configure the mobility peer on Catalyst 9800. This information can be collected from an AireOS controller by navigating to the AireOS GUI's **CONTROLLER** > **Mobility Management** > **Mobility Groups** and noting the MAC Address, IP Address and Group Name of the AireOS controller.

Step 3 Add the AireOS controller information into the Cisco Catalyst controller.On the Catalyst 9800's GUI , go to **Configuration** > **Mobility** and 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 the IP address for the mobility peer.

c) Additionally, when NAT is used, enter the optional public IP address to enter the mobility peer's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility peer's direct IP address.

d) Enter the mobility group to which you want to add the mobility peer.

e) Select the required status for Data Link Encryption.

f) 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.

g) Click **Apply to Device**.

h) (Optional) In the **Non-Local Mobility Group Multicast Configuration** section, click **Add** if you want the mobility messages to use multicast. This enables the controller to send only one copy of the message to the network, which in turn goes to the multicast group that contains all the mobility members.

i) Enter the mobility group name.

j) Enter the multicast IP (v4/v6) address for the mobility group.

k) Click Save.

Note On the Catalyst 9800 controller, control plane encryption is always enabled, which means that you need to have secure mobility enabled on the AireOS side. However, data link encryption is optional. If you enable it on the 9800 side, you will need to enable it on AireOS.

Step 4 Configure the mobility peer on the AireOS 8.8.111 (or 8.5-based IRCM Image) controller. To do so, collect the Catalyst 9800 controller mobility information. On the Catalyst 9800 GUI, navigate to **Configuration** > **Wireless** > **Mobility** > **Global Configuration** and note the **Mobility Group Name** and **Mobility MAC Address**. Collect the Hash value from the Catalyst 9800 controller if this is a virtual controller.

Step 5 Add the Catalyst 9800 controller information into the AireOS controller. To do so, navigate to **CONTROLLER** > **Mobility Management** > **Mobility Groups** > **New**, enter the values.

a) Enter the management interface IPv4/IPv6 address and the MAC address of the controller to be added in the respective text boxes.

If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IPv4/IPv6 address that is sent to the controller from the NAT device rather than the controller’s management interface IPv4/IPv6 address. Otherwise, mobility will fail among controllers in the mobility group.

b) In the **Group Name** text box, enter the name of the mobility group.

Note The mobility group name is case sensitive.

c) From the Secure Mobility drop-down list, choose **Enabled**.

d) From the **Data Tunnel Encryption** drop-down list, choose **Disabled** or **Enabled** based on what was configured on the peer Catalyst 9800 controller .

e) From the **High Cipher** drop-down list, choose **Enabled** You must enable **High Cipher** only if you require DTLS v1.2 encryption. The default value is **Disabled**. In disabled state, DTLS v1.0 encryption is enabled.

Note Note that this configuration must match the configuration on Catalyst 9800.

f) Enter the hash key of the peer mobility controller, which should be a virtual controller in the same domain.

Note Hash is only required in case of the virtual Catalyst 9800 -CL controller that uses a self-signed certificate. Appliances have a MIC certificate and don't need a hash.

Note Hash is not supported for IPv6 members.

g) Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the AireOS controller's **Static Mobility Group Members** page. Save the configuration by clicking the appropriate button.

Step 6 Verify the mobility tunnel between the peers is up and runnning. To do so, in the Catalyst 9800 controller's **Mobility Peer Configuration** section, view the list of devices that are part of this peer configuration. Ensure that the **Status** is **Up** .

CHAPTER 9

Configure Guest Anchor for Guest Access Services with Catalyst 9800 and AireOS IRCM Controllers

The Wireless Guest Access model addresses the need to provide internet access to guests in a secure and accountable manner. While there can be many different deployments, this section focuses on the implementation of wireless guest networking using a combination of controllers that includes a Foreign Anchor solution. It has a mixed deployment where Catalyst 9800, Cisco AireOS 8.8.111 (or 8.5-based IRCM Image) and Cisco AireOS 8.2/8.3/8.5 controllers co-exist and have designated roles for anchor and foreign depending upon the setup. In addition to one controller being designated as a guest anchor, the guest deployment may or may not have additional controllers in the DMZ for load balancing.

Table 9: Workflow to promote mobility in guest deployment scenario using a guest anchor

Step	Configuration
Mandatory	Ensure that you have configured a VLAN and assigned an interface for guest traffic. See Configure VLAN, on page 38 for more information.

Step	Configuration
Mandatory	Ensure that you have configured a Guest WLAN. See Configure WLAN and Associated Settings, on page 39 for more information. The guest WLAN is configured on every foreign controller that manages APs where guest access is required. Even though the anchor controller(s) is not specifically used to manage APs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor controller is a logical extension of the WLAN where user traffic is ultimately bridged (using CAPWAP between the AP and the foreign controller, and Secure Mobility/ EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor controller. **Note** It is extremely important to note that all parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign controllers. See Ensure Identical Parameter Configuration on Peer Controllers , on page 23 for more information.

Step	Configuration
Mandatory	Ensure that you have set up mobility groups that will be part of this deployment. There can be many possible combinations, only some of the cases are detailed below. Configure the mobility group as per your requirement. **Note** It is important to configure peer controllers to tunnel the traffic from one controller to another. However, when you are trying to set up the guest controller in the DMZ as an anchor controller, the mobility group name with the peer controller does not have to match, as usually the anchor controller will not have APs attached and clients cannot roam from one controller to the other in a DMZ. Setting up the peers ensures that the client can access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. See Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility, on page 24 OR See Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility, on page 40
Mandatory	Configure the mobility anchor based on your deployment setup. Choose from the following available choices listed in this document. Configure Mobility Anchors using the CLI, on page 46 Configure Mobility Anchors using the GUI, on page 65 • Configure a Catalyst 9800 as Anchor with another Catalyst 9800 as Foreign Controller • Configure Catalyst 9800 as Anchor and AireOS Controller (IRCM image) as Foreign Controller • Configure AireOS (IRCM Image) Controller as Anchor with Catalyst 9800 as Foreign Controller • Configure AireOS Controller (IRCM image) as Anchor and AireOS as Foreign Controller

Step	Configuration
Optional	Configure load balancing if you have more than one Catalyst 9800 controller in the DMZ. OR Configure load balancing if you have more than one AireOS controller (IRCM image) in the DMZ.
Optional	Verify the configuration.

- Configure Mobility Anchors using the CLI, on page 46
- Configure Mobility Anchors using the GUI, on page 65

Configure Mobility Anchors using the CLI

Mobility Anchor, also referred to as Guest tunneling or Auto Anchor Mobility, is a feature where all the client traffic that belongs to a WLAN (specially Guest WLAN) is tunneled to a predefined controller or set of controllers that are configured as Anchor for that specific WLAN. This feature helps to restrict clients to a specific subnet and have more control over the user traffic.

Using a mobility anchor forces clients to be anchored to a controller other than the one they first associate with. This forces their traffic to be tunneled to the DMZ. Then it must pass through the firewall and its associated policies before getting anywhere. This is done on a per-WLAN basis.

- Anchor Controller - Refers to one or more controllers deployed in the enterprise DMZ that are used to perform guest mobility secure/EoIP tunnel termination, web redirection, and user authentication.
- Foreign Controller - Refers to one or more controllers deployed in the enterprise that are used to perform guest mobility secure tunnel termination, web redirection, and user authentication.

Configure a Catalyst 9800 as Anchor with another Catalyst 9800 as Foreign Controller

This task is required when you designate the Catalyst 9800 in the DMZ as Guest Anchor and the Catalyst 9800 in the enterprise as the Foreign Controller.

Before you begin

- Create a WLAN Profile for guests that defines the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the above configurations match on the peer controllers.
- Build a mobility tunnel between the Foreign Catalyst 9800 controller and Anchor Catalyst 9800 controller.

First, log in to the foreign 9800 controller and define the anchor 9800 controller's ip address under the policy profile.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor-policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor** *anchor-ip-address priority number*

Example:

```
Device(config-wireless-policy)#mobility anchor 10.88.173.49 priority 3
```

Defines anchor 9800 ip address on the foreign controller.

Step 5 **central switching**

Example:

```
Device(config-wireless-policy)#central switching
```

Enables Central switching.

Step 6 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 7 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 8 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Link the Policy Profile with the WLAN inside the Policy Tag , on page 48

Link the Policy Profile with the WLAN inside the Policy Tag

This task is required after you have created an anchor policy profile. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated to the foreign controller that service this WLAN.

Before you begin

Ensure that you have created a anchor policy profile.

On the 9800 controller:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless tag policy** *name of policy tag*

Example:

```
Device(config)#wireless tag policy PT1
```

Configures the policy tag and enters the wireless policy configuration mode.

Step 4 **wlan** *name of WLAN profile* **policy** *name of policy profile*

Example:

```
Device(config-policy-tag)#wlan anchor-ssid policy anchor-policy
```

Creates a new policy tag or edits an existing one to link the Policy Profile with the WLAN inside the Policy Tag. This tag is assigned to the APs associated with the foreign controller that service this WLAN.

Step 5 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure the AireOS controller as the guest anchor controller .

Configure settings on the 9800 Anchor Controller

This task is required after you have configured the anchor controller settings on the foreign 9800 controller. Now, log in to the 9800 anchor controller and configure the settings to match the 9800 foreign controller settings.

- Create the anchor policy profile - this name must match the name on the 9800 foreign controller.
- Enable the export anchor on the anchor controller. This instruct this 9800 controller that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign 9800 controller sends the clients to the anchor 9800 WLC, it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 WLC knows which local Policy Profile to use.

Before you begin

- Create a WLAN Profile for guests that define the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the above configurations match on the peer controllers.
- Build a mobility tunnel between the Foreign Catalyst 9800 controller and Anchor Catalyst 9800 controller.

Follow the steps below:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy***name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor-policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor**

Example:

```
Device(config-wireless-policy)#mobility anchor
```

Configures this 9800 controller as the anchor controller.

Step 5 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 6 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 7 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

Step 8 **show wireless mobility summary**

Need sample output

Step 9 **show wireless client mac <> detail**

Need sample output

What to do next

On 9800 controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

```
Device#show wireless client summary
```

Configure Catalyst 9800 Controller as Anchor and AireOS Controller (IRCM image) as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller (IRCM image) as the foreign controller in the campus/enterprise.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

On the Catalyst 9800 anchor controller do the following:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode. Creates the anchor policy profile on the 9800 anchor controller. This instructs this Catalyst 9800 controller that it is the anchor 9800 controller for any WLAN that uses that Policy Profile. When the foreign AireOS controller sends the clients to the anchor 9800 controller, it informs about the WLAN name that the client is assigned to, so the anchor 9800 controller knows which local WLAN configuration to use and it also uses this name to know which local Policy Profile to use.

Step 4 **mobility anchor**

Example:

```
Device(config-wireless-policy)#mobility anchor
```

Configures this 9800 controller as the anchor controller.

Step 5 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 6 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 7 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure AireOS Controller (IRCM image) as Foreign Controller, on page 51

Configure AireOS Controller (IRCM image) as Foreign Controller

This task is required after you have configured the 9800 anchor controller. Now, log in to the AireOS foreign controller and configure the settings, so that when the foreign AireOS controller sends the clients to the anchor 9800 controller, it can inform about the WLAN name that the client is assigned to, for the anchor controller to know which local WLAN configuration to use.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

On the AireOS (IRCM image) controller,configure the following:

Step 1 **config wlan disable** *wlan-id*

Example:

```
Device >config wlan disable 2
```

Disables the SSID on the foreign AireOS controller. This clears up any associated configurations for this SSID/WLAN.

Step 2 **config wlan mobility anchor add** *wlan-id9800 controller's management interface*

Example:

```
Device >config wlan mobility anchor add 2 10.88.173.105
```

Adds the 9800 controller as the anchor for this SSID/WLAN.

Step 3 **config wlan enable** *wlan-id*

Example:

```
Device >wlan 2
```

Enables the WLAN ID to receive clients.

What to do next

On 9800 controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

To show the wlan configuration information:

```
Device#show run wlan
wlan wlan1 1 wlan1
 dot11ax target-waketime
 dot11ax twt-broadcast-support
wlan wlan2 2 wlan2
 dot11ax target-waketime
 dot11ax twt-broadcast-support
```

To display a summary of all WLANs configured on the controller:

```
Device#show wlan summary

Number of WLANs: 2

ID   Profile Name                     SSID                             Status Security
-----------------------------------------------------------------------------------------------
1    wlan1                            wlan1                            DOWN
[WPA2][802.1x][AES]

2    wlan2                            wlan2                            DOWN
[WPA2][802.1x][AES]
```

Verify the client state on the controller:

```
Device#show wireless client summary
Number of Clients: 1

MAC Address    AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
6038.e00b.011a AP687D.B45C.1300                               WLAN 1    Run
11n(5)   None       Foreign

Number of Excluded Clients: 0

eWLC-IRCM-C1#
8520:  {'Number of Clients': '1', 'Number of Excluded Clients': '0'}
8521:  +++ eWLC-IRCM-C1 with alias 'a': executing command 'show wireless client summary'
+++
show wireless client summary
Number of Clients: 1

MAC Address    AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
6038.e00b.011a AP687D.B45C.1300                               WLAN 1    Run
11n(5)   None       Foreign

Number of Excluded Clients: 0
```

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

```
Device#show ap tag summary
```

```
show ap summary

Number of APs.................................... 2

Global AP User Name.............................. Cisco123
Global AP Dot1x User Name........................ Not Configured
Global AP Dot1x EAP Method....................... EAP-FAST

AP Name                         Slots  AP Model              Ethernet MAC       Location
            Country     IP Address       Clients  DSE Location
------------------------------  -----  -------------------  -----------------
--------------------  ----------  ---------------  -------  --------------
APA0B4.3969.ADA6                3      AIR-AP3802I-B-K9       a0:b4:39:69:ad:a6  default
location      US          10.14.117.201    0        [0 ,0 ,0 ]
AP00A2.8900.3660                3      AIR-AP1852I-B-K9       00:a2:89:00:36:60  default
location      US          10.14.117.202    0        [0 ,0 ,0 ]
```

```
Device#show ap <ap-name> tag detail
```

```
Device#show wlan { summary | id | name | all }
```

```
Device#show wireless tag policy detailed <policy-tag-name>
```

```
Device#show wireless profile policy detailed <policy-profile-name>
```

On AireOS controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

To see the wlans and the details, configured on this controller:

```
Device >show wlan summary

Number of WLANs.................................. 4

WLAN ID  WLAN Profile Name / SSID                                               Status
  Interface Name        PMIPv6 Mobility
```

```
-------  -----------------------------------------------------------------------  --------
  --------------------  ---------------
1        testlab1-mob / testlab1-mob                                              Enabled
  management            none
2        testlab1-anchor-108 / testlab1-anchor-108                                Disabled
  management            none
3        testlab1-anchor-109 / testlab1-anchor-109                                Disabled
  management            none
4        testlab1-mob-psk / testlab1-mob-psk                                      Enabled
  management            none
```

To see more details of a particular wlan configured on this controller:

```
Device >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... testlab1
Network Name (SSID).............................. testlab1
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
Client Profiling Status
    Radius Profiling ............................ Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
    Local Profiling ............................. Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
  Radius-NAC State............................... Disabled
  SNMP-NAC State................................. Disabled
  Quarantine VLAN................................ 0
Maximum Clients Allowed.......................... Unlimited
Security Group Tag............................... Unknown(0)
Maximum number of Clients per AP Radio........... 200
ATF Policy....................................... 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 180 seconds
Session Timeout.................................. 86400 seconds
User Idle Timeout................................ Disabled
Sleep Client..................................... disable
Sleep Client Timeout............................. 720 minutes
Web Auth Captive Bypass Mode..................... None
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... none
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
WLAN Layer2 ACL.................................. unconfigured
WLAN URL ACL..................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ default-mdns-profile
DHCP Server...................................... Default
Central NAT Peer-Peer Blocking................... Unknown
DHCP Address Assignment Required................. Disabled
Static IP client tunneling....................... Disabled
Tunnel Profile................................... Unconfigured
PMIPv6 Mobility Type............................. none
    PMIPv6 MAG Profile........................... Unconfigured
    PMIPv6 Default Realm......................... Unconfigured
    PMIPv6 NAI Type.............................. Hexadecimal
    PMIPv6 MAG location.......................... WLC
Quality of Service............................... Silver
Per-SSID Rate Limits............................. Upstream Downstream
Average Data Rate................................   0    0
Average Realtime Data Rate.......................   0    0
Burst Data Rate..................................   0    0
Burst Realtime Data Rate.........................   0    0
Per-Client Rate Limits........................... Upstream Downstream
Average Data Rate................................   0    0
Average Realtime Data Rate.......................   0    0
Burst Data Rate..................................   0    0
Burst Realtime Data Rate.........................   0    0
Scan Defer Priority.............................. 4,5,6
Scan Defer Time.................................. 100 milliseconds
WMM.............................................. Allowed
WMM UAPSD Compliant Client Support............... Disabled
Media Stream Multicast-direct.................... Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... 802.1P (Tag=0)
Passive Client Feature........................... Disabled
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Radius Servers
   Authentication................................ Global Servers
   Accounting.................................... Global Servers
      Interim Update............................. Enabled
      Interim Update Interval.................... 0
      Framed IPv6 Acct AVP ...................... Prefix
   Dynamic Interface............................. Disabled
   Dynamic Interface Priority.................... wlan
Local EAP Authentication......................... Disabled
Radius NAI-Realm................................. Disabled
Mu-Mimo.......................................... Enabled
Security
   802.11 Authentication:........................ Open System
   FT Support.................................... Disabled
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Disabled
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
   CKIP ......................................... Disabled
   Web Based Authentication...................... Disabled
   Web Authentication Timeout.................... 300
   Web-Passthrough............................... Disabled
   Mac-auth-server............................... 0.0.0.0
   Web-portal-server............................. 0.0.0.0
   qrscan-des-key................................
   Conditional Web Redirect...................... Disabled
   Splash-Page Web Redirect...................... Disabled
   Auto Anchor................................... Enabled
   FlexConnect Local Switching................... Disabled
   FlexConnect Central Association............... Disabled
   flexconnect Central Dhcp Flag................. Disabled
   flexconnect nat-pat Flag...................... Disabled
   flexconnect Dns Override Flag................. Disabled
   flexconnect PPPoE pass-through................ Disabled
   flexconnect local-switching IP-source-guar.... Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication.............. Disabled
   FlexConnect Learn IP Address.................. Enabled
  Client MFP................................... Optional but inactive (WPA2 not configured)

   PMF........................................... Disabled
   PMF Association Comeback Time................. 1
   PMF SA Query RetryTimeout..................... 200
   Tkip MIC Countermeasure Hold-down Timer....... 60
   Eap-params.................................... Not Applicable
AVC Visibilty.................................... Disabled
AVC Profile Name................................. None
OpenDns Profile Name............................. None
OpenDns Wlan Mode................................ ignore
Flow Monitor Name................................ None
Split Tunnel Configuration
    Split Tunnel................................. Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
SIP CAC Fail Send-486-Busy Policy................ Enabled
SIP CAC Fail Send Dis-Association Policy......... Disabled
KTS based CAC Policy............................. Disabled
Assisted Roaming Prediction Optimization......... Disabled
802.11k Neighbor List............................ Enabled
802.11k Neighbor List Dual Band.................. Disabled
802.11v Directed Multicast Service............... Enabled
802.11v BSS Max Idle Service..................... Enabled
802.11v BSS Transition Service................... Enabled
802.11v BSS Transition Disassoc Imminent......... Disabled
802.11v BSS Transition Disassoc Timer............ 200
802.11v BSS Transition OpRoam Disassoc Timer..... 40
DMS DB is empty
Band Select...................................... Disabled
Load Balancing................................... Disabled
Multicast Buffer................................. Disabled
Universal Ap Admin............................... Disabled
Broadcast Tagging................................ Disabled
PRP.............................................. Disabled

 Mobility Anchor List
 WLAN ID     IP Address            Status                             Priority
 -------     ---------------       ------                             --------
 1           9.11.41.108           Up                                  3


802.11u........................................ Disabled

MSAP Services.................................. Disabled

Local Policy
----------------
Priority  Policy Name
--------  ---------------

Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
File Transfer QoS Policy......................... Silver
QoS Fastlane Status.............................. Disable
Selective Reanchoring Status..................... Disable
Lobby Admin Access............................... Disabled

 Fabric Status
--------------

Fabric status.................................... Disable
Vnid Name........................................
Vnid............................................. 0
Applied SGT Tag.................................. 0
Peer Ip Address.................................. 0.0.0.0
Flex Acl Name....................................
Flex Avc Policy Name.............................

U3-Interface................................... Disable

U3-Reporting Interval.......................... 30
```

Configure AireOS(withIRCM Image)Controller as Anchor with Catalyst 9800 as Foreign Controller

This task is required when you are setting up the AireOS controller as the guest anchor in the DMZ and the Catalyst 9800 as the foreign controller in the campus/enterprise. On the 9800 controller:

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy policy_anchored_t6
```

Creates the anchor policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor** *anchor-ip-address priority number*

Example:

```
Device(config-wireless-policy)#mobility anchor 192.168.5.56 priority 3
```

Defines AireOS ip address as anchor on the foreign controller. Now, the 9800 controller forwards the traffic of the SSID associated with this Policy Profile to the selected AireOS anchor.

Step 5 **no shutdown**

Enables the interface.

Step 6 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Link the Policy Profile with the WLAN inside the Policy Tag , on page 58

Link the Policy Profile with the WLAN inside the Policy Tag

This task is required after you have created an anchor policy profile. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated to the foreign controller that service this WLAN. On the 9800 controller:

Before you begin

Ensure that you have created a anchor policy profile.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless tag policy** *name of policy tag*

Example:

```
Device(config)#wireless tag policy PT2
```

Configures the policy tag and enters the wireless policy configuration mode.

Step 4 **wlan** *name of WLAN profile* **policy** *name of policy profile*

Example:

```
Device(config-policy-tag)#wlan ANCHOR_IRCM policy policy_anchored_t6
```

Creates a new policy tag or edits an existing one to link the Policy Profile with the WLAN inside the Policy Tag. This tag is assigned to the APs associated with the foreign controller that service this WLAN.

Step 5 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure AireOS Controller (with IRCM image) as Guest Anchor Controller, on page 59

Configure AireOS Controller (with IRCM image) as Guest Anchor Controller

This task is required when you are setting up the AireOS controller controller as the guest anchor in the DMZ and the Catalyst 9800 as the foreign controller in the campus/enterprise. After you have configured the anchor policy profile on 9800, on the AireOS controller:

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 **config wlan mobility anchor add** *wlan_id aireos anchor_controller_ip_address* **priority** *priority-number*

Example:

```
Device >config wlan mobility anchor add 27 192.168.5.56 priority 3
```

Configures the AireOS controller as anchor controller and assigns it a priority number for load balancing.

Step 2 **save config**

Example:

```
Device >save config
```

Step 3 **show mobility anchor {wlan | guest-lan}** *{wlan_id | guest_lan_id}*

Example:

```
Device >show mobility anchor

Mobility Anchor Export List


 Priority number, 1=Highest priority and 3=Lowest priority(default).

 WLAN ID     IP Address            Status                            Priority
 -------     ---------------       ------                            --------
 1           9.11.41.108           Up                                  1

 2           9.11.41.108           Up                                  2

 27          192.168.5.56          Up                                  3


 GLAN ID     IP Address            Status
 -------     ---------------       ------
```

What to do next

Verify the configuration on the 9800 controller.

```
# show run wlan
# show wlan summary
# show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <ap-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

The client summary status on the 9800 foreign controller

```
Device#sh wireless client summary
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:53:13.762 CET Fri Dec 3 2021
Number of Clients: 3

MAC Address    AP Name                              Type ID   State          Protocol Method     Role
------------------------------------------------------------------------------------------------------------------------
08cc.68bc.15ae AP9120-2-r3-sw2-Gi1-0-39             WLAN 1    Run            11n(5)   None       Local
6c40.0899.0466 AP9120-2-r3-sw2-Gi1-0-39             WLAN 27   Run            11ac     None       Export Foreign

6c41.6a0d.2e90 AP9120-2-r3-sw2-Gi1-0-39             WLAN 1    IP Learn       11n(5)   None       Local
```

The client summary status on the AireOS anchor controller

```
Device >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

Number of EoGRE Clients.......................... 0

                                                                GLAN/
                                                                RLAN/
MAC Address       AP Name                        Slot Status        WLAN  Auth Protocol
      Port Wired Tunnel  Role
----------------- ------------------------------ ---- ------------- ----- ----
---------------- ---- ----- ------- ----------------
6c:40:08:99:04:66 192.168.25.41                   N/A Associated     27   Yes  Mobile
      13   No    No      Export Anchor
```

The client details for a particular client on the Catalyst 9800 controller

```
Device#sh wi cli mac 6c40.0899.0466 detail
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:53:59.778 CET Fri Dec 3 2021


Client MAC Address : 6c40.0899.0466
Client MAC Type : Universally Administered Address
Client IPv4 Address : 4.41.0.46
Client IPv6 Addresses : fe80::6e40:8ff:fe99:466
                        2001:4:4:4:cc8:ce83:d5e6:12f6
                        2001:4:4:4:6e40:8ff:fe99:466
Client Username: N/A
AP MAC Address : d4e8.8019.f140
AP Name: AP9120-2-r3-sw2-Gi1-0-39
AP slot : 1
Client State : Associated
Policy Profile : policy_anchored_t6
Flex Profile : N/A
Wireless LAN Id: 27
WLAN Profile Name: ANCHOR_IRCM
Wireless LAN Network Name (SSID): ANCHOR_IRCM
BSSID : d4e8.8019.f14d
Connected For : 58 seconds
Protocol : 802.11ac
Channel : 60
Client IIF-ID : 0xa0000002
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1747 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : ON
Current Rate : m9 ss3
Supported Rates : 18.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Anchor IP Address           : 192.168.5.56
  Point of Attachment         : 0x9000000F
  Point of Presence           : 0xA0000001
  AuthC status                : False
  Move Count                  : 0
  Mobility Role               : Export Foreign
  Mobility Roam Type          : L3 Requested
  Mobility Complete Timestamp : 12/03/2021 10:53:05 CET
Client Join Time:
  Join Time Of Client : 12/03/2021 10:53:02 CET
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 55 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
```

```
AAA override passphrase : No
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 169
Multicast VLAN : 0
Anchor VLAN : 504
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_9000000f
  IIF ID             : 0x9000000F
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 2919A8C00000000B7FB6204E
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : None
  Local Policies:
        Service Template : wlan_svc_policy_anchored_t6_local (priority 254)
                VLAN             : 169
                Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name        : VLAN0169
                VLAN             : 169
                Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 20
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 24115
  Number of Bytes Sent : 8301
  Number of Packets Received : 102
  Number of Packets Sent : 33
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -40 dBm
  Signal to Noise Ratio : 49 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
```

```
EoGRE : Pending Classification
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
```

The client details for a particular client on the AireOS controller after the L3 roam.

```
Device >show client detail 6c:40:08:99:04:66
Client MAC Address............................... 6c:40:08:99:04:66
Client Username ................................. N/A
AP MAC Address................................... d4:e8:80:19:f1:40
AP Name.......................................... N/A
AP radio slot Id................................. N/A
Client State..................................... Associated
Client User Group................................
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 27
Wireless LAN Network Name (SSID)................. ANCHOR_IRCM
Wireless LAN Profile Name........................ ANCHOR_IRCM
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 00:00:00:00:00:ff
Connected For ................................... 73 secs
Channel.......................................... N/A
IP Address....................................... 4.41.0.46
Gateway Address.................................. 4.0.0.1
Netmask.......................................... 255.0.0.0
IPv6 Address..................................... fe80::6e40:8ff:fe99:466
IPv6 Address..................................... 2001:4:4:4:cc8:ce83:d5e6:12f6
IPv6 Address..................................... 2001:4:4:4:6e40:8ff:fe99:466
Association Id................................... 0
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Status Code...................................... 0
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
QoS Level........................................ Silver
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
Burst Real Time data Rate........................ 0
Avg Uplink data Rate............................. 0
Burst Uplink data Rate........................... 0
Avg Uplink Real time data Rate................... 0
Burst Uplink Real Time data Rate................. 0
802.1P Priority Tag.............................. disabled
Security Group Tag............................... Unknown(0)
KTS CAC Capability............................... No
Qos Map Capability............................... No
WMM Support...................................... Disabled
Supported Rates..................................
Mobility State................................... Export Anchor
Mobility Foreign IP Address...................... 192.168.25.41
Mobility Move Count.............................. 1
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Audit Session ID................................. 2919A8C00000000B7FB6204E
AAA Role Type.................................... none
Acct Interim Interval............................ 0
Local Policy Applied............................. none
IPv4 ACL Name.................................... none
AAA FlexConnect ACL Applied Status............... Unavailable
IPv4 ACL Applied Status.......................... Unavailable
IPv6 ACL Name.................................... none
```

```
IPv6 ACL Applied Status.......................... Unavailable
Layer2 ACL Name.................................. none
Layer2 ACL Applied Status........................ Unavailable
Client Type...................................... SimpleIP
mDNS Status...................................... Disabled
mDNS Profile Name................................ none
No. of mDNS Services Advertised.................. 0
Policy Type...................................... N/A
Encryption Cipher................................ None
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... Unknown
Interface........................................ vlan4
VLAN............................................. 504
Quarantine VLAN.................................. 0
Access VLAN...................................... 504
Local Bridging VLAN.............................. 504
Client Capabilities:
      CF Pollable................................ Not implemented
      CF Poll Request............................ Not implemented
      Short Preamble............................. Not implemented
      PBCC....................................... Not implemented
      Channel Agility............................ Not implemented
      Listen Interval............................ 0
      Fast BSS Transition........................ Not implemented
      11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
      WFD capable................................ No
      Manged WFD capable......................... No
      Cross Connection Capable................... No
      Support Concurrent Operation............... No
Fast BSS Transition Details:
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0
Assisted Roaming Prediction List details:


 Client Dhcp Required:     True
Allowed (URL)IP Addresses
-------------------------

AVC Profile Name: ............................... none
OpenDns Profile Name: ........................... none
Fastlane Client: ................................ No
Max DSCP: ....................................... 0
Client Statistics:
      Number of Bytes Received................... 0
      Number of Bytes Sent....................... 0
      Total Number of Bytes Sent................. 0
      Total Number of Bytes Recv................. 0
      Number of Bytes Sent (last 90s)............ 0
      Number of Bytes Recv (last 90s)............ 0
      Number of Packets Received................. 0
      Number of Packets Sent..................... 0
      Number of Interim-Update Sent.............. 0
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0
      Number of EAP Request Msg Timeouts......... 0
      Number of EAP Request Msg Failures......... 0
      Number of EAP Key Msg Timeouts............. 0
      Number of EAP Key Msg Failures............. 0
      Number of Policy Errors.................... 0
      Radio Signal Strength Indicator............ 0 dBm
      Signal to Noise Ratio..................... 0 dB
Client RBACL Statistics:
      Number of RBACL Allowed Packets........... 0
      Number of RBACL Denied Packets............ 0
Nearby AP Statistics:
```

Configure Mobility Anchors using the GUI

Mobility Anchor, also referred to as Guest tunneling or Auto Anchor Mobility, is a feature where all the client traffic that belongs to a WLAN (specially Guest WLAN) is tunneled to a predefined controller or set of controllers that are configured as Anchor for that specific WLAN. This feature helps to restrict clients to a specific subnet and have more control over the user traffic.

Using a mobility anchor forces clients to be anchored to a controller other than the one they first associate with. This forces their traffic to be tunneled to the DMZ. Then it must pass through the firewall and its associated policies before getting anywhere. This is done on a per-WLAN basis.

- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility secure/EoIP tunnel.
- Anchor WLC - Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility secure tunnel termination, web redirection, and user authentication.

Configure Mobility Anchor on Catalyst 9800 as Guest Anchor Controller with another Catalyst 9800 as Guest Foreign Controller

Before you begin

- Create a WLAN Profile for guests that define the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the WLAN profile name and policy profile name match between the anchor and foreign controllers
- Build a mobility tunnel between the foreign Catalyst 9800 controller and anchor Catalyst 9800 controller.

Step 1 On the **Configuration** > **Tags & Profiles** > **Policy** page, click the **Add** button and define the anchor Catalyst 9800 controller's ip address under the policy profile. To do so, on the **Mobility** tab, select the IP address of the anchor 9800 controller and move it to the **Selected** list of Anchors.

Step 2 Navigate to **ConfigurationTags & ProfilesTags** and create a policy tag that will link the policy profile to the WLAN profile and might be assigned to the APs associated to the foreign controller that service this WLAN.

Step 3 Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

Step 4 (Optional) Assign the Policy Tag to an AP or verify that it already has it. Navigate to **Configuration** > **Wireless** > **Access Points** > **AP Name** > **General** > **.**

Step 5 Log in to anchor Catalyst 9800 controller and create the anchor policy profile. Ensure it has the exact same name that you used on the foreign 9800 controller. Navigate to **Configuration > Tags & Profiles > Policy > + Add**

Step 6 Navigate to Mobility tab and enable Export Anchor. This instructs this 9800 controller that it is the anchor 9800 controller for any WLAN that uses that Policy Profile. When the foreign 9800 controller sends the clients to the anchor 9800 controller , it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 controller knows which local Policy Profile to use.

Note Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

Configure Mobility Anchor on Catalyst 9800 as Guest Anchor Controller and AireOS Controller (IRCM image) as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller as the foreign controller in the campus/enterprise.

First go to the Catalyst 9800 controller's GUI and next go to the AireOS controller's GUI to do the following:

Before you begin

- You must have created the mobility tunnel between the foreign controller and the anchor controller. Follow the procedure outlined above to create the mobility group.
- You must have created a WLAN Profile, Policy Profile and Policy Tag on both the 9800 controllers. Create a WLAN Profile. Enter the Profile Name, SSID and assign a WLAN ID and enable Status and Broadcast SSID once all configurations are complete and ready for deployment. Depending on what range of clients you want this SSID to be discovered, choose the Radio Frequency. Logically you should create a WLAN profile (the WLAN profile has the Profile name, the SSID name and WLAN ID and also the security type for the WLAN and advanced protocols). Next you should create a policy profile that will specify Virtual Local Area Network (VLAN) ID, If traffic is central or local switching, Mobiliy Anchors, Quality of Service(QoS), timers, among other settings. The WLAN profile and the policy profile can be linked together using the Policy tag.

Step 1 Log in to the Catalyst 9800 anchor controller and navigate to **Configuration** > **Tags & Profiles** > **Policy** and click **+Add** to create the anchor policy profile. Ensure that the name of the policy profile is the exact same name of the SSID configured on the AireOS controller, otherwise it will not work.

Step 2 Navigate to the **Mobility** tab and enable **Export Anchor**.

This instructs this 9800 controller that it is the anchor 9800 controller for any WLAN that uses that policy profile. When the foreign AireOS controller sends the clients to the anchor 9800 controller, it informs about the WLAN name that the client is assigned to, so the anchor 9800 controller knows which local WLAN configuration to use and it also uses this name to know which local policy profile to use.

Note Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

Step 3 Configure the AireOS controller as foreign. To do so, log in to the AireOS controller and navigate to **WLANs** > **WLANs**. Select the SSID configured earlier. Ensure that it matches the SSID configured on the Catalyst 9800 anchor controller. Navigate to the arrow at the end of the WLAN's row and select **Mobility Anchor**.

Step 4 Click the mobility anchor and navigate to **WLANs** > **Mobility Anchors** page. Click the **Mobility Anchor Create** button and select the IP address of the Catalyst 9800 controller to set the Catalyst 9800 controller as anchor for this SSID.

What to do next

Verify the configuration.

Configure Mobility Anchor on AireOS(IRCM Image) as Guest Anchor Controller and Catalyst 9800 as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller as the foreign controller in the campus/enterprise.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 Log in to the Foreign 9800 controller and define the Anchor 9800 controller's ip address under the policy profile. To do so, navigate to **Configuration > Tags & Profiles > Policy > + Add** > **Tags & Profiles** > **Policy** and click **Add** to create a new Policy Profile. In the **General** tab, enter the Name and enable the **Central Switching** toggle button. Next, on the **Mobility** tab, select the IP address of the Anchor 9800 controller and move it to the **Selected** list of Anchors.

Step 2 Link the Policy Profile with the WLAN inside the Policy Tag assigned (or that will be assigned) to the APs associated to the foreign controller that service this WLAN. Navigate to **Configuration** > **Tags & Profiles** > **Tags**and either create a new one or use an existing one.

Step 3 Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

Step 4 (Optional) Assign the Site to an AP or verify that it already has it. Navigate to **Configuration > Wireless > Access Points > AP name > General**.

Step 5 Configure the AireOS controller as anchor. Log in to the AireOS controller and navigate to **WLANs** > **WLANs**. Navigate to the drop down menu by clicking on the arrow to the right end of the WLAN's row and select **Mobility Anchor** from the drop-downn list to set it as the local anchor. Navigate to **WLAN** > **Mobility Anchor** > **WLAN SSID**, select the **Switch IP Address** and select the local to make it an anchor.

CHAPTER 10

Troubleshoot Common Issues for IRCM

Mobility tunnels are not coming up

Check if the CA certificates are configured correctly. To verify this try to join an AP to the controller. If it joins then the certificates are fine. otherwise, if the error is in dtls phase, please reconfigure the CA certificates on the controller

Issues with Mobility tunnel

1. Enable the mobility debugs.

   debug mobility handoff enable

   debug mobility error enable

   debug mobility dtls error enable

   debug mobility dtls event enable

   debug mobility pmtu-discovery enable

   debug mobility config enable

   debug mobility directory enable

2. Reproduce the configuration and verify the output.

   The following is an example of a successful mobility tunnel.

```
*capwapPingSocketTask: Feb 07 09:53:38.507: Client initiating connection on
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.507: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Received DTLS packet from mobility peer
172.16.0.21 bytes: 48
*capwapPingSocketTask: Feb 07 09:53:38.508: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 48 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.508: Record    : type=22, epoch=0, seq=0
*capwapPingSocketTask: Feb 07 09:53:38.508:    Hndshk : type=3, len=23 seq=0, frag_off=0,
 frag_len=23
*capwapPingSocketTask: Feb 07 09:53:38.508: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 48
!
!<--output-omited-->
!
*capwapPingSocketTask: Feb 07 09:53:38.511: dtls2_cert_verify_callback: Forcing
```

```
Certificate validation as success
*capwapPingSocketTask: Feb 07 09:53:38.511: Peer certificate verified.
*capwapPingSocketTask: Feb 07 09:53:38.511: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: Nothing to send on link 172.16.0.5:16667 <->
 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 503
*capwapPingSocketTask: Feb 07 09:53:38.511: Received DTLS packet from mobility peer
172.16.0.21 bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.511: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 56 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.511: Record    : type=22, epoch=0, seq=6
*capwapPingSocketTask: Feb 07 09:53:38.511:    Hndshk : type=13, len=6 seq=3, frag_off=0,
 frag_len=6
*capwapPingSocketTask: Feb 07 09:53:38.523: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.527: Received DTLS packet from mobility peer
172.16.0.21 bytes: 91
*capwapPingSocketTask: Feb 07 09:53:38.527: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 91 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.527: Record    : type=20, epoch=0, seq=8
*capwapPingSocketTask: Feb 07 09:53:38.527: Connection established for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: ciperspec 1
*capwapPingSocketTask: Feb 07 09:53:38.527: Nothing to send on link 172.16.0.5:16667 <->
 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 91
*mmMobility: Feb 07 09:53:38.527: DTLS Action Result message received
*mmMobility: Feb 07 09:53:38.527:  Key plumb succeeded
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: Connection established with
172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_db_status_up:895 Connections status up for
entry 172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: DTLS Connection established with
172.16.0.21:16667, Sending update msg to mobility HB
```

Recommended Solutions

Tunnel flaps periodically

Check if keepalive interval and count configuration is matching on both peers.

Both control and data are down

Check group name configuration: the peer group name must match the local group name on the peer.

Data port is down

Check data port plumbing.

Punting issue is suspected,

Check LSMPI/LFTS debug from kernel.

```
# Enable
echo 5 > /sys/module/lfts/parameters/lfts_log
sysctl lsmpi.transport_log=5
```

```
# Disable
echo 0 > /sys/module/lfts/parameters/lfts_log
sysctl lsmpi.transport_log=1
```

Sample output below:

Data for port 16666 (0x411a) and 16667 (0x411b), "Socket lookup for UDP was successful" means LFTS did intercept packet from LSMPI.

```
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16666
[LFTS Rx Verbose] Socket lookup for port: 16666, app_tag: 11, inst_id:0, ether_type: 8
[LFTS Rx Verbose] Socket lookup for UDP was successful.
[LSMPI Trans Rx Verbose] intercept: head ffff8800b3b2d000 data ffff8800b3b2d04e
[LSMPI Trans Rx Debug] intercept:len 101 total_offset 74
[LSMPI Trans Rx Verbose] SKB->Data
ffff8800b3b2d04e: 45000065 c6694000 3f1110cf 1e1e1e08
ffff8800b3b2d05e: 14141416 411a411a 00514c78 00100000
ffff8800b3b2d06e: 00000000 15000a00 00410000 00000144
ffff8800b3b2d07e: 00000000 00000000 23e8187e a1c3da7a
ffff8800b3b2d08e: 7fdd2116 78180cc5 64010016 1e1e1e08
[LSMPI Trans Rx Info] table_id:0x0|client_id:0x0|app_tag:11|inst_id:0
[LSMPI Trans Rx Info] raw_offset:0, opq_info_len:12, transport_punt_hdr_len:16,
opq_data_len:8[LSMPI Trans Rx Verbose] After possible feature header copy
ffff8800b3b2d04e: 45000065 c6694000 3f1110cf 1e1e1e08
ffff8800b3b2d05e: 14141416 411a411a 00514c78 00100000
ffff8800b3b2d06e: 00000000 15000a00 00410000 00000144
ffff8800b3b2d07e: 00000000 00000000 23e8187e a1c3da7a
ffff8800b3b2d08e: 7fdd2116 78180cc5 64010016 1e1e1e08
[LFTS Rx Debug] skb->len 101 proto 8 eth ffff8800b3b2d040 head ffff8800b3b2d000 data
ffff8800b3b2d04e
[LFTS Rx Verbose] netif_rx returned 0
ffff8802296004a0: 0101010c 07001a41 1a410000 00000000
ffff8802296004b0: 45c0006a ba764000 40111afd 14141416
ffff8802296004c0: 1e1e1e08 411a411a 0056fc7c 00100000
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
[LFTS Tx Verbose] injected ip packet
ffff8800b4137210: 4500006d cf274000 40110709 14141416
ffff8800b4137220: 1e1e1e08 411b411b 0059a921 00100008
ffff8800b4137230: 00000000 00000000 00000000 00000000
ffff8800b4137240: 00000000 00000100 3700006f 01002a01
ffff8800b4137250: 01000000 0003cb58 b0085716 f40bb05a
[LSMPI Trans Tx Debug] get_l3_info_l2_offset: skb->proto: 0x800
[LSMPI Trans Tx Debug] Getting L3 info from skb
[LSMPI Trans Tx Info] Transport Inj, ftr hdr len 16
[LSMPI Trans Rx Debug] L3 info:
table_id:0x0|prio:0x0|pal_if_handle:0x0|fea_hdr_len:16|client_id:0x0
[LSMPI Trans Tx Debug] Using Hdr type: 2|cause: 43
[LSMPI Trans Tx Debug] LSMPI Inject Buf
ffff880229600080: 01020000 0000006d 009d1000 20010000
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16667
[LFTS Rx Verbose] Socket lookup for port: 16667, app_tag: 8, inst_id:0, ether_type: 8
```

```
ffff880229600090: 00000000 00000000 01000001 40002b00
ffff8802296000a0: 0101010c 07001b41 1b410000 00000000
ffff8802296000b0: 4500006d cf274000 40110709 14141416
ffff8802296000c0: 1e1e1e08 411b411b 0059a921 00100008
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
[LFTS Tx Verbose] injected ip packet
ffff8800b4137210: 4500006d f5e64000 4011e049 14141416
ffff8800b4137220: 1e1e1e08 411b411b 00599e21 00100008
ffff8800b4137230: 00000000 00000000 00000000 00000000
ffff8800b4137240: 00000000 00000100 3700006f 01002a01
ffff8800b4137250: 01000000 0003cc58 b0086116 f40bb05a
[LSMPI Trans Tx Debug] get_l3_info_l2_offset: skb->proto: 0x800
[LSMPI Trans Tx Debug] Getting L3 info from skb
[LSMPI Trans Tx Info] Transport Inj, ftr hdr len 16
[LSMPI Trans Rx Debug] L3 info:
table_id:0x0|prio:0x0|pal_if_handle:0x0|fea_hdr_len:16|client_id:0x0
[LSMPI Trans Tx Debug] Using Hdr type: 2|cause: 43
[LSMPI Trans Tx Debug] LSMPI Inject Buf
ffff880229600480: 01020000 0000006d 009d1000 20010000
ffff880229600490: 00000000 00000000 01000001 40002b00
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16667
[LFTS Rx Verbose] Socket lookup for port: 16667, app_tag: 8, inst_id:0, ether_type: 8
ffff8802296004a0: 0101010c 07001b41 1b410000 00000000
ffff8802296004b0: 4500006d f5e64000 4011e049 14141416
ffff8802296004c0: 1e1e1e08 411b411b 00599e21 00100008
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
```

Mobility tunnels are going down

Check if peer IP addresses are correctly configured.

```
Device#show wireless mobility summary
Mobility Summary
Wireless Management VLAN: 10
Wireless Management IP Address: 9.10.10.17
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: test123-mob
Mobility Multicast Ip: 0.0.0.0
Link Status is Control Link Status : Data Link Status
DTLS Status is Control DTLS Status : Data DTLS Status
Controllers configured in the Mobility Domain:
 IP               Public Ip        Group Name                       Multicast IP      Link
 Status    DTLS Status                  PMTU
------------------------------------------------------------------------------------------
9.10.10.17        N/A               test123-mob                      0.0.0.0           N/A
               N/A
9.10.10.22        9.10.10.22        test123-mob                      0.0.0.0           UP
   : UP       Key Plumbed  : Key Plumbed  1385
9.10.10.24        9.10.10.24        test123-mob                      0.0.0.0           UP
   : UP       Key Plumbed  : Key Plumbed  1385
```

Recommended Solution

Check if the mobility group name is the same on the peer controllers.

```
Device#show wireless mobility summary
Mobility Summary
Wireless Management VLAN: 10
Wireless Management IP Address: 9.10.10.17
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: test123-mob
Mobility Multicast Ip: 0.0.0.0
Link Status is Control Link Status : Data Link Status
DTLS Status is Control DTLS Status : Data DTLS Status
Controllers configured in the Mobility Domain:
 IP               Public Ip         Group Name                            Multicast IP      Link
 Status    DTLS Status                  PMTU
------------------------------------------------------------------------------------------------
9.10.10.17        N/A               test123-mob                            0.0.0.0           N/A
              N/A
9.10.10.22        9.10.10.22        test123-mob                            0.0.0.0           UP
   : UP       Key Plumbed  : Key Plumbed  1385
9.10.10.24        9.10.10.24        test123-mob                            0.0.0.0           UP
   : UP       Key Plumbed  : Key Plumbed  1385
```

Check if the peers are added with data link encryption

```
Device#show running-config | inc mobility
wireless mobility group member ip 9.10.10.22 public-ip 9.10.10.22 group test123-mob
data-link-encryption
wireless mobility group member ip 9.10.10.24 public-ip 9.10.10.24 group test123-mob
data-link-encryption
wireless mobility group name test123-mob
```

Check if mping and cping of the peers working from AireOS controller.

```
Device>mping 9.10.10.24
Send count=3, Receive count=3 from 9.10.10.24
Device>cping 9.10.10.17
Send count=3, Receive count=3 from 9.10.10.17
```

DTLS keys plumb status shows NA

Check if the SSC (trust-point) configurations are fine on the box.

```
Device#show running-config | inc trust
```

Check if the data-link-encryption is used while configuring the mobility peers.

```
Device#show running-config | inc mobility
wireless mobility group member ip 9.10.10.22 public-ip 9.10.10.22 group test123-mob
data-link-encryption
wireless mobility group member ip 9.10.10.24 public-ip 9.10.10.24 group test123-mob
data-link-encryption
```

Tunnels are not coming up immediately

1. Wait for at least five minutes. Generally, it takes a minimum of five minutes for the tunnels to come up after the reboot.
2. Check if the IP addresses are same.
3. Check if the MAC address is same on AireOS controller.There was an issue on the EWLC, if the software load is changed, the MAC address of the wireless management interface is getting changed.

Possible Cause

Recommended Solution 1 - Disable and enable the radio on client

1. From the Anyconnect tool, disable and enable the radio.

2. From the **Control Panel** > **Network and Internet** > **Network Connections** window, try disabling and enabling the wireless interface.

Recommended Solution 2 - Check if the AP status is enabled

```
Device##show ap status
AP Name                             Status               Mode              Country
-------------------------------------------------------------------------
ap_3802_abc                 Enabled                    FlexConnect           IN
```

Recommended Solution 3 - Check if the AP state is registered

```
AP Name                            Slots    AP Model  Ethernet MAC    Radio MAC
Location              Country     IP Address                                State
------------------------------------------------------------------------------------------
ap_3802_abc                                3      3802I     a0e0.af4d.1d88  70db.9899.49e0
  default location      IN          9.10.10.144                            Registered
```

Recommended Solution 4 - Check if the AP admin and operational status of radio is enabled

```
Device#show ap dot11 5ghz summary
AP Name                          Mac Address     Slot    Admin State    Oper State    Width
  Txpwr           Channel
------------------------------------------------------------------------------------------
ap_3802_abc              70db.9899.49e0  1       Enabled        Up
20       1/6 (16 dBm)    (60)
```

Recommended Solution 5 - Check if the AP country is valid

```
Device#show ap summary
Number of APs: 1

AP Name                            Slots    AP Model  Ethernet MAC    Radio MAC
Location              Country     IP Address                                State
------------------------------------------------------------------------------------------
ap_3802_abc                      3      3802I     a0e0.af4d.1d88  70db.9899.49e0  default
location      IN          9.10.10.144                       Registered
```

Recommended Solution 5 - Check if the AP is broadcasting the BSSIDs

```
Device#show ap name ap_3802_abc wlan dot11 5ghz
WLAN ID    BSSID
-------------------------
7          70db.9899.49ef
6          70db.9899.49ee
1          70db.9899.49ed
14         70db.9899.49ec
13         70db.9899.49eb
10         70db.9899.49ea
9          70db.9899.49e9
```

Note Default behavior is WLANs whose WLAN ID below 16 will be pushed to AP.If you don't want this limitation then you need to create new site tag.

Recommended Solution 6 - Check if the radio interface is enabled on the AP

```
ap_2802_abc#show ip int brief
Interface            IP-Address      Method     Status                 Protocol   Speed
   Duplex
wired0               9.10.10.189     DHCP        up                        up         1000
      full
wired1               unassigned      unset       down                    down       n/a
```

```
    unknown
apphostintf1      unassigned      DHCP        up                       up         n/a
   n/a
wifi0                n/a             n/a      up             up                     n/a
     n/a
wifi1                n/a             n/a      administatively down   down       n/a
 n/a
```

Recommended Solution 7 - Check if the power level of the AP radio is good

```
abc-mob-1#show ap dot11 5ghz summary
AP Name                          Mac Address     Slot    Admin State    Oper State    Width
  Txpwr           Channel
------------------------------------------------------------------------------------------
ap_3802_abc              70db.9899.49e0  1       Enabled        Up
20       1/6 (16 dBm)    (60)
```

Recommended Solution 8 - Check if the Channel number is good one (should be 60 or 64 for 5gz radios)

```
abc-mob-1#show ap dot11 5ghz summary
AP Name                          Mac Address     Slot    Admin State    Oper State    Width
  Txpwr           Channel
------------------------------------------------------------------------------------------
ap_3802_abc              70db.9899.49e0  1       Enabled        Up
20       1/6 (16 dBm)    (60)
```

Recommended Solution 9 - Check if the client is in exclusion list (you can check using two commands)

```
Device#show wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                                        WLAN  State
Protocol Method     Role
------------------------------------------------------------------------------------------
1491.82b8.fdd4 ap_3802_abc                                   9     Run               11n(5)
 None       Local

Number of Excluded Clients: 1

MAC Address    AP Name                         WLAN   State             Protocol Method

------------------------------------------------------------------------------------------
1232.1233.1234                                 0      Excluded          N/A      None



Device#show wireless exclusionlist
Excluded Clients

MAC Address       Description                       Exclusion Reason
Time Remaining
------------------------------------------------------------------------------------------
1232.1233.1234    test                              Manually Excluded
         N/A
```

Recommended Solution 10 - Check if the wlan is enabled

```
Device#show wlan summary

Number of WLANs: 14

WLAN Profile Name                     SSID                             Status
-----------------------------------------------------------------------------
1    abc-mob-open                   abc-mob-open                   UP
2    abc-mob-mab                    abc-mob-mab                    UP
```

Recommended Solution 11 - Check if the policy profile is enabled

```
Device#show wireless profile policy summary

Number of Policy Profiles: 12

Policy Profile Name               Description                             Status
-----------------------------------------------------------------------------------------
pp-open
 ENABLED
pp-dot1x
 ENABLED
asim43-policy
ENABLED
guest-policy-tag
DISABLED
default-flex-profile
DISABLED
```

Recommended Solution 12 - Try creating a new UNIQUE wlan and join the client to it

```
wlan abc-mob-mab 2 abc-mob-mab
mac-filtering default
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
no shutdown
```

Recommended Solution 13 - If localmode scenario, check if the switching is central

```
Device#show running-config | sec named-policy-profile
wireless profile policy named-policy-profile
 aaa-override
 no central switching    → this is wrong, it should be "central switching" for locamode.
 cts sgt 2222
 ipv4 dhcp opt82 format apname
 nac
 no shutdown
```

Recommended Solution 14 - Make sure the client is near the AP physically

In the lab, place the client near the APs.

Recommended Solution 15 - Check if the auto-anchor configuration is enabled on the policy profile. It should not be enabled

```
Device#show running-config | sec pp-dot1x
wireless profile policy pp-dot1x
aaa-override
mobility anchor
cts inline-tagging
vlan 11
no shutdown
```

Recommended Solution 16 - Check if the ISE/AAA server is reachable

```
Device#
srihari-mob-1#test aaa group radius wpr wpr123 new-code
The process for the command is not responding or is otherwise unavailable
User successfully authenticated
```

```
USER ATTRIBUTES

username             0   "wpr"
Message-Authenticato 0   <hidden>
security-group-tag   0   "0015-25"
```

```
Device#ping 9.10.8.247
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.8.247, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
srihari-mob-1#
```

Recommended Solution 17 - Client is NOT able to get authenticated

1. Check if the client is in exclusion state.
2. Check if the credentials are same as configured on ISE/Local
3. Check if the secuty types are configured correctly on the client for this ssid.
4. Check if the ISE is able receive the request
5. Check the live-logs on ISE to see why the client is not getting authenticated.

AP Issues - Admin status is up, but oper status is down

Recommended Solution 1 - check if the "show ap tag summary" has no misconfiguration

```
Device#show ap tag summary
Number of APs: 1

AP Name                 AP Mac            Site Tag Name            Policy Tag Name
RF Tag Name             Misconfigured     Tag Source
------------------------------------------------------------------------------------------
ap_2802_abcdef         500f.804c.5d42   default-site-tag         pt-all
default-rf-tag                       No               Static
```

Check if the wifi radios are up on AP using "show ip interface brief" If they are down, to do devshell and bring them up.

```
Device#devshell
EXITING CISCO SHELL. PLEASE EXECUTE EXIT IN DEVSHELL TO GET BACK TO CISCO SHELL.
BusyBox v1.23.2 (2018-06-19 13:03:00 PDT) built-in shell (ash)
Device:/# ifconfig wifi1 up
Device:/#ifconfig wifi0 up
```

Check the country code on AP and Controller for that AP

On the controller

```
Device#show ap status
AP Name                             Status     Mode              Country
-------------------------------------------------------------------------
ap_2802_abcdefg                     Enabled    Local             IN
```

Check if the global dot11 radio is shutdowned from configuration

```
Device#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#no ap dot11 5ghz shutdown
Device(config)#no ap dot11 24ghz shutdown
```

Check if the country code for the AP and the radios on AP has same

On the controller

```
Device#show ap status
AP Name                             Status     Mode              Country
-------------------------------------------------------------------------
```

```
ap_3802_abcdefg                        Disabled   Local             IN
ap_1852_abcdefg_hi                     Enabled    FlexConnect       IN
```

CHAPTER 11

Additional References for IRCM Configuration

To get a detailed understanding of a particular area of IRCM configuration, refer to the following documents:

Related Topic	Document Title
To understand IRCM deployment scenarios	Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide
To configure mobility tunnels on Catalyst 9800 controllers	Configure Mobility Topologies on Catalyst 9800 Wireless LAN Controllers (WLCs)
To configure WLAN Anchor Mobility on Catalyst 9800 controllers	Configure WLAN Anchor Mobility Feature on Catalyst 9800