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 2
2	Configure WLAN, on page 3

Table 2: Mobility specific configurations

Step	Task
1	Ensure Identical Parameter Configuration on Peer Controllers , on page 7
2	Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility, on page 8

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

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 4

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 6

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 7.

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
```