Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide

Revised: November 16, 2021

Introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and services across different wireless LAN controllers that runs on different software and controllers.

This document specifically covers the IRCM support between catalyst 9800 wireless controllers and interoperability with AireOS controllers. It covers the cases of:

1. Customers with existing Aireos controllers in their networks and adding additional catalyst 9800 wireless controllers (Brownfield).
2. Customers with Aireos Controllers deployed as Guest anchor and additional catalyst 9800 wireless controllers added.
3. Customers deploying multiple catalyst 9800 wireless controllers (Green field).

Prerequisites

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

- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1e or later.
- Supported Cisco AireOS Wireless Controllers running Cisco AireOS 8.5 IRCM supported 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
- The IRCM feature is not supported on the following Cisco AireOS Wireless Controllers:
    - Cisco 2504 Wireless Controllers
    - Cisco Flex7510 Wireless Controllers
    - Cisco WiSM 2 Controllers
    - Cisco Virtual Wireless Controllers (vWLCs)

Overview

Cisco catalyst 9800 wireless controller uses CAPWAP based tunnels for mobility. The mobility control channel will be always encrypted and the mobility data channel can be optionally encrypted. This is called Secure Mobility.

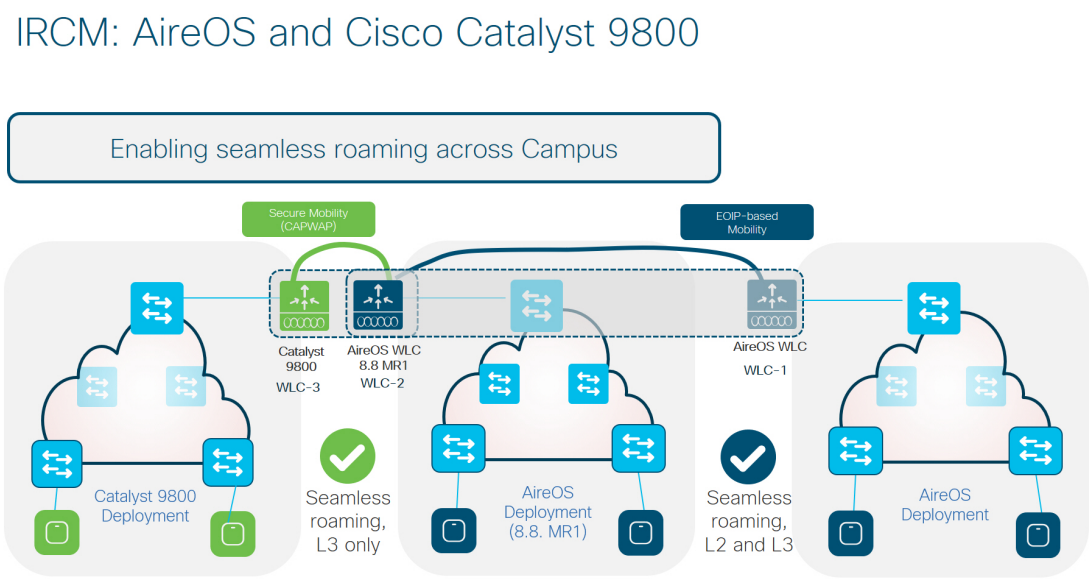
AireOS uses EoIP tunnels for mobility. Support for CAPWAP based encrypted mobility (Secure Mobility) was brought in in 8.5. However the support for IRCM with Catalyst 9800 wireless controller is present only in 8.8.111 and above and in the 8.5 IRCM supported release.

Deployments and Use Cases

Let's consider few common scenarios where customer will use a mix of C9800 and AireOS controllers:

1. Roaming across catalyst 9800 wireless and AireOS controller.
2. AireOS controller as guest anchor with catalyst 9800 wireless/ AireOS as export anchor.
3. Cisco 9800 wireless controller as guest anchor with AireOS / catalyst 9800 wireless as export anchor.

Let's examine the first one: Roaming across AireOS and catalyst 9800 wireless controllers.



- WLC-1–Any AireOS controller running 8.2 / 8.3 / 8.5
- 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.

Note The Cisco 5508 and 8510 Wireless Controllers do not support tunnel encryption protocols. They support IRCM with unencrypted mobility tunnels only.

- WLC-3–Any catalyst 9800 wireless controller.

- 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 will be permitted both L2 and L3 roaming are possible (Existing AireOS Mobility Scenarios).
- Seamless Client roaming between WLC-2 and WLC-3 will be permitted but will be L3 roaming only.
- Seamless Roaming between WLC-1 and WLC-3 is not permitted.

Note Secure Mobility tunnels will have Mobility control tunnel encrypted always . Data tunnel used to tunnel client traffic can also be optionally be encrypted.

Another important scenario is related to guest: AireOS controller as guest anchor with Catalyst 9800 wireless and AireOS controllers as export anchor.

Seamless Layer 3 Roaming

All the roaming between the C9800 and AireOS controllers is Layer 3 roaming. This means that no matter what VLAN the SSID is mapped to on each WLC, the client will always be anchored to the first WLC it joins. In other words, the point of attachment to the wired network doesn't change with roaming, even if the VLAN on the wired side is the same on both WLCs.

In the migration design phase, when defining a common SSID for roaming, it's recommended to use a different VLAN ID and subnet on the Catalyst 9800 and on the AireOS WLC.

As a result, clients will get a different IP whether they join first the Catalyst 9800 or AireOS WLC; seamless roaming is guaranteed either way because the client will always keep its IP address on the VLAN/ subnet it joined first.

Mapping the same SSID to a different VLAN ID on both wireless controllers might not be desired/possible in the following scenarios:

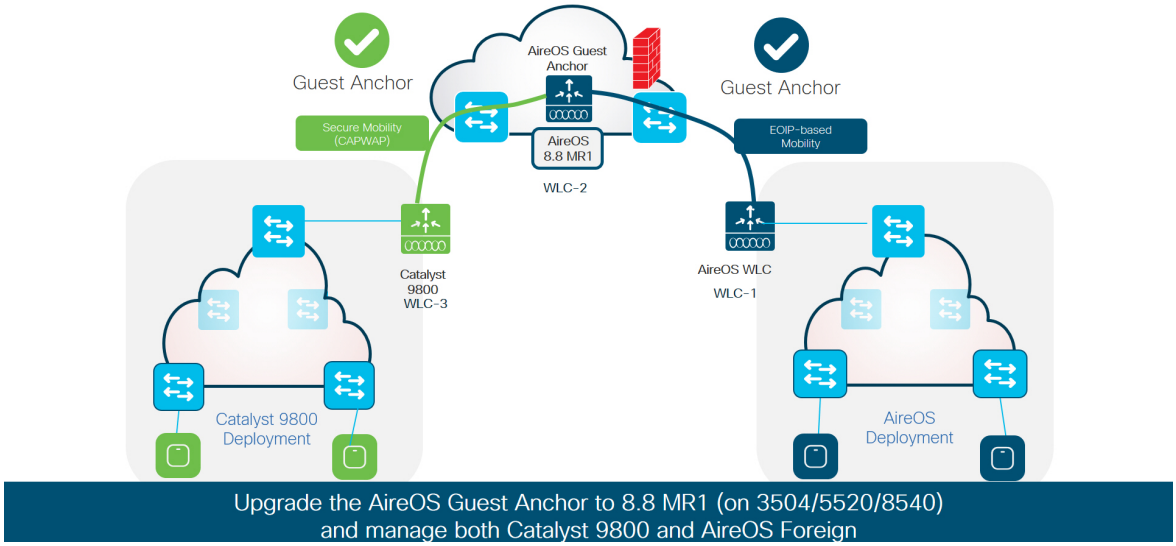
- The customer is not willing to change the subnet design to add another VLAN/subnet for clients that join the newly added Catalyst 9800. This might also involve changes in the AAA and firewall settings.
- The customer leverages public IP subnets so they don't have another spare subnet to assign to clients on the same SSID.
- The customer is using static IP for wireless devices.

In the above cases, just map the same VLAN/subnet to the SSID on both the Catalyst 9800 and AireOS WLC; the only suggestion would be to run the following recommended releases:

- Cisco IOS XE code: Release 16.12.5 or 17.3.3 and above.
- AireOS code: Release 8.5.176 IRCM or 8.10.151 and above

Refer to the Cisco TAC URL
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html#anc21
for the latest recommended releases.

Guest : AireOS and Cisco Catalyst 9800

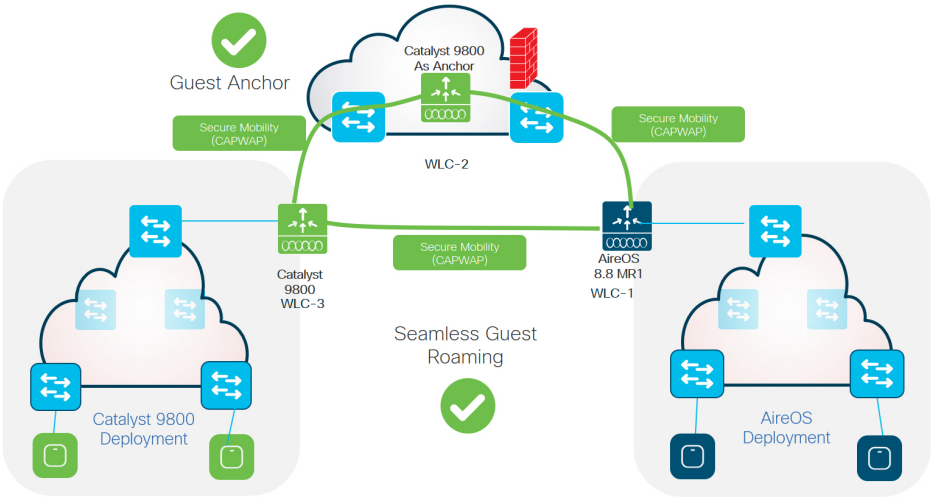


- This will be the prime deployment for existing brownfield Wireless customers looking to introduce the catalyst 9800 wireless controller in to the existing wireless network and already have a Guest Anchor solution.
- The Anchor controller will needs to be upgraded to be paired up with Catalyst 9800. Once upgraded WLC2 can act as guest anchor in DMZ for both WLC1 and WLC-3.
- WLC-1 – Any AireOS controller running 8.2 / 8.3 / 8.5.
- 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-3 – Any Cisco catalyst 9800 wireless controllers
- Above 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.

Note Secure Mobility tunnels will have Mobility control tunnel encrypted always . Data tunnel used to tunnel client traffic can also be optionally be encrypted.

There is another use case for Guest: Catalyst 9800 wireless controller as guest anchor with AireOS / catalyst 9800 wireless as export anchor.

Guest : AireOS and Cisco Catalyst 9800



- WLC-3–Any catalyst 9800 wireless controllers.
- WLC-2–Any catalyst 9800 wireless controllers.
- 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 (catalyst 9800 wireless controller) and WLC3 (AireOS) as well.

Configuration Details on AireOS 8.8.111 (or 8.5-based IRCM Image)

This is the configuration for setting up the Mobility peer with secure mobility.

Mobility Group Member > New

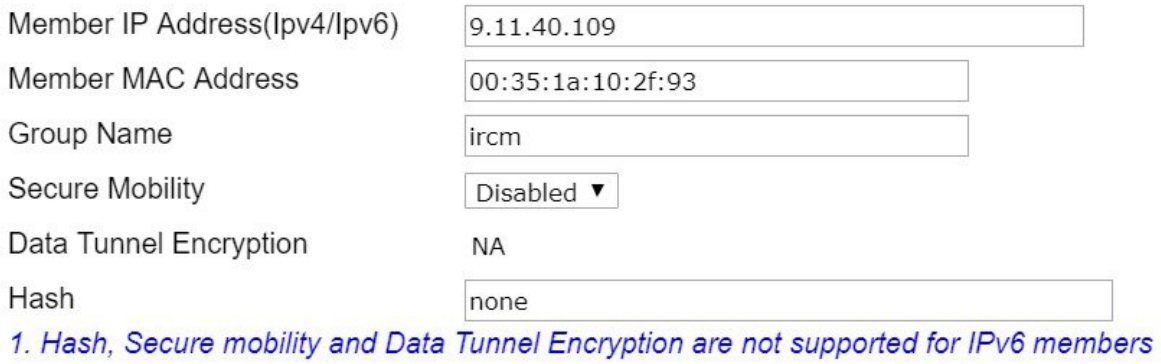
Member IP Address(Ipv4/Ipv6)	172.20.227.73
Member MAC Address	00:0c:29:a8:d5:77
Group Name	ircm
Secure Mobility	Enabled ▼
Data Tunnel Encryption	Disabled ▼
Hash	9509719f279241e0e16daf5174d10f41b59a4443

1. Hash, Secure mobility and Data Tunnel Encryption are not supported for IPv6 members

Note Ensure that Secure Mobility is set to Enabled.

Data Tunnel Encryption can be enabled or not to encrypt client data traffic. The same configuration need to be done on both sides for the tunnel to come up.

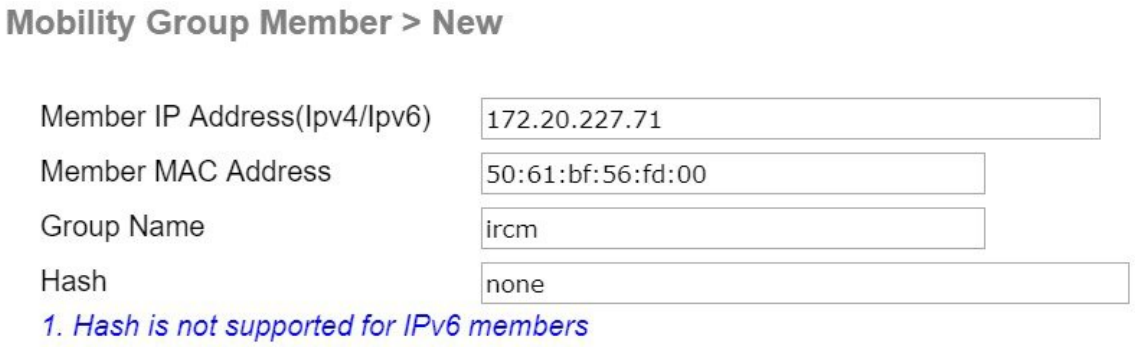
Following is the configuration for setting up the Mobility peer for EOIP mobility:



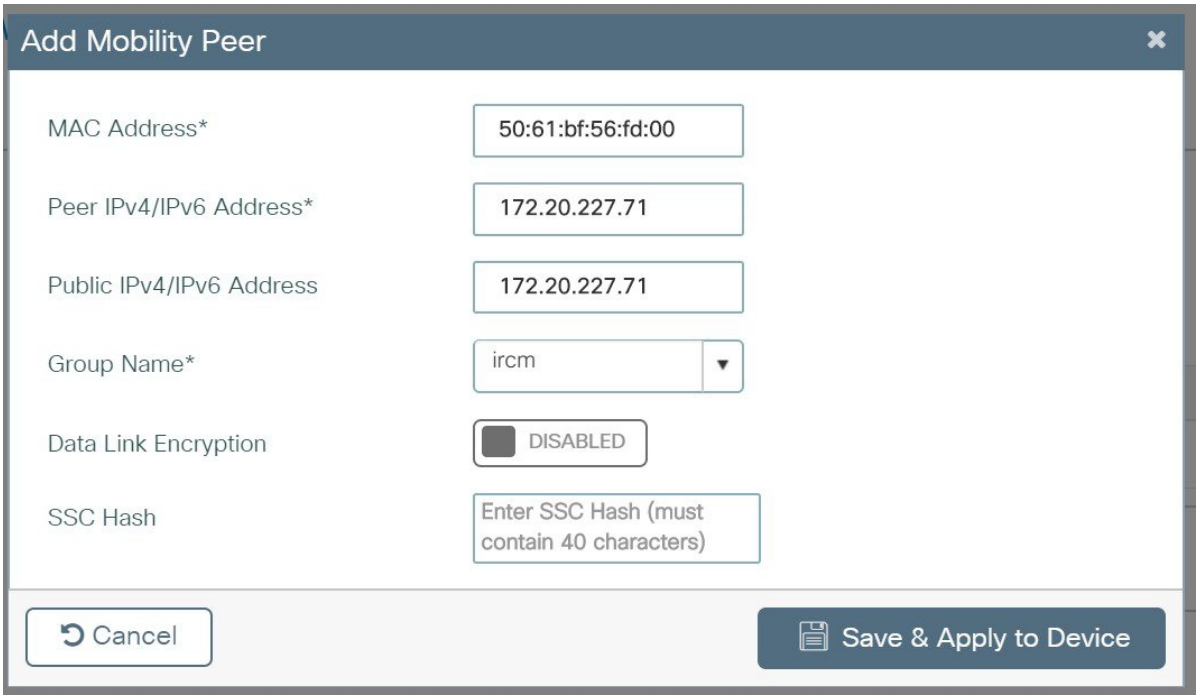
Note Secure Mobility should be disabled and Data Encryption is not applicable.

Configuration Details on AireOS 8.2/8.3/8.5 CCO

For older AireOS builds you will not even have an option to configure of secure mobility as only EOIP based mobility is supported.

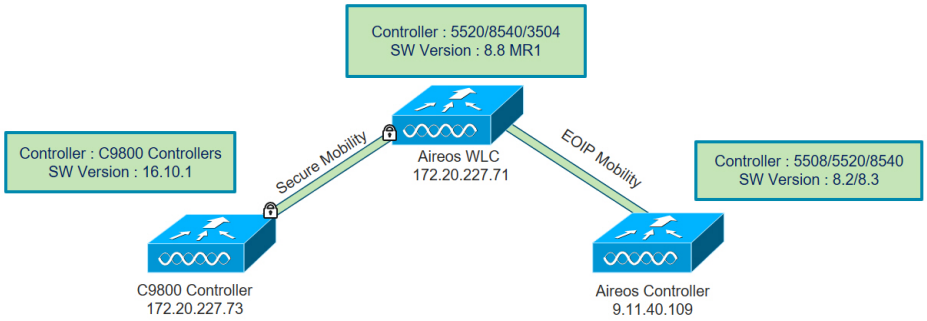


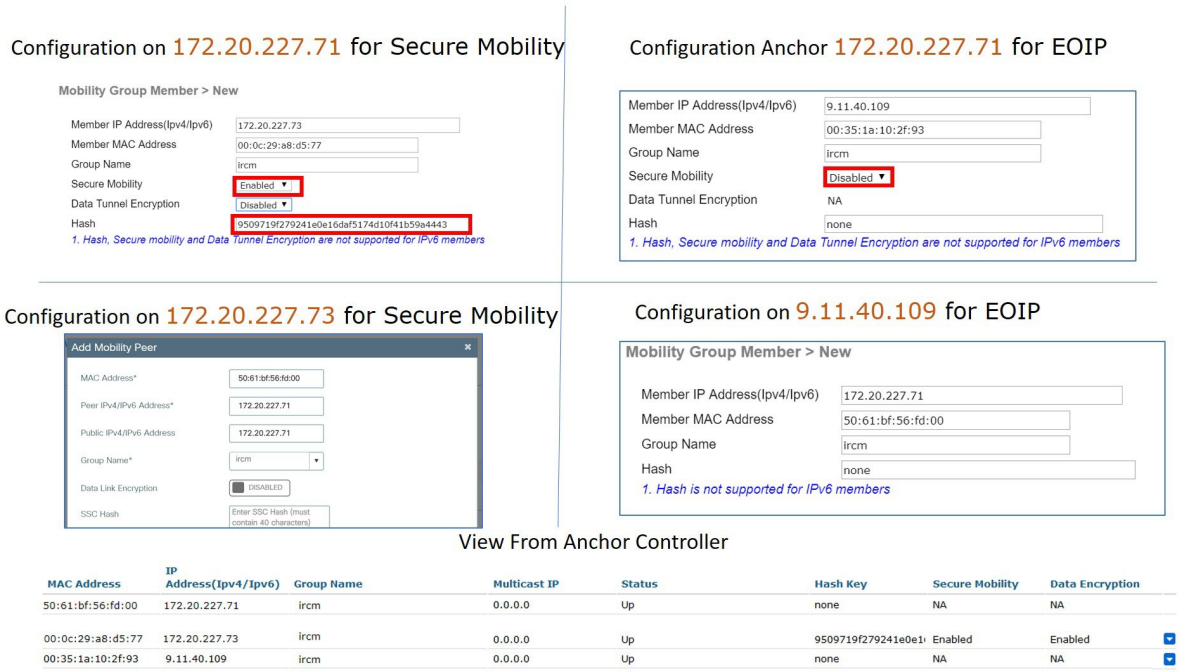
Configuration Details on Catalyst 9800 Wireless Controller



Catalyst 9800 wireless controller has only secure Mobility by default, so you don't have to configure it. Data encryption can be enabled optionally.

Sample diagram and configuration:





CLI Configuration Details for Mobility Peer on AireOS

```
config mobility group domain ircm
config mobility group member add 00:0c:29:a8:d5:77 172.20.227.73 ircm  encrypt enable
```

- If the peer catalyst 9800 wireless controller is virtual , configure the hash using command:

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

- Optionally enable data tunnel encryption using command:

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

The hash configure above can be obtained by running the following command on catalyst 9800 wireless controller:

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

CLI Configuration for Mobility Peer on Catalyst 9800 Wireless

```
wireless mobility group name ircm
wireless mobility mac-address 000c.29a8.d577
wireless mobility group member mac-address 5061.bf56.fd00 ip 172.20.227.71 public-ip 172.20.227.71 group ircm
 data-link-encryption
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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