Wireless Network Configuration Use Cases

- Wireless Network Configuration Use Case, on page 1
- High Availability Use Cases, on page 1
- Wireless Mobility Use Cases, on page 4

Wireless Network Configuration Use Case

The following topic helps you understand the wireless network configuration.

High Availability Use Cases

The following topics help you understand the high availability (HA) use cases for wireless networks.

Configure Cisco Wireless Controller HA

Cisco Wireless Controller HA allows you to use a wireless controller as a backup for a primary wireless controller. The active wireless controller handles all the APs, client traffic, and shares the AP and client database with the standby wireless controller. If there is a failover, the standby wireless controller takes over immediately, resulting in zero client service downtime and zero SSID outage.

Before you begin

- Ensure that both the wireless controllers are of the same form factors.
- Ensure that both the wireless controllers are running the same software version.
- Wireless controller HA supports a maximum redundancy port link latency of 80 ms round-trip time (RTT), minimum bandwidth of 60 Mbps, and minimum maximum transmission unit (MTU) of 1500.
- Ensure that you connect the redundancy ports of both the wireless controllers physically or through a Layer 2 virtual network. If you connect redundancy ports through a Layer 2 virtual network, ensure that the link latency, bandwidth, and MTU requirements are met.
- For the Cisco Catalyst 9800-CL Wireless Controllers running on ESXi, KVM, and Hyper-V, ensure that the redundancy port connects to the same vswitch.

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory and Add a Network Device.

If the wireless controller isn't available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display Information About Your Inventory.

Step 3 Use the **show redundancy** command to verify that the operating redundancy mode is **Non-redundant** on both the wireless controllers.

Step 4 Click the menu icon (≡) and choose **Provision** > **Inventory**.

Step 5 Check the check box next to the required wireless controller, and then click **Actions** > **Provision** > **Configure WLC HA**.

Step 6 Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** addresses.

You must configure the IP addresses used for redundancy management IP and peer redundancy management IP in the same subnet as the management interface of the wireless controller. Ensure that these IP addresses are unused IP addresses within that subnet range.

Step 7 Enter the **Netmask**.

Step 8 From the **Select Secondary WLC** drop-down list, choose the secondary wireless controller.

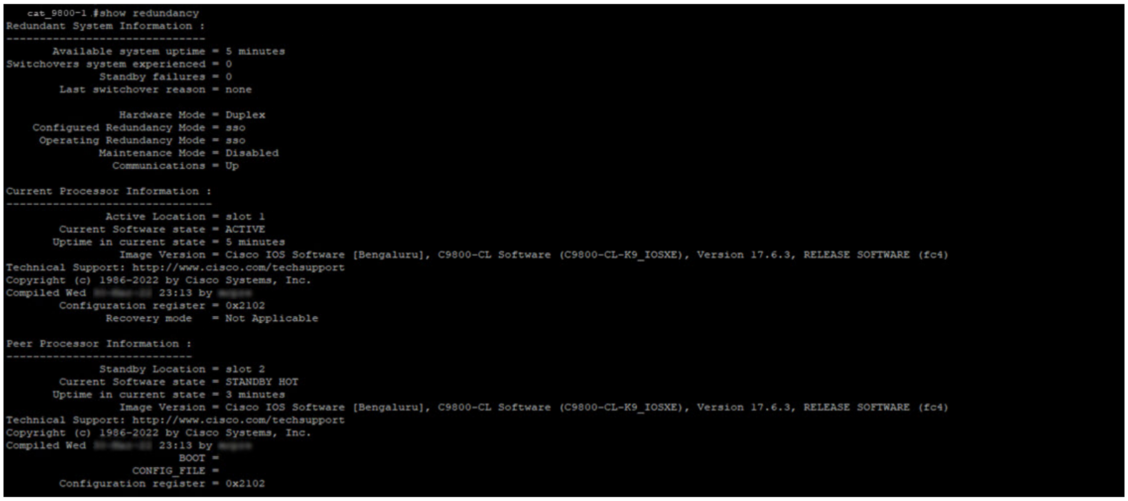
Step 9 Since the Cisco Catalyst 9800-CL Wireless Controller doesn't have a dedicated redundancy port, choose the interface that will be used for the redundancy port.

Note Appliance-based Cisco Catalyst 9800 Series Wireless Controllers have dedicated redundancy ports, and redundancy port interface selection isn't necessary for these devices.

Step 10 Click **Configure HA**.

What to do next

To verify the status of HA, use the **show redundancy** command. Following is a sample output of this command:



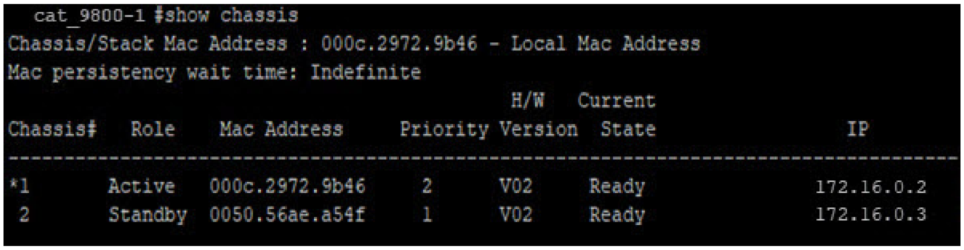
```
   cat_9800-1 #show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 5 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 5 minutes
                 Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
        Configuration register = 0x2102
               Recovery mode   = Not Applicable

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
       Uptime in current state = 3 minutes
                 Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
                          BOOT =
                   CONFIG_FILE =
        Configuration register = 0x2102
```

To verify the **Priority** of the primary wireless controller, use the **show chassis** command. The **Priority** of the primary wireless controller is changed to 2 to ensure that its role is **Active**. Following is a sample output of this command:



```
  cat_9800-1 #show chassis
Chassis/Stack Mac Address : 000c.2972.9b46 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
-------------------------------------------------------------------------------------
*1       Active   000c.2972.9b46     2       V02     Ready                172.16.0.2
 2       Standby  0050.56ae.a54f     1       V02     Ready                172.16.0.3
```

Configure Cisco Wireless Controller N+1 HA

Cisco Wireless Controller N+1 HA allows you to use a wireless controller as a backup for multiple primary wireless controllers. Cisco DNA Center doesn't support stateful switchover for N+1 HA and each wireless controller must be managed separately.

Note

- Cisco DNA Center supports the N+1 HA configurations for primary and secondary wireless controllers. Cisco DNA Center doesn't support tertiary wireless controller configurations.
- If you edit the primary wireless controller configuration, reprovision the secondary wireless controller manually with the updated configurations.

Step 1 Ensure that you have the wireless controller in your inventory. For more information, see About Inventory and Add a Network Device.

If the wireless controller isn’t available in the inventory, use the Discovery feature to discover it. For more information, see Discover Your Network.

Step 2 Ensure that both the wireless controllers are in the **Managed** state in the inventory. For more information, see Display Information About Your Inventory.

Step 3 Create enterprise and guest wireless SSIDs. For more information, see Create SSIDs for an Enterprise Wireless Network and Create SSIDs for a Guest Wireless Network.

Step 4 If you created a wireless network profile during SSID creation, assign it to the primary wireless controller-managed site.

Click the menu icon (≡) and choose **Design** > **Network Profiles**, and then click the corresponding **Assign Site** option for the wireless network profile.

Step 5 Provision the primary wireless controller. Choose the role as **Active Main WLC**. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 6 Provision the secondary wireless controller. Choose the role as **Active Main WLC** and choose the secondary managed AP location same as the managed AP location for the primary wireless controller. For more information, see Provision a Cisco AireOS Controller and Provision a Cisco Catalyst 9800 Series Wireless Controller.

Step 7 Provision the APs. For more information, see Provision a Cisco AP—Day 1 AP Provisioning

Wireless Mobility Use Cases

The following topics help you understand the mobility configuration use cases for wireless networks.

Configure Wireless Mobility

Mobility configuration in Cisco DNA Center allows you to establish a tunnel between Cisco Wireless Controllers in a network allowing them to communicate with each other and dynamically share information. The mobility tunnel enables seamless roaming of clients within a wireless network. This procedure describes the steps to configure a mobility tunnel between wireless controllers for the following use cases:

- Two newly added wireless controllers with the same mobility group: The two wireless controllers are newly added to Cisco DNA Center and are not yet provisioned.
- Two existing wireless controllers with the same mobility group: The wireless controllers are already added and provisioned on Cisco DNA Center and have the same mobility group name.
- Two existing wireless controllers with different mobility group: The wireless controllers are already added and provisioned on Cisco DNA Center and have different mobility group name.
- Two existing wireless controllers with a third wireless controller: Adding a new wireless controller to an existing mobility group between two wireless controllers.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory and Display Information About Your Inventory.
- For more information on wireless mobility configuration, see Mobility Configuration Overview.

Step 1 For newly added wireless controllers with the same mobility group, do the following:

a) Run the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the controllers.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure Mobility Group.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 2 For two existing wireless controllers with same mobility group, do the following:

a) Verify that the wireless controllers have the same mobility group name configured. For more information, see About Inventory and Display Information About Your Inventory.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure Mobility Group.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

Step 3 For two existing wireless controllers with different mobility group, do the following:

a) Verify that the wireless controllers have the mobility group name configured. For more information, see About Inventory and Display Information About Your Inventory.
b) Choose one of the wireless controllers and configure the mobility group, adding the other wireless controller as the peer. For more information, see Configure Mobility Group.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the second wireless controller. Adding it as a peer for the first wireless controller automatically provisions it with the same mobility group name and peer configurations.

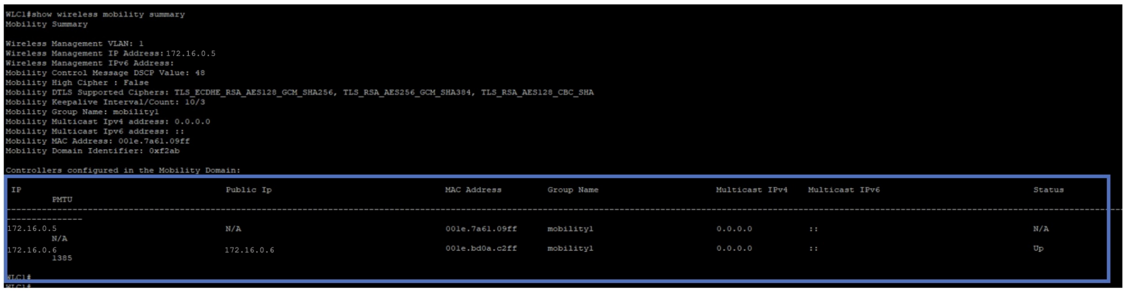
Step 4 For adding a new wireless controller to an existing mobility group between two wireless controllers, do the following:

a) Verify that the existing wireless controllers have the mobility tunnel established between them by checking the mobility group name and the mobility peer information in the **Mobility** tab. For more information, see About Inventory and Display Information About Your Inventory.
b) Choose the newly added wireless controller and configure the mobility group, adding the other two existing wireless controllers as peers. For more information, see Configure Mobility Group.
c) Verify the configurations before provisioning.
d) Provision the wireless controller.

Note You don't have to provision the existing two wireless controllers. Adding them as a peer for the newly added wireless controller automatically provisions it with the same mobility group name and peer configurations.

What to do next

After provisioning, run the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status.

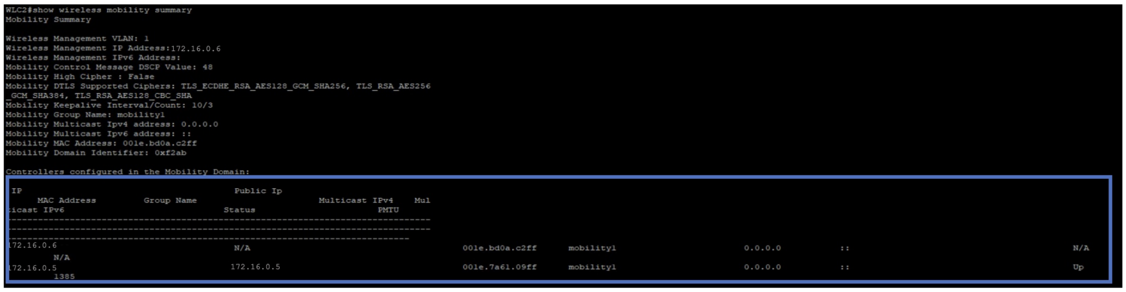


```
WLC1#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.5
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: mobility1
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.7a61.09ff
Mobility Domain Identifier: 0xf2ab

Controllers configured in the Mobility Domain:
 IP                                  Public Ip                            MAC Address       Group Name                    Multicast IPv4    Multicast IPv6                                Status
        PMTU
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------
172.16.0.5                           N/A                                  001e.7a61.09ff    mobility1                     0.0.0.0           ::                                            N/A
        N/A
172.16.0.6                           172.16.0.6                           001e.bd0a.c2ff    mobility1                     0.0.0.0           ::                                            Up
        1385

WLC1#
WLC1#
```



```
WLC2#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.6
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256
_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: mobility1
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.bd0a.c2ff
Mobility Domain Identifier: 0xf2ab

Controllers configured in the Mobility Domain:
 IP                                  Public Ip
     MAC Address         Group Name                       Multicast IPv4    Mul
ticast IPv6                      Status                            PMTU
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------------------------------------------
172.16.0.6
                                     N/A                                  001e.bd0a.c2ff    mobility1                     0.0.0.0           ::                                            N/A
        N/A
172.16.0.5                           172.16.0.5                           001e.7a61.09ff    mobility1                     0.0.0.0           ::                                            Up
        1385
```

Configure Anchor/Foreign Wireless Mobility

The anchor/foreign wireless configuration on Cisco DNA Center allows you to establish wireless mobility between Cisco Wireless Controllers on different wireless networks. In an anchor/foreign setup, the foreign wireless controller encapsulates the client L3 traffic in the mobility tunnel and forwards it to the anchor wireless controller. The anchor wireless controller decapsulates the tunnel and switches the client traffic. This procedure describes the steps to configure anchor/foreign wireless mobility for the following use cases:

- Configuring two newly added wireless controllers - one anchor and one foreign wireless controller.
- Configuring three newly added wireless controllers - one anchor and two foreign wireless controllers.
- Configuring three newly added wireless controllers - one foreign and two anchor wireless controllers.
- Deleting the anchor/foreign setup.

Before you begin

- Ensure that you have the Cisco Wireless Controllers in your inventory and they are in **Managed** state. For more information, see About Inventory and Display Information About Your Inventory.
- Use the **show wireless mobility summary** command to verify that there's no existing mobility tunnel between the wireless controllers.

Step 1 Create an SSID for the wireless network and associate it with a new wireless network profile. For more information, see Create SSIDs for an Enterprise Wireless Network or Create SSIDs for a Guest Wireless Network.

In the **Associate SSID to Profile** step, choose the **Add Profile** option and configure as below:

- **Profile Name**: Enter a name for the profile.
- **Fabric**: Choose **No**.

- **Do you need Anchor for this SSID?**: Choose **Yes**.

Step 2 For a scenario with one anchor and one foreign wireless controller, do the following:

a) Assign the newly created wireless profile to the site managed by the foreign wireless controller.

To assign a site:

- Click the menu icon (≡) and choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, Edit and Delete a Site.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the anchor **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision a Cisco AP—Day 1 AP Provisioning.

Step 3 For a scenario with one anchor and two foreign wireless controllers, do the following:

a) Assign the newly created wireless profile to the sites managed by the foreign wireless controllers.

- Click the menu icon (≡) and choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, Edit and Delete a Site.

b) Provision the anchor wireless controller.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)** (select both foreign sites).
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the foreign wireless controllers.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)**.

- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision a Cisco AP—Day 1 AP Provisioning.

Step 4 For a scenario with one foreign and two anchor wireless controllers, do the following:

a) Assign the newly created wireless profile to the sites managed by both wireless controllers (foreign and anchor).

- Click the menu icon (≡) and choose **Design** > **Network Profiles**
- Choose the profile and click **Assign Site**. For information on creating sites, see Create, Edit and Delete a Site.

b) Provision the foreign wireless controller.

- Choose the wireless controller role as **Active Main WLC** and select the **Managed AP location(s)** (select both foreign and anchor sites).
- Configure other advance settings, if required, and deploy.

For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

c) Provision the anchor wireless controllers.

- Choose the wireless controller role as **Anchor WLC** and select the **Managed AP location(s)**.
- Configure the interface details.
- Configure other advance settings, if required, and deploy.

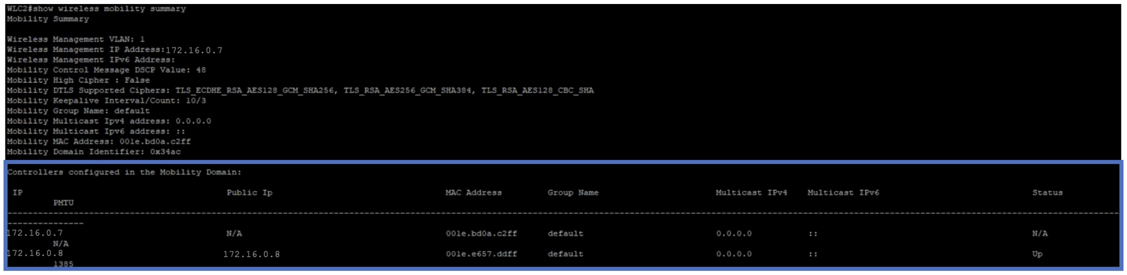
For more information on provisioning wireless controllers, see Provision a Cisco Catalyst 9800 Series Wireless Controller or Provision a Cisco AireOS Controller.

d) Provision the APs under the wireless controllers.

Ensure that APs have the correct SSID. For more information on AP provisioning, see Provision a Cisco AP—Day 1 AP Provisioning.

What to do next

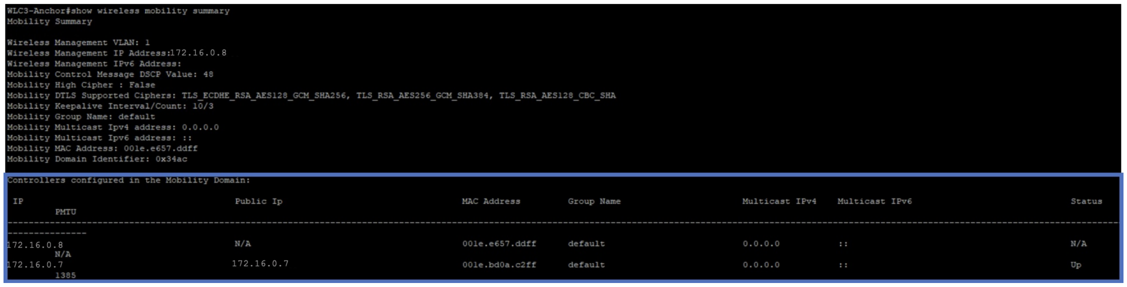
After provisioning, Cisco DNA Center automatically creates a mobility tunnel between the anchor and foreign wireless controllers. Use the **show wireless mobility summary** command on each of the controllers to verify the mobility tunnel status. Following is a sample output of the command:



```
WLC2#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.7
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.bd0a.c2ff
Mobility Domain Identifier: 0x34ac
Controllers configured in the Mobility Domain:

 IP                                       Public Ip                                MAC Address       Group Name                    Multicast IPv4   Multicast IPv6                        Status
        PMTU
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------
172.16.0.7                                N/A                                      001e.bd0a.c2ff    default                       0.0.0.0          ::                                    N/A
        N/A
172.16.0.8                               172.16.0.8                                001e.e657.ddff    default                       0.0.0.0          ::                                    Up
        1385
```



```
WLC3-Anchor#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 1
Wireless Management IP Address:172.16.0.8
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.e657.ddff
Mobility Domain Identifier: 0x34ac
Controllers configured in the Mobility Domain:

 IP                                       Public Ip                                MAC Address       Group Name                    Multicast IPv4   Multicast IPv6                        Status
        PMTU
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------
172.16.0.8                                N/A                                      001e.e657.ddff    default                       0.0.0.0          ::                                    N/A
        N/A
172.16.0.7                               172.16.0.7                                001e.bd0a.c2ff    default                       0.0.0.0          ::                                    Up
        1385
```

Verify the following mobility configurations on the wireless controllers.

- Both wireless controllers have the same WLAN and policy profile.
- The policy tag is created on foreign wireless controller and mapped to the AP.
- The VLAN interface is created for the anchor wireless controller and is mapped to the policy profile.

Delete the anchor/foreign setup

To delete the anchor/foreign setup, do the following:

1. Ensure that the mobility tunnel between the anchor and foreign wireless controllers is in *up* state.
2. Delete the SSID that was created for the wireless network.
   a. Click the menu icon (≡) and choose **Design** > **Network Settings**.
   b. Click the **Wireless** tab.
   c. From the left hierarchy tree, choose **Global**.
   d. In the **SSID** table, choose the SSID and click **Delete**.
3. Provision the foreign wireless controllers.

   In the provision **Summary** window, ensure that the SSID details are removed.

   After provisioning, Cisco DNA Center automatically deletes the mobility tunnel between the anchor and foreign wireless controllers and the WLAN and policy profile is deleted on all the wireless controllers.