Configuring Mobility

Configuring Mobility Controller

Configuring Converged Access Controllers

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before You Begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

SUMMARY STEPS

1. **wireless mobility controller**
2. **wireless mobility controller peer-group** *SPG1*
3. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
4. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
5. **wireless mobility controller peer-group** *SPG2*
6. **wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
7. **wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.
Step 2	**wireless mobility controller peer-group** *SPG1* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Creates a peer group named SPG1.
Step 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	Adds a mobility agent to the peer group. **Note** The 10.10.20.2 is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.
Step 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	Adds another member to the peer group SPG1.
Step 5	**wireless mobility controller peer-group** *SPG2* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2`	Creates another peer group SPG2.
Step 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	Adds a member to peer group SPG2.
Step 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Switch(config)# wireless mobility controller peer-group SPG2
Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (GUI)

Before You Begin

- Ensure that the device is in mobility controller state.
- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Step 1 Choose **Controller** > **Mobility Management** > **Switch Peer Group**.
The **Mobility Switch Peer Groups** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Switch Peer Group Name**
b) **Bridge Domain ID**
c) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

Before You Begin

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

SUMMARY STEPS

1. **wireless mobility group name** *group-name*
2. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr*
3. **wireless mobility group keepalive interval** *time-in-seconds*
4. **wireless mobility group keepalive count** *count*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Switch(config)# wireless mobility group name Mygroup`	Creates a mobility group named Mygroup.
Step 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	Adds a mobility controller to the Mygroup mobility group. **Note** When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.
Step 3	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Switch(config)# wireless mobility group keepalive interval 5`	Configures the interval between two keepalives sent to a mobility member.
Step 4	**wireless mobility group keepalive count** *count* **Example:** `Switch(config)# wireless mobility group keepalive count 3`	Configures the keep alive retries before a member status is termed DOWN.

```
Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3
```

Configuring Local Mobility Group (GUI)

Before You Begin

Mobility controllers can belong to only one mobility group and can know mobility controllers in several mobility groups.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.

The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the following details:

a) **Mobility Group Name**

b) **Mobility Keepalive Interval**

c) **Mobility Keepalive Count**

d) **Multicast IP Address** if you want to enable multicast mode to send mobile announce messages to the mobility members.

Note If you do not enable multicast IP address, the device uses unicast mode to send mobile announce messages.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Adding a Peer Mobility Group (CLI)

Before You Begin

MCs belong to only one group, and can know MCs in several groups.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	Adds the member as a peer MC in a different group than the Mygroup.

Adding a Peer Mobility Group (GUI)

Before You Begin

Mobility controllers belong to only one group, and can know several mobility groups.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Peer**.

The **Mobility Peer** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Mobility Member IP**
b) **Mobility Member Public IP**
c) **Mobility Member Group Name**
d) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

SUMMARY STEPS

1. **wlan** open21
2. **no mobility anchor sticky**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** open21 **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:** `Switch(config-wlan)# no mobility anchor sticky`	Disables the default sticky mobility anchor.

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before You Begin

You can configure a mobility oracle on a known mobility controller.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **group** *group-name*
2. **wireless mobility oracle ip** *oracle-ip-addr*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3`	Creates and adds a MC to a mobility group.
Step 2	**wireless mobility oracle ip** *oracle-ip-addr* **Example:** `Switch(config)# wireless mobility oracle ip 10.10.10.10`	Configures the mobility controller as mobility oracle.

```
Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10
```

Pointing the Mobility Controller to a Mobility Oracle (GUI)

Before You Begin

You can configure a mobility oracle on a known mobility controller.

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.
The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the **Mobility Oracle IP Address**.

Note To make the mobility controller itself a mobility oracle, select the **Mobility Oracle Enabled** check box.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Guest Controller

A guest controller is used when the client traffic is tunneled to a guest anchor controller in the demilitarized zone (DMZ). The guest client goes through a web authentication process. The web authentication process is optional, and the guest is allowed to pass traffic without authentication too.

Enable the WLAN on the mobility agent on which the guest client connects with the mobility anchor address of the guest controller.

On the guest controller WLAN, which can be Cisco 5500 Series WLC, Cisco WiSM2, or Cisco 5700 Series WLC, configure the IP address of the mobility anchor as its own IP address. This allows the traffic to be tunneled to the guest controller from the mobility agent.

Note With Cisco 5700 Series WLC as the guest anchor controller and Cisco 5500 Series WLC or Cisco WiSM2 as export foreign controller, the guest user role per user is not supported on the Cisco 5700 Series WLC.

SUMMARY STEPS

1. **wlan** *wlan-id*
2. **mobility anchor** *guest-anchor-ip-addr*
3. **client vlan** *vlan-name*
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** *wlan-id* **Example:** `Switch(config)# wlan Mywlan1`	Creates a WLAN for the client.
Step 2	**mobility anchor** *guest-anchor-ip-addr* **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors (GA) IP address on the MA. **Note** To enable guest anchor on the mobility controller, you need not enter the IP address. Enter the **mobility anchor** command in the WLAN configuration mode to enable GA on the mobility controller.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a VLAN to the client's WLAN.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the WLAN.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Guest Anchor

SUMMARY STEPS

1. **wlan** Mywlan1
2. **mobility anchor** <guest-anchors-own-ip-address>
3. **client vlan**<vlan-name>
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** Mywlan1 **Example:** `Switch(config)# wlan Mywlan1`	Creates a wlan for the client.
Step 2	**mobility anchor** <guest-anchors-own-ip-address> **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors IP address on the guest anchor (GA). The GA assigns its own address on itself.
Step 3	**client vlan**<vlan-name> **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a vlan to the clients wlan.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the wlan.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Mobility Controller Managing Mobility Agent

Overview

A mobility controller (MC) can support up to 16 MAs. Most of the wireless and common configurations such as AAA, ACL, and so on are generally the same across all the switches. However, in the earlier Cisco IOS XE releases, these configurations were required to be done explicitly on all the MAs, which constituted the distributed mode. The Mobility Controller managing Mobility Agent feature addresses this issue using which you can push these wireless and common configurations from the MC to the MAs. This helps you to easily configure, monitor, and troubleshoot all the MAs from the MC. This constitutes the centralized mode.

An MC can have both centrally managed and non-centrally managed MAs at the same time. A centrally managed MA receives a set of configurations that are configured on the MC. A non-centrally managed MA does not receive any configuration from the MC. While an MA is being centrally managed, it is not possible for you to modify any of the configurations that are pushed from the MC to the MA.

The mobility controller (MC) pushes all the relevant configurations over the existing CAPWAP tunnels to all the centrally managed MAs. The MC also pushes any incremental configurations that might get added on the MC to the MAs.

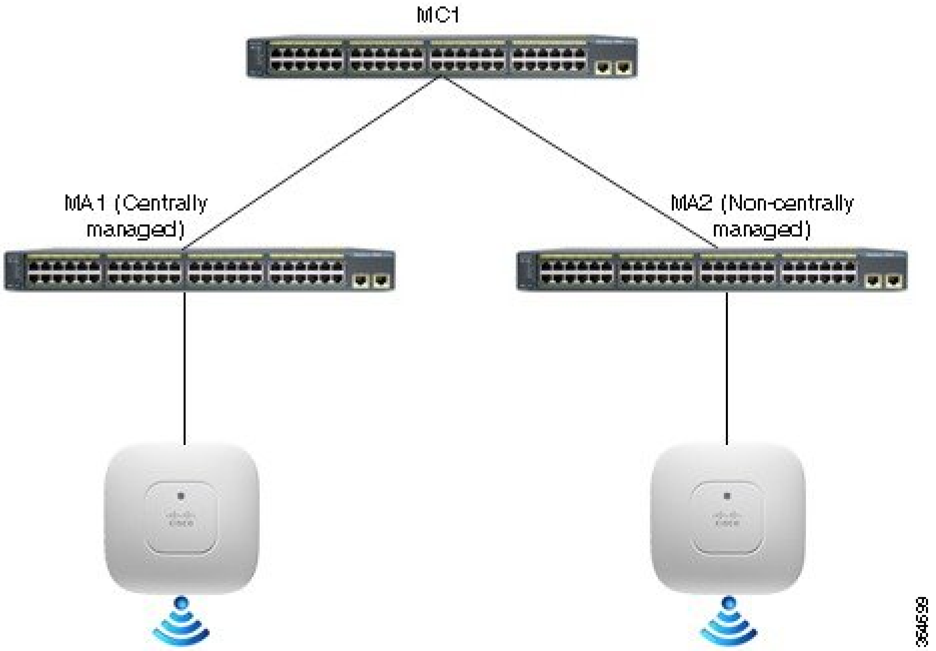
Note Before you can use this feature, you must have the day 0 configuration that is required to bring up the CAPWAP tunnel between the MC and the MA.

The following sections of the configuration are sent to the MAs:

- Common configuration—This is the configuration, which is shared between wired and wireless such as the security configuration namely authentication, authorization, and accounting.
- Wireless configuration—All wireless configuration.

For a complete list of commands that synchronized between MC and MA, see *MC Managing MA - List of Commands Synchronized Between MC and MA* at http://www.cisco.com/c/en/us/td/docs/wireless/controller/mc-ma/mc-ma-sync.html.

Figure 1: MC Centrally Managing MAs



Differences between Distributed and Centralized Modes

Distributed Mode	Centralized Mode
To be configured on the MC: • MA to MC Mobility Peering Configuration • Wireless LAN • Wireless QoS Policies • Wireless Flexible NetFlow/AVC • Wireless Security ACL • AAA Global Configurations • Location • CleanAir, RRM, Client Link • Global and Per AP Configuration	To be configured on MC: • MA to MC Mobility Peering Configuration • Wireless LAN • Wireless Security ACL • AAA Global Configurations • Location • CleanAir, RRM, Client Link • Global and Per AP Configuration

Distributed Mode	Centralized Mode
To be configured on the MA: • MA to MC Mobility Peering Configuration • Wireless LAN • Wireless QoS Policies • Wireless Flexible NetFlow/AVC • Wireless Security ACL • AAA Global Configurations • Location • CleanAir, RRM, Client Link • Global and Per AP Configuration	To be configured on the MA: • MA to MC Mobility Peering Configuration • Wireless QoS Policies • Wireless Flexible NetFlow/AVC

Feature History

Release	Remarks
Cisco IOS XE Release 3.7.0E	This feature was introduced on the Catalyst 3850 and Catalyst 3650 Series Switches.
Cisco IOS XE Release 3.7.1E	Support for this feature was added to Catalyst 4500E Supervisor Engine 8-E.

Restrictions

- The centralized mode is supported only with the converged access solution platforms and not with the Cisco Wireless AireOS platforms such as Cisco 5500 or 8500 Series Wireless Controllers.
- Once the MA is in centralized mode, the globally managed configuration is disabled and the rest of the configuration and monitoring are available on the Web GUI.
- This feature is not supported on Cisco Prime Infrastructure.
- Out-of-sync Reload: When the MC detects the MA to be out of sync, the MA is forced to reload and then resync the entire configuration from the MC after coming up.
- Following are some of the scenarios when the MC and the MA can go out of sync:
    - A new MA joins the MC and the MA is centrally managed
    - When an MA is moved from one MC to another MC
- QoS config is not pushed from the MC to the MA.

- The MC pushes all the configurations to all the centrally managed MAs. It is not possible to select a subset of the configurations and then push to a particular group of MAs instead of all the MAs.
- L3 roaming cannot be done because WLAN configuration is pushed from the MC.

Configuring MC Managing MA (GUI)

Step 1 On the Mobility Controller, choose **Configuration** > **Controller** > **Mobility Management** > **Switch Peer Group**.

Step 2 Create a new switch peer group member or edit a switch group member.

Step 3 On the **Switch Peer Group > New/Switch Peer Group > Modify** page, select the **Centralized mode** check box to set a member MA as centrally managed from the MC.

Step 4 Save the configuration.

Step 5 On the Mobility Agent's GUI's home page, you can verify that the status is shown as **Centrally Managed**.

Example

This example shows how to create a WLAN on an MC and synchronize the WLAN configuration with centrally managed MCs.

Step 1 On the MC, create a WLAN named **MCMA_Demo**.

Step 2 Click **Apply**.
WLAN is created but disabled by default.

Step 3 Enable the WLAN–On the **WLAN > Edit** page, uncheck the **Status** check box.

Step 4 Change the **Interface/Interface Group (G)** to **VLAN0022**.

Step 5 In the **Security** tab, set the **Layer 2 Security** to **None**.

Step 6 Click **Apply** and then click **Save Configuration**.
This synchronizes the configuration with the centrally managed MAs.

Step 7 On the MA, navigate to the **WLANs** page.
The **MCMA_Demo** WLAN created on the MC and synchronized with the MA is displayed.

Configuring MC Managing MA (CLI)

Step 1 On the MC:

a) Configure the wireless management interface by entering this command:

```
Switch(config)# wireless management interface vlan vlan-id
```

b) Configure a switch peer group (SPG) by entering this command:

```
Switch(config)# wireless mobility controller peer-group spg-name
```

c) Add an MA to the SPG and configure it to be centrally managed by entering this command: (Use only centralized option)

```
Switch# wireless mobility controller peer-group spg-name member ip ip-addr mode centralized
```

Step 2 On the MA:

a) Specify the IP address of the MC by entering this command:

```
Switch(config)# wireless mobility controller ip mc-ip-addr
```

b) Configure the wireless management interface by entering this command:

```
Switch(config)# wireless management interface vlan vlan-id
```

Step 3 Centralized monitoring:

a) From the MC, you can see the status of MA by entering this command:

```
Switch# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                              : Mobility Controller
Mobility Protocol Port                     : 16666
Mobility Group Name                        : default
Mobility Oracle IP Address                 : 0.0.0.0
DTLS Mode                                  : Enabled
Mobility Domain ID for 802.11r             : 0xac34
Mobility Keepalive Interval                : 10
Mobility Keepalive Count                   : 3
Mobility Control Message DSCP Value        : 48
Mobility Domain Member Count               : 1

IP         Public IP        Link   Status     Centralized(Cfgd : Running)
----------------------------------------------------------------------------------
1.1.1.1     1.1.1.1          UP   : UP         Enabled        Enabled
3.3.3.1     3.3.3.1          DOWN : DOWN       Enabled        Enabled
```

Centralized Mode Configured	Centralized Mode Running	What it Means
Disabled	Disabled	The MA is not configured as centrally managed on the MC.
Enabled	Disabled	The MA is configured as centrally managed on the MC, but tunnel to the MA is still down or the MA is yet to acknowledge the message from the MC in which the MC informs the MA that it is centrally managed.
Enabled	Enabled	The MA is configured as centrally managed on the MC and the MA is running in Centrally Managed mode.

Centralized Mode Configured	Centralized Mode Running	What it Means
Disabled	Enabled	Not applicable.

b) You can see all the MAs that have been configured on the MC irrespective of the SPG and irrespective of whether they are centrally managed or not by entering this command:

```
Switch# show cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 16

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.155
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 16
Last rcvd cfg rev on MA = 16
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 16
Last sent cfg timestamp = 1427826323 sec 936009397 nsec
----------------


Members: No. of MAs configured on the MC
System Rev No on MC: What version number the MC is at

Entry
```

The above example output shows that the MA is operational and has received the configuration from the MC.

c) To see the configurations that were executed on the MC and buffered in the CMM agent because they are interesting and need to be synced, enter this command:

```
Switch# show cmm config

Current version number: 17
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
access-list 1 permit any
wlan MCMA_Demo 4 MCMA_Demo
client vlan 22
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Note The configuration from the MC is synchronized with the MAs only after "wr memory" command is run on the MC.

Step 4 Remote commands: You can execute commands on the MA remotely from the MC. For example, you can enter this command on the MC to see if the client has reached the uptime:

```
Switch# remote command 1.1.1.1 sh wcdb da all

Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
                Foreign Clients           = 0
                MTE Clients               = 0


Mac Address       VlanId   IP Address     Src If             Auth     Mob
----------      ---------  -------------  --------          -----   -------
ec55.f9c6.35c3     22        53.1.1.2    0x00D19B00000001C5  RUN    ANCHOR
```

You can also remotely log on to the MA from the MC by entering this command:

```
Switch# remote login 1.1.1.1

Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


User Access Verification

Password:
MA1>en
Password:
MA1#
```

Example

This example shows how to create a WLAN on an MC and synchronize the WLAN configuration with centrally managed MCs.

Step 1 On the MC, create a WLAN named MCMA_Demo by entering this command:

```
Switch(config)# wlan MCMA_Demo 1 MCMA_Demo
Switch(config-wlan)# exit
Switch(config)# exit
```

Step 2 Enter this command to check the configuration:

```
Switch# sh cmm config

Current version number: 3
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
wlan MCMA_Demo 1 MCMA_Demo
exit
```

Step 3 Enter this command to check the number of MAs that are configured to be centrally managed:

```
Switch# sh cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 2

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 2
Last sent cfg timestamp = 1432843797 sec 57656031 nsec
----------------
```

Step 4 See the WLAN details by entering this command:

```
Switch# sh wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID          VLAN Status
---------------------------------------------------
1        MCMA_Demo    MCMA_Demo       1    DOWN
```

Step 5 Save the configuration by entering this command:

```
Switch# wr memory

Building configuration...
Compressed configuration from 7612 bytes to 3409 bytes[OK]
```

Step 6 Check the synchronization status on the MA by entering this command:

```
Switch# sh cmm member-table

CMM Member Table
----------------
Total No Of Members = 1
```

```
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 2
Last rcvd cfg rev on MA = 2
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1432847325 sec 107200589 nsec
----------------
```

Step 7 On the MA, enter the following command to see that the WLAN that was created in the MC is now synchronized with the MA:

```
Switch# sh wlan summary

Number of WLANs: 1

WLAN  Profile Name    SSID           VLAN Status
---------------------------------------------------
1    MCMA_Demo     MCMA_Demo          1    DOWN
```

Example Logs where multiple configurations are synchronized

```
MC -

MC#sh cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:
wlan open 2 open
assisted-roaming dual-list
assisted-roaming neighbor-list
broadcast-ssid
ccx aironet-iesupport
channel-scan defer-priority 4
client association limit ap 0
client association limit radio 0
client vlan default
exclusionlist
exclusionlist timeout 60
ip access-group web none
mac-filtering test
mobility anchor sticky
radio all
security wpa
security wpa akm dot1x
security wpa wpa2
security wpa wpa2 ciphers aes
security dot1x authentication-list test
security dot1x encryption 104
security ft over-the-ds
security ft reassociation-timeout 20
security static-wep-key authentication open
security tkip hold-down 60
security web-auth authentication-list test2
security web-auth parameter-map test3
service-policy client input un
service-policy client output un
service-policy input unk
service-policy output unk
session-timeout 1800
no shutdown
exit


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 3

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 3
Last sent cfg timestamp = 1433441315 sec 669464681 nsec
----------------


MC#sh wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                           VLAN Status
--------------------------------------------------------------------------------
1    test                             test                           1    DOWN
2    open                             open                           1    UP

MC#wr mem
Building configuration...
Compressed configuration from 7972 bytes to 3619 bytes[OK]
MC#
MC#
MC#
MC#
MC#sh wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                           VLAN Status
--------------------------------------------------------------------------------
1    test                             test                           1    DOWN
2    open                             open                           1    UP

MC#sh cmm config
Current version number: 4
To sync and save configuration to Mobility Agents execute: "wr memory"

Config commands present in the buffer:


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4
```

```
entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488804 sec 349065646 nsec
----------------


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 3
Last rcvd cfg rev on MA = 3
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_STALE
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488812 sec 349323943 nsec
----------------


MC#sh cmm member-table
CMM Member Table
----------------
Total No Of Members = 1
System Rev No on MC = 4

entry 0
--------
entry_status            = In use
ip_addr                 = 10.5.84.12
SPG Name                = SPG1
Centrally Managed       = True
Applied Cfg rev on MA   = 4
Last rcvd cfg rev on MA = 4
Tunnel State            = Up
Status                  = CMM_MEMBER_STATUS_IN_SYNC
Last sent cfg rev to MA = 4
Last sent cfg timestamp = 1433488820 sec 349544632 nsec
----------------
MC#




MA -



MA21#sh cmm config
Current version number: 3
Centrally Managed: True
MA21#sh wlan sum
MA21#sh wlan summary

Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
```

```
--------------------------------------------------------------------------------
1    test                             test                           1    DOWN

MA21#
Building configuration...

*Jun  5 07:21:18.295: %SYS-5-CONFIG_I: Configured from console by vty1
*Jun  5 07:21:18.314: %CMM-6-CONFIG_SYNC_SAVE_MSG: Saving config rev#4 received
from Mobility Controller.Compressed configuration from 13033 bytes to 4340 bytes[OK]

MA21#sh cmm config
Current version number: 4
Centrally Managed: True
MA21#sh wlan summary

Number of WLANs: 2

WLAN Profile Name                     SSID                           VLAN Status
--------------------------------------------------------------------------------
1    test                             test                           1    DOWN
2    open                             open                           1    UP


MA21#sh run wlan
wlan test 1 test
 shutdown
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
 security web-auth parameter-map test3
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#
MA21#sh run wlan ?
  WORD  Wlan profile name to display
  |     Output modifiers
  <cr>

MA21#sh run wlan open
wlan open 2 open
 assisted-roaming dual-list
 assisted-roaming neighbor-list
 ip access-group web none
 mac-filtering test
 security dot1x authentication-list test
 security web-auth authentication-list test2
 security web-auth parameter-map test3
 service-policy client input un
 service-policy client output un
 service-policy input unk
 service-policy output unk
 no shutdown
MA21#
MA21#
```