Managing Mesh and Flex+Bridge Modes

Introduction to Mesh Support in Cisco Wave 2 Indoor Access Points

Provides wireless coverage without structural changes except for mounting and power source for the APs.

Restrictions and Guidelines

- Some of the older Cisco Indoor APs do not support Mesh network.

Note The unsupported APs display the message **This AP does not support Mesh mode due to misaligned or non-contiguous radio MAC** in CLI mode.

Introduction to Flex+Bridge Mode on Mobility Express Day 0 Configuration

This feature adds Mesh support on Mobility Express for supporting indoor and outdoor APs in Flex+Bridge mode. The advantage of using Mesh AP is that it reduces the network setup costs as the Mesh AP takes the role of the controller so a separate controller is not required.

The Mesh on ME supports only the default FlexConnect group. More FlexConnect groups cannot be created.

In this release, you can bulk import MAC addresses in the CSV file format using the ME GUI.

Restrictions and Guidelines on Mobility Express Flex+Bridge Mode

- AP type Mobility Express mode is not supported on an external AP with the MAP role to prevent MAP going nonresponsive.

- The following APs are supported:

    - **RAP-ME:** Cisco AireOS 1542, 1562, 1815s, 3802s, IW6300, and ESW6300 APs

    - **MAPs**: Cisco AireOS 1542, 1562, 1815s, 3802s, IW6300, and ESW6300 APs

    - **FlexConnect APs behind MAPs:** Cisco indoor and outdoor Access Points

Configuring Day 0 Flex+Bridge on a Root Access Point(GUI)

Step 1   Power the seleted RAP.

Step 2   Connect to the **CiscoAirProvision** SSID using a Wi-Fi enabled laptop.

Enter the default password – password.

> **Note**   **CiscoAirProvision** SSID is broadcasted at 2.4GHz band.

Step 3   Open the web address **http://192.168.1.1** in a browser.

This page redirects to the initial configuration wizard.

Step 4   Create an admin account on the controller by specifying the following parameters and then click **Start**.

    a.   Enter an admin username. Maximum up to 24 ASCII characters

    b.   Enter the password. Maximum up to 24 ASCII characters

    When specifying a password, ensure that

       - The password must contain characters from at least three of the following classes – lowercase letters, uppercase letters, digits, special characters.

• No character in the password can be repeated more than three times consecutively.

• The new password must not be the same as the associated username and the username reversed.

• The password must not be cisco, ocsic, or any variants obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s

Step 5   Set up your controller by specifying the values.

On the **Set Up Your Controller** screen, using the checklist, follow the Configuring Mobility Express controller using Over-the-Air Setup Wizard the step 4 table in *Mobility Express Deployment guide*.

Slide the Mesh option to **Enable**.

Note   When Mesh is enabled, the AP is configured to Flex + Bridge mode. Disabling configures the AP to FlexConnect mode.

Step 6   Boot the AP using GUI to configure Mobility Express.

Configuring Day 0 Flex+Bridge on a Root Access Point (CLI)

Step 1   Power the selected RAP.

Step 2   Enter the following parameters when prompted

    a.   Username

    b.   Password

    c.   System name

    d.   Country Code

Step 3   Configure the RAP in Flex+ Bridge mode.

Enter **Yes** on the **Set the internal AP to Flex+Bridge mode** prompt.

Note   If you enter No, then the AP loads the previous Mobility Express image in FlexConnect mode. Default is **No**.

Upgrading the Software on the Root Access Point(GUI)

Step 1   Choose **Management** > **Software Update** to open the **Software Update** page.

Step 2   Disable Auto AP-Type Conversion option.

Step 3   Disable **Efficient Join** when the MAP and RAP used are not of the same model.

Step 4   Click **Apply**.

Step 5 From the **Transfer Mode** drop-down list, choose **TFTP/SFTP** mode.

Step 6 In the **IP Address** (IPv4) field, enter the IP address of the server

Step 7 In the **File Path** field, enter the TFTP/SFTP server directory path of the software file

Step 8 Choose from one of the two update options

- Click **Update** to update the software immediately.
- You can also set up a schedule to execute the update.

   a. Enable Schedule Update.

   b. Select the date and time from the **Set Update Time** field

After the image predownload is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the Auto Restart check box, you can manually reboot the controller. After the upgrade, choose **Advanced** > **Controller Tools** and click **Restart Controller**.

Importing Multiple MAC Addresses (GUI)

Step 1 Choose **Wireless** > **WLAN Users** to open the **WLAN Users** page.

Step 2 Choose the **Local MAC Addresses** tab

Step 3 Click **Import** to import a CSV file.

The Import Mac ID File window is displayed.

Step 4 In the **Import Mac ID File** window, upload a comma-separated values (CSV) file.

Click the **Choose File** button and browse to the CSV file containing the MAC address and select **OK**.

Note The format for the CSV file is displayed as an example.

```
MAC ID,Type,WLAN ID,Description
00:73:ee:4a:31:00,b,0,MAP1562
00:42:ec:4a:5v:80,w,0, RAP1562E
```

Step 5 Choose **Yes** to import the CSV file.

After the file is imported, a summary is displayed. You may click the **Click Here** option to see the list of MAC IDs which failed to be imported and the reason for the failure.

Configuring the MAP to Bridge Mode (GUI)

Step 1 Choose **Wireless Settings** > **Access Points** > to open the **Access Points Administration** page.

Step 2 Check the current type for the AP of interest.

If the type is ME Capable, convert it to CAPWAP.

    a. Select the AP check box.

    b. Choose **Convert to CAPWAP**, to convert the AP to CAPWAP mode.

    Proceed once the type is changed to CAPWAP successfully.

Step 3 Select the **AP Edit** button to edit the AP settings.

The **Edit AP** dialogue appears, choose **Yes**.

Step 4 In the **AutoAP (Active Controller)** > **General** tab, change the **Operating Mode** to **Bridge** from the drop-down list.

A window is displayed with the message to configure the channel and Tx Power settings. Click **OK**.

Step 5 Choose the Radio 2 (5GHz) tab

    a. From the **Channel** drop-down list, select the desired channel.

    b. From the **Transmit Power** drop-down list, select the desired power value.

Step 6 Click **Apply**.

Step 7 Verify if the AP is a part of the Mesh network by entering this command in the controller:

show mesh ap tree

Configuring FlexConnect Group (CLI)

Step 1 Enable VLAN support on FlexConnect Group by entering this command:

config flexconnect group *group-name* **vlan** {**enable** | **disable**}

Step 2 Configure the Native VLAN for the default-flexgroup by entering this command:

config flexconnect group *group-name* **vlan native** *vlan-id*

Step 3 Enable VLAN override-ap on FlexConnect Group by entering this command:

config flexconnect group *group-name* **vlan override-ap** {**enable** | **disable**}

```
Warning! This might result in clearing AP specific wlan-vlan mappings and vlan acl mappings.
Are you sure ? (y/n) Y
```

Configuring FlexConnect Group with WLAN-VLAN Mappings (CLI)

Step 1 Create WLAN-VLAN Mapping in FlexConnect Group by entering this command:

config flexconnect group *group-name* **wlan-vlan wlan** *wlan-id* {**add** | **delete**} **vlan** *vlan-id*

Step 2   View the flexconnect group details by entering this command:

show flexconnect group detail *group-name*

Step 3   View the Flexconnect WLAN-VLAN details by entering this command:

show flexconnect wlan vlan

Enabling Expert View for Global Mesh Configuration (GUI)

Step 1   Choose the green arrow icon facing each other located at the top right section of the main page.

A confirmation window appears, click **OK**.

Step 2   Choose **Wireless Settings** > **Mesh** to open the **Mesh settings** page

Step 3   Configure the Mesh settings in the following tabs.

    a.   **General**: similar to AireOS controller settings

    b.   **Mesh RAP Downlink backhaul**: Configure the global RAP backhaul at 2.4 GHz or 5 GHz.

    c.   **Convergence**: Configure the mode

    d.   **Ethernet bridging**: Configure the VLAN Transparent

    e.   **Security**: Configure the security parameters

Step 4   Save the configuration.

Configure Mesh on Access Points (GUI)

Step 1   Select **Wireless Settings** > **Access Points** to open the **Access Points Administration** page.

Step 2   Choose the Edit option on the desired AP.

The AP configuration window is displayed. Select **Mesh** tab

Step 3   Configure the Mesh settings for the AP.

Step 4   Save the configuration.

Troubleshooting

This section contains the following:

Mesh Tree with RAPs, Bakchaul Disabled on Internal RAP (ME) Causes External RAP into ME/Reboot Silently

In this scenario, the switchport connected to one of the RAPs was a root fowarding port because the switch behind the MAP was selected as the root bridge. This is not supported because in mesh networks, the switch connected to the main RAP must be a root bridge.

Here is how you can view the incorrect configuration:

```
Device#show spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
             Port        37 (GigabitEthernet1/0/37)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
             Address     00cc.fc7e.b980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Gi1/0/1            Desg FWD 4         128.1    P2p
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
Gi1/0/19           Desg FWD 4         128.19   P2p
Gi1/0/21           Desg FWD 4         128.21   P2p
Gi1/0/22           Desg FWD 4         128.22   P2p
Gi1/0/23           Desg FWD 4         128.23   P2p

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------

Gi1/0/24           Desg FWD 4         128.24   P2p
Gi1/0/37           Root FWD 4         128.37   P2p ==>>> Result of incorrect default config
Gi1/0/41           Desg FWD 4         128.41   P2p
Gi1/0/43           Desg FWD 4         128.43   P2p
Gi1/0/48           Desg FWD 4         128.48   P2p
```

When this occurs, a change in topology (such as MAPs roaming with Ethernet bridging switch behind) causes ports to temporarily block themselves and go into listening mode to detect loops.

The following example shows this temporary block:

```
Device#sh spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
```

```
              Port        37 (GigabitEthernet1/0/37)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
              Address      00cc.fc7e.b980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Gi1/0/1            Desg FWD 4         128.1    P2p
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
Gi1/0/19           Desg FWD 4         128.19   P2p
Gi1/0/21           Desg FWD 4         128.21   P2p
Gi1/0/22           Desg FWD 4         128.22   P2p
Gi1/0/23           Desg FWD 4         128.23   P2p

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------

Gi1/0/24           Desg FWD 4         128.24   P2p
Gi1/0/37           Root FWD 4         128.37   P2p
Gi1/0/41           Desg FWD 4         128.41   P2p
Gi1/0/43           Altn BLK 4         128.43   P2p ===>>> Temporary block
Gi1/0/48           Desg FWD 4         128.48   P2p
```

The following example shows that the ports have gone to listening mode to detect loops:

```
Device#sh spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
             Port        43 (GigabitEthernet1/0/43)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

   Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
              Address     00cc.fc7e.b980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  15  sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------
Gi1/0/1            Desg FWD 4         128.1    P2p
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
Gi1/0/19           Desg FWD 4         128.19   P2p
Gi1/0/21           Desg FWD 4         128.21   P2p
Gi1/0/22           Desg FWD 4         128.22   P2p
Gi1/0/23           Desg FWD 4         128.23   P2p

Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------------------

Gi1/0/24           Desg FWD 4         128.24   P2p
Gi1/0/37           Desg FWD 4         128.37   P2p
Gi1/0/41           Desg FWD 4         128.41   P2p
Gi1/0/43           Root LIS 4         128.43   P2p ===>>>>> Listen for loops
Gi1/0/48           Desg FWD 4         128.48   P2p
```

During this stage, Virtual Router Redundancy Protocol (VRRP) from MobilityExpress does not reach the external RAP, causing ME-capable RAP to start its own instance of switchdrvr. When the port opens again,

VRRP detects a duplicate ME and shuts down the AP immediately to bring down switchdrvr (hence the silent reboot).

In a topology that has multiple switches and default settings, the root bridge is selected based on MAC address of the devices. This is not a preferred selection in mesh networks. Ensure that the switch connected to a RAP is always configured to the primary root bridge. You can do this by using the **spanning-tree vlan** *vlan-id* **root primary** command.

After the root bridge is selected, all ports connected to RAPs are designated forwarding ports and are never blocked on this switch. The switch behind the MAP instead becomes the root port, which blocks the port on changes in topology or goes into the listening mode to detect loops.

VLAN Trunking Disabled After RAP Reboots

This scenario occurs when the Mobility Express setup is configured with Ethernet bridging and the RAP reboots, resulting in the AP VLAN trunking configuration getting lost.

- To reconfigure AP VLAN trunking on the RAP when the the AP is in Bridge only mode, enter the following commands:

  ```
  config ap vlan-trunking enabled ap-name

  config ap vlan-trunking native vlan-id ap-name
  ```

- To reconfigure AP VLAN trunking on the RAP when the the AP is in Flex+Bridge mode, enter the following commands:

  ```
  config flexconnect group default-flex-group vlan enable

  config flexconnect group default-flex-group vlan native vlan-id
  ```

Note   We recommend you to perform the Flex+Bridge mode commands when the AP is in Flex+Bridge mode, as bridge-only mode configuration is over-written after the RAP rejoins.