Configuring Point-to-Point Mesh Link with Ethernet Bridging on Mobility Express APs

Contents

Introduction

This document describes the process of deploying Point-to-Point mesh links with Ethernet Bridging using Cisco Mobility Express (ME) software.

About Mobility Express

This document uses Cisco 1542 outdoor Access Points. Mesh support on Mobility Express software for indoor and outdoor APs in Flex+Bridge mode was introduced in release 8.10.

The following AP models are supported:

- **As an ME Root AP:** Cisco AireOS 1542, 1562, 1815s, 3802s APs

- **As a Mesh AP**: Cisco AireOS 1542, 1562, 1815s, 3802s APs

Mobility Express (ME) is a solution that replaces the Autonomous AP mode and software. It allows a lighter version of AireOS based Wireless LAN Controller (WLC) software to run on the Access Point itself. Both WLC and AP code is stored inside a single partition of the AP memory. A Mobility Express deployment does not require a license file, nor license activation.

Once the device running Mobility Express capable software is powered on, the "AP part" first boots up. A few minutes later, the controller part also initializes. Once a console session is established, an ME capable device will show the WLC prompt. In order to enter the underlying AP shell, a command `apciscoshell` can be used:

<#root>

```
(Cisco Controller) >

apciscoshell

!!Warning!!: You are entering ap shell. This will stop you from establishing new telnet/SSH/Web session
 Also the exsisting sessions will be suspended till you exit the ap shell.
 To exit the ap shell, use 'logout'

User Access Verification
Username:

admin

Password:

********

RAP>

logout


(Cisco Controller) >
```

Prerequisites

Components Used

- 2x 1542D-E Access Points
- 2x 3560-CX Cisco Switches
- 2x Laptops
- 1x Console Cable

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.
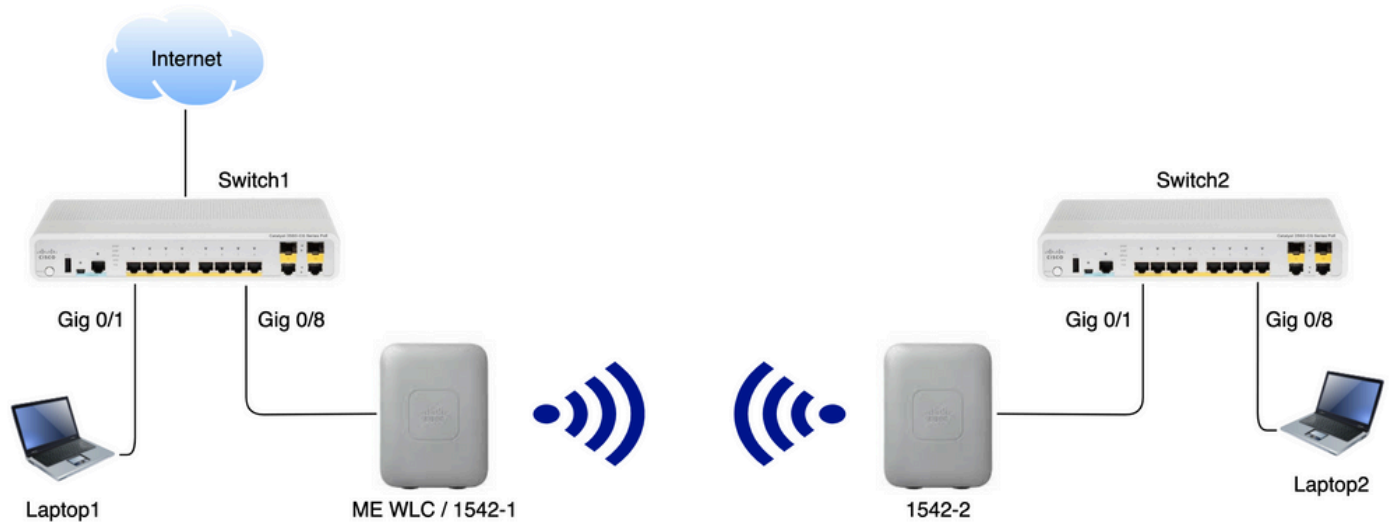
Network Diagram

All the devices in this network will be located inside the 192.168.1.0/24 subnet. The Mobility Express AP (controller) will have its management interface untagged, while the native VLAN on all ports will be VLAN 39. AP 1542-1 will take the role of a controller and Root Access Point (RAP), while AP 1542-2 will take the role of Mesh Access Point (MAP). This table contains the IP addresses of all devices in the network:

Note: Tagging the management interface can cause issues with the AP joining the internal WLC process. If you decide to tag the management interface, ensure that the wired infrastructure part is configured accordingly.

Device	IP Address
Default Gateway	192.168.1.1
Laptop 1	192.168.1.100
Laptop 2	192.168.1.101
Mobility Express WLC	192.168.1.200
1542-1 (RAP)	192.168.1.201

1542-2 (MAP)	192.168.1.202

Configuration

Switch Configurations

Switch ports where laptops are connected are configured as access ports with the VLAN set to 39:

<#root>

Switch1

```
#show run interface Gig 0/1

Current configuration : 205 bytes
!
interface GigabitEthernet0/1
 description Laptop1
 switchport access vlan 39
 switchport mode access
end
```

<#root>

Switch2

```
#show run interface Gig 0/8

Current configuration : 205 bytes
!
interface GigabitEthernet0/8
 description Laptop2
 switchport access vlan 39
 switchport mode access
end
```

Switch ports where APs are connected will be in trunk mode with the native VLAN set to 39:

<#root>

Switch1

```
#show run interface Gig 0/8
Building configuration...
!
interface GigabitEthernet0/8
 description 1542-1 (RAP)
 switchport mode trunk
 switchport trunk native vlan 39
end
```

<#root>

Switch2

```
#show run interface Gig 0/1
Building configuration...
!
interface GigabitEthernet0/1
 description 1542-1 (RAP)
 switchport mode trunk
 switchport trunk native vlan 39
end
```

Factory reset of the APs

It is recommended to perform a factory reset of the APs before starting a new deployment. This can be done by pressing the mode/reset button on the AP, plugging the power in and continuing to hold it for more than 20 seconds. This will ensure that all previous configuration has been wiped. The AP will be accessible via a console connection with default username of `Cisco` and password of `Cisco` (case sensitive).

A factory reset does not necessarily move an AP back to lightweight mode if it is already running in Mobility Express. An important step is to identify if your APs are running a lightweight image or a Mobility express image.

If your AP is lightweight, you can convert it to Mobility Express by downloading the mobility express code. If the AP is already in mobility express mode, you have to follow the upgrade process in the GUI of the access point/controller to change the software version.

Example of a show version from AP running lightweight image :

cisco AIR-AP1562I-E-K9 ARMv7 Processor rev 1 (v7l) with 1028616/605344K bytes of memory. Processor board ID FCZ2150Z099 AP Running Image : 8.5.151.0 Primary Boot Image : 8.5.151.0 Backup Boot Image : 0.0.0.0 1 Gigabit Ethernet interfaces 2 802.11 Radios Radio Driver version : 9.0.5.5-W8964 Radio FW version : 9.1.8.1 NSS FW version : 2.4.26

This is an example of AP already running in Mobility Express software :

AP#show version . .. AP Running Image : 8.10.185.0 Primary Boot Image : 8.10.185.0 Backup Boot Image : 8.10.185.0 . .. . AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE

Downloading the lightweight capwap image to 1542-2 (MAP)

Laptop 1 will be used as a TFTP server. AP 1542-2 can be initially connected to Switch 1 Gig 0/8 port just so that the upgrade can be performed. On software.cisco.com, under 1542 lightweight images, download 15.3.3-JJ1 (full name *ap1g5-k9w8-tar.153-3.JK9.tar*) which corresponds to the 8.10.185 release image. The latest lightweight AP image will always correspond to the latest ME version.

Place the image in the TFTP root folder. Connect the console cable, login using the default credentials (username is `Cisco` and password is also `Cisco`). Assign the IP address to the AP and perform the upgrade using following commands:

```
#capwap ap ip 192.168.1.202 255.255.255.0 192.168.1.1
#archive download-sw /reload tftp://192.168.1.100/ap1g5-k9w8-tar.153-3.JK9.tar
```

AP will perform the upgrade and then reboot. Confirm that the upgrade has been successful using `show version` command:

```
<#root>

MAP#

show version

.
..
AP Running Image     : 8.10.185.0
Primary Boot Image   : 8.10.185.0
Backup Boot Image    : 8.8.125.0
```

AP will be unplugged from Switch 1 and plugged back into the Switch 2.

> **Note**: By upgrading the image of the MAP manually, we are avoiding the image upgrade process taking place over-the-air once the mesh link is established.

Downloading Mobility Express capable image to AP 1542-1 (RAP)

Under Mobility Express 8.10.105 releases for 1542 AP, we can see 2 available files: .tar and .zip. Download the .tar file

Aironet 1542I Outdoor Access Point

Release 8.10.185.0

🔔 My Notifications

Related Links and Documentation
Release Notes for 8.10.185.0

File Information	Release Date	Size	
Cisco 1540 Series Mobility Express Release 8.10 Software,to be used for conversion from Lightweight Access Points only. 🔒 AIR-AP1540-K9-ME-8-10-185-0.tar Advisories 📑	24-Mar-2023	60.80 MB	⬇ 🛒
Cisco 1540 Series Mobility Express Release 8.10 Software. Access Point image bundle, to be used for software update and/or supported access points images. 🔒 AIR-AP1540-K9-ME-8-10-185-0.zip Advisories 📑	24-Mar-2023	503.27 MB	⬇ 🛒

Download the .tar file

Unlike a physical WLC, ME Access Points do not have enough flash memory to store all the AP images, so having a TFTP server accessible at all times is necessary if you want to join further APs to your Mobility Express access point. This step is not necessary if we manually upgrade the APs like in this example.

In order to perform the upgrade, connect the console to the AP 1542-1, assign an IP address to it and perform the upgrade of the image:

```
#capwap ap ip 192.168.1.201 255.255.255.0 192.168.1.1
#ap-type mobility-express tftp://192.16.1.100/AIR-AP1540-K9-ME-8-10-185.tar
```

Once the upgrade is finished, the AP reboots. Soon after the AP is up, the controller part starts booting up as well. We soon see the zero-day provisioning SSID "CiscoAirProvision" being broadcasted.

If you ar eon console, you can see a CLI wizard but do not configure the AP that way. The over-the-air GUI wizard is the way to go.
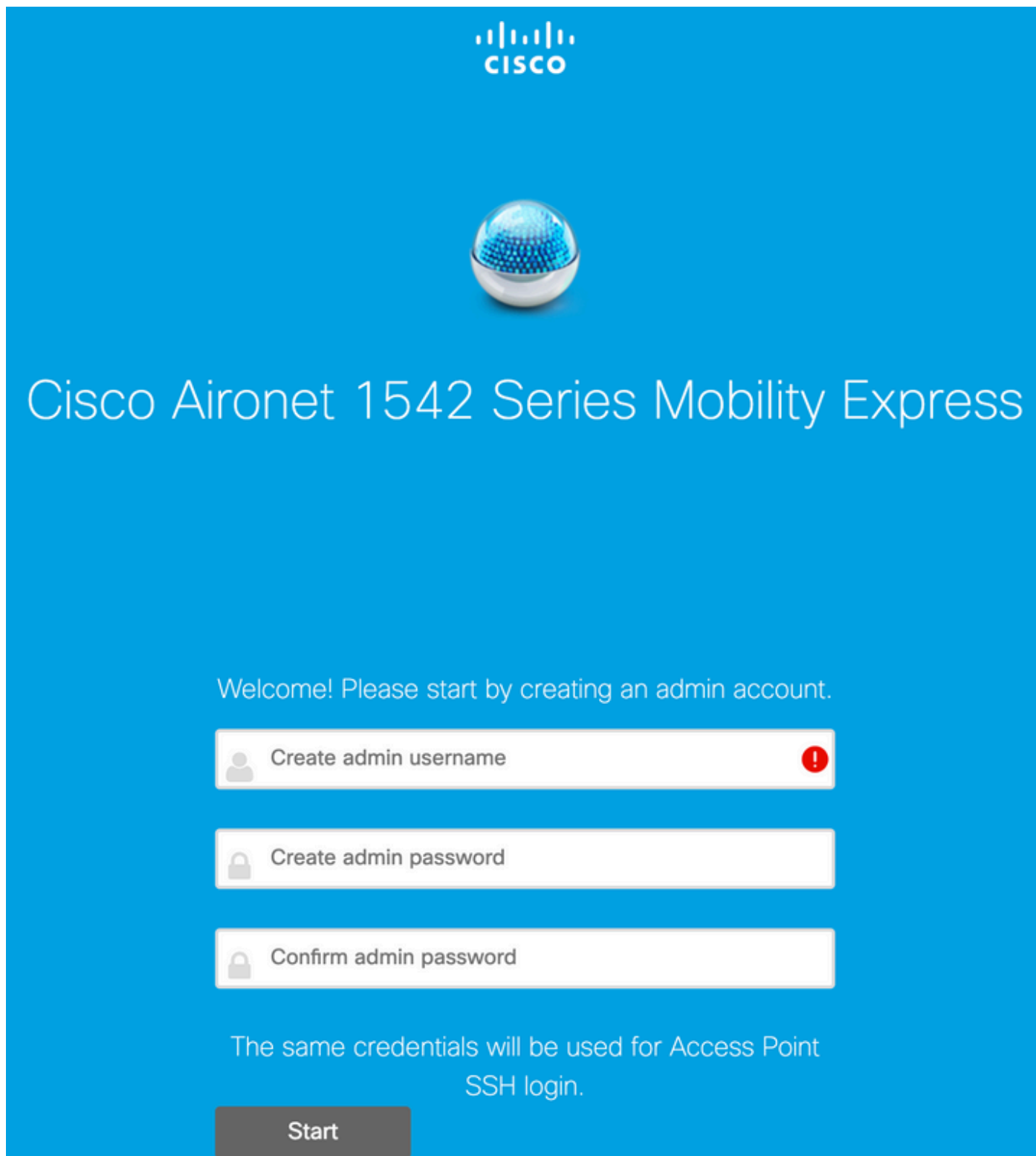
Zero-day SSID Provisioning

Connect to the "CiscoAirProvision" SSID broadcasted by the AP using the password **password**. The laptop gets an IP address from the subnet 192.168.1.0/24.

In case you do not see the SSID being broadcasted, it is still possible that the AP is in "Mobility express CAPABLE" but not running as mobility express. You then would have to connect to the AP CLI and enter **ap type mobility-express** and the AP reboots and broadcasts the provisioning SSID.

It is also possible to convert the AP between local mode and mesh mode using "capwap ap mode local/flex-bridge" if you need to, during this setup.

Open the address **http://192.168.1.1** in a web browser. This page redirects to the initial configuration

wizard. Create an admin account on the controller by specifying admin username and password and then clickStart.

In the next step set up the controller by specifying the values.

Field Name	Description
System Name	Enter the system name for the Mobility Express AP. Example: MobilityExpress-WLC

Country	Choose a country from the drop-down list.
Date & Time	Choose the current date and time. **Note:** The wizard attempts to import the clock information (date and time) from the computer using JavaScript. It is highly recommended that you confirm the clock settings before continuing. The access points depend on clock settings to join the WLC.
Timezone	Choose the current time zone.
NTP Server	Enter the NTP server details.
Management IP	Enter the Management IP address. NOTE : It must be different from the IP assigned to the access point ! In this example, while the AP got the .201 IP, we assign .200 in the configuration wizard. both will be used.
Subnet Mask	Enter the subnet mask address.
Default Gateway	Enter the default gateway.

In this setup, the DHCP server will be running on Switch 1, so there is no need to enable it on the ME WLC. Slide the Mesh option to **Enable** and click **Next**.

In the next step create the wireless network by specifying the following fields:

Field Name	Description
Network Name	Enter the network name.
Security	Choose the **WPA2 Personal** security type from the drop-down list.
Passphrase	Specify the Pre-Shared Key (PSK).
Confirm passphrase	Re-enter and confirm the pass phrase.

This network can be disabled in later stage.

In the Advanced Settings tab, leave the **RF Parameter Optimization** slider disabled and click **Next**

Once the settings are confirmed, the WLC will reboot:

The controller has been fully configured and will restart in 60 seconds.

Next Steps:
After the controller is restarted, it will be accessible from the network by going to this URL –
https://192.168.1.200

1	Controller Settings

Username	admin
System Name	ME
Country	Netherlands (NL)
Date & Time	11/05/2019 10:31:39
Timezone	Amsterdam, Berlin, Rome, Vienna
NTP Server	–
Management IP Address	192.168.1.200
Management IP Subnet	255.255.255.0
Management IP Gateway	192.168.1.1
Mesh	Yes

✖	Controller DHCP

2	Wireless Network Settings

✔	Employee Network

Network Name	Employee
Security	WPA2 Personal
Passphrase:	••••••

Additional mesh configuration

Before establishing the mesh link, MAP needs to be converted to flex-bridge mode. The RAP will already be in flex-bridge mode if the mesh option has been enabled during initial config. This can be done from the CLI:

<#root>

MAP#

```
capwap ap mode flex-bridge
```

```
MAP#[*11/05/2019 18:26:28.1599] AP Rebooting: Reset Reason - AP mode changed
```

In order for MAP top join the ME controller, it needs to be authorized. On MAP, find the mac address of its ethernet interface:

<#root>

MAP#

show interfaces wired 0

wired0   Link encap:Ethernet HWaddr

00:EE:AB:83:D3:20

```
          inet addr:192.168.1.202  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:183 errors:0 dropped:11 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:80
          RX bytes:19362 (18.9 KiB)  TX bytes:22536 (22.0 KiB)
```

From laptop 1, access the ME controller web interface via https://192.168.1.200. After expert mode has been enabled (top right corner), a mesh tab will appear under Wireless settings. Under mac filtering, add the ethernet MAC address of the MAP:

Add MAC Address

MAC Address: 00:EE:AB:83:D3:20

Description: MAP ❓

Type: WhiteList ▼

Profile Name: Any WLAN/RLAN ▼

⊘ Apply   ⊗ Cancel

Note: Any subsequent AP in bridge or flex-bridge mode that is being joined to ME WLC needs to be authorized as well

After setting this up, a mesh link should be established. In order for wired client behind the MAP to pass the traffic over the mesh link, Ethernet Bridging needs to be enabled on the MAP under **Wireless Settings > Access Poins > MAP > Mesh**:

If the mesh link is using a 5GHz band, it can be affected by radar signatures. Once the RAP detects a radar event, it will switch to another channel. It is recommended to enable the Channel Change Notification so RAP notifies the MAP that the channel will be switched. This significantly lowers the convergence time as MAP does not have to scan all the available channels:

Verify

We can verify that the MAP has joined by running `show mesh ap summary` command:

```
<#root>

(Cisco Controller) >

show mesh ap summary


AP Name              AP Model             BVI MAC           CERT MAC          Hop  Bridge Group Name
-----------------    -------------------  ----------------  ----------------- ---  -----------------
RAP                  AIR-AP1542I-E-K9     00:fd:22:19:8c:f8  11:22:33:44:55:66 0   default
MAP                  AIR-AP1542D-E-K9     00:ee:ab:83:d3:20  11:22:33:44:55:66 1   default

Number of Mesh APs................................ 0
Number of RAPs................................... 0
Number of MAPs................................... 0
Number of Flex+Bridge APs....................... 2
Number of Flex+Bridge RAPs...................... 1
Number of Flex+Bridge MAPs...................... 1
```

In order to test if the link is passing through the traffic, we will try to ping from Laptop 1 to Laptop 2:

```
<#root>

VAPEROVI:~ vaperovi$

ping 192.168.1.101


PING192.168.1.101 (192.168.1.101): 56 data bytes
64 bytes from192.168.1.101: icmp_seq=0 ttl=64 time=5.461 ms
64 bytes from192.168.1.101: icmp_seq=1 ttl=64 time=3.136 ms
64 bytes from192.168.1.101: icmp_seq=2 ttl=64 time=2.875 ms
```

Note: You will be able to ping MAP or RAP ip address only once the mesh link has been established.

Troubleshooting

On the MAP/RAP:

- `debug mesh events`

On ME WLC:

- `debug capwap events enable`
- `debug capwap errors enable`
- `debug mesh events enable`

Example of a successful join process observed from MAP (some messages have been redacted as they are

not relevant):

<#root>

```
MAP#debug mesh events
Enabled all mesh event debugs

[*11/05/2019 18:28:24.5699] EVENT-MeshRadioBackhaul[1]: Sending SEEK_START to Channel Manager
[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]:
```

Starting regular seek

```
[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: channels to be seeked: 100
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[0]: start scanning on channel 1.
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[1]: start scanning on channel 100.
[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADD_LINK to MeshLink
[*11/05/2019 18:28:06.5699] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: AWPP adjacency added channel(100)
[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADJ_FOUND to Channel Manager 0x64
[*11/05/2019 18:28:06.5699] EVENT-MeshChannelMgr[1]: Adj found on channel 100.
[*11/05/2019 18:28:07.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:08.5499] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[0]: continue scanning on channel 2.
[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:09.0399] EVENT-MeshChannelMgr[1]: continue scanning on channel 104.
[*11/05/2019 18:28:09.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:10.7899] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:11.0199] EVENT-MeshChannelMgr[0]: continue scanning on channel 3.
[*11/05/2019 18:28:11.0399] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:11.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:11.3099] EVENT-MeshChannelMgr[1]: continue scanning on channel 108.
[*11/05/2019 18:28:13.0199] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:13.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:13.2499] EVENT-MeshChannelMgr[0]: continue scanning on channel 4.
[*11/05/2019 18:28:13.3099] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:13.5599] EVENT-MeshChannelMgr[1]: continue scanning on channel 112.
[*11/05/2019 18:28:15.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:15.2499] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:15.5099] EVENT-MeshChannelMgr[0]: continue scanning on channel 5.
[*11/05/2019 18:28:15.5599] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:15.8099] EVENT-MeshChannelMgr[1]: continue scanning on channel 116.
.
..
.
[*11/05/2019 18:28:35.7999] EVENT-MeshChannelMgr[1]: Mesh BH requests to switch to channel 100, width 20
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: abort scanning.
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: Set to configured channel 1, width 20 MHz
[*11/05/2019 18:28:36.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:37.5099] EVENT-MeshRadioBackhaul[1]: Sending LINK_UP to MeshLink
[*11/05/2019 18:28:37.5099] CRIT-MeshLink: Set Root port Mac: D4:78:9B:7B:DF:11 BH Id: 2 Port:54 Device
[*11/05/2019 18:28:37.5099] EVENT-MeshLink: Sending NOTIFY_SECURITY_LINK_UP to MeshSecurity
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Intermodule message NOTIFY_SECURITY_LINK_UP
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Start full auth to parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: start_auth, Parent(D4:78:9B:7B:DF:11) state changed to A
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: Opening wpas socket
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: start socket to WPA supplicant
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: MeshSecurity::wpas_init my_mac=00:EE:AB:83:D3:20, userna
[*11/05/2019 18:28:38.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6799] EVENT-MeshSecurity: Generating pmk r0 as child(D4:E8:80:A0:D0:B1)
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: pmk(eap) r0 generated for D4:78:9B:7B:DF:11: 5309c9fb 0
```

```
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: EAP authentication is done, Parent(D4:78:9B:7B:DF:11) s
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Child(D4:E8:80:A0:D0:B1) generating keys to Parent D4:7
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_AUTH_RSP, Parent(D4:78:9B:7B:DF:11) stat
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent D4:78:9B:
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mac: D4:78:9B:7B:DF:11 bh_id:2 auth_result: 1
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Sending NOTIFY_SECURITY_DONE to Control
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mesh Link:Security success on parent :D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Uplink Auth done: Mac: D4:78:9B:7B:DF:11 Port:54 Device:DEV
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_REASSOC_RSP, Parent(D4:78:9B:7B:DF:11)
```

state changed to STATE_RUN

```
[*11/05/2019 18:28:40.6899] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: auth_complete Result(PASS)
.
..
.
[*11/05/2019 18:28:45.6799] CAPWAP State: Discovery
[*11/05/2019 18:28:45.6799] Discovery Request sent to 192.168.1.200, discovery type STATIC_CONFIG(1)
[*11/05/2019 18:28:45.6899] Discovery Request sent to 192.168.1.200, discovery type STATIC_CONFIG(1)
[*11/05/2019 18:28:45.6899] Sent Discovery to mobility group member 1. 192.168.1.200, type 1.
[*11/05/2019 18:28:45.7099] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)
[*11/05/2019 18:28:46.9699] AP GW IP Address updated to 192.168.1.1
[*11/05/2019 18:28:47.3999] Flexconnect Switching to Standalone Mode!
[*11/05/2019 18:28:47.4599] EVENT-MeshLink: Sending NOTIFY_CAPWAP_COMPLETE to Control
[*11/05/2019 18:28:47.4599] EVENT-MeshControl: Capwap Complete Notification: bh:2 Result:2
[*11/05/2019 18:28:47.4599] EVENT-MeshControl: Received CAPWAP Disconnect for: bh_id(2), D4:78:9B:7B:DF
[*11/05/2019 18:28:47.4899]
```

Discovery Response from 192.168.1.200

```
.
..
.
Adding Ipv4 AP manager 192.168.1.200 to least load
[*11/05/2019 18:28:55.1299] WLC: ME ApMgr count 1, ipTransportTried 0, prefer-mode 1, isIpv4OrIpv6Stati
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load 1, AP
[*11/05/2019 18:28:55.1399] capwapSetTransportAddr returning: index 0, apMgrCount 0
[*11/05/2019 18:28:55.1399]
[*11/06/2019 13:23:36.0000]
[*11/06/2019 13:23:36.0000] CAPWAP State: DTLS Setup
[*11/06/2019 13:23:36.0000] DTLS connection created sucessfully local_ip: 192.168.1.202 local_port: 524
[*11/06/2019 13:23:36.8599] Dtls Session Established with the AC 192.168.1.200, port 5246
[*11/06/2019 13:23:36.8599]
[*11/06/2019 13:23:36.8599] CAPWAP State: Join
[*11/06/2019 13:23:36.8699] Sending Join request to 192.168.1.200 through port 5248
[*11/06/2019 13:23:36.8899] Join Response from 192.168.1.200
[*11/06/2019 13:23:36.8899] AC accepted join request with result code: 0
.
..
.
CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:37.4999] Starting Post Join timer
[*11/06/2019 13:23:37.4999]
[*11/06/2019 13:23:37.4999] CAPWAP State: Image Data
[*11/06/2019 13:23:37.5099] AP image version 8.10.105.0 backup 8.8.125.0, Controller 8.10.105.0
[*11/06/2019 13:23:37.5099] Version is the same, do not need update.
[*11/06/2019 13:23:37.6399] do NO_UPGRADE, part1 is active part
[*11/06/2019 13:23:37.6499]
[*11/06/2019 13:23:37.6499] CAPWAP State: Configure
[*11/06/2019 13:23:37.6599] DOT11_CFG[0] Radio Mode is changed from Remote Bridge to Remote Bridge
.
..
```

```
.
[*11/06/2019 13:23:38.7799] DOT11_CFG[0]: Starting radio 0
[*11/06/2019 13:23:38.7799] DOT11_CFG[1]: Starting radio 1
[*11/06/2019 13:23:38.8899] EVENT-MeshRadioBackhaul[0]: BH_RATE_AUTO
[*11/06/2019 13:23:38.8899] EVENT-MeshSecurity: Intermodule message LSC_MODE_CHANGE
[*11/06/2019 13:23:38.9099] CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:38.9999] Setting Prefer-mode IPv4
[*11/06/2019 13:23:39.0499]
[*11/06/2019 13:23:39.0499]
```

CAPWAP State: Run

```
[*11/06/2019 13:23:39.0499] EVENT-MeshCapwap: CAPWAP joined controller
[*11/06/2019 13:23:39.0599] CAPWAP moved to RUN state stopping post join timer
[*11/06/2019 13:23:39.1599] CAPWAP data tunnel ADD to forwarding SUCCEEDED
[*11/06/2019 13:23:39.2299]
```

AP has joined controller ME

```
[*11/06/2019 13:23:39.2599]
```

Flexconnect Switching to Connected Mode

```
!
```

Tips, tricks and common mistakes

- By upgrading the MAP and RAP to the same image version over the wire, we are avoiding image download going over the air (which can be problematic in "dirty" RF environments).
- Increasing the channel width of the 5GHz backhaul link can lead to lower SNR and false radar detections (mainly on 80MHz and 160 MHz).
- Mesh link connectivity should not be tested by pinging MAP or RAP. They will not be pingable once the mesh link comes up.
- It's highly recommended to test out the setup in a controlled environment before deploying it on site.
- If APs with external antennas are being used, make sure to consult the deployment guide to check which antennas are compatible and which port they should be plugged in.
- In order to bridge the traffic from different VLANs over the mesh link, VLAN Transparent feature needs to be disabled.
- Consider having a syslog server local to the APs, as it can provide debug information otherwise only available with a console connection.