Configure Point-to-Point Mesh Link with Ethernet Bridging on Embedded Wireless Controller with C9124 Access Points

Contents

Introduction Prerequisites Requirements Components Used **Background Information** Ethernet Bridging Embedded Wireless Controller on Catalyst Access Point **Configure** Network Diagram Configurations Switch Configurations EWC and RAP Configuration Configure MAP Verify Troubleshoot Useful commands Example 1: RAP receives adjacency from MAP and succeeds authentication Example 2: MAP Mac address not added to WLC or incorrectly added Example 3: RAP looses MAP Tips, Tricks and Recommendations References

Introduction

This document describes how to configure P2P Mesh Link with Ethernet Bridging on Embedded Wireless Controller (eWC) with C9124 Access Points.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800.
- Cisco Catalyst Access Points (APs).
- Embedded Wireless Controller on Catalyst Access Points.
- Mesh technology.

Components Used

The information in this document is based on these software and hardware versions:

- EWC IOS® XE 17.12.2.
- 2x APs C9124.
- 2x Power Injectors AIR-PWRINJ-60RGD1.
- 2x switches;
- 2x laptops;
- 1x AP C9115.

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.

Background Information

Ethernet Bridging

The mesh network solution, which is part of the Cisco unified wireless network solution, enables two or more Cisco Mesh Access Points (hereafter called mesh access points) to communicate with each other over one or more wireless hops to join multiple LANs or to extend WiFi coverage.

Cisco mesh access points are configured, monitored, and operated from and through any Cisco Wireless LAN controller that is deployed in the mesh networking solution.

Supported mesh networking solution deployments are of one of three general types:

- Point-to-point deployment
- Point-to-multipoint deployment
- Mesh deployment

This document focuses on how to configure point-to-point mesh deployment and Ethernet bridging on the same.

In point-to-point mesh deployment, the mesh access points provide wireless access and backhaul to wireless clients, and can simultaneously support bridging between one LAN and a termination to a remote Ethernet device or another Ethernet LAN.



Refer to<u>Mesh Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers</u>for detailed information on each of these deployment types.

The Cisco Catalyst 9124 Series outdoor mesh AP is a wireless device designed for wireless client access and point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity.

The outdoor access point is a standalone unit that can be mounted on a wall or overhang, on a rooftop pole, or on a street light pole.

You can operate the C9124 in one of these mesh roles:

- Roof-top Access Point (RAP)
- Mesh Access Point (MAP)

RAPs have a wired connection to a Cisco wireless LAN controller. They use the backhaul wireless interface to communicate with nearby MAPs. RAPs are the parent node to any bridging or mesh network and connect a bridge or mesh network to the wired network, so there can be only one RAP for any bridged or mesh network segment.

MAPs have no wired connection to a Cisco Wireless LAN controller. They can be completely wireless and support clients that communicate with other MAPs or RAPs, or they can be used to connect to peripheral devices or a wired network.

Embedded Wireless Controller on Catalyst Access Point

The Cisco Embedded Wireless Controller (EWC) on Catalyst Access Points is a software-based controller integrated into Cisco Catalyst 9100 Access Points.

In a Cisco EWC network, an Access Point (AP) that runs the wireless controller function is designated as the active AP.

The other access points, which are managed by this active AP, are referred to as subordinate APs.

The active EWC has two roles:

• It functions and operates as a Wireless LAN Controller (WLC) to manage and control the subordinate APs. The subordinate APs operate as lightweight access points to serve clients.

• It operates as an access point to serve clients.

To have a product overview about EWC on APs, please visit the <u>Cisco Embedded Wireless Controller on</u> <u>Catalyst Access Points Data Sheet</u>.

To know how to deploy EWC on your network please visit the <u>Cisco Embedded Wireless Controller on</u> <u>Catalyst Access Points (EWC) White Paper</u>.

This document focuses on C9124 as EWC and assumes there is already an AP 9124 in EWC mode.

Configure

Network Diagram

All the devices in this network are located inside the 192.168.100.0/24 subnet except the laptops that are in VLAN 101 with subnet 192.168.101.0/25.

The EWC AP (WLC) has its management interface untagged, and the native VLAN on switchports is set to VLAN 100.

AP AP9124_RAP has the role of a eWC and Root Access Point (RAP), while AP9124_MAP takes the role of Mesh Access Point (MAP).

In this lab an AP C9115 is also placed behind the MAP to show that we can have APs to join a WLC over a Mesh link.

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	Static on VLAN 100: 192.168.100.1
Laptop1	DHCP on VLAN 101
Laptop2	DHCP on VLAN 101
Switch1 (DHCP server)	VLAN 100 SVI: Static on VLAN 100: 192.168.100.1 (DHCP server)
Switch1 (DHCP server)	VLAN 101 SVI: Static on VLAN 101: 192.168.101.1 (DHCP server)
Switch2	VLAN 100 SVI: DHCP on VLAN 100
Switch2	VLAN 101 SVI: DHCP on VLAN 101
9124EWC	Static on VLAN 100: 192.168.100.40
AP9124_RAP	DHCP on VLAN 100
AP9124_MAP	DHCP on VLAN 100
AP9115	DHCP on VLAN 100



Network Diagram



Note: The C9124 APs are powered using AIR-PWRINJ-60RGD1 with the guidelines in the <u>Cisco</u> <u>Catalyst 9124AX Series Outdoor Access Point Hardware Installation Guide</u>.

Configurations

This document assumes there is already an AP 9124 running EWC with initial deployment done as per <u>Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) White Paper</u>.

For other Tips and Tricks regarding conversion process the please check the <u>Convert Catalyst 9100 Access</u> <u>Points to Embedded Wireless Controller</u> document.

Switch Configurations

Here are the switches relevant configurations.

Switch ports where APs are connected are in trunk mode with the native VLAN set to 100 and allowing VLAN 101.

During staging of the APs, you need to configure the MAP as MAP, therefore you need to make the AP join

the eWC via ethernet. Here we use Switch1 port G1/0/2 for staging the MAP. After staging the MAP is moved to Switch2.

Switchports where laptops are connected are configured as access ports on VLAN 101.

Switch1:

```
ip dhcp excluded-address 192.168.101.1 192.168.101.10
ip dhcp excluded-address 192.168.100.1 192.168.100.10
I
ip dhcp pool AP_VLAN100
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 192.168.1.254
1
ip dhcp pool VLAN101
network 192.168.101.0 255.255.255.0
default-router 192.168.101.1
dns-server 192.168.1.254
interface GigabitEthernet1/0/1
 description AP9124_RAP (EWC)
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 end
interface GigabitEthernet1/0/2
 description AP9124_MAP_Staging
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 end
interface GigabitEthernet1/0/8
 description laptop1
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
 end
Switch2:
interface GigabitEthernet0/1
 description AP9124_MAP
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet0/8
 description laptop2
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end
interface GigabitEthernet0/1
 description AP9115
 switchport trunk native vlan 100
```

switchport trunk allowed vlan 100,101 switchport mode trunk end

EWC and RAP Configuration

After Day0 configuration of the EWC AP, the embedded AP needs to joins itself.

1. Add the Ethernet mac addresses of Root AP and Mesh AP to Device Authentication. Go to **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Device Authentication**, click button +**Add:**

Q. Search Menu Items	Configuration * > Security * > A	AA								
Dashboard	+ AAA Wizard									
Monitoring ,	Servers / Groups AAA Method	List AAA A	dvanced							
	Global Config	MAC Addres	ss Serial Number							
Administration	RADIUS Fallback	+ Add	× Delete		P> Select	File		① Luplo	ad File	
C Licensing	Device Authentication		MAC Address	۲	Attribute List Name	т	Description	T	WLAN Profile	Ŧ
X Troubleshooting	AP Policy	0	3c5731c5ac2c 3c5731c5a9f8		None		MeshAP-RootAP MeshAP-MAP			
	Password Policy	H A	1 > > 10 -							1 - 2 of 2 items
	AAA Interface									

MAC Addresses in Device Authentication

CLI commands:

```
9124EWC(config)#username 3c5731c5ac2c mac description MeshAP-RootAP
9124EWC(config)#username 3c5731c5a9f8 mac description MeshAP-MAP
```

The Ethernet mac address can be confirmed by running the "show controllers wired 0" from the AP CLI. Example from root AP:

```
AP3C57.31C5.AC2C#show controllers wired 0
wired0 Link encap:Ethernet HWaddr 3C:57:31:C5:AC:2C
```

Access to the underlying AP shell can be completed with the command "wireless ewc-ap ap shell username x" as exemplified:

9124EWC#wireless ewc-ap ap shell username admin [...] admin@192.168.255.253's password: AP3C57.31C5.AC2C>en Password: AP3C57.31C5.AC2C# AP3C57.31C5.AC2C#logout Connection to 192.168.255.253 closed.



Note: This command is equivalent to *apciscoshell* that was previously available in Mobility Express controllers.

If the AP management username and password are not specified in the AP profile, use the default username **Cisco** and password **Cisco** instead.

2. Add Authentication and Authorization Methods:

Q Search Menu Items	Configuration * > Security * >	AAA		
Dashboard	+ AAA Wizard			
	Servers / Groups AAA Meth	od List AAA Advanced Quick Setup: AAA Authent	ication	×
	Authentication	Method List Name*	MESH Authentication	
	Authorization	Type*	dot1x V	- 1
C Licensing	Accounting	Group Type	local 🔹	- 1
X Troubleshooting		Available Server Groups	Assigned Server Groups	
		radius A Idap tacacs+		
		-	· · · ·	
		Cancel	🗎 Apply to	o Device

Authentication Method List

Q Search Menu Items	Configuration * > Security * > A	AA		
📷 Dashboard	+ AAA Wizard			
Monitoring >	Servers / Groups AAA Method	Quick Setup: AAA Authoria	zation	×
	Authentication	Method List Name*	MESH_Authorization	
	Authorization	Туре*	credential-download 🗸 🧃	
	Accounting	Group Type	local 🔻 🛈	32
		Authenticated	0	
X Troubleshooting		Available Server Groups	Assigned Server Groups	
		radius Idap		~
		lacacs*	< >	<u>^</u>
			~ « ·	¥.
		Cancel		Apply to Device

Authorization Method List

CLI commands:

```
9124EWC(config)#aaa authentication dot1x MESH_Authentication local
9124EWC(config)#aaa authorization credential-download MESH_Authorization local
```

3. Go to **Configuration** > **Wireless** > **Mesh**. As the setup in this document requires Ethernet bridging, enable **Ethernet Bridging Allow BPDUs**:

Q. Search Menu Items	Configuration * > Wireless * > Mesh					
Dashboard	Global Config Profiles					
Monitoring >	General			Alarm		🖹 Apply
Configuration	Ethernet Bridging Allow BPDU	Ø	,	Max Hop Count	4	
Administration	Subset Channel Sync Backhaul	U		Recommended Max Children for MAP	10	
C Licensing	Extended UNII B Domain Channels	D	F	Recommended Max Children for RAP Parent Change Count	3	
	RRM Auto-DCA	0	L	Low Link SNR (dB)	12	
	Security		,	High Link SNR (dB)	60	
Walk Me Through >	PSK Provisioning	o		Association Count	10	
	Default PSK	0				

Ethernet Bridging Allow BPDU

CLI commands:

9124EWC(config)#wireless mesh ethernet-bridging allow-bdpu



Note: By default, the mesh APs are not forwarding BPDUs over the mesh link.

If you do not have any redundant link between the 2 sites, then it is not needed.

If there are redundant links then you need to allow BPDUs. If this is not done, you risk creating a STP loop in the network.

4. Configure the **default-mesh-profile** where you select the previously configured AAA Authentication and Authorization methods. **Click** and edit the **default-mesh-profile**.

Go to the **Advanced** tab and select the **Authentication** and **Authorization** methods. Enable option **Ethernet Bridging**.

Q. Search Menu Items	Configuration * > Wireless * > Mesh	Edit Mesh Profile			×
Dashboard	Global Config Profiles + Add × Delete	Changes in the configuration for Se save and reload for the cha	curity Mode, BGN, Client-Access, and Range inges to take effect. Controller can be reloaded	will reload associated APs, except d from 'Administration -> Managen	Primary AP. Primary AP requires controller to nent -> Backup & Restore -> Reload'
Configuration	Number of Profiles : 1 Name T Bridge Group Name	General Advanced		5 GHz Band Backhaul	
Administration	default-mesh-profile	Security	EAP	Rate Types	auto 💌
C Licensing		Authentication Method	MESH_Authentica	2.4 GHz Band Backhaul	
		Authorization Method Ethernet Bridging	MESH_Authorizati 👻 💈	Rate Types Fast Roaming	auto
Waik Me Through >		VLAN Transparent		Fast Teardown	0
		Bridge Group			
		Bridge Group Name	Enter Name		
		Strict Match	0		
		"D Cancel			Update & Apply to Device

Edit default-mesh-profile

CLI commands:

```
9124EWC(config)#wireless profile mesh default-mesh-profile
9124EWC(config-wireless-mesh-profile)#description "default mesh profile"
9124EWC(config-wireless-mesh-profile)#ethernet-bridging
9124EWC(config-wireless-mesh-profile)#ethernet-vlan-transparent
9124EWC(config-wireless-mesh-profile)#method authentication MESH_Authentication
9124EWC(config-wireless-mesh-profile)#method authorization MESH_Authorization
```

Special callout to the option VLAN Transparent:

This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic:

- If VLAN Transparent is enabled, then VLAN tags are not handled and packets are bridged as untagged packets.
 - No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames.
- If VLAN Transparent is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access, or normal mode).
 - If the Ethernet port is set to Trunk mode, then Ethernet VLAN tagging must be configured.



Tip: To use AP VLAN tagging, you must uncheck the VLAN Transparent check box.

If you do not use VLAN tagging, it means the RAP and MAP are on Native VLAN configured on the Trunk ports. In this condition, if you want other devices behind MAP to be on the Native VLAN (here VLAN 100), then you need to enable VLAN Transparent.

5. The internal AP joins the EWC and you can verify the AP join state using the command "show ap summary":

9124EWC#show ap summary Number of APs: 1						
CC = Country Code RD = Regulatory Domain						
AP Name	Slots AP Model	Ethernet MAC Radio MAC	CC RD	IP Address	State	Location
AP3C57.31C5.AC2C	2 C9124AXI-B	3c57.31c5.ac2c 4ca6.4d23.ae	e0 US - B	192.168.100.11	Registered	default location

show ap summary

You can also see the AP joined via the GUI where the AP show up as Flex+Bridge mode. For convenience you can change the name of the AP now. In this setup it is used the name AP9124_RAP:

Q Search Menu Items	Configuration * > Wireless * > Access P	Points	Edit AP		×
Dashboard	 All Access Points 		General Interfaces Inventory Geolocatio	n Mesh Advanced	_î
			General	Tags	
(Monitoring		Current Active	AP Name* AP3C57.31C5.AC2C	Policy default-policy-tag 👻	2
Configuration		AP3057.3105.AD20	Location* default location	Site default-site-tag 👻	2
(c) Administration			Base Radio MAC 4ca6.4d23.aee0	RF default-rf-tag 🔹	2
C Licensing	Total APs : 1	Admin 1	Ethernet MAC 3c57.31c5.ac2c	Write Tag Config to AP	- 1
Y Troubleshooting	: AP Model : S	Slots : Status Up Time	Admin Status	Version	
64	1C5.AC2C 🔥 🕍 C9124AXI-B	2 O days 1 h mins 37 sec	AP Mode Flex+Bridge +	Primary Software Version 17.12.2.35	- I
	H 4 1 ⊨ H 10 ¥		Operation Status Registered	Predownloaded Status None	

AP General details

You can edit the **Geolocation** and then in the **Mesh** tab, make sure its **Role** is configured as **Root** AP and the **Ethernet Port Configuration** is set to **trunk** with corresponding VLAN IDs:

Q. Search Menu Items	Configuration * > Wireless * > Access Points	Edit AP			×	
Dashboard	 All Access Points 		General Interfaces Inventory Geolocation General		ion Mesh Advanced Ethernet Port Configuration	i
Monitoring > Image: Configuration >		Current Active	Block Child Daisy Chaining	0	• Ethernet Bridging on the ass to configure this section succes	oclated Mesh Profile should be enabled shully
 Administration Licensing 	Total APs : 1	Admin 1	Daisy Chaining strict- RAP Preferred Parent MAC	0000.0000.0000	Port Mode	0 v normal v
Y Troubleshooting	I AP Model I Slots	Status Up Time O days 1 h mins 37 sed	Role	Root		
Walk Me Through 5			Remove PSK	ÎII.		
	5 GHz Radios		Backhaul			
	> 2.4 GHz Radios		Radio Type and Slot AP	can be changed only for a Root		
	> Dual-Band Radios		Backhaul Radio Type	5ghz 🔻		
	> Country		Backhaul Slot ID	1		
	> LSC Provision		Rate Types	auto		
	> AP Certificate Policy		Uncel			Update & Apply to Device

Mesh Role Root

Edit AP						×
General Interfaces	Inventory	Geolocation	Mesh	Advanced		Â
General			Ethernet P	Port Configuration		
Block Child			 Ethern to config 	et Bridging on the asso ure this section success	ciated Mesh Profile sh fully	ould be enabled
Daisy Chaining Daisy Chaining strict- RAP	0		Port		0	•
Preferred Parent MAC	0000.0000.0000		Mode		trunk	▼
Role	Root	•	Native VI	_AN ID*	100	
			Allowed	VLAN IDs	101	(
Remove PSK	圓					
Backhaul						
Radio Type and Slot of AP	can be changed only fo	or a Root				
Backhaul Radio Type	5ghz	•				
Backhaul Slot ID	1	•				ľ
Rate Types	auto	•				•
Cancel					📑 Upda	te & Apply to Device

Ethernet Port Configuration

Configure MAP

It is now time to join the 9124 MAP.

1. Connect the MAP AP to the Switch1 for staging. The AP joins the EWC and shows in the AP list. Change its name to something like AP9124_MAP and configure it as **Mesh Role** in the **Mesh** tab. Click **Update & Apply to Device**:

Q. Search Menu Items	Configuration * > Wireless * > Access F	Points	Edit AP				×
Dashboard	 All Access Points 		General Interfaces	Inventory	Geolocation	Mesh Advanced Ethernet Port Configuration	
Monitoring > Configuration >		Current Active	Block Child Daisy Chaining	0		• Ethernet Bridging on the asso to configure this section succes	ociated Mesh Profile should be enabled shully
Administration	Total APs : 2		Daisy Chaining strict- RAP		_	Port Mode	0 v
Troubleshooting	AP Name : AP Model	i Slots i Status	Preferred Parent MAC	Mesh	•	Native VLAN ID*	100
	AP9124_RAP ▲ ▲ C9124AXI-B	2	Remove PSK	<u>ا</u>		NORG (DATIO	
			Backhaul				
	> 5 GHz Radios		Backhaul Radio Type	Sghz	Ŧ		
	> 2.4 GHz Radios		Backhaul Slot ID	1	v		
	> Dual-Band Radios		Rate Types	auto	•		
	> Country						
	> LSC Provision		Cancel				Update & Apply to Device

MAP configuration

2. Disconnect the AP from Switch1 and connect to Switch2 as per the Network Diagram. The MAP joins the EWC via wireless interface through the RAP.



Note: As the APs are powered via power injector, the AP does not go down, and as the setup is in a controlled environment, the Switch2 is physically close and we can simply move the cable from one switch to the other.

You can connect a console cable to the AP and see what happens via console. Here are some important messages seen.



Note: From release 17.12.1, the default console baud rate of the 802.11AX APs is changed from 9600 bps to 115200 bps.

MAP looses connectivity to EWC:

AP9124_MAP#

[*01/11/2024	14:08:23.0214]	chatter: Device wiredO notify state change link DO
[*01/11/2024	14:08:28.1474]	Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=83,
[*01/11/2024	14:08:28.1474]	
[*01/11/2024	14:08:31.1485]	Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=83, N
[*01/11/2024	14:08:31.1486]	
[*01/11/2024	14:08:33.4214]	chatter: Device wiredO notify state change link U
[*01/11/2024	14:08:34.1495]	Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=83, Na
[*01/11/2024	14:08:34.1495]	
L*01/11/2024	14:08:37.1505	Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=84, 1
L*01/11/2024	14:08:37.1505	
[*01/11/2024	14:08:40.1515	Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=84, 1
[*01/11/2024	14:08:40.1515	
[*01/11/2024	14:08:43.1524]	Max retransmission count exceeded, going back to l

[]		
[*01/11/2024 14:0	8:48.1537] C	RIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Blocklis
[*01/11/2024 14:0	8:48.1538] C	RIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Remove as
[*01/11/2024 14:0	8:48.1539] C	RIT-MeshLink: Link Down Block Root port Mac: 3C:!
[*01/11/2024 14:0	8:48.1542] C	RIT-MeshWiredBackhaul[0]: Remove as uplink

MAP moves to discovery mode via wireless and finds the RAP via Radio Backhaul on channel 36, finds EWC and joins it:

[*01/11/2024 14:08:51.3893] CRIT-MeshRadioBackhaul[1]: Set as uplink [*01/11/2024 14:08:51.3894] CRIT-MeshAwppAdj[1][4C:A6:4D:23:AE:F1]: Set as Pa [*01/11/2024 14:08:51.3915] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (mon0) [*01/11/2024 14:08:51.3926] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (apbh [*01/11/2024 14:08:51.4045] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (apbhr0) [*01/11/2024 14:08:51.4053] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (mon0) CRIT-MeshLink: Set Root port Mac: 4C:A6:4D:23:AE: [*01/11/2024 14:08:53.3898] [*01/11/2024 14:08:53.3904] Mesh Reconfiguring DHCP. [*01/11/2024 14:08:53.8680] DOT11_UPLINK_EV: wgb_uplink_set_port_authorized: ([*01/11/2024 14:08:53.9232] CRIT-MeshSecurity: Mesh Security successful authe [...] [*01/11/2024 14:09:48.4388] Discovery Response from 192.168.100.40 [*01/11/2024 14:09:59.0000] Started wait dtls timer (60 sec) [*01/11/2024 14:09:59.0106] CAPWAP State: DTLS Setup [*01/11/2024 14:09:59.0106] [*01/11/2024 14:09:59.0987] dtls_verify_server_cert: Controller certificate vertificate vertif [*01/11/2024 14:09:59.8466] [*01/11/2024 14:09:59.8466] CAPWAP State: Join [*01/11/2024 14:09:59.8769] Sending Join request to 192.168.100.40 through por [*01/11/2024 14:10:04.7842] Sending Join request to 192.168.100.40 through por [*01/11/2024 14:10:04.7953] Join Response from 192.168.100.40, packet size 139 [...] [*01/11/2024 14:10:06.6919] CAPWAP State: Run [*01/11/2024 14:10:06.8506] AP has joined controller 9124EWC [*01/11/2024 14:10:06.8848] Flexconnect Switching to Connected Mode! [...]

MAP is now joined to EWC via RAP.

AP C9115 can now get an IP address on VLAN 100 and then join the EWC:



Warning: Keep in mind that VLAN 100 is the switchports trunk Native VLAN. In order for the traffic from the AP on VLAN 100 to reach the WLC on VLAN 100, the mesh link must have **VLAN Transparent enabled**. This is done in the mesh profile Ethernet Bridging section.

```
[*01/19/2024 11:40:55.0710] ethernet_port wired0, ip 192.168.100.14, netmask 2
[*01/19/2024 11:40:58.2070]
[*01/19/2024 11:40:58.2070] CAPWAP State: Init
[*01/19/2024 11:40:58.2150]
[*01/19/2024 11:40:58.2150] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2400] Discovery Request sent to 192.168.100.40, discover
[*01/19/2024 11:40:58.2530]
                                                                                              Discovery Request sent to 255.255.255.255, discovery
[*01/19/2024 11:40:58.2600]
[*01/19/2024 11:40:58.2600] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2670] Discovery Response from 192.168.100.40
[*01/19/2024 11:40:58.2670] Found Configured MWAR '9124EWC' (respIdx 1).
[*01/19/2024 15:13:56.0000] Started wait dtls timer (60 sec)
[*01/19/2024 15:13:56.0070]
[*01/19/2024 15:13:56.0070] CAPWAP State: DTLS Setup
L...]
[*01/19/2024 15:13:56.1660] dtls_verify_server_cert: Controller certificate vertificate ve
```

[*01/19/2024	15:13:56.9000]	<pre>sudi99_request_check_and_load: Use HARSA SUDI cert</pre>
[*01/19/2024	15:13:57.2980	·
[*01/19/2024	15:13:57.2980	CAPWAP State: Join
[*01/19/2024	15:13:57.3170]	shared_setenv PART_BOOTCNT 0 &> /dev/null
[*01/19/2024	15:13:57.8620]	Sending Join request to 192.168.100.40 through por
[*01/19/2024	15:14:02.8070]	Sending Join request to 192.168.100.40 through por
[*01/19/2024	15:14:02.8200]	Join Response from 192.168.100.40, packet size 139
[*01/19/2024	15:14:02.8200]	AC accepted previous sent request with result code
[*01/19/2024	15:14:03.3700]	Received wlcType 2, timer 30
[*01/19/2024	15:14:03.4440]	
[*01/19/2024	15:14:03.4440]	CAPWAP State: Image Data
[*01/19/2024	15:14:03.4440]	AP image version 17.12.2.35 backup 17.9.4.27, Cont
[*01/19/2024	15:14:03.4440]	Version is the same, do not need update.
[*01/19/2024	15:14:03.4880]	status 'upgrade.sh: Script called with args:[NO_UI
[*01/19/2024	15:14:03.5330]	do NO_UPGRADE, part2 is active part
[*01/19/2024	15:14:03.5520]	
[*01/19/2024	15:14:03.5520]	CAPWAP State: Configure
[*01/19/2024	15:14:03.5600]	Telnet is not supported by AP, should not encode
[*01/19/2024	15:14:03.6880]	Radio [1] Administrative state DISABLED change to
L*01/19/2024	15:14:03.6890	Radio [0] Administrative state DISABLED change to
L*01/19/2024	15:14:03.8670	
[*01/19/2024	15:14:03.86/0]	CAPWAP State: Run
[*01/19/2024]	15:14:03.9290]	AP has joined controller 9124EWC
[*01/19/2024	15:14:03.9310]	Flexconnect Switching to Connected Mode!

As this is an EWC AP, it contains only the AP image that corresponds to its own model (here a C9124 runs ap1g6a). When you join a different model of AP you have a Non-Homogeneous network.

In these conditions, if the AP is not on the same version, it needs to download the same version, therefore make sure you have a valid TFTP/SFTP server and location, with the AP images, configured in the EWC > Administration > Software Management:

Ci	CiscoSWImages > Images > 9800 > C9800-AP-universalk9.17.12.02								
	↑↓ Sort ~ \equiv View ~								
	Name Name	Date modified	Туре	Size					
1	\sim A long time ago								
	controller_version.info	11/14/2023 2:11 PM	INFO File	1 KB					
	📑 readme.txt	11/14/2023 2:11 PM	Notepad++ Docu	1 KB					
	C9800-AP-iosxe-wlc.bin	11/14/2023 2:11 PM	BIN File	303,222 KB					
2	🔲 📄 version.info	11/14/2023 1:51 PM	INFO File	1 KB					
	ap1g8 Type: INFO File	11/14/2023 1:51 PM	File	67,010 KB					
	ap3g3 Size: 11 bytes Date modified: 11	11/14/2023 1:51 PM	File	55,880 KB					
	ap1g6	11/14/2023 1:51 PM	File	67,840 KB					
	ap1g6a	11/14/2023 1:51 PM	File	84,200 KB					
1	ap1g7	11/14/2023 1:51 PM	File	73,400 KB					
	ap194	11/14/2023 1:51 PM	File	38,720 KB					
	ap1g5	11/14/2023 1:51 PM	File	36,640 KB					

TFTP server with AP images folder

Cisco Em	Welcome admin 🛛 🐐 家 🎤 🖺 🌣		
Q. Search Menu Items	Administration > Software Ma	anagement	
Dashboard	Software Upgrade	Wireless network is Non-Homogeneous. De Mode	sktop (HTTP) mode is not supported.
Monitoring ,		Image Server*	192.168.100.16
🗞 Configuration		Image Path*)-AP-universak9.17.12.02
Administration >		Parallel Mode	DISABLED (
C Licensing		Save	Save & Download Activate Cancel
		A.A	

AP Images

The AP shows in the AP list and you can assign a PolicyTag:

Cisco Embedded Wireless Controller on Catalyst Access Points Welcome admin 🐇 🕫 🖉 🖺 🏟 🔞 🥹 🕄 Search Affe and Clients 🔍													
Q. Search Menu Items	Configuration * > Wirele	Access Pol	ints	Edit AP									
				General Interfaces	General Interfaces Inventory Geolocation ICap Advanced								
ashboard	 All Access Point 	5		General		Tags							
Monitoring >			Current Active	AP Name*	AP9115	Policy	LocalSWTag 👻 💈						
Configuration			AP9124_RAP	Location*	default location	Site	default-site-tag 🗸						
(O) Administration				Base Radio MAC	1cd1.e079.66e0	RF	default-rf-tag 🗸						
C Licensing	Total APs : 3			Ethernet MAC	84f1.47b3.2cdc	Write Tag Config to AP	0						
	AP Name	AP Model	Slots : Status Up	ime Admin Status		Version							
See House and they	AP9115 da	C9115AXE-B	2 🔮 0 da min	36 secs AP Mode	Flex	Primary Software Version	17.12.2.35						
	AP9124_MAP	C9124AXI-B	2 S 8 di min	37 secs operation Status	Registered	Predownloaded Status	Predownloading						
	AP9124_RAP 4	C9124AXI-B	2 🔮 min	40 secs Fabric Status	Disabled	Predownloaded Version	0.0.0.0						
wate the unrough y	B − 6 1 F − 8	10 👻		CleanAir NSI Key		Next Retry Time	0						
				LED Settings		Boot Version	1.1.2.4						
	5 GHz Radios			LED State	ENABLED	INC Marrian	17 10 0 05						





AP Operational View

Verify

You can see the mesh tree via GUI which also gives the output from CLI if you use the command "*show wireless mesh ap tree*". On the GUI go to **Monitoring** > **Wireless** > **Mesh:**

Q. Search Menu Items	Monitoring * > Wireless * > Mesh							
📷 Dashboard	AP Convergence							
Monitoring >	Global Stats							
	Number of Bridge APs	0	Number of Flex+Bridge APs	2				
Configuration	Number of RAPs	0	Number of Flex+Bridge RAPs	1				
	Number of MAPs	0	Number of Flex+Bridge MAPs	1				
(C) Administration ,	Tree							
C Licensing								
Wilk Me Through	AP Name (Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Utll,Clients) [Sector 1]							



On the RAP and MAP you can verify the mesh backhaul using the command "show mesh backhaul":

```
AP9124_RAP#show mesh backhaul
Wired Backhaul: 0 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
0 16 TRUE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16
                       0
                                  T/F: T F T T F T Filtered
Wired Backhaul: 1 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
1 Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16 0
                                  T/F: F F F F F F F Filtered
_____
Radio Backhaul: 0 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
2 INITIAL ACCESS UP
                      Invalid FALSE FALSE TRUE FALSE FALSE ALLOWED
                                                                                RADIO
No Radio Adjacency Exists
                                   -----
Radio Backhaul: 1 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
3 MAINT DOWNLINK UP Invalid FALSE TRUE FALSE FALSE TRUE
                                                               ALLOWED
                                                                                RADIO
Mesh AWPP Radio adjacency info
Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W),
     BlockListed(B), Authenticated(A), HTCapable(H), VHTCapable(V)
     OldParent(O), BGScan(S)
Address
             Cost RawCost LinkCost ReportedCost Snr BCount Ch Width Bgn Flags: P O C N R W B A H V S Reject reason
4C:A6:4D:23:9D:51 Invalid Invalid 0 0 76 0 36 20 MHz - (T/F): F F T F T F T F T F T F T
_____
```

RAP show mesh backhaul

AP9124_MAP#show mesh backhaul Wired Backhaul: 0 [3C:57:31:C5:A9:F8] idx Cost Uplink InterfaceType 0 Invalid FALSE WIRED Mesh Wired Adjacency Info Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A) Address Cost RawCost BlistCount Flags: P C R W B A Reject reason T/F: F F T F T T Blocklisted: GW UNREACHABLE 3C:57:31:C5:A9:F8 16 16 32 Wired Backhaul: 1 [3C:57:31:C5:A9:F8] idx Cost Uplink InterfaceType 1 Invalid FALSE WIRED Mesh Wired Adjacency Info Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A) Address Cost RawCost BlistCount Flags: P C R W B A Reject reason 3C:57:31:C5:A9:F8 16 16 0 T/F: F F F F F F F Filtered Radio Backhaul: 0 [4C:A6:4D:23:9D:51] idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType 2 INITIAL ACCESS UP Invalid FALSE FALSE TRUE FALSE FALSE ALLOWED RADIO No Radio Adjacency Exists Radio Backhaul: 1 [4C:A6:4D:23:9D:51] Hops to Root: 1 idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType 3 MAINT UPLINK UP 217 TRUE TRUE FALSE FALSE TRUE ALLOWED RADIO Mesh AWPP Radio adjacency info Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W), BlockListed(B), Authenticated(A), HTCapable(H), VHTCapable(V) OldParent(0), BGScan(S) Cost RawCost LinkCost ReportedCost Snr BCount Ch Width Bgn Flags: P O C N R W B A H V S Reject reason Address 4C:A6:4D:23:AE:F1 217 272 256 16 70 0 36 20 MHz - (T/F): T F F T T T F T T T F -AP9124_MAP#!

MAP show mesh backhaul

You can verify Mesh VLAN Trunking configuration on the AP side:

AP9124_RAP#show mesh ethernet vlan config static Static (Stored) ethernet VLAN Configuration

Ethernet Interface: 0 Interface Mode: TRUNK Native Vlan: 100 Allowed Vlan: 101,

Ethernet Interface: 1 Interface Mode: ACCESS Native Vlan: 0 Allowed Vlan: Ethernet Interface: 2 Interface Mode: ACCESS Native Vlan: 0 Allowed Vlan:

Laptop2 connected on Switch2 received IP address from VLAN 101:

C:\	Users	s∖lu	ke≻i	pcon	fi	g									
Wir	ndows	IP	Conf	igur	at	ic	n								
Eti	hernet	: ad	apte	r us	b_	_xł	ıci	i :							
	Conne	ecti	.on-s	peci	fi	c	DN	IS	St	Jft	Fi>	٢.			
	IPv4	Add	lress	• •	•		•	•		•	•	•	•		192.168.101.12
	Subne	et M	lask	• •		•		•			•			-	255.255.255.0
	Defau	ult	Gate	way						٠		•	•	-	192.168.101.1

The Laptop1 placed on Switch1 received an IP from VLAN 101:

Ethernet adapter Ethernet 6_White:

Connection-specific DNS	Suffix . :	
Link-local IPv6 Address	: f	e80::d1d6:f607:ff02:4217%18
IPv4 Address	: 1	.92.168.101.13
Subnet Mask	: 2	55.255.255.0
Default Gateway	: 1	.92.168.101.1

C:\Users\tantunes>ping 192.168.101.12 -i 192.168.101.13

Pinging 192.168.101.12 with 32 bytes of data: Reply from 192.168.101.12: bytes=32 time=5ms TTL=128 Reply from 192.168.101.12: bytes=32 time=5ms TTL=128 Reply from 192.168.101.12: bytes=32 time=7ms TTL=128 Reply from 192.168.101.12: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.101.12: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 5ms, Maximum = 7ms, Average = 5ms



Note: Please note that to test ICMP between Windows devices you need to allow ICMP on the system firewall. By default Windows devices block ICMP in the system firewall.

Another simple test to verify Ethernet bridging is having SVI for VLAN 101 on both switches and setting Switch2 SVI to DHCP. Switch2 SVI for VLAN 101 gets IP from VLAN 101 and you can ping Switch 1 VLAN 101 SVI for vlan 101 connectivity check:

<#root>

Switch2#show ip int br Interface IP-Address OK? Method Status Protocol Vlan1 unassigned YES NVRAM up down Vlan100 192.168.100.61 YES DHCP up up

Vlan101 192.168.101.11 YES DHCP up up

GigabitEthernetO/1 unassigned YES unset up up [...]

Switch2# Switch2#ping 192.168.101.1 source 192.168.101.11 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.101.1, timeout is 2 seconds: Packet sent with a source address of 192.168.101.11 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms Switch2# <#root> Switch1#sh ip int br Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.11 YES NVRAM up up Vlan100 192.168.100.1 YES NVRAM up up Vlan101 192.168.101.1 YES NVRAM up up GigabitEthernet1/0/1 unassigned YES unset up up [...] Switch1#ping 192.168.101.11 source 192.168.101.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.101.11, timeout is 2 seconds: Packet sent with a source address of 192.168.101.1 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

Local mode AP C9115 also joined the EWC:

Q Search Menu Items	Configuration * > Wireless * > Access Points															
Dashboard		✓ All Access Points														
	•	>					Current Active				Current S	Preferred Active				
Configuration	>	>					AP9	124_RAP			Not Appl	AP9124_RAP				
O Administration	dministration >															
C Licensing		Iotal APs : 3						Admin								
		AP Name	:	AP Model	÷	Slots	÷	Status	Up Tim	e :	IP Address	Base Radio MAC	:	Ethernet MAC	÷	AP Mode
Troubleshooting		AP9115	<u>а</u> .[4]	C9115AXE-B		2		۲	0 days mins 30	0 hrs 35) secs	192.168.100.14	1cd1.e079.66e0		84f1.47b3.2cdc		Flex
		AP9124_MAP	A 141	C9124AXI-B		2		0	0 days mins 59	0 hrs 52 secs	192.168.100.12	4ca6.4d23.9d40		3c57.31c5.a9f8		Flex+Bridge
		AP9124_RAP	山田	C9124AXI-B		2		٢	0 days mins 57	2 hrs 46 7 secs	192.168.100.11	4ca6.4d23.aee0		3c57.31c5.ac2c		Flex+Bridge

AP 9115 Joined to the EWC

Switch1#

Created 3 WLANs, open, PSK and dot1x mapped to a Policy Profile with VLAN 101 defined in the Access Policies:



AP9115 Operational Configuration

Wireless clients are able to connect to the WLANs:

Q Search Merci term	Monitoring * > Wineless * > Clients														
Deshboard	Deshcoard Clents Seeping Clents Excluded Clents														
Monitoring	- 20	Colored C													
R Configuration	Select	ed 0 out of 2 Clerits													
Administration ,	0	Client MRC Address	T	Pet T Address	Pv6 Address	AP Name	T	908 D	T	550 7	WLAN D	۲	Client Type	T	State 7
A	0	9294.4038-0572	¢	192,168,101,14	No.0010004.007.Notaci572	APR/16		1		0,040	4		W,AN		Ren -
C Looning	0	aeex3434216c	¢	192,168,101,15	MdD:acce:3483634(216)	AP9015		1		PSK, III, Ab	5		96,499		ha .

Troubleshoot

In this section, useful commands and some tips, tricks and recommendations are presented.

Useful commands

On RAP/MAP:

AP9124_RAP#show mesh	
adjacency	MESH Adjacency
backhaul	MESH backhaul
bgscan	MESH Background Scanning
channel	MESH channels
client-debug-filter	MESH client debugging filter set
config	MESH config paramenter
convergence	MESH convergence info
dfs	MESH dfs information
dhcp	Flex-mesh Internal DHCP Server
ethernet	show mesh ethernet bridging
forwarding	MESH Forwarding
history	MESH history of events
least-congested-scan	Mesh least congested channel scan
linktest	MESH linktest stats
nat	Flex-mesh NAT/PAT
res	MESH RES info
security	MESH Security Show
stats	MESH stats
status	MESH status
stp	MESH daisychain STP info
timers	MESH Adjacency timers

show mesh

AP9124_RAP#debug	mesh
adjacency	MESH adjacency debugs
ap-link	MESH link debugs
bg-scan	Mesh background scanning debugs
channel	MESH channel debugs
clear	RESET all MESH debugs
client	Debug mesh clients
convergence	MESH convergence debugs
dhcp	MESH Internal DHCP debugs
dump-pkts	Dump mesh packets
events	MESH events
filter	MESH debug filter
forward-mcast	Mesh forwarding mcast debugs
forward-table	Mesh forwarding table debugs
history	MESH history of events
level	Enable different mesh debug levels
linktest	Mesh linktest debugs
nat	Mesh NAT debugs
path-control	MESH path-control debugs
port-control	MESH port-control debugs
security	MESH security debugs
stp	MESH daisychain STP debugs
wpa_supplicant	Mesh WPA_SUPPLICANT debugs
wstp	MESH WSTP debugs

RAP/MAP debug mesh options

On WLC:

9124EWC#show wireless mesh ?	
airtime-fairness	Shows Mesh AP Airtime Fairness information
ap	Shows mesh AP related information
cac	Shows Mesh AP cac related information
config	Show mesh configurations
convergence	Show mesh convergence details.
ethernet	Show wireless mesh ethernet
neighbor	Show neighbors of all connected mesh Aps
persistent-ssid-broadcast	Shows Mesh AP persistent ssid broadcast
	information
rrm.	Show wireless mesh rrm information

show wireless mesh

To debug on the WLC the best start point is to use RadioActive trace with the MAC address of the MAP/RAP.

Example 1: RAP receives adjacency from MAP and succeeds authentication

<#root>

```
AP9124_RAP#show debug
mesh:
adjacent packet debugging is enabled
event debugging is enabled
mesh linktest debug debugging is enabled
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshRadic
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshAwpp/
Jan 16 14:47:01 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:01.9560] EVENT-MeshAwpp/
Jan 16 14:47:01 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:01.9570] CLSM[4C:A6:4D:2
Jan 16 14:47:04 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:04.9588] EVENT-MeshRadi
Jan 16 14:47:04 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:04.9592] EVENT-MeshLink
Jan 16 14:47:04 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:04.9600] EVENT-MeshSecur
Jan 16 14:47:05 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:05.1008] EVENT-MeshSecu
Jan 16 14:47:05 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:05.1011] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.1172] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
                                    [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
Jan 16 14:47:06 AP9124_RAP kernel:
                                   [*01/16/2024 14:47:06.2033] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
                                   [*01/16/2024 14:47:06.2139] EVENT-MeshSecu
                                   [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:
```

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2144] EVENT-MeshLink Jan 16 14:47:06 AP9124 RAP kernel: [*01/16/2024 14:47:06.2146] EVENT-MeshAwppA

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2147] EVENT-MeshAwpp/ Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwpp/ Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwpp/ Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3576] EVENT-MeshRadic Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadic Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadic

Example 2: MAP Mac address not added to WLC or incorrectly added

<#root>

Jan	16	14:52:13	AP9124_RAP	kernel:	[*01/16/2024 [*01/16/2024	14:52:13.6402]	INFO-MeshRadio
Jan	16	14.32.13 14.52.15	AP9124_RAP	kernel.	[*01/10/2024]	14.32.13.7407 14.52.15.7407	EVENT_MochPadi
Jan	16	14.52.15 14.52.15	AF 9124 AF	kornol:	[01/10/2024]	14.52.15.7400 14.52.15.7400	TNEO_MochPadio
Jan	16	14.52.15 14.52.15	AF 9124 AF	kornol:	[01/10/2024]	14.52.15.7409 14.52.15.7409	EVENT_Mochlink
Jan	16	14.52.15	AD0124 DAD	kornol:	[01/10/2024]	14.52.15.7411 14.52.15.7411	EVENT_MoshSocu
Jan	16	14.52.15 11.52.15	ADQ124	kornol:	[01/10/2024]	14.52.15.7419 11.52.15.7583	EVENT_MoshSocu
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7586]	EVENT-MeshSecu
Tam	10	14.50.15	200104 D2D	here al.			
Jan	Τ0	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7586]	EVENT-MesnSecur
-	1.0	4					
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7620]	INFO-Meshkadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7620	INFO-Meshkadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7621	INFO-MeshAwppA
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7621	0x3C 0x5/ 0x31
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7621	INFO-MeshAwppAc
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7621	INFO-MeshAwppAc
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7621	INFO-MeshAwppA
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622]	OXTT OXTT OXTT
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622]	INFO-MeshAwppA
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622]	INFO-MeshAwppAd
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622]	Oxaa Oxff OxOO
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622	INFO-MeshAwppAc
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7623	INFO-MeshAwppAc
Jan	16	14:52:15	AP9124_RAP	kernel:	L*01/16/2024	14:52:15.7623	Oxaa Oxtt Oxaa
Jan	16	14:52:15	AP9124_RAP	kernel:	$\lfloor *01/16/2024$	14:52:15.7623	INFO-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7636]	EVENT-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7637]	INFO-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7642]	EVENT-MeshLink:
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7642]	EVENT-MeshSecu

Example 3: RAP looses MAP

Jan Jan Jan Jan Jan Jan	16 16 16 16 16 16	14:48:58 14:48:59 14:48:59 14:48:59 14:48:59 14:49:00 14:49:00	AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP	kernel: kernel: kernel: kernel: kernel: kernel: kernel:	[*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024	14:48:58.9929] 14:48:59.2889] 14:48:59.7894] 14:48:59.9931] 14:48:59.9932] 14:49:00.2891] 14:49:00.7891] 14:49:00.9037]	INFO-MeshRadiol INFO-MeshAwppAd INFO-MeshAwppAd INFO-MeshRadiol INFO-MeshRadiol INFO-MeshAwppAd INFO-MeshAwppAd INFO-MeshAwppAd
Jan Jan	16 16 16	14:49:00 14:49:01	AP9124_RAP AP9124_RAP	kernel: kernel:	[*01/16/2024 [*01/16/2024 [*01/16/2024	14:49:00.9938] 14:49:01.2891]	INFO-MeshRadiol INFO-MeshAwppA
Jan	16	14 : 49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5480]	EVENT-MeshAwppA
Jan	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5481]	EVENT-MeshRadio
Jan	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5481]	EVENT-MeshRadic
Jan	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5488]	EVENT-MeshRadic
Jan	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5489]	INFO-MeshRadio
Jan							
0 411	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5501]	EVENT-MeshRadic
Jan	16 16	14:49:25 14:49:25	AP9124_RAP AP9124_RAP	<pre>kernel: kernel:</pre>	[*01/16/2024 [*01/16/2024	14:49:25.5501] 14:49:25.5501]	EVENT-MeshRadic EVENT-MeshAdj[1

Tips, Tricks and Recommendations

- 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).
- It is highly recommended to test out the setup in a controlled environment before deploying it on site.
- If testing Ethernet bridging with windows laptops on each side, please note that to test ICMP between Windows devices you need to allow ICMP on the system firewall. By default Windows devices block ICMP in the system firewall.
- 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 are supposed to 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.

References

Cisco Embedded Wireless Controller on Catalyst Access Points Data Sheet

Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) White Paper

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