Configuration d'une liaison maillée point à point avec pontage Ethernet sur un contrôleur sans fil intégré avec points d'accès C9124

Table des matières

```
Introduction
Conditions préalables
   Exigences
    Composants utilisés
Informations générales
   Pontage Ethernet
   Contrôleur sans fil intégré sur le point d'accès Catalyst
Configurer
   Diagramme du réseau
   Configurations
       Configurations de commutateurs
       Configuration EWC et RAP
       Configurer MAP
   <u>Vérifier</u>
Dépannage
       Commandes utiles
       Exemple 1 : le protocole RAP reçoit la contiguïté du protocole MAP et réussit l'authentification
       Exemple 2 : l'adresse MAC MAP n'a pas été ajoutée au WLC ou a été ajoutée incorrectement
       Exemple 3 : Le RAP perd la MAP
       Conseils, astuces et recommandations
Références
```

Introduction

Ce document décrit comment configurer la liaison maillée P2P avec pontage Ethernet sur contrôleur sans fil intégré (eWC) avec points d'accès C9124.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs LAN sans fil Cisco (WLC) 9800.
- Points d'accès (AP) Cisco Catalyst.
- · Contrôleur sans fil intégré sur les points d'accès Catalyst.

• Technologie de maillage.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- EWC IOS® XE 17.12.2
- 2 points d'accès C9124
- 2 injecteurs de puissance AIR-PWRINJ-60RGD1.
- 2 commutateurs ;
- 2 ordinateurs portables ;
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Pontage Ethernet

La solution de réseau maillé, qui fait partie de la solution de réseau sans fil unifié de Cisco, permet à deux ou plusieurs points d'accès maillés Cisco (ci-après appelés points d'accès maillés) de communiquer entre eux sur un ou plusieurs sauts sans fil pour rejoindre plusieurs réseaux locaux ou pour étendre la couverture Wi-Fi.

Les points d'accès maillés Cisco sont configurés, surveillés et exploités depuis et via tout contrôleur LAN sans fil Cisco déployé dans la solution de réseau maillé.

Les déploiements de solutions réseau maillées pris en charge sont de l'un des trois types suivants :

- Déploiement point à point
- Déploiement point à multipoint
- Déploiement maillé

Ce document se concentre sur la façon de configurer le déploiement de maillage point à point et le pontage Ethernet sur le même.

Dans un déploiement maillé point à point, les points d'accès maillés fournissent un accès sans fil et une liaison aux clients sans fil, et peuvent simultanément prendre en charge le pontage entre un LAN et une terminaison vers un périphérique Ethernet distant ou un autre LAN Ethernet.



Pontage Ethernet sans fil

Référez-vous <u>au Guide de déploiement de maillage pour les</u> contrôleurs<u>sans fil de la gamme</u> <u>Cisco Catalyst 9800</u> pour des informations détaillées sur chacun de ces types de déploiement.

Le point d'accès maillé extérieur de la gamme Cisco Catalyst 9124 est un périphérique sans fil conçu pour l'accès client sans fil et le pontage point à point, le pontage point à multipoint et la connectivité sans fil maillée point à multipoint.

Le point d'accès extérieur est une unité autonome qui peut être montée sur un mur ou un porte-àfaux, sur un poteau de toit ou sur un poteau d'éclairage public.

Vous pouvez utiliser le C9124 dans l'un des rôles de maillage suivants :

- Point d'accès sur le toit (RAP)
- Point d'accès maillé (MAP)

Les RAP disposent d'une connexion câblée à un contrôleur LAN sans fil Cisco. Ils utilisent l'interface sans fil de liaison pour communiquer avec les MAP voisins. Les RAP sont le noeud parent de tout réseau de pontage ou maillé et connectent un pont ou un réseau maillé au réseau câblé. Il ne peut donc y avoir qu'un RAP pour tout segment de réseau ponté ou maillé.

Les MAP n'ont pas de connexion câblée à un contrôleur LAN sans fil Cisco. Ils peuvent être entièrement sans fil et prendre en charge les clients qui communiquent avec d'autres MAP ou RAP, ou ils peuvent être utilisés pour se connecter à des périphériques ou à un réseau câblé.

Contrôleur sans fil intégré sur le point d'accès Catalyst

Le contrôleur sans fil intégré Cisco (EWC) sur les points d'accès Catalyst est un contrôleur logiciel intégré aux points d'accès Cisco Catalyst 9100.

Dans un réseau Cisco EWC, un point d'accès qui exécute la fonction de contrôleur sans fil est désigné comme point d'accès actif.

Les autres points d'accès, qui sont gérés par ce point d'accès actif, sont appelés points d'accès subordonnés.

Le CEE actif a deux rôles :

• Il fonctionne comme un contrôleur LAN sans fil (WLC) pour gérer et contrôler les points d'accès subordonnés. Les points d'accès subordonnés fonctionnent comme des points d'accès légers pour servir les clients.

• Il fonctionne comme un point d'accès pour servir les clients.

Pour obtenir une présentation du produit EWC sur les points d'accès, consultez la <u>fiche technique</u> <u>du contrôleur sans fil intégré Cisco sur les points d'accès Catalyst</u>.

Pour savoir comment déployer le CEE sur votre réseau, consultez le <u>livre blanc Cisco Embedded</u> <u>Wireless Controller on Catalyst Access Points (EWC) (Contrôleur sans fil intégré Cisco sur points</u> <u>d'accès Catalyst</u>).

Ce document se concentre sur C9124 en tant que EWC et suppose qu'il y a déjà un AP 9124 en mode EWC.

Configurer

Diagramme du réseau

Tous les périphériques de ce réseau sont situés dans le sous-réseau 192.168.100.0/24, à l'exception des ordinateurs portables qui se trouvent dans le VLAN 101 avec le sous-réseau 192.168.101.0/25.

L'interface de gestion du point d'accès EWC (WLC) n'est pas étiquetée et le VLAN natif sur les ports de commutation est défini sur VLAN 100.

Le point d'accès AP9124_RAP a le rôle d'un eWC et d'un point d'accès racine (RAP), tandis que le point d'accès AP9124_MAP a le rôle de point d'accès maillé (MAP).

Dans ces travaux pratiques, un AP C9115 est également placé derrière le MAP pour montrer que nous pouvons avoir des AP pour joindre un WLC sur une liaison maillée.

Cette table contient les adresses IP de tous les périphériques du réseau :

Remarque : le marquage de l'interface de gestion peut causer des problèmes avec l'AP joignant le processus WLC interne. Si vous décidez d'étiqueter l'interface de gestion, assurez-vous que la partie d'infrastructure filaire est configurée en conséquence.

Périphérique	Adresse IP
Passerelle par défaut	Statique sur VLAN 100 : 192.168.100.1
Ordinateur portable1	DHCP sur VLAN 101
Ordinateur portable2	DHCP sur VLAN 101
Switch1 (convour DHCD)	VLAN 100 SVI : statique sur VLAN 100 :
	192.168.100.1 (serveur DHCP)

Switch1 (serveur DHCP)	VLAN 101 SVI : statique sur VLAN 101 : 192.168.101.1 (serveur DHCP)				
Commutateur2	VLAN 100 SVI : DHCP sur VLAN 100				
Commutateur2	VLAN 101 SVI : DHCP sur VLAN 101				
9124CEE	Statique sur VLAN 100 : 192.168.100.40				
AP9124_RAP	DHCP sur VLAN 100				
AP9124_MAP	DHCP sur VLAN 100				
AP9115	DHCP sur VLAN 100				



Diagramme du réseau



Remarque : les points d'accès C9124 sont alimentés à l'aide de la carte AIR-PWRINJ-60RGD1 conformément aux instructions du <u>Guide d'installation matérielle des points</u> <u>d'accès extérieurs de la gamme Cisco Catalyst 9124AX</u>.

Configurations

Ce document suppose qu'il existe déjà un AP 9124 exécutant EWC avec le déploiement initial effectué selon le <u>livre blanc du contrôleur sans fil intégré Cisco sur les points d'accès Catalyst</u> (<u>EWC</u>).

Pour d'autres conseils et astuces concernant le processus de conversion, veuillez consulter le document <u>Convertir les points d'accès Catalyst 9100 en contrôleur sans fil intégré</u>.

Configurations de commutateurs

Voici les configurations pertinentes des commutateurs.

Les ports de commutateur où les AP sont connectés sont en mode trunk avec le VLAN natif défini sur 100 et autorisant le VLAN 101.

Lors de la mise en place des AP, vous devez configurer le MAP en tant que MAP, par conséquent vous devez faire en sorte que l'AP rejoigne le eWC via ethernet. Ici, nous utilisons le port G1/0/2 du commutateur Switch1 pour préparer le MAP. Une fois le transfert terminé, le MAP est déplacé vers le commutateur 2.

Les ports de commutateur où les ordinateurs portables sont connectés sont configurés comme ports d'accès sur le VLAN 101.

Commutateur 1 :

```
ip dhcp excluded-address 192.168.101.1 192.168.101.10
ip dhcp excluded-address 192.168.100.1 192.168.100.10
1
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
```

Commutateur 2 :

```
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
```

Configuration EWC et RAP

Après la configuration Day0 du point d'accès EWC, le point d'accès intégré doit se joindre à luimême.

1. Ajoutez les adresses MAC Ethernet du point d'accès racine et du point d'accès maillé à l'authentification du périphérique. Accédez à Configuration > Security > AAA > AAA Advanced > Device Authentication, cliquez sur le bouton +Add :

Q. Search Menu Items	Configuration * > Security * > AA	A								
Dashboard	+ AAA Wizard									
Monitoring ,	Servers / Groups AAA Method L	st AAA Adv	ranced							
	Global Config	MAC Address	Serial Number							
(O) Administration	RADIUS Fallback	+ Add	× Delete		B	Select File		 Uplos 	d File	
C Licensing	Attribute List Name		MAC Address	Ţ	Attribute List Name	T	Description	т	WLAN Profile	Ŧ
	Device Authentication	0	3c5731c5ac2c		None		MeshAP-RootAP			
X Troubleshooting	AP Policy		3c5731c5a9f8		None		MeshAP-MAP			
	Password Policy	H 4	1 > > 10 ▼							1 - 2 of 2 items
	AAA Interface									

Adresses MAC dans l'authentification des périphériques

Commandes CLI :

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

L'adresse MAC Ethernet peut être confirmée en exécutant la commande « show controllers wired 0 » à partir de l'interface de ligne de commande du point d'accès. Exemple du point d'accès racine : L'accès au shell AP sous-jacent peut être complété avec la commande "wireless ewc-ap ap shell username x" comme illustré :

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. 9124EWC#



Remarque : cette commande équivaut à apciscoshell qui était auparavant disponible dans

les contrôleurs Mobility Express.

Si le nom d'utilisateur et le mot de passe de gestion AP ne sont pas spécifiés dans le profil AP, utilisez le nom d'utilisateur par défaut Cisco et le mot de passe Cisco à la place.

Q Search Menu Items	Configuration * > Security * > AA	A		
Dashboard	+ AAA Wizard			
(2) Monitoring >	Servers / Groups AAA Method I	List AAA Advanced	potion	
	Authentication	Quick Setup. AAA Authentic		
Configuration >	Authorization	Method List Name*	MESH_Authentication	
() Administration	Accounting	Туре*	dot1x v	
C Licensing	noodining	Group Type	local 🔹	
		Available Server Groups	Assigned Server Groups	
Walk Me Through 3		radius ^ Idap tacacs+	x x x x x x x x x x x x	
		Cancel		y to Device

2. Ajouter des méthodes d'authentification et d'autorisation :



Q Search Menu Items	Configuration * > Security * > A	A		
ashboard	+ AAA Wizard			
Monitoring >	Servers / Groups AAA Method	Quick Setup: AAA Authoria	zation	×
Configuration	Authentication	Method List Name*	MESH_Authorization	
Administration		Туре*	credential-download 🗸 (i)	
C Licensing	Accounting	Group Type	local 🔻 (i	24
Troubleshooting		Authenticated	Assigned Server Groups	
Walk Me Through >		radius Idap tacacs+		
		Cancel		Apply to Device

Liste des méthodes d'autorisation

Commandes CLI :

3. Accédez à Configuration > Wireless > Mesh. Comme la configuration dans ce document nécessite le pontage Ethernet, activez le pontage Ethernet Autoriser les BPDU :

arch Menu Items Configuration * > Wireless * > Mesh	h		
ashboard Global Config Profiles			
onitoring >		Alarm	
onfiguration > Ethernet Bridging Allow BPDU		Max Hop Count	4
Subset Channel Sync	D	Recommended Max Children for MAP	10
Backhaul		Recommended Max Children for RAP	20
Extended UNII B Domain Channels	D	Parent Change Count	3
RRM	D	Low Link SNR (dB)	12
Auto-DCA	O	High Link SNR (dB)	60
Security		Association Count	10
PSK Provisioning	D		
Default PSK	D		

Pontage Ethernet Autoriser BPDU

Commandes CLI :

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



Remarque : par défaut, les AP maillés ne transfèrent pas les BPDU sur la liaison maillée.

Si vous n'avez pas de liaison redondante entre les 2 sites, elle n'est pas nécessaire.

S'il existe des liaisons redondantes, vous devez autoriser les unités BPDU. Si ce n'est pas le cas, vous risquez de créer une boucle STP dans le réseau.

4. Configurez le profil de maillage par défaut où vous sélectionnez les méthodes AAA Authentication and Authorization précédemment configurées. Cliquez sur et modifiez le profil de maillage par défaut.

Accédez à l'onglet Advanced et sélectionnez les méthodes Authentication et Authorization. Activez l'option Pontage Ethernet.

Q. Search Menu Items	Configuration * > Wireless * > Mesh	Edit Mesh Profile					×
Dashboard	Global Config Profiles	Changes in the configuration for Se save and reload for the cha	ecurity Mode, BGN, Client-Acce inges to take effect. Controller of	A iss, and Range wi can be reloaded f	II reload associated APs, except rom 'Administration -> Manager	Primary AP. Primary AP requires contr nent -> Backup & Restore -> Reload*	roller tc
Configuration	Number of Profiles : 1 Name Y Bridge Group Name	General Advanced			5 GHz Band Backhaul		
Administration	default-mesh-profile	Security					
C Licensing	H 4 1 > H 10 -	Method	EAP 🔹		Rate Types	auto	
\$ (4		Authentication Method	MESH_Authentica 🔻	8	2.4 GHz Band Backhaul		
Troubleshooting		Authorization Method	MESH_Authorizati 👻		Rate Types	auto 🔻	
		Ethernet Bridging			Fast Roaming		
Walk Me Through >		VLAN Transparent Ethernet Bridging	•		Fast Teardown	0	
		Bridge Group					
		Bridge Group Name Strict Match	Enter Name				
		Cancel				Update & Apply to Dev	vice

Modifier le profil de maillage par défaut

Commandes CLI :

```
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
```

Légende spéciale pour l'option VLAN Transparent :

Cette fonction détermine la manière dont un point d'accès maillé gère les balises VLAN pour le trafic ponté Ethernet :

- Si VLAN Transparent est activé, les balises VLAN ne sont pas gérées et les paquets sont pontés en tant que paquets non balisés.
 - Aucune configuration des ports Ethernet n'est requise lorsque le VLAN transparent est activé. Le port Ethernet transmet les trames étiquetées et non étiquetées sans les interpréter.
- Si la fonction VLAN Transparent est désactivée, tous les paquets sont traités en fonction de la configuration VLAN sur le port (agrégation, accès ou mode normal).
 - Si le port Ethernet est défini sur le mode Trunk, l'étiquetage VLAN Ethernet doit être configuré.



Conseil : pour utiliser l'étiquetage VLAN AP, vous devez décocher la case VLAN Transparent.

Si vous n'utilisez pas l'étiquetage VLAN, cela signifie que les protocoles RAP et MAP se trouvent sur le VLAN natif configuré sur les ports d'agrégation. Dans cette condition, si vous voulez que les autres périphériques derrière MAP se trouvent sur le VLAN natif (ici VLAN 100), vous devez activer le VLAN transparent.

5. Le point d'accès interne rejoint le CEE et vous pouvez vérifier l'état de jointure du point d'accès à l'aide de la commande « 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	сс	RD	IP Address	State	Location
AP3C57.31C5.AC2C	2 C9124AXI-B	3c57.31c5.ac2c	4ca6.4d23.aee0	US	- B	192.168.100.11	Registered	default location

show ap summary

Vous pouvez également voir le point d'accès joint via l'interface graphique où le point d'accès apparaît en mode Flex+Bridge. Pour plus de commodité, vous pouvez changer le nom de l'AP maintenant. Dans cette configuration, il est utilisé sous le nom AP9124_RAP :

Q. Search Menu Items	Configuration * > Wireless * > Access I	Points	Edit AP			×
Dashboard	 All Access Points 		General Interfaces General	Inventory Geolocation	Mesh Advanced	Î
Monitoring >		Current Active	AP Name*	AP3C57.31C5.AC2C	Policy	default-policy-tag 👻
Configuration		AP3C57.31C5.AC2C	Location*	default location	Site	default-site-tag 👻 💈
Administration			Base Radio MAC	4ca6.4d23.aee0	RF	default-rf-tag 👻
C Licensing	Total APs : 1	Artmin :	Ethernet MAC	3c57.31c5.ac2c	Write Tag Config to AP	0
	: AP Model :	Slots : Status Up Time	Admin Status	ENABLED	Version	
	1C5.AC2C 🔥 🕍 C9124AXI-B	2 O days 1 h mins 37 sec	AP Mode	Flex+Bridge -	Primary Software Version	17.12.2.35
	⊢ ⊣ 1 ► ⊢ 10 ▼		Operation Status	Registered	Predownloaded Status	None

Détails généraux AP

Vous pouvez modifier la géolocalisation, puis dans l'onglet Maillage, assurez-vous que son rôle est configuré en tant qu'AP racine et que la configuration de port Ethernet est définie sur l'agrégation avec les ID de VLAN correspondants :

O. Search Menu Items	Configuration * > Wireless * > Access Points		Edit AP					
Dashboard	 All Access Points 		General Interfaces	Inventory	Geolocation	Mesh Advanced		
			General	_		Ethemet Port Connguration		
Configuration		AP3C57.31C5.AC2C	Block Child	0		Ethernet Bridging on the asso to configure this section succes	ciated Mesh Profile should be enabled sfully	
رُنَ Administration			Daisy Chaining strict-	0		Port	0	
C Licensing	Total APs : 1	Admin :	Preferred Parent MAC	0000.0000.0000		Mode	normal	
X Troubleshooting	: AP Model : Slots	Status Up Time	Role	Root	•			
		mins 37 sec		-				
			Remove PSK	Ш				
Walk Me Through >	> 5 GHz Radios		Backhaul					
	> 2.4 GHz Radios		Radio Type and Slot AP	can be changed only fo	or a Root			
	> Dual-Band Radios		Backhaul Ratio Type	Sahz	•			
	> Country		Backhaul Slot ID	1	•			
	LSC Provision		Rate Types	auto	•			
	> AP Certificate Policy		Cancel				Update & Apply to Device	

Racine du rôle de maillage

Edit AP							×
General Interfaces	Inventory	Geolocation	Mesh	Advanced			
General			Ethernet P	Port Configuration			l
Block Child	0		 Ethern to config 	et Bridging on the asso ure this section succes	ociated Mesh Profile sl ssfully	hould be enabled	
Daisy Chaining Daisy Chaining strict- RAP	0		Port		0	•	
Preferred Parent MAC	0000.0000.0000		Mode		trunk	•	L
Role	Root	•	Native VI	LAN ID*	100		L
			Allowed	VLAN IDs	101	()	L
Remove PSK	圓						L
							L
Backhaul							L
Radio Type and Slot of AP	can be changed only f	or a Root					
Backhaul Radio Type	5ghz	•					
Backhaul Slot ID	1	•					ľ
Rate Types	auto	•					•
Cancel					Upda	ate & Apply to Device	

Configuration du port Ethernet

Configurer MAP

Il est maintenant temps de rejoindre le MAP 9124.

1. Connectez le point d'accès MAP au commutateur Switch1 pour le transfert. Le point d'accès rejoint le CEE et apparaît dans la liste AP. Changez son nom en quelque chose comme AP9124_MAP et configurez-le en tant que Rôle de maillage dans l'onglet Maillage. Cliquez sur Update & Apply to Device :

Search Menu Items	Configuration * > Wireless * > Access Point	8	Edit AP				×
	V All Access Points		General Interfaces	Inventory	Geolocation	Mesh Advanced	
Dashboard	 All Access Folits 		General			Ethernet Port Configuration	
Monitoring		Current Active	Block Child	0		Ethernet Bridging on the assoc to configure this section success	iated Mesh Profile should be enabled fully
Configuration			Daisy Chaining	0			
O Administration			Daisy Chaining strict- RAP	0		Port	0 •
C Licensing	Total APs : 2	Admin :	Preferred Parent MAC	0000.0000.0000		Mode	trunk
X Troubleshooting	AP Name : AP Model	I Slots I Status	Role	Mesh	•	Native VLAN ID*	100
	AP9124_MAP A M C9124AXI-B				Allowed VLAN IDs	101	
	AP9124_RAP A C9124AXI-B	2	Remove PSK				
	H 4 1 F H 10 -						
			Backhaul				
	5 GHz Radios		Backhaul Radio Type	5ghz	w		
	> 2.4 GHz Radios		Backhaul Slot ID	1	v		
	> Dual-Band Radios		Rate Types	auto	•		
	> Country						
	LSC Provision		Cancel				Update & Apply to Device

configuration MAP

2. Déconnectez le point d'accès du commutateur Switch1 et connectez-vous au commutateur Switch2 conformément au schéma du réseau. Le MAP rejoint le CEE via une interface sans fil via le RAP.



Remarque : comme les points d'accès sont alimentés via un injecteur de puissance, le point d'accès ne tombe pas en panne et comme la configuration est dans un environnement contrôlé, le commutateur 2 est physiquement proche et nous pouvons simplement déplacer le câble d'un commutateur à l'autre.

Vous pouvez connecter un câble de console au point d'accès et voir ce qui se passe via la console. Voici quelques messages importants vus.



Remarque : à partir de la version 17.12.1, le débit en bauds par défaut des points d'accès 802.11AX passe de 9 600 bits/s à 115200 bits/s.

MAP perd la connectivité au CEE :

AP9124_MAP#		
[*01/11/2024	14:08:23.0214]	chatter: Device wired0 notify state change link D
[*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,
[*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,
[*01/11/2024	14:08:34.1495]	
[*01/11/2024	14:08:37.1505]	Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=84,
[*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,
[*01/11/2024	14:08:40.1515]	

[*01/11/2024 14:08:43.1524] Max retransmission count exceeded, going back to [
[...]
[*01/11/2024 14:08:48.1537] CRIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Blocklist
[*01/11/2024 14:08:48.1538] CRIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Remove as
[*01/11/2024 14:08:48.1539] CRIT-MeshLink: Link Down Block Root port Mac: 3C:!
[*01/11/2024 14:08:48.1542] CRIT-MeshWiredBackhaul[0]: Remove as uplink

MAP passe en mode découverte via le sans fil et trouve le RAP via Radio Backhaul sur le canal 36, trouve EWC et le rejoint :

```
[*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)
[*01/11/2024 14:08:53.3898] CRIT-MeshLink: Set Root port Mac: 4C:A6:4D:23:AE:
[*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 auther
Γ...]
[*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]
[*01/11/2024 14:09:59.0106] CAPWAP State: DTLS Setup
[*01/11/2024 14:09:59.0987] dtls_verify_server_cert: Controller certificate vertificate ve
[*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 point
[*01/11/2024 14:10:04.7842] Sending Join request to 192.168.100.40 through point
[*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 est maintenant joint au CEE via RAP.

Le point d'accès C9115 peut maintenant obtenir une adresse IP sur VLAN 100, puis rejoindre le CEE :



Avertissement : gardez à l'esprit que VLAN 100 est le VLAN natif trunk switchports. Pour que le trafic du point d'accès sur VLAN 100 atteigne le WLC sur VLAN 100, la liaison maillée doit avoir VLAN Transparent activé. Cette opération est effectuée dans la section Pontage Ethernet du profil de maillage.

[*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, discover
[*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

[]		
[*01/19/2024	15:13:56.1660]	dtls_verify_server_cert: Controller certificate vertificate vertif
[*01/19/2024	15:13:56.9000]	sudi99_request_check_and_load: Use HARSA SUDI cer
[*01/19/2024	15:13:57.2980]	
[*01/19/2024	15:13:57.2980]	CAPWAP State: Join
[*01/19/2024	15:13:57.3170]	<pre>shared_setenv PART_BOOTCNT 0 &> /dev/null</pre>
[*01/19/2024	15:13:57.8620]	Sending Join request to 192.168.100.40 through pol
[*01/19/2024	15:14:02.8070]	Sending Join request to 192.168.100.40 through pol
[*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, Con
[*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_U
[*01/19/2024	15:14:03.5330]	do NO_UPGRADE, part2 is active part
[*01/19/2024	15:14:03.5520]	
L*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
L*01/19/2024	15:14:03.6880	Radio [1] Administrative state DISABLED change to
[*01/19/2024	15:14:03.6890]	Radio [0] Administrative state DISABLED change to
[*01/19/2024	15:14:03.86/0]	
[*01/19/2024]	15:14:03.8670]	CAPWAP State: Run
[*01/19/2024]	15:14:03.9290]	AP has joined controller 9124EWC
L*01/19/2024	15:14:03.9310]	Flexconnect Switching to Connected Mode!

Comme il s'agit d'un AP EWC, il contient uniquement l'image AP qui correspond à son propre modèle (ici un C9124 exécute ap1g6a). Lorsque vous rejoignez un autre modèle de point d'accès, vous avez un réseau non homogène.

Dans ces conditions, si l'AP n'est pas sur la même version, il doit télécharger la même version, donc assurez-vous que vous avez un serveur et un emplacement TFTP/SFTP valide, avec les images AP, configurées dans le EWC > Administration > Software Management :

Ci	CiscoSWImages > Images > 9800 > C9800-AP-universalk9.17.12.02							
	↑↓ Sort ~ $≡$ View ~							
	Name	Date modified	Туре	Size				
1	∼ 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				
	🔲 📄 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 Sizes 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				

Serveur TFTP avec dossier d'images AP

Cisco Embedded Wireless Controller on Catalyst Access Points Welcome admin 🕋 🕫 🦧 🖺									
Q. Search Menu Items	Administration > Software M	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						
		0.0							

Images AP

Le point d'accès apparaît dans la liste des points d'accès et vous pouvez attribuer un PolicyTag :

Cisco Ember	dded Wireless Con	ntroller on Catalyst	Access Points		Welcome admin	* * 4 8 * *	B O C Search APs and Cl	ents Q					
Q. Search Menu Items	Configuration * > Wi	ireless* > Access Po	ints		Edit AP								
		linto			General Interfaces	Inventory Geolocation	ICap Advanced						
E Dashboard	 All Access Po 	ints			General		Tags						
Monitoring >	> Current Active				AP Name*	AP9115	Policy	LocalSWTag 👻 💈					
Configuration			AP9124_	RAP	Location*	default location	Site	default-site-tag 👻 💈					
(Ô) 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 : Stat	nin : tus Up Time	Admin Status	ENABLED	Version						
M HOUSEANDOLING	AP9115	dial C9115AXE-B	2 C	0 days 0 hr mins 36 secs	AP Mode	Flex	Primary Software Version	17.12.2.35					
	AP9124_MAP	▲ 🕍 C9124AXI-B	2 C	8 days 6 hrs mins 37 secs	Operation Status	Registered	Predownloaded Status	Predownloading					
	AP9124_RAP	▲ 🕍 C9124AXI-B	2 C	mins 40 secs	Fabric Status	Disabled	Predownloaded Version	0.0.0.0					
Waik Me Inrough 2	8 → 1 > -	н 10 👻			CleanAir NSI Key		Next Retry Time	0					
					LED Settings		Boot Version	1.1.2.4					
	5 GHz Radios	l.			LED State	ENABLED	Inc thereins	17 10 0 05					





Vue opérationnelle AP

Vérifier

Vous pouvez voir l'arbre maillé via l'interface graphique qui donne également le résultat de l'interface de ligne de commande si vous utilisez la commande "show wireless mesh ap tree". Dans l'interface graphique utilisateur, accédez à 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	
	Tree				
C Licensing					
Will Me Through 3	AP Name [Hop Ctr,Link SNR,BG Name,Channel [Sector 1] AP9124_RAP [0, 0, Default, (36), 0000.000 AP9124_RAP [1, 73, Default, (36), 00 Number of Bridge AP9 : 2 Number of RAPs : 1 Number of NAPs : 1 (*) Wait for 3 minutes to update or Ethe (*) Not in this Controller	Pref Parent,Chan Util,Clients] 0.0000, 3%, 0] 0.0000.0000, 3%, 0] rnet Connected Hesh AP.			

Arborescence des points d'accès maillés

Sur les protocoles RAP et MAP, vous pouvez vérifier la liaison maillée à l'aide de la commande "show mesh backhaul" :



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 3C:57:31:C5:A9:F8 16 16 32 T/F: F F T F T T Blocklisted: GW UNREACHABLE 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) 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: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 afficher une liaison maillée

Vous pouvez vérifier la configuration de l'agrégation de VLAN maillé côté AP :

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:

L'ordinateur portable 2 connecté au commutateur 2 a reçu l'adresse IP du VLAN 101 :



L'ordinateur portable 1 placé sur le commutateur 1 a reçu une adresse IP du VLAN 101 :

Ethernet adapter Ethernet 6_White:

Connection-spect	ific DNS	Suffix . :	
Link-local IPv6	Address	:	fe80::d1d6:f607:ff02:4217%18
IPv4 Address		:	192.168.101.13
Subnet Mask		:	255.255.255.0
Default Gateway		:	192.168.101.1

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



Remarque : pour tester le protocole ICMP entre des périphériques Windows, vous devez l'autoriser sur le pare-feu système. Par défaut, les périphériques Windows bloquent le protocole ICMP dans le pare-feu système.

Un autre test simple pour vérifier le pontage Ethernet est d'avoir une interface SVI pour VLAN 101 sur les deux commutateurs et de définir l'interface SVI du commutateur 2 sur DHCP. L'interface SVI du commutateur 2 pour VLAN 101 obtient l'adresse IP du VLAN 101 et vous pouvez envoyer une requête ping à l'interface SVI du commutateur 1 pour VLAN 101 pour vérifier la connectivité du VLAN 101 :

<#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 GigabitEthernet0/1 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 !!!!! 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
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
Switch1#

Le point d'accès en mode local C9115 a également rejoint le CEE :

Q, Search Menu Items	Configuration * > Wireless * > Access Points															
Dashboard	 All Access P 	oints														
Monitoring >					Current Active AP9124_RAP				Current Standby Not Applicable				Preferred Active AP9124_RAP			
Administration	Total APs : 3															
	AP Name	:	AP Model	:	Slots	:	Admin Status	Up Time	:	IP Address	Base Radio MAC	:	Ethernet MAC	:	AP Mode	
Troubleshooting	AP9115	山田	C9115AXE-B	2		٢		0 days 0 hr mins 30 se	s 35 cs	192.168.100.14	1cd1.e079.66e0		84f1.47b3.2cdc		Flex	
	AP9124_MAP	њы	C9124AXI-B		2		٢	0 days 0 hr mins 59 se	s 52 cs	192.168.100.12	4ca6.4d23.9d40		3c57.31c5.a9f8		Flex+Bridge	
	AP9124_RAP	њы	C9124AXI-B		2		۲	0 days 2 hr mins 57 se	s 46 cs	192.168.100.11	4ca6.4d23.aee0		3c57.31c5.ac2c		Flex+Bridge	

AP 9115 joint au CEE

Création de 3 WLAN, ouverts, PSK et dot1x mappés à un profil de stratégie avec VLAN 101 défini

dans les politiques d'accès :

AP Operational Configuration Viewer			
		AP9	115
WLANs a Local	nd Policies swTag	Site pr default- Ren	operties site-tag note
WLAN 🔶 : open SSID : open Policy 🌒 : LocalSWProfile VLAN ID : 101 Security : Open WLAN 馣 : PSK_WLAN SSID : PSK_WLAN Policy 🌒 : LocalSWProfile VLAN ID : 101 Security : WPA2 (PSK)	WLAN 🔶 : dot1x SSID : dot1x Policy 💽 : LocalSWProfile VLAN ID : 101 Security : WPA2	AP Join : default-ap-profile LED State : O Rogue Detection : O	Flex Profile : default-flex-pro Native VLAN ID : 100

Configuration opérationnelle AP9115

Les clients sans fil peuvent se connecter aux WLAN :

Q Search Merculterra	Monitori	ng* > Wireless	• >	Clients													
Dashboard	Clients	Sleeping Clie	-	Excluded Clie	rits.												
(2 Monitoring >	×	O															
R. Configuration	Select	nd 0 out of 2 Clients															
(3) Administration	0	Client MRC Address	T	Pvit T Address	Pv6 Address	AP Name	٣	Set D	٣	550	Ŧ	WUAN D	٣	Client Type	٣	State	1
A	0	\$254,4034-(572	ø	192,168,101,14	5x80-5004.40#3x8xx572	APR:15		1		open		4		W.M		Run	
C coming	0	acc.3434.216c	÷	192.166.101.15	N801acce:3485N341216c	AP9015		1		196,000	1	5		96,495		nur.	

Dépannage

Cette section présente des commandes utiles et quelques conseils, astuces et recommandations.

Commandes utiles

Sur 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

Options de maillage de débogage RAP/MAP

Sur 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

Pour déboguer sur le WLC, le meilleur point de départ est d'utiliser la trace RadioActive avec l'adresse MAC du MAP/RAP.

Exemple 1 : le protocole RAP reçoit la contiguïté du protocole MAP et réussit l'authentification

<#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-MeshRadic
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-MeshSecu
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.1173]
                                                                EVENT-MeshSecu
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.2033] EVENT-MeshSecu
                                    [*01/16/2024 14:47:06.2139] EVENT-MeshSecu
Jan 16 14:47:06 AP9124_RAP kernel:
Jan 16 14:47:06 AP9124_RAP kernel:
                                    [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecu
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

Exemple 2 : l'adresse MAC MAP n'a pas été ajoutée au WLC ou a été ajoutée incorrectement

<#root>

Jan	16	14:52:13	AP9124_RAP	kernel:	[*01/16/2024	14:52:13.6402]	INFO-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7407]	INFO-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7408]	EVENT-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7409]	INFO-MeshRadio
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7411]	EVENT-MeshLink
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7419]	EVENT-MeshSecu
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7583]	EVENT-MeshSecu
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7586]	EVENT-MeshSecu
Jan	16	14 : 52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7586]	EVENT-MeshSecur
lan	16	14.52.15	ΔΡ9124 ΒΔΡ	kernel.	Γ*01/16/2024	14.52.15 76201	TNFO-MeshRadio
lan	16	14.52.15	AP9124 RAP	kernel:	[*01/16/2024]	14.52.15.7020	INFO-MeshRadio
Jan	16	14:52:15	AP9124 RAP	kernel:	[*01/16/2024]	14:52:15.7621]	TNFO-MeshAwnnA
Jan	16^{-10}	14:52:15	AP9124 RAP	kernel:	[*01/16/2024	14:52:15.7621]	0x3c 0x57 0x31
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	INFO-MeshAwppA
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	Oxff Oxff Oxff
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-MeshAwppA
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7622]	0xaa 0xff 0x00
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	14:52:15.7623]	INFO-MeshAwppA
Jan	16	14:52:15	AP9124_RAP	kernel:	[*01/16/2024	14:52:15.7623]	Oxaa Oxff Oxaa
Jan	16	14:52:15	AP9124_RAP	kernel:	[*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

<#root>

Jan Jan Jan Jan Jan Jan Jan Jan Jan	16 16 16 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 14:49:00 14:49:00 14:49:01 14:49:01	AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP	<pre>kernel: kernel: kernel: kernel: kernel: kernel: kernel: kernel: kernel:</pre>	[*01/16/2024 [*01/16/2024 [*01/16/2024 [*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] 14:49:00.9937] 14:49:00.9938] 14:49:01.2891] 14:49:25.5480]	INFO-MeshRadiol INFO-MeshAwppAd INFO-MeshAwppAd INFO-MeshRadiol INFO-MeshRadiol INFO-MeshAwppAd INFO-MeshAwppAd INFO-MeshRadiol INFO-MeshRadiol INFO-MeshAwppAd
Jan Jan	16 16	14:49:25 14:49:25	AP9124_RAP ap9124_rap	kernel: kernel:	[*01/16/2024 [*01/16/2024	14:49:25.5481] 14:49:25.5481]	EVENT-MeshRadio
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	16	14 : 49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5501]	EVENT-MeshRadic
Jan	16	14:49:25	AP9124_RAP	kernel:	[*01/16/2024	14:49:25.5501]	EVENT-MeshAdj[]
Jan Jan Jan Jan	16 16 16 16	14:49:25 14:49:25 14:49:25 14:49:25 14:49:25	AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP AP9124_RAP	kernel: kernel: kernel: kernel:	[*01/16/2024 [*01/16/2024 [*01/16/2024 [*01/16/2024	14:49:25.5502] 14:49:25.5511] 14:49:25.5512] 14:49:25.5513]	EVENT-MeshRadio EVENT-MeshLink EVENT-MeshSecu EVENT-MeshLink

Conseils, astuces et recommandations

- En mettant à niveau le MAP et le RAP vers la même version d'image sur le câble, nous évitons le téléchargement d'image sur l'antenne (ce qui peut être problématique dans les environnements RF « sales »).
- Il est vivement recommandé de tester la configuration dans un environnement contrôlé avant de la déployer sur site.
- Si vous testez le pontage Ethernet avec des ordinateurs portables Windows de chaque côté, notez que pour tester le protocole ICMP entre des périphériques Windows, vous devez autoriser le protocole ICMP sur le pare-feu système. Par défaut, les périphériques Windows bloquent le protocole ICMP dans le pare-feu système.
- Si des points d'accès avec des antennes externes sont utilisés, assurez-vous de consulter le guide de déploiement pour vérifier quelles antennes sont compatibles et quel port elles sont censées être branchées.
- Afin de ponter le trafic de différents VLAN sur la liaison maillée, la fonctionnalité VLAN

Transparent doit être désactivée.

• Envisagez d'avoir un serveur syslog local aux AP, car il peut fournir des informations de débogage autrement seulement disponibles avec une connexion console.

Références

Fiche technique du contrôleur sans fil intégré Cisco sur les points d'accès Catalyst

Livre blanc sur le contrôleur sans fil intégré Cisco sur les points d'accès Catalyst (EWC)

Configuration d'une liaison maillée point à point avec pontage Ethernet sur les points d'accès Mobility Express

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.