

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

Table des matières

[Introduction](#)

[À propos de Mobility Express](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configurations de commutateurs](#)

[Réinitialisation en usine des points d'accès](#)

[Téléchargement de l'image capwap légère vers 1542-2 \(MAP\)](#)

[Téléchargement de l'image compatible Mobility Express vers AP 1542-1 \(RAP\)](#)

[Provisionnement SSID jour zéro](#)

[Configuration de maillage supplémentaire](#)

[Vérifier](#)

[Dépannage](#)

[Conseils, astuces et erreurs courantes](#)

Introduction

Ce document décrit le processus de déploiement de liaisons maillées point à point avec pontage Ethernet à l'aide du logiciel Cisco Mobility Express (ME).

À propos de Mobility Express

Ce document utilise des points d'accès extérieurs Cisco 1542. La prise en charge du maillage sur le logiciel Mobility Express pour les points d'accès intérieurs et extérieurs en mode Flex+Bridge a été introduite dans la version 8.10.

Les modèles de points d'accès suivants sont pris en charge :

- En tant qu'AP racine ME : Cisco AireOS 1542, 1562, 1815s, 3802s AP
- En tant que point d'accès maillé : Cisco AireOS 1542, 1562, 1815 et 3802 points d'accès

Mobility Express (ME) est une solution qui remplace le mode et le logiciel Autonomous AP. Il permet d'exécuter une version plus légère du logiciel Wireless LAN Controller (WLC) basé sur AireOS sur le point d'accès lui-même. Le code WLC et le code AP sont stockés dans une seule

partition de la mémoire AP. Un déploiement Mobility Express ne nécessite pas de fichier de licence, ni d'activation de licence.

Une fois que le périphérique exécutant le logiciel compatible Mobility Express est sous tension, la « partie AP » démarre d'abord. Quelques minutes plus tard, la partie contrôleur s'initialise également. Une fois qu'une session de console est établie, un périphérique compatible ME affiche l'invite du WLC. Afin d'entrer le shell AP sous-jacent, une commande `apciscoshell` peut être utilisée :

```
<#root>
```

```
(Cisco Controller) >
```

```
apciscoshell
```

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

```
User Access Verification
```

```
Username:
```

```
admin
```

```
Password:
```

```
*****
```

```
RAP>
```

```
logout
```

```
(Cisco Controller) >
```

Conditions préalables

Composants utilisés

- 2 points d'accès 1542D-E
- 2 commutateurs Cisco 3560-CX
- 2 ordinateurs portables
- 1 câble de console

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.

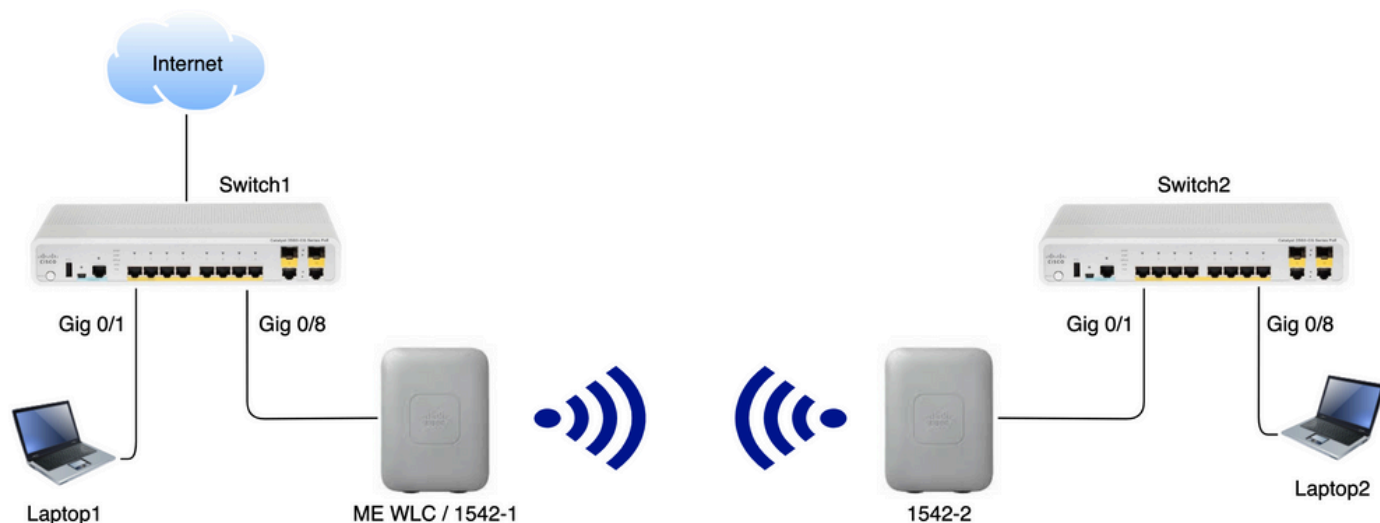
Diagramme du réseau

Tous les périphériques de ce réseau seront situés dans le sous-réseau 192.168.1.0/24. L'interface

de gestion du point d'accès Mobility Express (contrôleur) ne sera pas étiquetée, tandis que le VLAN natif sur tous les ports sera le VLAN 39. L'AP 1542-1 jouera le rôle d'un contrôleur et d'un point d'accès racine (RAP), tandis que l'AP 1542-2 jouera le rôle de point d'accès maillé (MAP). 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	192.168.1.1
Ordinateur portable 1	Commutateurs 192.168.1.100
Ordinateur portable 2	Commutateurs 192.168.1.101
WLC Mobility Express	Commutateurs 192.168.1.200
1542-1 (RAP)	Commutateurs 192.168.1.201
1542-2 (CARTE)	Commutateurs 192.168.1.202



Configuration

Configurations de commutateurs

Les ports de commutateur où les ordinateurs portables sont connectés sont configurés comme ports d'accès avec le VLAN défini sur 39 :

```
<#root>
```

```
switch1
```

```
#show run interface Gig 0/1
```

```
Current configuration : 205 bytes
```

```
!
```

```
interface GigabitEthernet0/1
```

```
description Laptop1
switchport access vlan 39
switchport mode access
end
```

<#root>

switch2

```
#show run interface Gig 0/8
```

```
Current configuration : 205 bytes
```

```
!
```

```
interface GigabitEthernet0/8
description Laptop2
switchport access vlan 39
switchport mode access
end
```

Les ports de commutateur où les AP sont connectés seront en mode trunk avec le VLAN natif défini sur 39 :

<#root>

switch1

```
#show run interface Gig 0/8
```

```
Building configuration...
```

```
!
```

```
interface GigabitEthernet0/8
description 1542-1 (RAP)
switchport mode trunk
switchport trunk native vlan 39
end
```

<#root>

switch2

```
#show run interface Gig 0/1
```

```
Building configuration...
```

```
!
```

```
interface GigabitEthernet0/1
description 1542-1 (RAP)
switchport mode trunk
switchport trunk native vlan 39
end
```

Réinitialisation en usine des points d'accès

Il est recommandé de réinitialiser les points d'accès avant de commencer un nouveau déploiement. Pour ce faire, appuyez sur le bouton mode/reset du point d'accès, branchez l'alimentation et maintenez-le enfoncé pendant plus de 20 secondes. Cela permet de s'assurer que toute la configuration précédente a été effacée. Le point d'accès sera accessible via une connexion console avec le nom d'utilisateur par défaut de Cisco et le mot de passe de Cisco (sensible à la casse).

Une réinitialisation en usine ne fait pas nécessairement revenir un point d'accès en mode léger s'il est déjà en cours d'exécution dans Mobility Express. Une étape importante consiste à déterminer si vos points d'accès exécutent une image légère ou une image Mobility Express.

Si votre point d'accès est léger, vous pouvez le convertir en Mobility Express en téléchargeant le code Mobility Express. Si le point d'accès est déjà en mode Mobility Express, vous devez suivre le processus de mise à niveau dans l'interface graphique du point d'accès/contrôleur pour changer la version du logiciel.

Exemple de show version à partir d'un point d'accès exécutant une image légère :

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

Voici un exemple d'AP déjà exécuté dans le logiciel Mobility Express :

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

Téléchargement de l'image capwap légère vers 1542-2 (MAP)

L'ordinateur portable 1 sera utilisé comme serveur TFTP. Le point d'accès 1542-2 peut être initialement connecté au port Gigabit 0/8 du commutateur 1 afin que la mise à niveau puisse être effectuée. Sur software.cisco.com, sous 1542 images légères, téléchargez 15.3.3-JJ1 (nom complet ap1g5-k9w8-tar.153-3.JK9.tar) qui correspond à l'image de la version 8.10.185. La dernière image de point d'accès léger correspondra toujours à la dernière version de ME. Placez l'image dans le dossier racine TFTP. Connectez le câble de console, connectez-vous en utilisant les identifiants par défaut (le nom d'utilisateur est Cisco et le mot de passe est également Cisco). Attribuez l'adresse IP au point d'accès et effectuez la mise à niveau à l'aide des commandes suivantes :

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

Le point d'accès effectue la mise à niveau, puis redémarre. Vérifiez que la mise à niveau a réussi à l'aide de la commande show version :

```
<#root>
```

```
MAP#
```

```
show version
```

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

Le point d'accès sera débranché du commutateur 1 et rebranché au commutateur 2.

Remarque : en mettant à niveau manuellement l'image du MAP, nous évitons que le processus de mise à niveau d'image ne se fasse par liaison radio une fois la liaison maillée établie.

Téléchargement de l'image compatible Mobility Express vers AP 1542-1 (RAP)

Sous Mobility Express 8.10.105 pour 1542 AP, nous pouvons voir 2 fichiers disponibles : .tar et .zip. Télécharger le fichier .tar

Aironet 1542I Outdoor Access Point

Release 8.10.185.0

[My Notifications](#)

[Related Links and Documentation](#)

[Release Notes for 8.10.185.0](#)

File Information

Release Date

Size

Cisco 1540 Series Mobility Express Release 8.10 Software, to be used for conversion from Lightweight Access Points only.

24-Mar-2023

60.80 MB



[AIR-AP1540-K9-ME-8-10-185-0.tar](#)

[Advisories](#)

Cisco 1540 Series Mobility Express Release 8.10 Software. Access Point image bundle, to be used for software update and/or supported access points images.

24-Mar-2023

503.27 MB



[AIR-AP1540-K9-ME-8-10-185-0.zip](#)

[Advisories](#)

Télécharger le fichier .tar

Contrairement à un WLC physique, les points d'accès ME n'ont pas assez de mémoire flash pour stocker toutes les images d'AP, donc avoir un serveur TFTP accessible à tout moment est nécessaire si vous voulez joindre d'autres AP à votre point d'accès Mobility Express. Cette étape n'est pas nécessaire si nous mettons à niveau manuellement les AP comme dans cet exemple.

Afin d'effectuer la mise à niveau, connectez la console à l'AP 1542-1, attribuez-lui une adresse IP

et effectuez la mise à niveau de l'image :

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

Une fois la mise à niveau terminée, l'AP redémarre. Peu de temps après que le point d'accès est activé, la partie contrôleur commence également à démarrer. Nous voyons bientôt le SSID de mise en service « CiscoAirProvision » de type « zero-day » diffusé.

Si vous êtes sur la console, vous pouvez voir un assistant CLI mais ne configurez pas l'AP de cette façon. L'assistant de l'interface graphique en direct est la solution.

Provisionnement SSID jour zéro

Connectez-vous au SSID « CiscoAirProvision » diffusé par le point d'accès à l'aide du mot de passe password. L'ordinateur portable obtient une adresse IP du sous-réseau 192.168.1.0/24.

Si vous ne voyez pas le SSID en cours de diffusion, il est toujours possible que le point d'accès soit dans "Mobility express CAPABLE" mais ne fonctionne pas comme mobility express. Vous devez alors vous connecter à l'interface de ligne de commande de l'AP et entrer ap type mobility-express et l'AP redémarre et diffuse le SSID de mise en service.

Il est également possible de convertir le point d'accès entre le mode local et le mode maillé en utilisant « capwap ap mode local/flex-bridge » si nécessaire, pendant cette configuration.

Ouvrez l'adresse <http://192.168.1.1> dans un navigateur Web. Cette page redirige vers l'assistant de configuration initiale. Créez un compte admin sur le contrôleur en spécifiant le nom d'utilisateur et le mot de passe admin, puis cliquez sur Démarrer.



Cisco Aironet 1542 Series Mobility Express

Welcome! Please start by creating an admin account.

The same credentials will be used for Access Point
SSH login.

Dans l'étape suivante, configurez le contrôleur en spécifiant les valeurs.

Nom du champ	Description
Nom du système	Saisissez le nom système du point d'accès Mobility Express. Exemple : MobilityExpress-WLC

Pays	Sélectionnez un pays dans la liste déroulante.
Date et heure	Sélectionnez la date et l'heure actuelles. Remarque : l'assistant tente d'importer les informations d'horloge (date et heure) à partir de l'ordinateur à l'aide de JavaScript. Il est vivement recommandé de confirmer les paramètres de l'horloge avant de continuer. Les points d'accès dépendent des paramètres d'horloge pour joindre le WLC.
Fuseau horaire	Sélectionnez le fuseau horaire actuel.
Serveur NTP	Entrez les détails du serveur NTP.
IP de gestion	Saisissez l'adresse IP de gestion. REMARQUE : Elle doit être différente de l'adresse IP attribuée au point d'accès ! Dans cet exemple, tandis que l'AP a obtenu l'IP .201, nous assignons .200 dans l'assistant de configuration. les deux seront utilisés.
Subnet Mask (Masque de sous-réseau)	Saisissez l'adresse du masque de sous-réseau.
Passerelle par défaut	Saisissez la passerelle par défaut.

Dans cette configuration, le serveur DHCP sera exécuté sur le commutateur 1, il n'est donc pas nécessaire de l'activer sur le WLC ME. Faites glisser l'option Maillage sur Activer puis cliquez sur Next.



1 Set Up Your Controller

System Name ?

Country ?

Date & Time

Timezone ?

NTP Server ?

Enable IP Management(Management Network) ?

Management IP Address ?

Subnet Mask

Default Gateway

Mesh

Enable DHCP Server (Management Network)

À l'étape suivante, créez le réseau sans fil en spécifiant les champs suivants :

Nom du champ	Description
Nom du réseau	Saisissez le nom du réseau.
Sécurité	Sélectionnez la Type de sécurité WPA2 personnel dans la liste déroulante.
Phrase De Passe	Spécifiez la clé prépartagée (PSK).
Confirmer la phrase secrète	Saisissez à nouveau et confirmez la phrase de


	passse.
--	---------


Ce réseau peut être désactivé ultérieurement.


 Cisco Aironet 1542 Series Mobility Express

- 1 Set Up Your Controller 
- >
- 2 Create Your Wireless Networks 

Employee Network

Network Name 

Security 

Passphrase 

Confirm Passphrase

Dans l'onglet Advanced Settings, laissez la Optimisation des paramètres RF désactivé et cliquez sur Suivant



Cisco Aironet 1542 Series Mobility Express

1 Set Up Your Controller 



2 Create Your Wireless Networks



3 Advanced Setting



RF Parameter Optimization

Back

Next

Une fois les paramètres confirmés, le WLC redémarre :



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

Next Steps:

After the controller is restarted, it will be accessible from the network by going to this URL -

<https://192.168.1.200>

1 Controller Settings

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

x Controller DHCP

2 Wireless Network Settings

✓ Employee Network

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

Configuration de maillage supplémentaire

Avant d'établir le lien maillé, le protocole MAP doit être converti en mode Flex-Bridge. Le RAP est déjà en mode Flex-Bridge si l'option de maillage a été activée lors de la configuration initiale. Pour ce faire, utilisez l'interface de ligne de commande :

```
<#root>
```

```
MAP#
```

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

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

Pour que le MAP rejoigne le contrôleur ME, il doit être autorisé. Sur MAP, recherchez l'adresse MAC de son interface Ethernet :

<#root>

MAP#

```
show interfaces wired 0
```

```
wired0    Link encap:Ethernet  HWaddr
```

```
00:EE:AB:83:D3:20
```

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

À partir de l'ordinateur portable 1, accédez à l'interface Web du contrôleur ME via <https://192.168.1.200>. Une fois le mode expert activé (en haut à droite), un onglet de maillage apparaît sous Wireless settings (Paramètres sans fil). Sous mac filtering, ajoutez l'adresse MAC Ethernet du MAP :

The screenshot shows the Cisco Aironet 1542 Series Mobility Express web interface. The left sidebar contains a navigation menu with 'Mesh' highlighted. The main content area is titled 'Mesh settings' and has a 'Mesh' button. Below this, there are tabs for 'General', 'Mesh RAP Downlink backhaul', 'Convergence', 'Ethernet bridging', 'Security', and 'MAC Filtering', with 'MAC Filtering' selected. The 'MAC Filtering' page includes a search bar, an 'Add MAC Address' button, a 'Refresh' button, and a table with columns for 'MAC Address', 'Type', 'Profile Name', and 'Description'. The table is currently empty, and the status shows 'Number of Blacklist:0' and 'Number of Whitelist:0'.



Add MAC Address

MAC Address

00:EE:AB:83:D3:20

Description

MAP



Type

WhiteList



Profile Name

Any WLAN/RLAN



Apply

Cancel

Remarque : tout AP suivant en mode pont ou flex-pont qui est joint au WLC ME doit également être autorisé

Une fois cette configuration effectuée, une liaison maillée doit être établie. Pour que le client filaire derrière le MAP puisse transmettre le trafic sur la liaison maillée, le pontage Ethernet doit être activé sur le MAP sous Wireless Settings > Access Points > MAP > Mesh:

Cisco Aironet 1542 Series Mobility Express

ACCESS POINTS ADMINISTRATION

Access Points 1

Q Search

Refresh

Select	Manage	Type	Location
<input type="checkbox"/>		ME Capable	default location

10 Items per page

RAP(Active Controller)

General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) Mesh

AP Role: Root

Bridge Type: Outdoor

Bridge Group Name:

Strict Matching BGN:

Daisy Chaining:

Preferred Parent:

Backhaul Interface: 802.11a/n/ac

Bridge Data Rate (Mbps): auto

Install Mapping on Radio Backhaul:

Ethernet Link Status: UP

PSK Key TimeStamp: Delete PSK

Mesh RAP Downlink backhaul

5 GHz 2.4 GHz

Ethernet Bridging

State

Acti...	Interface Name	Oper Status	Mode	VLAN Id
<input type="checkbox"/>	GigabitEthernet0	UP	Access	0

1 - 1 of 1 items

Apply Cancel

Si la liaison maillée utilise une bande de 5 GHz, elle peut être affectée par les signatures radar. Une fois que le RAP détecte un événement radar, il passe à un autre canal. Il est recommandé d'activer la notification de changement de canal afin que RAP notifie le MAP que le canal sera commuté. Cela réduit considérablement le temps de convergence, car le MAP n'a pas besoin d'analyser tous les canaux disponibles :

General Mesh RAP Downlink backhaul **Convergence** Ethernet bridging Security MAC Filtering

Mode

Channel Change Notification

Background Scanning

Vérifier

Nous pouvons vérifier que le MAP a rejoint en exécutant la commande show mesh ap summary :

```
<#root>
```

```
(Cisco Controller) >
```

```
show mesh ap summary
```

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

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

Afin de tester si la liaison passe par le trafic, nous allons essayer d'envoyer une requête ping de l'ordinateur portable 1 à l'ordinateur portable 2 :

```
<#root>
```

```
VAPEROVI:~ vaperovi$
```

```
ping 192.168.1.101
```

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

Remarque : vous ne pourrez envoyer une requête ping à l'adresse IP MAP ou RAP qu'une

fois le lien maillé établi.

Dépannage

Sur le MAP/RAP :

- debug mesh events

Sur le WLC ME :

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

Exemple d'un processus de jointure réussi observé à partir du MAP (certains messages ont été supprimés car ils ne sont pas pertinents) :

<#root>

MAP#debug mesh events

Enabled all mesh event debugs

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

[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]:

Starting regular seek

[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: channels to be sought: 100

[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[0]: start scanning on channel 1.

[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[1]: start scanning on channel 100.

[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADD_LINK to MeshLink

[*11/05/2019 18:28:06.5699] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: AWPP adjacency added channel(100)

[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADJ_FOUND to Channel Manager 0x64

[*11/05/2019 18:28:06.5699] EVENT-MeshChannelMgr[1]: Adj found on channel 100.

[*11/05/2019 18:28:07.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:08.5499] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[0]: continue scanning on channel 2.

[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:09.0399] EVENT-MeshChannelMgr[1]: continue scanning on channel 104.

[*11/05/2019 18:28:09.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:10.7899] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:11.0199] EVENT-MeshChannelMgr[0]: continue scanning on channel 3.

[*11/05/2019 18:28:11.0399] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:11.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:11.3099] EVENT-MeshChannelMgr[1]: continue scanning on channel 108.

[*11/05/2019 18:28:13.0199] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:13.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:13.2499] EVENT-MeshChannelMgr[0]: continue scanning on channel 4.

[*11/05/2019 18:28:13.3099] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:13.5599] EVENT-MeshChannelMgr[1]: continue scanning on channel 112.

[*11/05/2019 18:28:15.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:15.2499] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:15.5099] EVENT-MeshChannelMgr[0]: continue scanning on channel 5.

[*11/05/2019 18:28:15.5599] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:15.8099] EVENT-MeshChannelMgr[1]: continue scanning on channel 116.

```
.
..
.
[*11/05/2019 18:28:35.7999] EVENT-MeshChannelMgr[1]: Mesh BH requests to switch to channel 100, width 20 MHz
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: abort scanning.
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: Set to configured channel 1, width 20 MHz
[*11/05/2019 18:28:36.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:37.5099] EVENT-MeshRadioBackhaul[1]: Sending LINK_UP to MeshLink
[*11/05/2019 18:28:37.5099] CRIT-MeshLink: Set Root port Mac: D4:78:9B:7B:DF:11 BH Id: 2 Port:54 Device:DEV
[*11/05/2019 18:28:37.5099] EVENT-MeshLink: Sending NOTIFY_SECURITY_LINK_UP to MeshSecurity
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Intermodule message NOTIFY_SECURITY_LINK_UP
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Start full auth to parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: start_auth, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: Opening wpas socket
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: start socket to WPA supplicant
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: MeshSecurity::wpas_init my_mac=00:EE:AB:83:D3:20, user=
[*11/05/2019 18:28:38.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6799] EVENT-MeshSecurity: Generating pmk r0 as child(D4:E8:80:A0:D0:B1)
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: pmk(eap) r0 generated for D4:78:9B:7B:DF:11: 5309c9fb 0
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: EAP authentication is done, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Child(D4:E8:80:A0:D0:B1) generating keys to Parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_AUTH_RSP, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mac: D4:78:9B:7B:DF:11 bh_id:2 auth_result: 1
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Sending NOTIFY_SECURITY_DONE to Control
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mesh Link:Security success on parent :D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Uplink Auth done: Mac: D4:78:9B:7B:DF:11 Port:54 Device:DEV
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_REASSOC_RSP, Parent(D4:78:9B:7B:DF:11)
```

state changed to STATE_RUN

```
[*11/05/2019 18:28:40.6899] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: auth_complete Result(PASS)
```

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

Discovery Response from 192.168.1.200

```
.
..
.
Adding Ipv4 AP manager 192.168.1.200 to least load
[*11/05/2019 18:28:55.1299] WLC: ME ApMgr count 1, ipTransportTried 0, prefer-mode 1, isIpv4orIpv6Static 1
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load 1, AP Mgr Count 1
[*11/05/2019 18:28:55.1399] capwapSetTransportAddr returning: index 0, apMgrCount 0
[*11/05/2019 18:28:55.1399]
[*11/06/2019 13:23:36.0000]
[*11/06/2019 13:23:36.0000] CAPWAP State: DTLS Setup
[*11/06/2019 13:23:36.0000] DTLS connection created successfully local_ip: 192.168.1.202 local_port: 5246
[*11/06/2019 13:23:36.8599] Dtls Session Established with the AC 192.168.1.200, port 5246
```

```

[*11/06/2019 13:23:36.8599]
[*11/06/2019 13:23:36.8599] CAPWAP State: Join
[*11/06/2019 13:23:36.8699] Sending Join request to 192.168.1.200 through port 5248
[*11/06/2019 13:23:36.8899] Join Response from 192.168.1.200
[*11/06/2019 13:23:36.8899] AC accepted join request with result code: 0
.
..
.
CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:37.4999] Starting Post Join timer
[*11/06/2019 13:23:37.4999]
[*11/06/2019 13:23:37.4999] CAPWAP State: Image Data
[*11/06/2019 13:23:37.5099] AP image version 8.10.105.0 backup 8.8.125.0, Controller 8.10.105.0
[*11/06/2019 13:23:37.5099] Version is the same, do not need update.
[*11/06/2019 13:23:37.6399] do NO_UPGRADE, part1 is active part
[*11/06/2019 13:23:37.6499]
[*11/06/2019 13:23:37.6499] CAPWAP State: Configure
[*11/06/2019 13:23:37.6599] DOT11_CFG[0] Radio Mode is changed from Remote Bridge to Remote Bridge
.
..
.
[*11/06/2019 13:23:38.7799] DOT11_CFG[0]: Starting radio 0
[*11/06/2019 13:23:38.7799] DOT11_CFG[1]: Starting radio 1
[*11/06/2019 13:23:38.8899] EVENT-MeshRadioBackhaul[0]: BH_RATE_AUTO
[*11/06/2019 13:23:38.8899] EVENT-MeshSecurity: Intermodule message LSC_MODE_CHANGE
[*11/06/2019 13:23:38.9099] CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:38.9999] Setting Prefer-mode IPv4
[*11/06/2019 13:23:39.0499]
[*11/06/2019 13:23:39.0499]

CAPWAP State: Run

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

AP has joined controller ME

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

Flexconnect Switching to Connected Mode

!
```

Conseils, astuces et erreurs courantes

- 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 »).
- L'augmentation de la largeur de canal de la liaison de liaison 5 GHz peut entraîner une diminution du SNR et des fausses détections radar (principalement sur 80 MHz et 160 MHz).
- La connectivité des liaisons maillées ne doit pas être testée en envoyant une requête ping à MAP ou RAP. Ils ne pourront pas envoyer de requête ping une fois que le maillage sera

activé.

- Il est vivement recommandé de tester la configuration dans un environnement contrôlé avant de la déployer sur site.
- 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 doivent 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.

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.