

# Configuración del Link de Malla Punto a Punto con Puente Ethernet en los AP de Mobility Express

## Contenido

[Introducción](#)

[Acerca de Mobility Express](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuración](#)

[Configuraciones de switch](#)

[Restablecimiento de fábrica de los puntos de acceso](#)

[Descarga de la imagen capwap ligera a 1542-2 \(MAP\)](#)

[Descarga de imágenes compatibles con Mobility Express en AP 1542-1 \(RAP\)](#)

[Aprovisionamiento de SSID de día cero](#)

[Configuración de malla adicional](#)

[Verificación](#)

[Resolución de problemas](#)

[Consejos, trucos y errores comunes](#)

## Introducción

Este documento describe el proceso de implementación de links de malla punto a punto con Ethernet Bridging usando el software Cisco Mobility Express (ME).

## Acerca de Mobility Express

Este documento utiliza puntos de acceso exteriores Cisco 1542. La compatibilidad de malla en el software Mobility Express para puntos de acceso interiores y exteriores en el modo Flex+Bridge se introdujo en la versión 8.10.

Se soportan los siguientes modelos de AP:

- Como punto de acceso raíz ME: puntos de acceso Cisco AireOS 1542, 1562, 1815s, 3802s
- Como punto de acceso de malla: puntos de acceso Cisco AireOS 1542, 1562, 1815s, 3802s

Mobility Express (ME) es una solución que reemplaza el modo y el software de AP autónomo. Permite ejecutar una versión más ligera del software Wireless LAN Controller (WLC) basado en AireOS en el propio punto de acceso. Tanto el código WLC como el AP se almacenan dentro de

una sola partición de la memoria AP. Una implementación de Mobility Express no requiere un archivo de licencia ni activación de licencia.

Una vez que se enciende el dispositivo que ejecuta el software compatible con Mobility Express, se inicia primero la "parte AP". Unos minutos más tarde, la parte del controlador también se inicializa. Una vez que se establece una sesión de consola, un dispositivo con capacidad ME mostrará el mensaje del WLC. Para ingresar el shell AP subyacente, se puede utilizar un comando `apciscoshell`:

```
<#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) >
```

## Prerequisites

### Componentes Utilizados

- 2 puntos de acceso 1542D-E
- 2 switches Cisco 3560-CX
- 2 portátiles
- 1 cable de consola

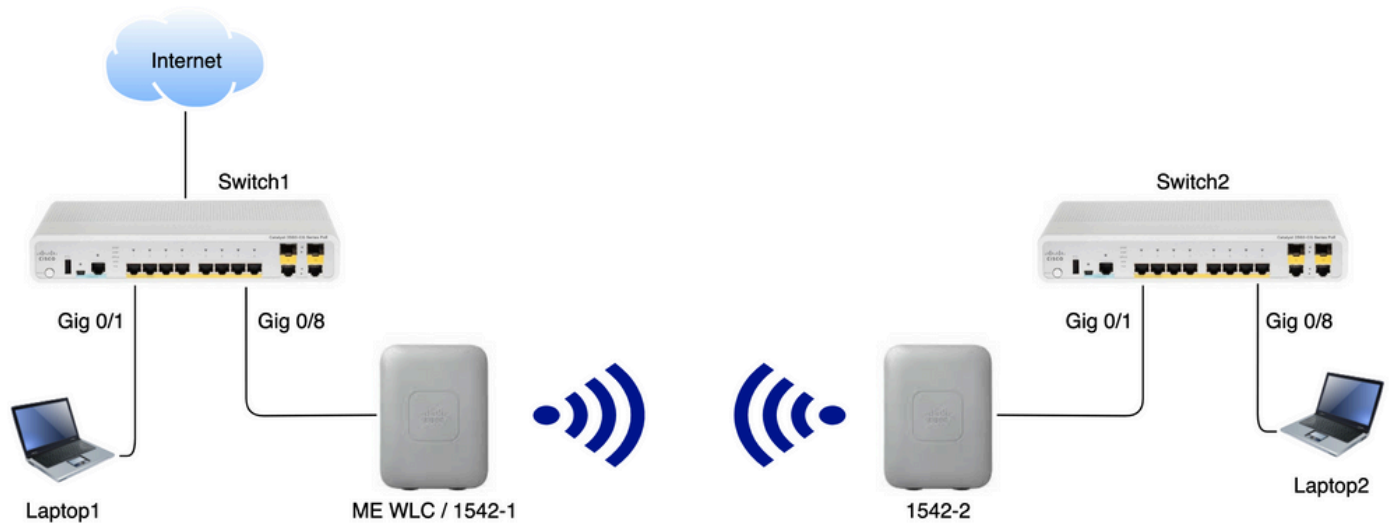
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Diagrama de la red

Todos los dispositivos de esta red se ubicarán dentro de la subred 192.168.1.0/24. El AP (controlador) de Mobility Express no tendrá su interfaz de administración etiquetada, mientras que la VLAN nativa en todos los puertos será VLAN 39. El AP 1542-1 asumirá la función de controlador y punto de acceso raíz (RAP), mientras que el AP 1542-2 asumirá la función de punto de acceso de malla (MAP). Esta tabla contiene las direcciones IP de todos los dispositivos de la red:

Nota: Etiquetar la interfaz de administración puede causar problemas con el AP que se une al proceso interno del WLC. Si decide etiquetar la interfaz de administración, asegúrese de que la parte de la infraestructura cableada esté configurada en consecuencia.

Dispositivo	IP Address
Gateway predeterminado	192.168.1.1
Portátil 1	192.168.1.100
Portátil 2	192.168.1.101
WLC de Mobility Express	192.168.1.200
1542-1 (RAP)	192.168.1.201
1542-2 (MAP)	192.168.1.202



## Configuración

### Configuraciones de switch

Los puertos de switch a los que se conectan los portátiles se configuran como puertos de acceso con la VLAN establecida en 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
```

Los puertos del switch donde se conectan los AP estarán en modo trunk con la VLAN nativa configurada en 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
```

## Restablecimiento de fábrica de los puntos de acceso

Se recomienda realizar un restablecimiento de fábrica de los AP antes de iniciar una nueva implementación. Esto se puede hacer presionando el botón de modo/reset en el AP, enchufando el poder adentro y continuando mantenerlo por más de 20 segundos. Esto garantizará que se haya borrado toda la configuración anterior. Se podrá acceder al AP a través de una conexión de consola con el nombre de usuario predeterminado de Cisco y la contraseña de Cisco (distingue entre mayúsculas y minúsculas).

Un restablecimiento de fábrica no necesariamente mueve un AP de nuevo al modo ligero si ya se está ejecutando en Mobility Express. Un paso importante es identificar si sus AP están ejecutando una imagen ligera o una imagen de Mobility Express.

Si su AP es ligero, puede convertirlo a Mobility Express descargando el código de Mobility Express. Si el AP ya está en el modo express de la movilidad, usted tiene que seguir el proceso de actualización en la GUI del punto de acceso/controlador para cambiar la versión del software.

Ejemplo de un show version de AP que ejecuta una imagen ligera :

```
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
```

Este es un ejemplo de AP que ya se ejecuta en el software 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
```

## Descarga de la imagen capwap ligera a 1542-2 (MAP)

El portátil 1 se utilizará como servidor TFTP. El AP 1542-2 se puede conectar inicialmente al puerto 0/8 del Switch 1 Gig sólo para que se pueda realizar la actualización. En [software.cisco.com](http://software.cisco.com), bajo 1542 lightweight images, descargue 15.3.3-JJ1 (nombre completo ap1g5-k9w8-tar.153-3.JK9.tar) que corresponde a la imagen de la versión 8.10.185. La última imagen ligera de AP siempre corresponderá a la última versión de ME.

Coloque la imagen en la carpeta raíz TFTP. Conecte el cable de la consola e inicie sesión con las credenciales predeterminadas (el nombre de usuario es Cisco y la contraseña es también Cisco). Asigne la dirección IP al AP y realice la actualización con los siguientes comandos:

```
#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
```

El AP realizará la actualización y luego se reiniciará. Confirme que la actualización haya sido exitosa usando el comando 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
```

El AP se desconectará del Switch 1 y se conectará nuevamente al Switch 2.

---

Nota: Al actualizar la imagen del MAP manualmente, evitamos que el proceso de actualización de la imagen se realice por el aire una vez que se establece el link de malla.

---

## Descarga de imágenes compatibles con Mobility Express en AP 1542-1 (RAP)

En las versiones de Mobility Express 8.10.105 para 1542 AP, podemos ver 2 archivos disponibles: .tar y .zip. Descargue el archivo .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. <a href="#">AIR-AP1540-K9-ME-8-10-185-0.tar</a> <a href="#">Advisories</a>	24-Mar-2023	60.80 MB	
Cisco 1540 Series Mobility Express Release 8.10 Software. Access Point image bundle, to be used for software update and/or supported access points images. <a href="#">AIR-AP1540-K9-ME-8-10-185-0.zip</a> <a href="#">Advisories</a>	24-Mar-2023	503.27 MB	

Descargue el archivo .tar

A diferencia de un WLC físico, los puntos de acceso ME no tienen suficiente memoria flash para almacenar todas las imágenes AP, por lo que tener un servidor TFTP accesible en todo momento es necesario si desea unir más AP a su punto de acceso Mobility Express. Este paso no es necesario si actualizamos manualmente los AP como en este ejemplo.

Para realizar la actualización, conecte la consola al AP 1542-1, asígnele una dirección IP y realice la actualización de la imagen:

```
#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
```

Una vez que se termina la actualización, el AP se reinicia. Poco después de que el AP esté activo, la parte del controlador comienza a arrancar también. Pronto veremos que se emite el SSID de aprovisionamiento de día cero "CiscoAirProvisioning".

Si está en la consola, puede ver un asistente CLI pero no configure el AP de esa manera. El asistente de GUI por aire es el camino a seguir.

## Aprovisionamiento de SSID de día cero

Conéctese al SSID "CiscoAirProvisioning" transmitido por el AP usando la contraseña password. El portátil obtiene una dirección IP de la subred 192.168.1.0/24.

En caso de que no vea el SSID que se transmite, es posible que el AP esté en "Mobility Express CAPABLE" pero no se esté ejecutando como Mobility Express. A continuación, tendría que conectarse a la CLI del AP e ingresar el tipo de ap mobility-express y el AP se reinicia y transmite el SSID de aprovisionamiento.

También es posible convertir el AP entre el modo local y el modo de malla usando "capwap ap ap mode local/flex-bridge" si es necesario, durante esta configuración.

Abra la dirección <http://192.168.1.1> en un navegador web. Esta página redirige al asistente de configuración inicial. Cree una cuenta de administrador en el controlador especificando el nombre de usuario y la contraseña del administrador y luego haga clic en Start.



# 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.

En el siguiente paso, configure el controlador especificando los valores.

Nombre del campo	Descripción
Nombre del sistema	Introduzca el nombre del sistema para el AP de Mobility Express. Ejemplo: MobilityExpress-WLC
País	Seleccione un país de la lista desplegable.



Fecha y hora	<p>Elija la fecha y la hora actuales.</p> <p>Nota: El asistente intenta importar la información del reloj (fecha y hora) del equipo mediante JavaScript. Se recomienda encarecidamente que confirme la configuración del reloj antes de continuar. Los puntos de acceso dependen de la configuración del reloj para unirse al WLC.</p>
Zona horaria	Elija la zona horaria actual.
Servidor NTP	Introduzca los detalles del servidor NTP.
IP de administración	Introduzca la dirección IP de gestión. NOTA: Debe ser diferente de la IP asignada al punto de acceso. En este ejemplo, mientras que el AP obtuvo la IP .201, asignamos .200 en el asistente de configuración. se utilizarán ambos.
Máscara de subnet	Introduzca la dirección de máscara de subred.
Gateway predeterminado	Introduzca la puerta de enlace predeterminada.

En esta configuración, el servidor DHCP se ejecutará en el switch 1, por lo que no es necesario activarlo en el WLC ME. Deslice la opción Malla hasta Habilitar y haga clic en 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)

En el paso siguiente, cree la red inalámbrica especificando los campos siguientes:

Nombre del campo	Descripción
Nombre de red	Introduzca el nombre de la red.
Security	Elija el Tipo de seguridad WPA2 Personal de la lista desplegable.
Frase de contraseña	Especifique la clave precompartida (PSK).
Confirmar frase de contraseña	Vuelva a introducir y confirme la frase de paso.

Esta red se puede desactivar más adelante.

 Cisco Aironet 1542 Series Mobility Express

1 Set Up Your Controller 


>


2 Create Your Wireless Networks


∨

---

### Employee Network

Network Name  

Security  

Passphrase  

Confirm Passphrase

En la ficha Configuración avanzada, deje el Optimización de parámetros de RF deslizador desactivado y haga clic en Next



# Cisco Aironet 1542 Series Mobility Express

1 Set Up Your Controller 



2 Create Your Wireless Networks



3 Advanced Setting



RF Parameter Optimization

Back

Next

Una vez que se confirman los ajustes, el WLC se reiniciará:



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:	*****

## Configuración de malla adicional

Antes de establecer el link de malla, MAP debe convertirse al modo flex-bridge. El RAP ya estará en modo flex-bridge si la opción de malla se ha habilitado durante la configuración inicial. Esto se puede hacer desde la CLI:

```
<#root>
```

```
MAP#
```

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

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

Para que MAP top se una al controlador ME, debe estar autorizado. En MAP, busque la dirección MAC de su interfaz 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)
```

Desde el portátil 1, acceda a la interfaz web del controlador ME a través de <https://192.168.1.200>. Una vez activado el modo experto (esquina superior derecha), aparecerá una pestaña de malla en Wireless settings (Parámetros inalámbricos). En filtrado de MAC, agregue la dirección MAC de Ethernet del MAP:

The screenshot shows the Cisco Aironet 1542 Series Mobility Express web interface. The left sidebar contains a navigation menu with 'Monitoring', 'Wireless Settings', 'WLANs', 'Access Points', 'Access Points Groups', 'WLAN Users', 'Guest WLANs', 'DHCP Server', 'Mesh', 'Management', 'Services', and 'Advanced'. The 'Mesh' option is highlighted with a red box. 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 and highlighted by a red box. 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 currently 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

Nota: Cualquier AP subsiguiente en el modo bridge o flex-bridge que se esté uniendo al WLC ME también debe ser autorizado

Después de configurar esto, se debe establecer un link de malla. Para que el cliente por cable detrás del MAP pase el tráfico sobre el link de malla, el puente Ethernet debe estar habilitado en el MAP en 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

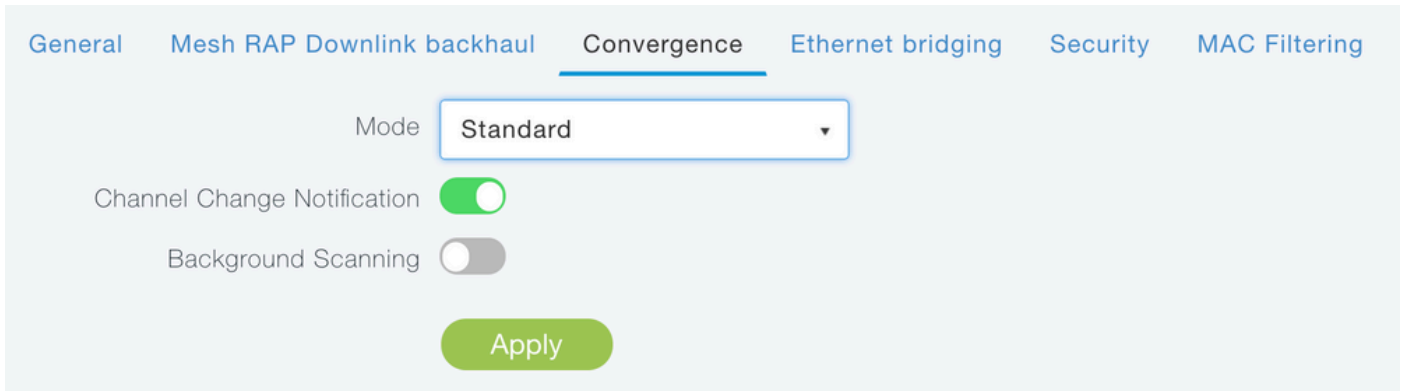
Acti...	Interface Name	Oper Status	Mode	VLAN Id
<input type="checkbox"/>	GigabitEthernet0	UP	Access	0

1 - 1 of 1 items

Apply Cancel

Si el link de malla utiliza una banda de 5 GHz, puede verse afectado por las firmas de radar. Una vez que el RAP detecte un evento de radar, cambiará a otro canal. Se recomienda habilitar la Notificación de cambio de canal para que RAP notifique al MAP que el canal será conmutado. Esto reduce significativamente el tiempo de convergencia ya que MAP no tiene que escanear todos los canales disponibles:





## Verificación

Podemos verificar que el MAP se haya unido ejecutando el comando 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
```

Para probar si el link está pasando a través del tráfico, intentaremos hacer ping desde el Laptop 1 al Laptop 2:

```
<#root>
```

```
VAPEROVI:~ vaperovi$
```

```
ping 192.168.1.101
```

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

---

Nota: Podrá hacer ping a la dirección IP de MAP o RAP sólo una vez que se haya

---

---

establecido el link de malla.

---

## Resolución de problemas

En el MAPA/RAP:

- debug mesh events

En ME WLC:

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

Ejemplo de un proceso de unión exitoso observado desde MAP (algunos mensajes han sido censurados ya que no son relevantes):

<#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

!
```

## Consejos, trucos y errores comunes

- Al actualizar el MAP y el RAP a la misma versión de imagen a través del cable, evitamos que la descarga de imágenes se realice por el aire (lo que puede resultar problemático en entornos de RF "sucios").
- El aumento del ancho del canal del enlace de red de retorno de 5 GHz puede provocar una reducción del SNR y falsas detecciones de radares (principalmente en 80 MHz y 160 MHz).
- La conectividad del link de malla no se debe probar haciendo ping en MAP o RAP. No se podrán realizar ping una vez que aparezca el enlace de malla.

- Se recomienda encarecidamente probar la configuración en un entorno controlado antes de implementarla in situ.
- Si se utilizan AP con antenas externas, asegúrese de consultar la guía de implementación para verificar qué antenas son compatibles y qué puerto deben conectarse.
- Para unir el tráfico de diferentes VLAN sobre el link de malla, la función VLAN Transparent debe ser inhabilitada.
- Considere la posibilidad de tener un servidor syslog local para los AP, ya que puede proporcionar información de depuración que, de lo contrario, sólo está disponible con una conexión de consola.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).