Configurazione del collegamento Mesh point-to-point con Ethernet Bridging sui Mobility Express AP

Sommario

Introduzione

Questo articolo spiega il processo di installazione di collegamenti mesh point-to-point con Bridging Ethernet utilizzando il software Cisco Mobility Express (ME) sui punti di accesso esterni Cisco 1542. Il supporto Mesh sul software Mobility Express per i punti di accesso interni ed esterni in modalità Flex+Bridge è stato introdotto nella versione 8.10.

Sono supportati i seguenti modelli AP:

- **Come punto di accesso principale ME:Cisco AireOS 1542, 1562, 1815s, 3802s AP**
- **Come punto di accesso mesh: Cisco AireOS 1542, 1562, 1815s, 3802s AP**

Informazioni su Mobility Express

Mobility Express (ME) è una soluzione che sostituisce la modalità e il software Autonomous AP. Consente di eseguire una versione più leggera del software Wireless LAN Controller (WLC) basato su AireOS sul punto di accesso stesso. Sia il codice WLC che il codice AP vengono archiviati in una singola partizione della memoria AP. Un'implementazione di Mobility Express non richiede un file di licenza né l'attivazione della licenza.

Una volta acceso il dispositivo su cui è in esecuzione il software Mobility Express, la "parte AP" si avvia. Alcuni minuti dopo verrà inizializzata anche la parte controller. Una volta stabilita una

sessione console, un dispositivo compatibile con ME visualizzerà il prompt del WLC. Per immettere la shell AP sottostante, è possibile utilizzare un comando apciscoshell:

```
(Cisco Controller) >apciscoshell
!!Warning!!: You are entering ap shell. This will stop you from establishing new telnet/SSH/Web
sessions to controller.
 Also the exsisting sessions will be suspended till you exit the ap shell.
 To exit the ap shell, use 'logout'

User Access Verification
Username: admin
Password: ********
RAP>logout
(Cisco Controller) >
```

Prerequisiti

Componenti usati

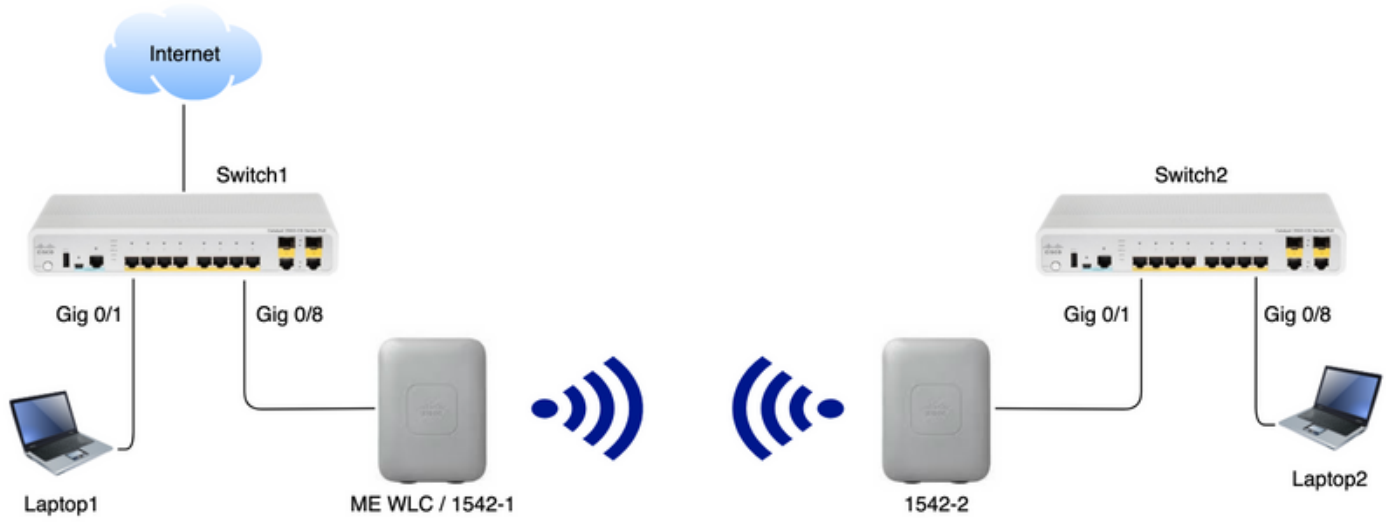
- 2 access point 1542D-E
- 2 switch Cisco 3560-CX
- 2 notebook
- Cavo console 1x

Esempio di rete

Tutti i dispositivi della rete si troveranno nella subnet 192.168.1.0/24. L'interfaccia di gestione del Mobility Express AP (controller) sarà senza tag, mentre la VLAN nativa su tutte le porte sarà la VLAN 39. L'AP 1542-1 assumerà il ruolo di controller e di punto di accesso radice (RAP), mentre l'AP 1542-2 assumerà il ruolo di punto di accesso mesh (MAP). La tabella seguente contiene gli indirizzi IP di tutti i dispositivi della rete:

> **Nota**: l'aggiunta di tag all'interfaccia di gestione può causare problemi all'access point che si unisce al processo WLC interno. Se si decide di contrassegnare l'interfaccia di gestione, verificare che la parte dell'infrastruttura cablata sia configurata di conseguenza.

Sul dispositivo bootflash o slot0:	Indirizzo IP
Gateway predefinito	192.168.1.1
Notebook 1	192.168.1.100
Notebook 2	192.168.1.101
Mobility Express WLC	192.168.1.200
1542-1 (MAPPA)	192.168.1.201
1542-2 (RAP)	192.168.1.202



Configurazione

Configurazioni switch

Le porte degli switch a cui i notebook sono collegati sono configurate come porte di accesso con la VLAN impostata su 39:

```
Switch1#show run interface Gig 0/1

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

```
Switch2#show run interface Gig 0/8

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

Le porte degli switch a cui sono connessi i punti di accesso saranno in modalità trunk con la VLAN nativa impostata su 39:

```
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
```

```
Switch2#show run interface Gig 0/1
Building configuration...
!
interface GigabitEthernet0/1
 description 1542-1 (MAP)
 switchport mode trunk
 switchport trunk native vlan 39
end
```

Ripristino dei punti di accesso in fabbrica

Si consiglia di eseguire un reset di fabbrica degli access point prima di avviare una nuova distribuzione. A tale scopo, premere il pulsante mode/reset sull'access point, collegare l'alimentazione e continuare a mantenerla in posizione per più di 20 secondi. In questo modo, verrà garantita la cancellazione di tutte le configurazioni precedenti. L'access point sarà accessibile tramite una connessione console con il nome utente predefinito Cisco e la password Cisco (con distinzione tra maiuscole e minuscole).

Download dell'immagine del capwap leggero su 1542-2 (MAP)

Il notebook 1 verrà utilizzato come server TFTP. AP 1542-2 può essere inizialmente collegato alla porta dello switch 1 Gig 0/8 solo in modo da poter eseguire l'aggiornamento. Su software.cisco.com, sotto 1542 lightweight images, scaricare la versione 15.3.3-JJ1 (nome completo *ap1g5-k9w8-tar.153-3.JK.tar*) corrispondente all'immagine della versione 8.10.105. L'ultima immagine Lightweight AP corrisponderà sempre all'ultima versione di ME. Posizionare l'immagine nella cartella radice TFTP. Collegare il cavo della console, eseguire il login utilizzando le credenziali predefinite (il nome utente è Cisco e la password è anche Cisco). Assegnare l'indirizzo IP all'access point ed eseguire l'aggiornamento utilizzando i seguenti comandi:

```
#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.JK.tar
```

AP eseguirà l'aggiornamento e quindi riavvierà il sistema. Verificare che l'aggiornamento sia stato completato con il comando show version:

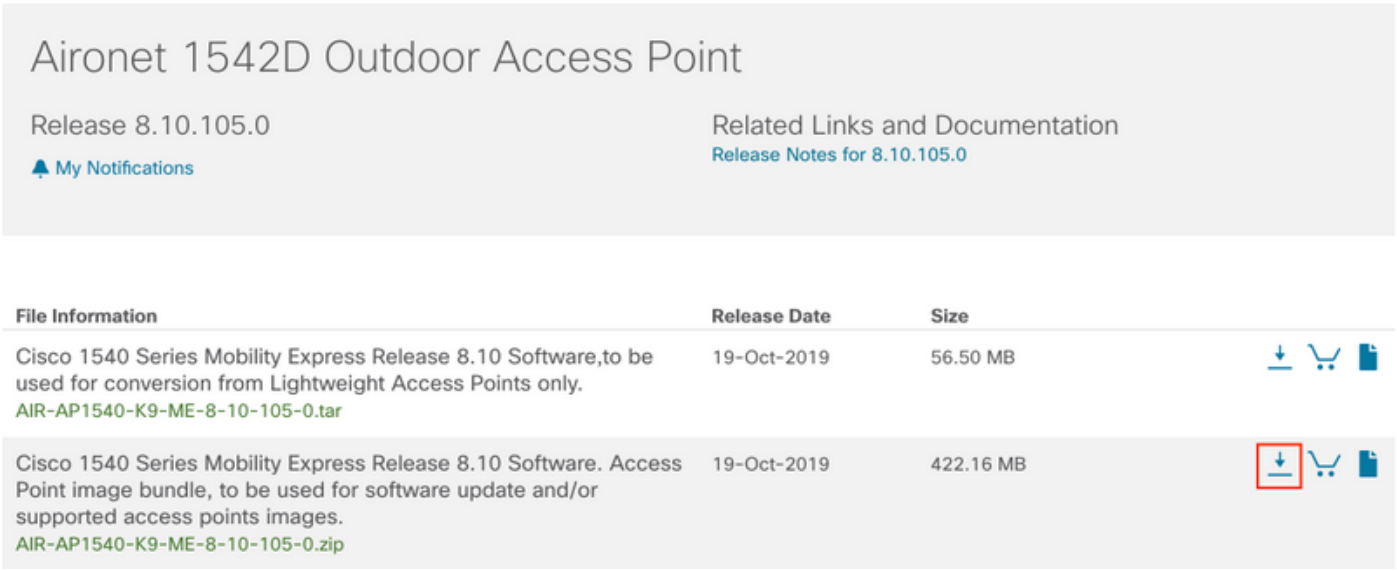
```
RAP#show version
.
..
AP Running Image     : 8.10.105.0
Primary Boot Image   : 8.10.105.0
Backup Boot Image    : 8.8.125.0
```

L'access point verrà scollegato dallo switch 1 e ricollegato allo switch 2.

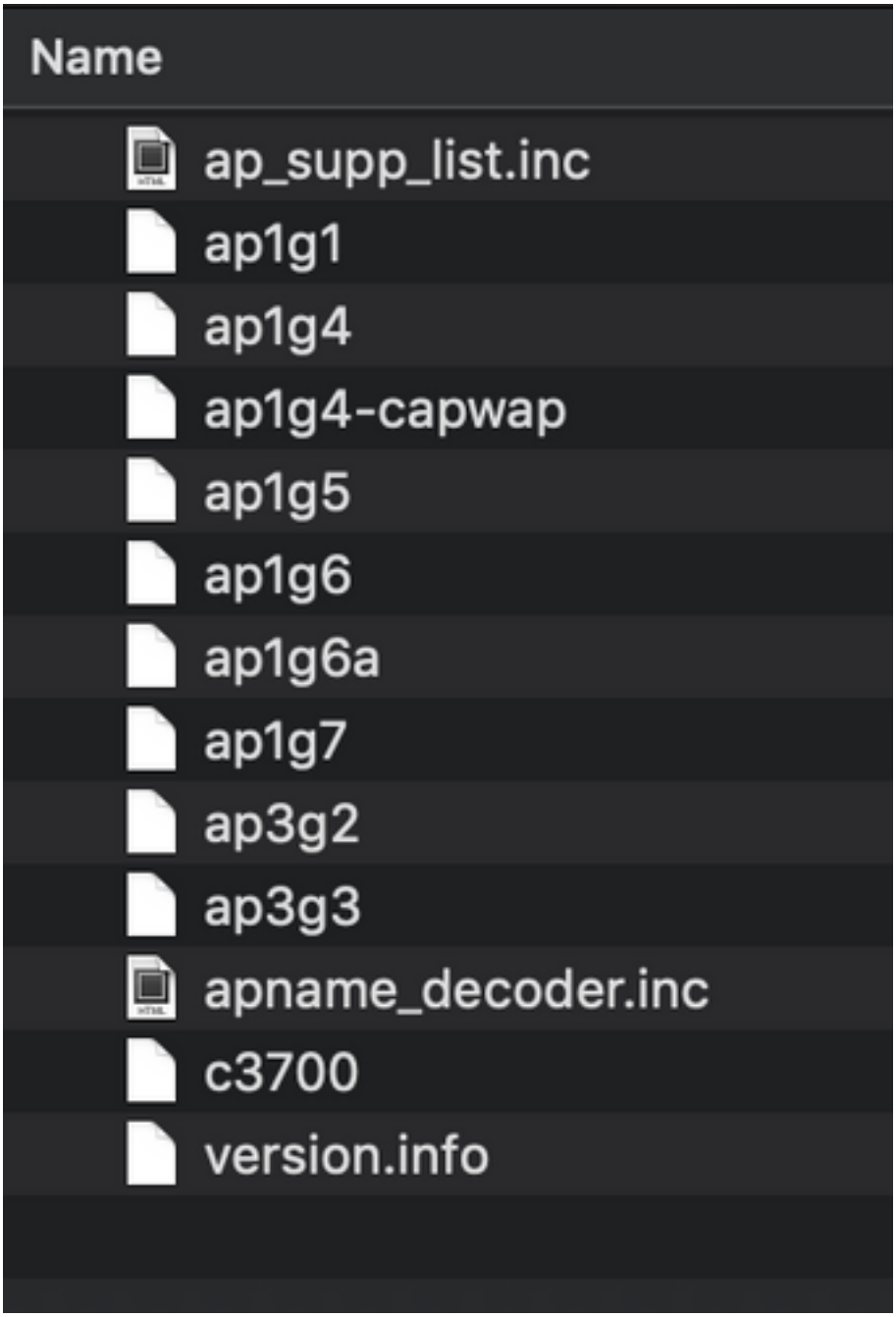
> **Nota:** Aggiornando manualmente l'immagine del MAP, si evita che il processo di aggiornamento dell'immagine avvenga via etere una volta stabilito il collegamento mesh.

Download dell'immagine compatibile con Mobility Express in AP 1542-1 (RAP)

In Mobility Express 8.10.105 release per 1542 AP, sono disponibili due file: .tar e .zip. Scarica il bundle .zip ed estrailo.



A differenza di un WLC fisico, i punti di accesso ME non hanno memoria flash sufficiente per memorizzare tutte le immagini AP, quindi è necessario avere un server TFTP accessibile in ogni momento. Estrarre il file zip e copiarne il contenuto nella directory principale del server TFTP. Il file estratto conterrà più immagini PA:



Il file di testo *apname_decoder.inc* contiene tutti i nomi corrispondenti dell'immagine PA:

```
/*AP Models and their Associated Image Names*/
AP1850(ap1g4)
AP1830(ap1g4)
AP4800(ap3g3)
AP3800(ap3g3)
AP2800(ap3g3)
AP1560(ap3g3)
IW6300(ap3g3)
ESW6300(ap3g3)
AP1815i(ap1g5)
AP1815w(ap1g5)
AP1815m(ap1g5)
AP1540(ap1g5)      <<<<<<< This one will be used for upgrade
AP1840(ap1g5)
```

Per eseguire l'aggiornamento, collegare la console all'access point 1542-1, assegnargli un indirizzo IP ed eseguire l'aggiornamento dell'immagine:

```
#capwap ap ip 192.168.1.201 255.255.255.0 192.168.1.1
#ap-type mobility-express tftp://192.16.1.100/ap1g5
```

Al termine dell'aggiornamento, l'access point verrà riavviato. Subito dopo l'accensione dell'access point, anche la parte controller verrà avviata. Presto vedremo il provisioning SSID "CiscoAirProvision" a giorno zero trasmesso.

Verificare che l'aggiornamento sia stato completato con il comando show version:

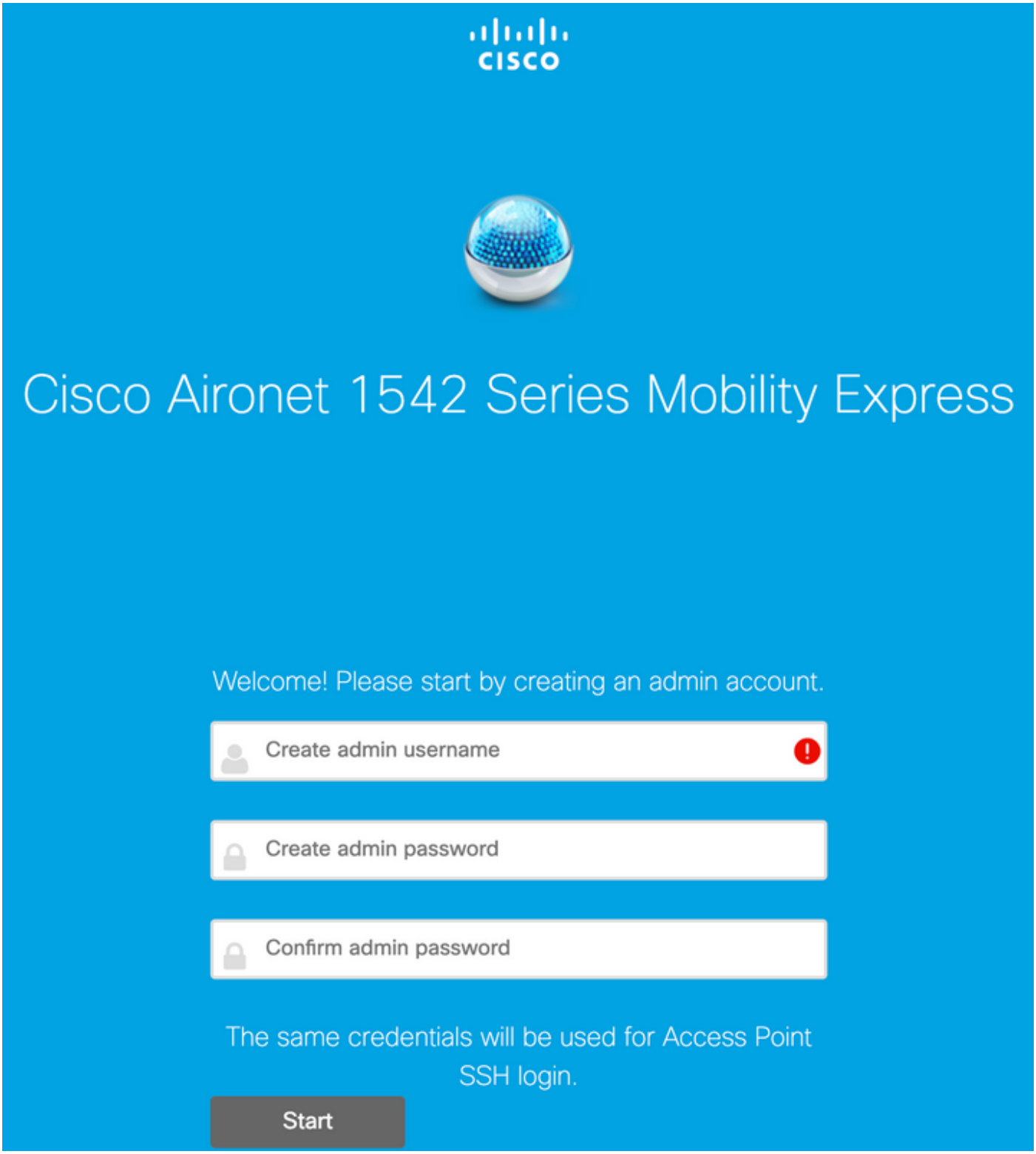
```
RAP#show version
.
..

AP Running Image     : 8.10.105.0
Primary Boot Image   : 8.10.105.0
Backup Boot Image    : 8.10.105.0
.
..
.
AP Image type    : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
```

Provisioning SSID con zero giorni

Connettersi al SSID "CiscoAirProvision" trasmesso dall'access point utilizzando la **password**. Il notebook riceverà un indirizzo IP dalla subnet 192.168.1.0/24.

Nel caso in cui il SSID non venga trasmesso, è possibile che l'access point sia in "Mobility express CAPABLE" ma non in esecuzione come mobility express. A questo punto, è necessario connettersi alla CLI dell'access point e immettere **il tipo di access point mobility-express** e l'access point deve riavviare e trasmettere il provisioning SSID.

Aprire l'indirizzo **http://192.168.1.1** in un browser Web. Questa pagina reindirizza alla configurazione guidata iniziale. Creare un account amministratore nel controller specificando il nome utente e la password dell'amministratore, quindi fare clic su Avvia.

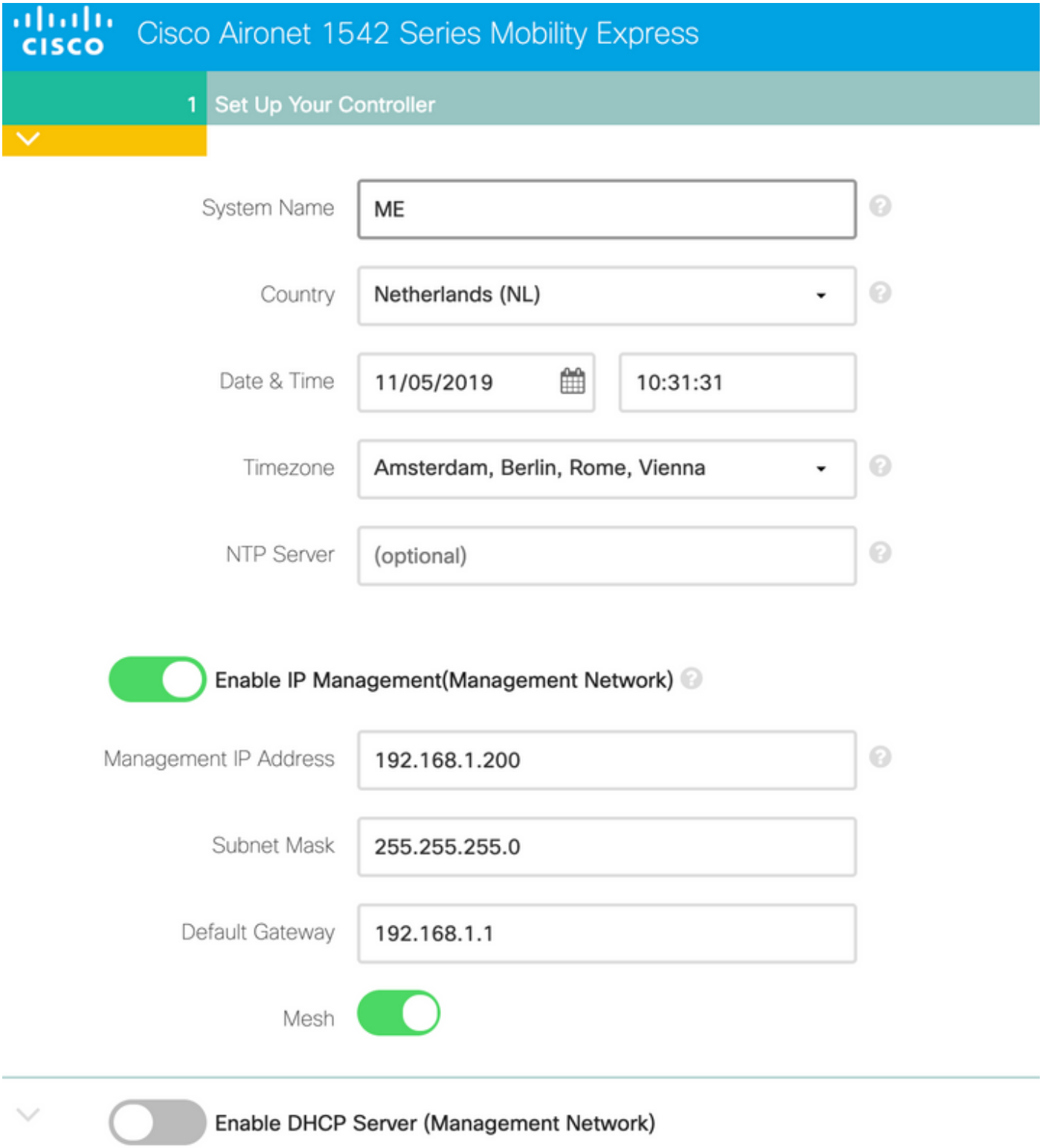


Nel passaggio successivo impostare il controller specificando i valori.

Nome campo	Descrizione
Nome sistema	Immettere il nome del sistema per il punto di acc Mobility Express. Esempio: Mobility Express-WL
Paese	Scegliere un paese dall'elenco a discesa.
Data e ora	Scegliere la data e l'ora correnti. **Nota: la procedura guidata tenta di importare le informazioni sull'orologio (data e ora) dal comput utilizzando JavaScript. Si consiglia di confermare**

	impostazioni dell'orologio prima di continuare. Gl access point dipendono dalle impostazioni dell'o per il collegamento al WLC.
Fuso orario	Scegliere il fuso orario corrente.
Server NTP	Immettere i dettagli del server NTP.
IP di gestione	Immettere l'indirizzo IP di gestione. NOTA: Deve diverso dall'indirizzo IP assegnato al punto di ac In questo esempio, mentre l'access point ha otte .201 IP, viene assegnato .200 nella configurazio guidata. verranno utilizzati entrambi.
Subnet mask	Immettere l'indirizzo della subnet mask.
Gateway predefinito	Immettere il gateway predefinito.

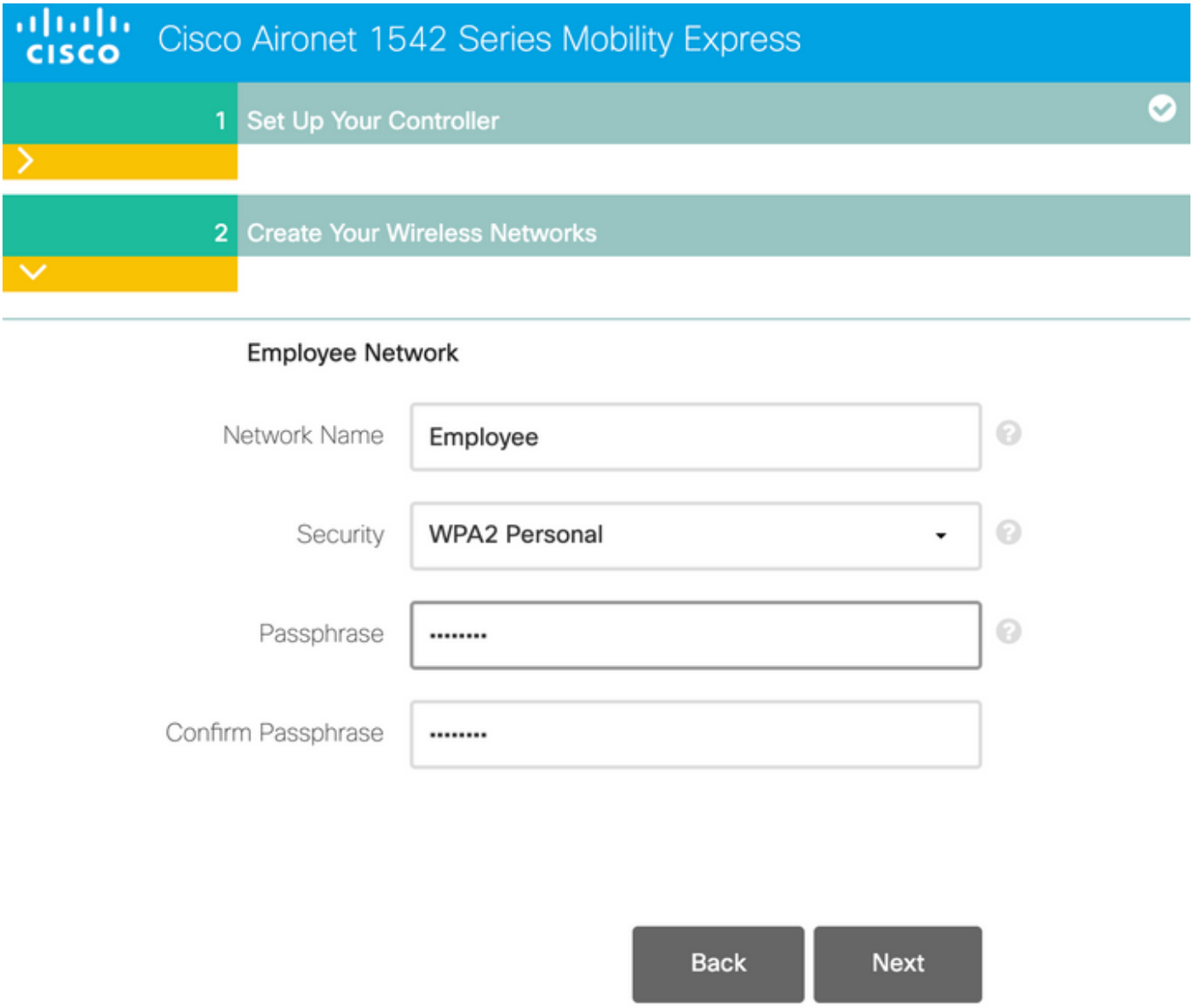
In questa configurazione, il server DHCP sarà in esecuzione sullo switch 1, quindi non è necessario abilitarlo sul WLC ME. Fate scorrere l'opzione Mesh fino a **Attiva** e fare clic su **Avanti**.



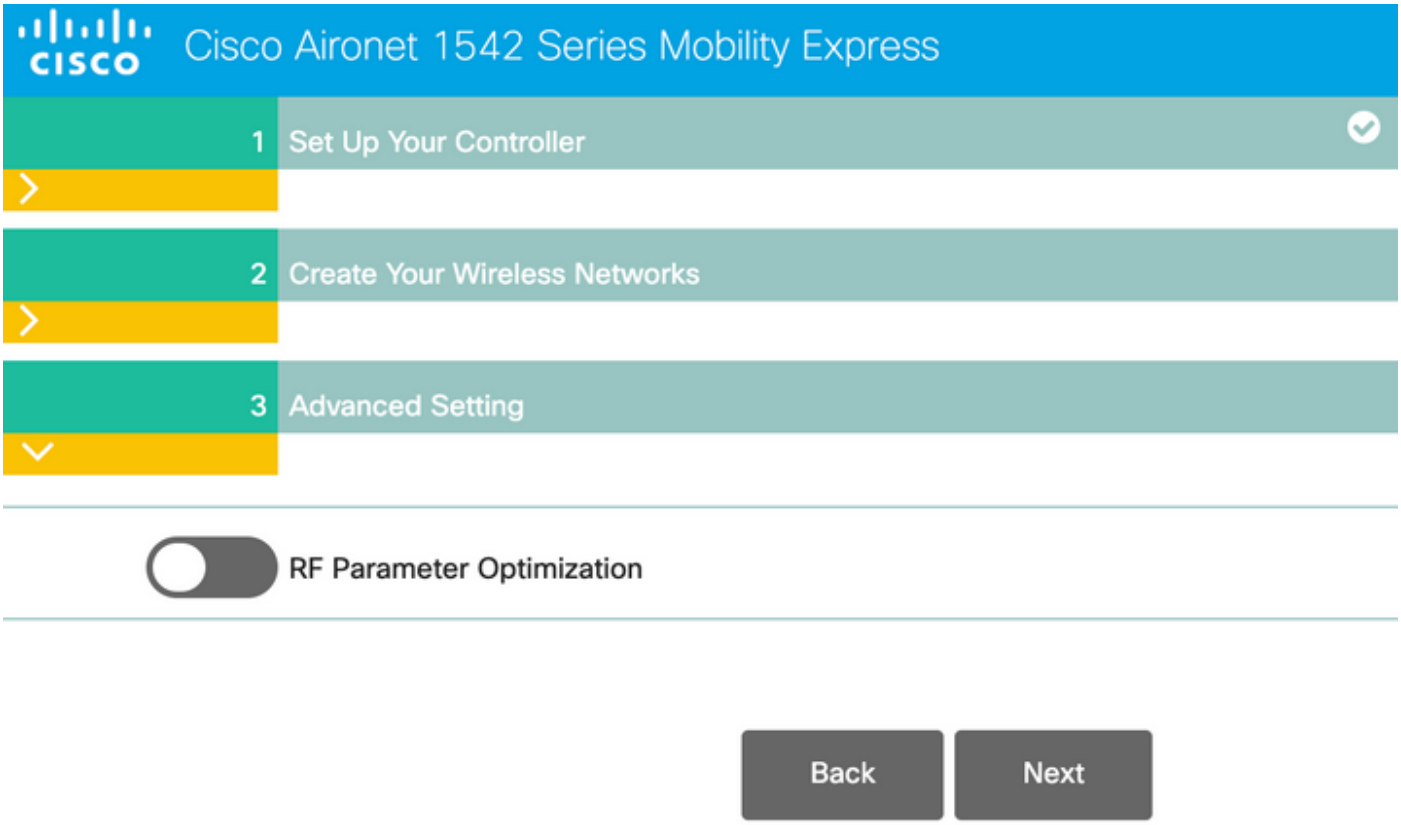
Nel passaggio successivo creare la rete wireless specificando i campi seguenti:

Nome campo	Descrizione
Nome rete	Immettere il nome della rete.
Sicurezza	Scegliere Tipo di protezione **personale WPA2** dall'elenco a discesa.
Passphrase	Specificare la chiave precondivisa (PSK).
Conferma passphrase	Reimmettere e confermare la passphrase.

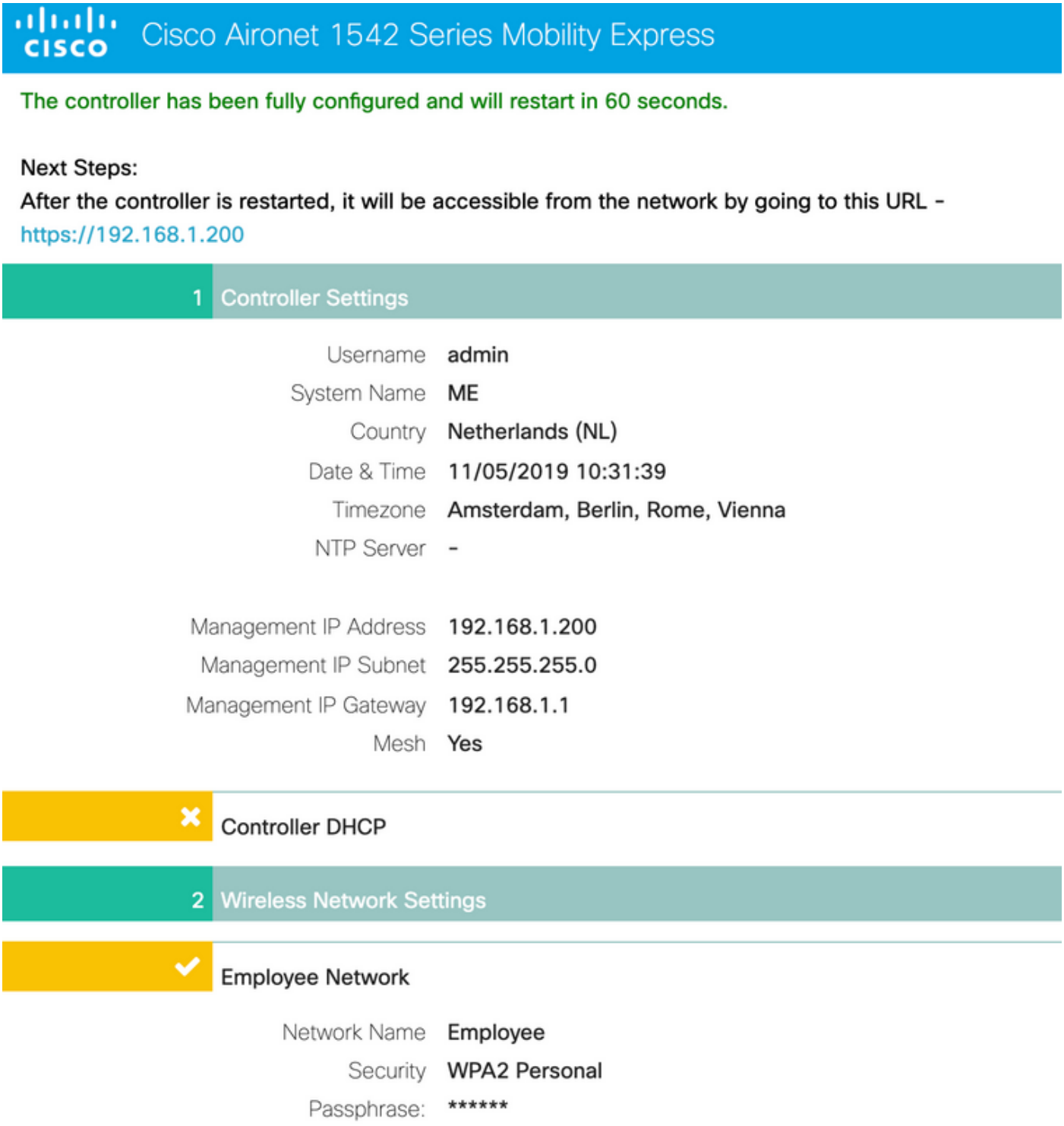
Questa rete può essere disabilitata in un secondo momento.



Nella scheda Impostazioni avanzate, lasciare **Ottimizzazione parametri RF** dispositivo di scorrimento disattivato e fare clic su **Avanti**



Una volta confermate le impostazioni, il WLC si riavvia:



Configurazione mesh aggiuntiva

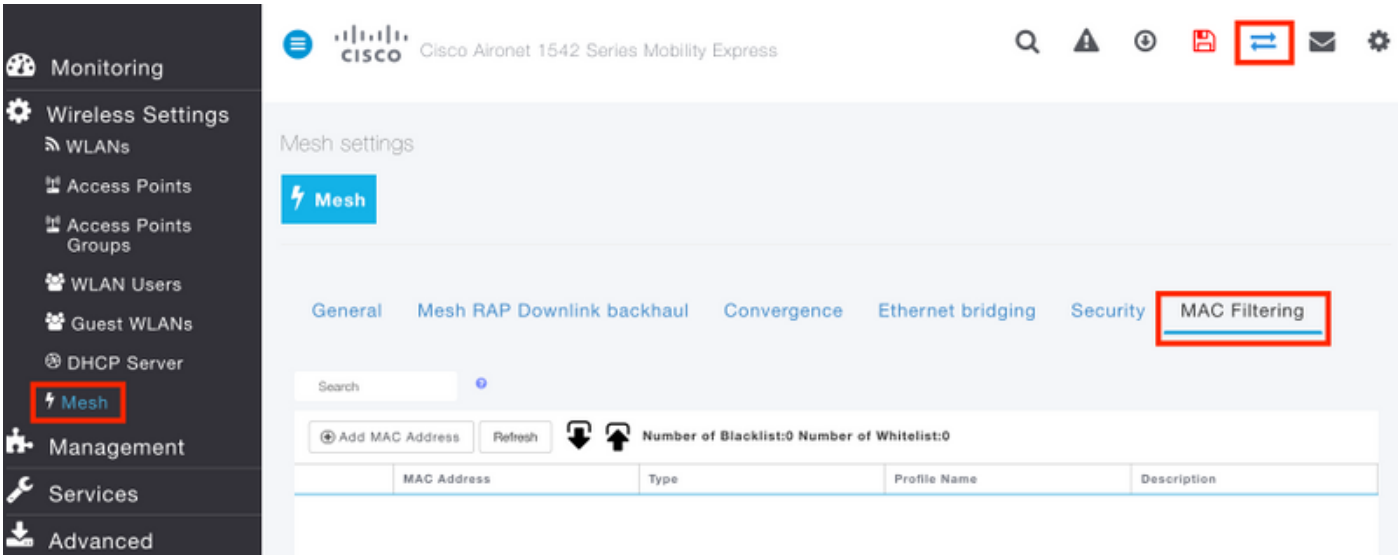
Prima di stabilire il collegamento con rete, è necessario convertire MAP in modalità flex-bridge. Se l'opzione mesh è stata abilitata durante la configurazione iniziale, il sistema RAP sarà già in modalità flex-bridge. Questa operazione può essere eseguita dalla CLI:

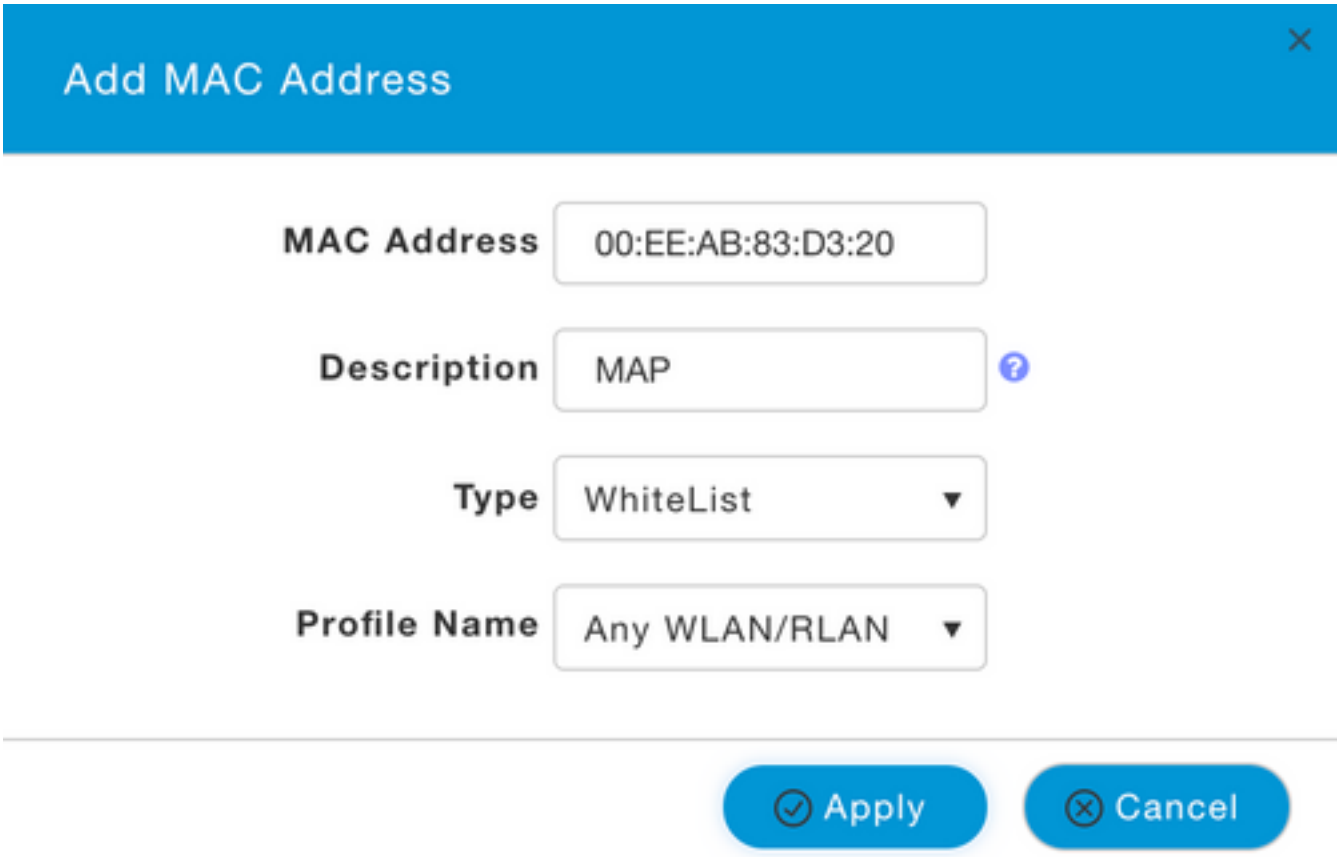
```
MAP# capwap ap mode flex-bridge

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

Affinché MAP top si unisca al controller ME, deve essere autorizzato. Su MAP, individuare l'indirizzo MAC dell'interfaccia Ethernet:

```
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)
```

Dal laptop 1, accedere all'interfaccia Web del controller ME tramite https://192.168.1.200. Dopo aver attivato la modalità Expert (angolo superiore destro), appare una scheda mesh in Impostazioni wireless. In mac filtering, aggiungere l'indirizzo MAC Ethernet del MAP:

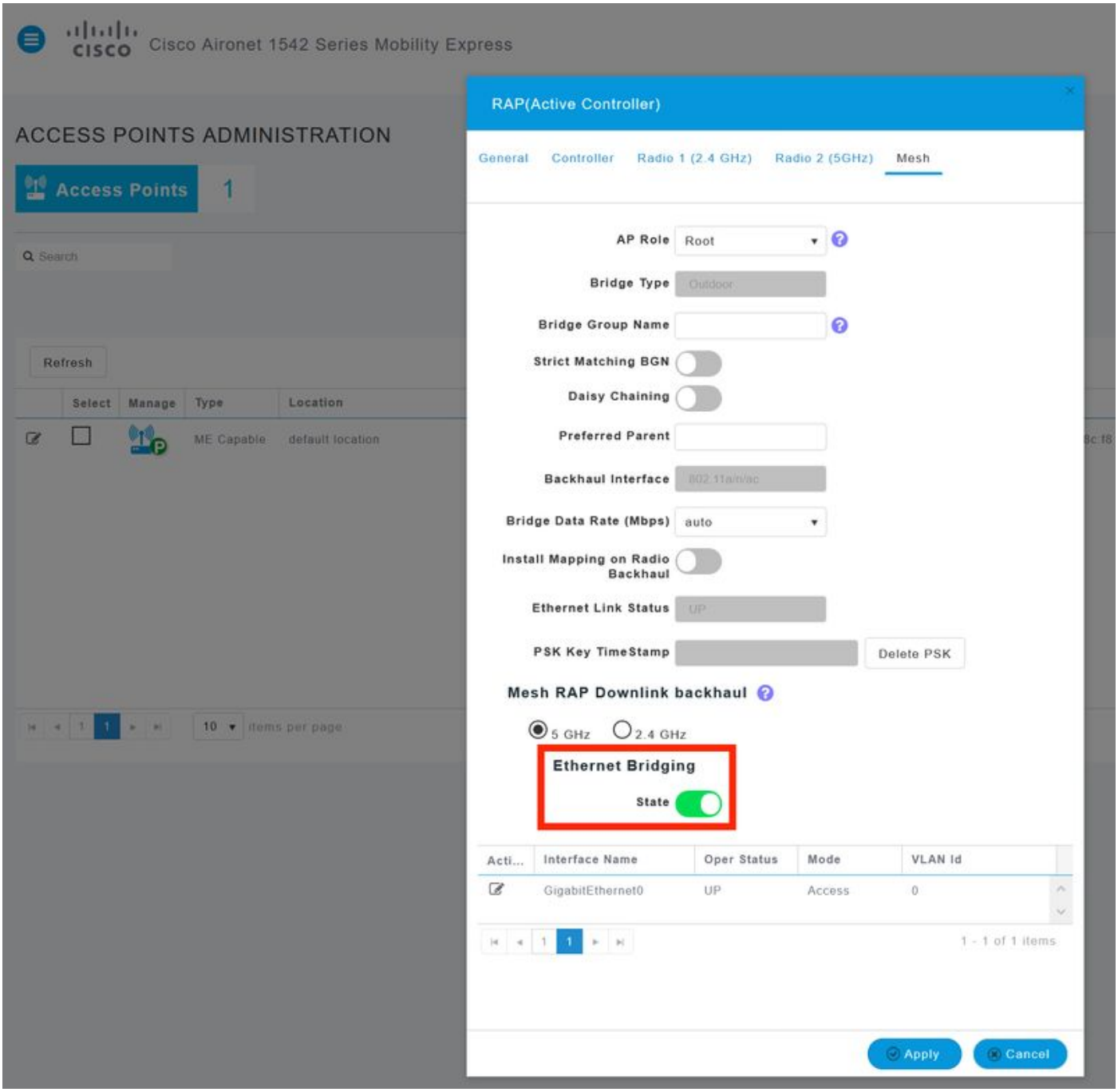




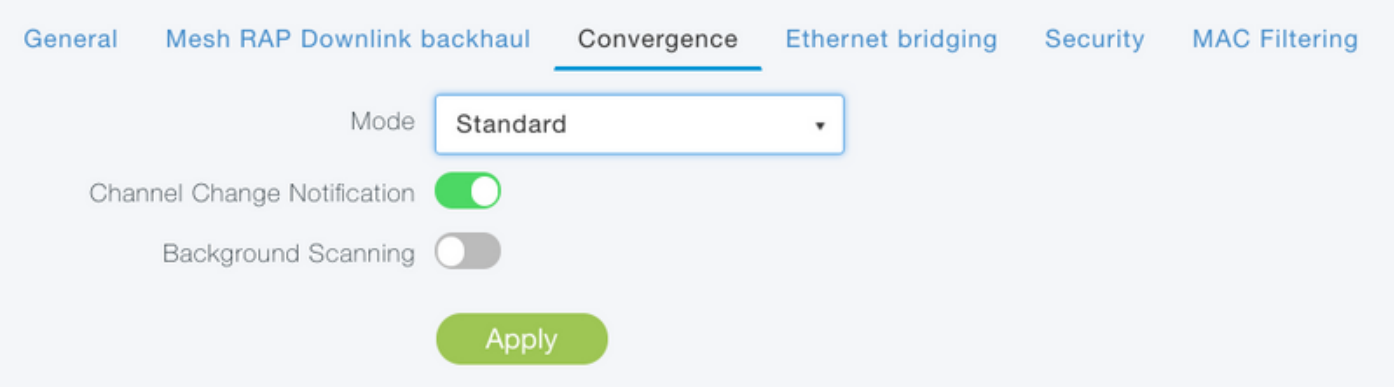
Nota: qualsiasi access point successivo in modalità bridge o flex-bridge aggiunto a ME WLC

deve essere autorizzato

Dopo aver impostato questa impostazione, si dovrebbe stabilire un collegamento mesh. Affinché il client cablato dietro la MAPPA possa passare il traffico sul collegamento a rete, è necessario abilitare il bridging Ethernet sulla MAPPA in **Impostazioni wireless > Access Point > MAPPA > Rete**:



Se il collegamento mesh utilizza una banda a 5 GHz, può essere influenzato dalle firme radar. Una volta che il RAP rileva un evento radar, passa a un altro canale. Si consiglia di attivare la Notifica di modifica del canale in modo che RAP notifichi al MAP che il canale verrà commutato. Ciò riduce notevolmente il tempo di convergenza in quanto MAP non deve scansionare tutti i canali disponibili:



Verifica

Èpossibile verificare che il MAP sia stato aggiunto eseguendo il comando show mesh ap summary:

```
(Cisco Controller) >show mesh ap summary

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

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
```

Per verificare se il collegamento sta attraversando il traffico, tenteremo di eseguire il ping tra il notebook 1 e il notebook 2:

```
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:** Sarà possibile eseguire il ping dell'indirizzo IP MAP o RAP solo dopo aver stabilito il collegamento mesh.

Risoluzione dei problemi

Sulla mappa/piano d'azione:

- `debug mesh events`

Su WLC personale:

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

Esempio di processo di partecipazione riuscito osservato da MAP (alcuni messaggi sono stati eliminati perché non rilevanti):

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

[*11/05/2019 18:28:24.5699] EVENT-MeshRadioBackhaul[1]: Sending SEEK_START to Channel Manager
[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: Starting regular seek
[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: channels to be seeked: 100
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[0]: start scanning on channel 1.
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[1]: start scanning on channel 100.
[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADD_LINK to MeshLink
[*11/05/2019 18:28:06.5699] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: AWPP adjacency added
channel(100) bgn() snr(99)
[*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:DEVNO_BH_R1
[*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 ASSOC
[*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, username(18)=c1540-00eeab83d320
[*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 0521f380 e2cdacd2 ad2dd4be 350c71f3 8810947f b4f3946b 10aabcbf
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: EAP authentication is done,
Parent(D4:78:9B:7B:DF:11) state changed to KEY_INIT
[*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 KEY_VALIDATE
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent
D4:78:9B:7B:DF:11, informing Mesh Link
[*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:DEVNO_BH_R1 notify bridge to start PCP
[*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 2
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load
1, AP ip: (192.168.1.202)
[*11/05/2019 18:28:55.1399] capwapSetTransportAddr returning: index 0, apMgrCount 0
[*11/05/2019 18:28:55.1399]
[*11/06/2019 13:23:36.0000]
[*11/06/2019 13:23:36.0000] CAPWAP State: DTLS Setup
[*11/06/2019 13:23:36.0000] DTLS connection created sucessfully local_ip: 192.168.1.202
local_port: 5248 peer_ip: 192.168.1.200 peer_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!
```

Suggerimenti, trucchi ed errori comuni

- Aggiornando MAP e RAP alla stessa versione dell'immagine via cavo, si evita che il download dell'immagine avvenga via etere (cosa che può essere problematica in ambienti RF "sporchi").
- Aumentando la larghezza del canale del collegamento backhaul a 5 GHz si possono ridurre le rilevazioni di SNR e false radar (principalmente su 80 MHz e 160 MHz).
- La connettività del collegamento mesh non deve essere verificata eseguendo il ping di MAP o RAP. Non sarà possibile eseguire il ping una volta che il collegamento alla rete viene visualizzato.
- Si consiglia vivamente di testare l'installazione in un ambiente controllato prima di distribuirla in loco.
- Se vengono utilizzati access point con antenne esterne, consultare la guida alla distribuzione per verificare quali antenne sono compatibili e a quale porta collegarle.
- Per creare un ponte tra il traffico di diverse VLAN sul collegamento mesh, è necessario disabilitare la funzione VLAN Transparent.
- Prendere in considerazione la presenza di un server syslog locale per gli access point, in quanto può fornire informazioni di debug altrimenti disponibili solo con una connessione alla console.