Konfigurieren der Punkt-zu-Punkt-Mesh-Verbindung mit Ethernet-Bridging auf Mobility Express-APs

Inhalt

Einleitung

Dieses Dokument beschreibt den Prozess der Bereitstellung von Point-to-Point-Mesh-Verbindungen mit Ethernet Bridging mithilfe der Cisco Mobility Express (ME)-Software.

Informationen zu Mobility Express

In diesem Dokument werden Cisco 1542 Outdoor Access Points verwendet. In Version 8.10 wurde die Mesh-Unterstützung der Mobility Express-Software für APs im Innen- und Außenbereich im Flex+Bridge-Modus eingeführt.

Folgende AP-Modelle werden unterstützt:

- **Als ME Root AP:**Cisco AireOS 1542, 1562, 1815s, 3802s APs
- **Als Mesh-AP**: Cisco AireOS 1542, 1562, 1815s, 3802s APs

Mobility Express (ME) ist eine Lösung, die den autonomen AP-Modus und die Software ersetzt. Es ermöglicht eine einfachere Version der auf AireOS basierenden Wireless LAN Controller (WLC)-Software, die auf dem Access Point selbst ausgeführt wird. Sowohl der WLC- als auch der AP-Code werden in einer einzigen Partition des AP-Speichers gespeichert. Für eine Mobility Express-Bereitstellung ist weder eine Lizenzdatei noch eine Lizenzaktivierung erforderlich.

Sobald das Gerät, auf dem die Mobility Express-fähige Software ausgeführt wird, eingeschaltet ist, wird zunächst der "AP-Teil" gestartet. Einige Minuten später wird auch der Controller-Teil initialisiert. Sobald eine Konsolensitzung eingerichtet ist, zeigt ein ME-fähiges Gerät die WLC-Eingabeaufforderung an. Um die zugrunde liegende AP-Shell einzugeben, kann der Befehl apciscoshell verwendet werden:

```
<#root>

(Cisco Controller) >

apciscoshell

!!Warning!!: You are entering ap shell. This will stop you from establishing new telnet/SSH/Web sessions
 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) >
```

Voraussetzungen

Verwendete Komponenten

- 2 x 1542D-E Access Points
- 2 Cisco Switches der Serie 3560-CX
- 2 Notebooks
- 1 Konsolenkabel

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

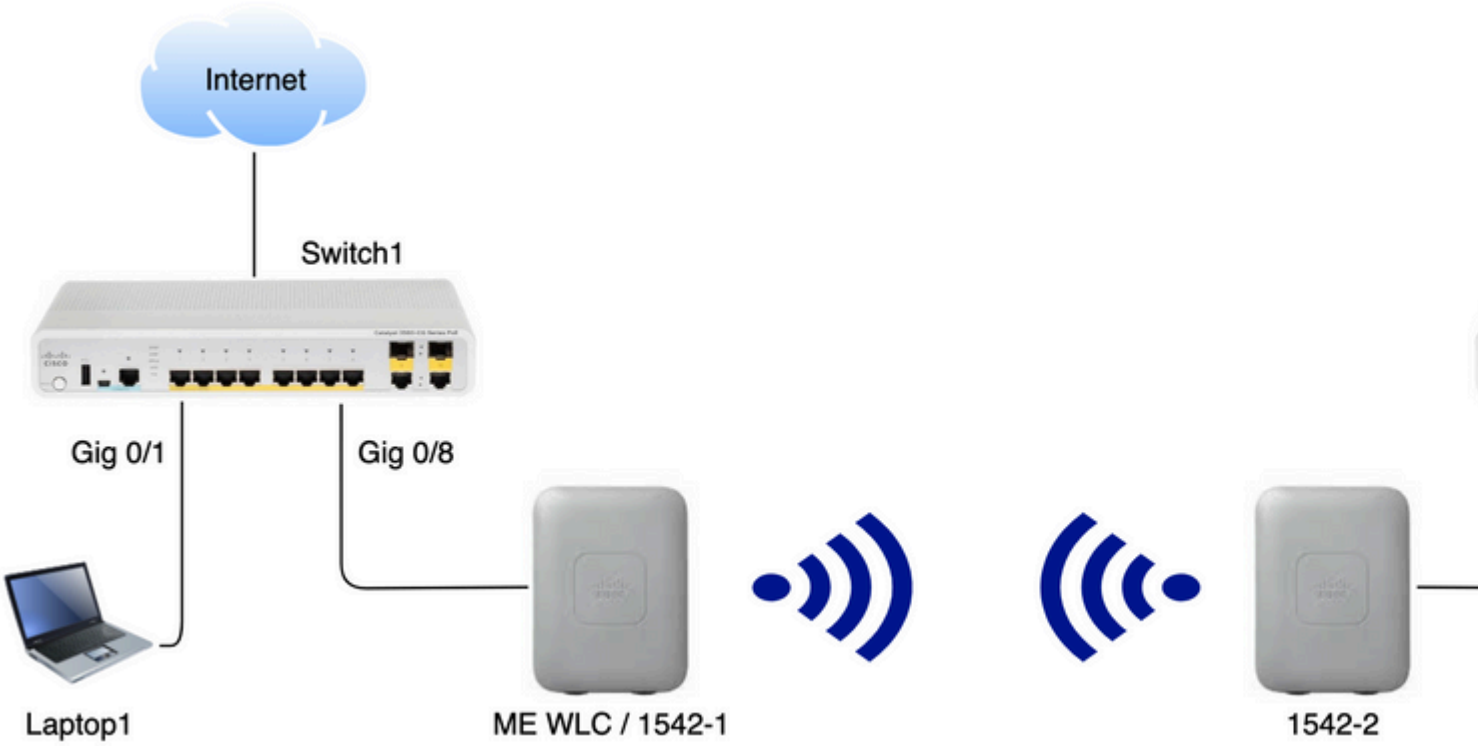
Netzwerkdiagramm

Alle Geräte in diesem Netzwerk befinden sich im Subnetz 192.168.1.0/24. Die Verwaltungsschnittstelle des Mobility Express AP (Controllers) ist nicht markiert, während das native VLAN an allen Ports VLAN 39 ist. AP 1542-1 übernimmt die Rolle eines Controllers und eines Root Access Point (RAP), während AP 1542-2 die Rolle eines Mesh Access Point (MAP) übernimmt. Die nachfolgende Tabelle enthält die IP-Adressen aller Geräte im Netzwerk:

> **Hinweis**: Das Tagging der Management-Schnittstelle kann Probleme verursachen, wenn der Access Point dem internen WLC-Prozess beitritt. Wenn Sie sich entscheiden, die Management-Schnittstelle zu taggen, stellen Sie sicher, dass der Teil der kabelgebundenen Infrastruktur entsprechend konfiguriert ist.

"Slot0:"	IP-Adresse
Standardgateway	192.168.1.1

Laptop 1	192.168.1.100
Laptop 2	192.168.1.101
Mobility Express WLC	192.168.1.200
1542-1 (KARTE)	192.168.1.201
1542-2 (RAP)	192.168.1.202



Konfiguration

Switch-Konfigurationen

Switch-Ports, an die Laptops angeschlossen sind, werden als Access-Ports konfiguriert, wobei das VLAN auf 39 festgelegt ist:

<#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
```

Die Switch-Ports, an denen die APs angeschlossen sind, befinden sich im Trunk-Modus, wobei das native VLAN auf 39 festgelegt ist:

<#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 (MAP)
 switchport mode trunk
 switchport trunk native vlan 39
end
```

Zurücksetzen der APs auf Werkseinstellungen

Es wird empfohlen, die Access Points vor Beginn einer neuen Bereitstellung auf die Werkseinstellungen zurückzusetzen. Dies kann durch Drücken der Modus-/Reset-Taste am Access Point, Einstecken des Netzkabels und Halten des Kabels für mehr als 20 Sekunden erfolgen. Dadurch wird sichergestellt, dass alle vorherigen Konfigurationen gelöscht wurden. Der Zugriff auf den Access Point erfolgt über eine Konsolenverbindung mit dem Standardbenutzernamen Cisco und dem Passwort Cisco (Groß- und Kleinschreibung beachten).

Ein Zurücksetzen auf die Werkseinstellungen führt nicht notwendigerweise dazu, dass ein Access Point in den Lightweight-Modus zurückversetzt wird, wenn er bereits in Mobility Express ausgeführt wird. Ein wichtiger Schritt besteht darin, festzustellen, ob auf Ihren APs ein Lightweight-Image oder ein Mobility Express-Image ausgeführt wird.

Wenn Ihr AP ein Lightweight AP ist, können Sie ihn in Mobility Express umwandeln, indem Sie den Mobility Express-Code herunterladen. Wenn sich der AP bereits im Mobility Express-Modus befindet, müssen Sie den Upgrade-Prozess in der GUI des Access Points/Controllers durchlaufen, um die Softwareversion zu ändern.

Beispiel einer Version von AP, die ein Lightweight-Image verwendet:

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

Dies ist ein Beispiel für einen AP, der bereits in der Mobility Express-Software ausgeführt wird:

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

Herunterladen des leichten CAPWAP-Bilds auf 1542-2 (MAP)

Laptop 1 wird als TFTP-Server verwendet. AP 1542-2 kann zu Beginn an den Switch 1 Gig 0/8 Port angeschlossen werden, nur damit das Upgrade durchgeführt werden kann. Laden Sie auf software.cisco.com unter 1542 Lightweight-Images 15.3.3-JJ1 (vollständiger Name *ap1g5-k9w8-tar.153-3.JK9.tar) herunter,* der dem Image der Version 8.10.185 entspricht. Das neueste leichte AP-Image entspricht immer der neuesten ME-Version.
Speichern Sie das Bild im TFTP-Stammordner. Schließen Sie das Konsolenkabel an, und melden Sie sich mit den Standardanmeldedaten an (Benutzername ist Cisco, Kennwort ist ebenfalls Cisco). Weisen Sie dem Access Point die IP-Adresse zu, und führen Sie die Aktualisierung mithilfe der folgenden Befehle durch:

```
#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
```

AP führt das Upgrade durch und startet dann neu. Vergewissern Sie sich mit dem Befehl show version, dass das Upgrade erfolgreich war:

<#root>

RAP#

show version

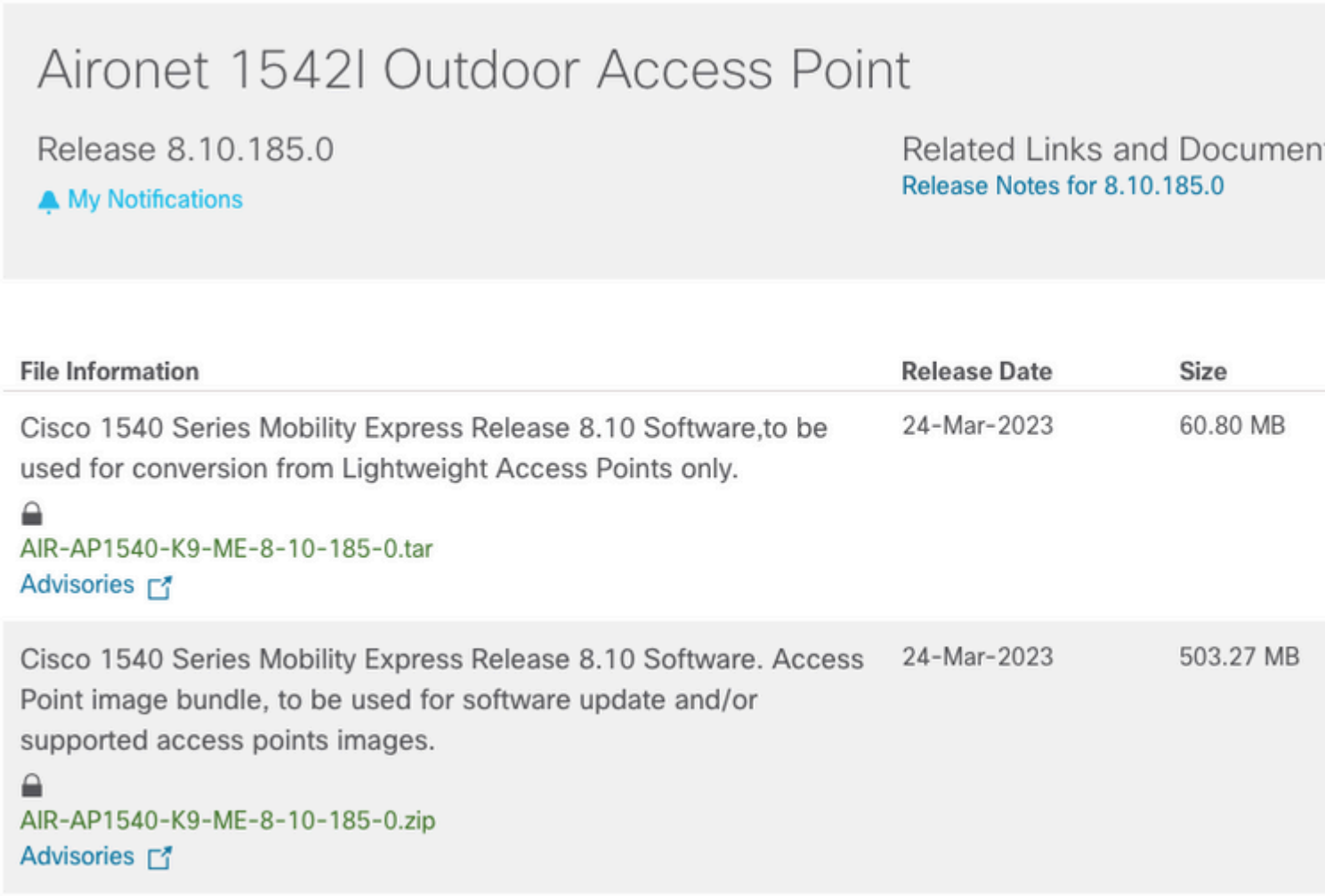
```
.
..
AP Running Image     : 8.10.185.0
Primary Boot Image   : 8.10.185.0
Backup Boot Image    : 8.8.125.0
```

AP wird von Switch 1 getrennt und wieder an Switch 2 angeschlossen.

> **Hinweis**: Durch das manuelle Upgrade des MAP-Images vermeiden wir, dass das Image-Upgrade drahtlos erfolgt, sobald die Mesh-Verbindung hergestellt ist.

Herunterladen eines Mobility Express-fähigen Images auf AP 1542-1 (RAP)

Unter Mobility Express 8.10.105, Versionen für 1542 AP, werden zwei verfügbare Dateien angezeigt: .tar und .zip. TAR-Datei herunterladen



TAR-Datei herunterladen

Im Gegensatz zu einem physischen WLC verfügen die ME-Access Points nicht über genügend Flash-Speicher, um alle AP-Images zu speichern. Daher ist es erforderlich, einen TFTP-Server bereitzustellen, auf den jederzeit zugegriffen werden kann, wenn Sie weitere APs mit Ihrem Mobility Express Access Point verbinden möchten. Dieser Schritt ist nicht erforderlich, wenn die Access Points wie in diesem Beispiel manuell aktualisiert werden.

Um das Upgrade durchzuführen, verbinden Sie die Konsole mit dem AP 1542-1, weisen Sie ihr eine IP-Adresse zu, und führen Sie das Upgrade des Images durch:

```
#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
```

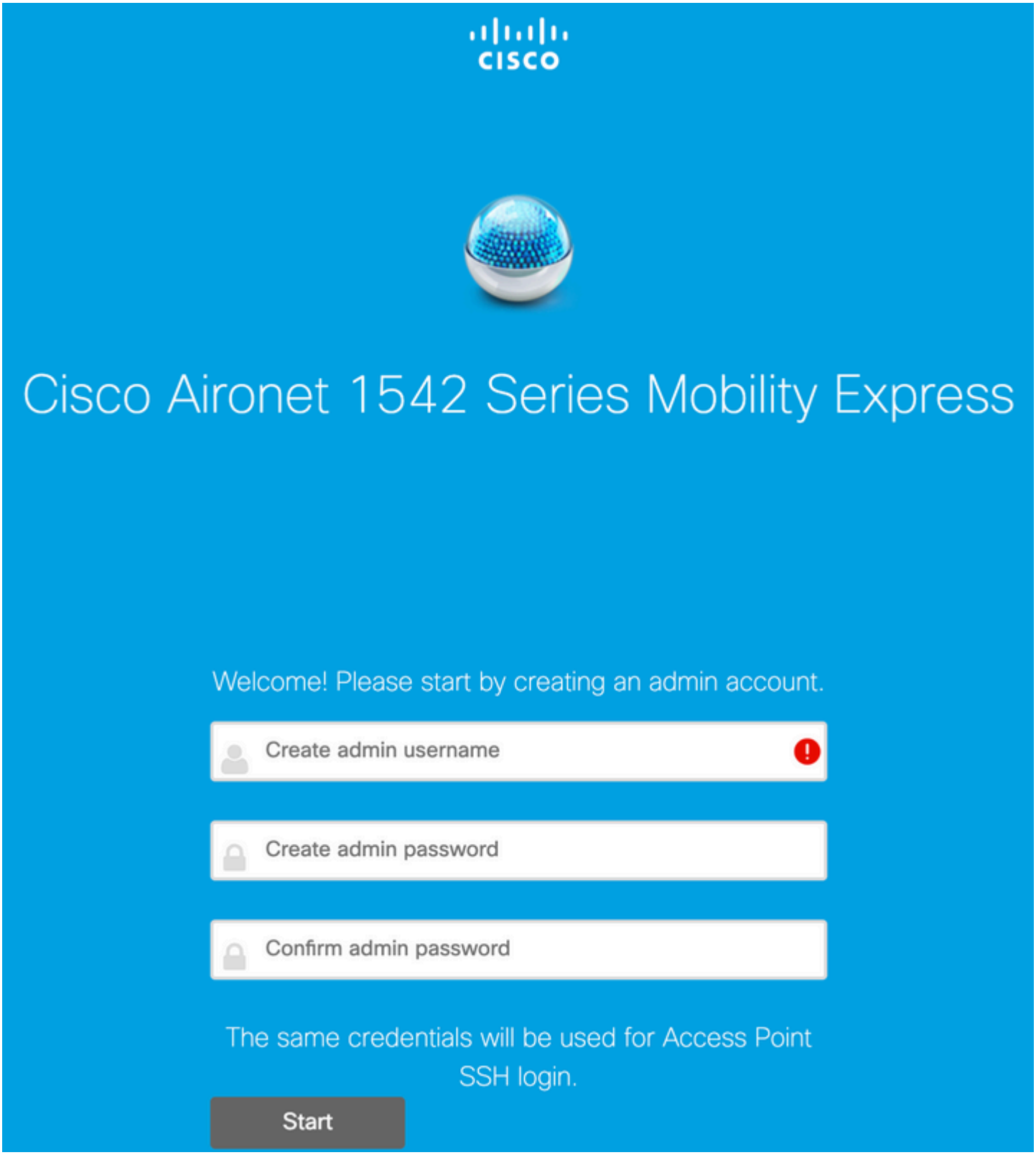
Nach Abschluss des Upgrades wird der Access Point neu gestartet. Kurz nachdem der AP gestartet wurde, startet auch der Controller-Teil. Daher sollte bald die Zero-Day-Bereitstellung der SSID "CiscoAirProvision" ausgestrahlt werden.

Wenn Sie sich in der Konsole befinden, sehen Sie einen CLI-Assistenten, konfigurieren den Access Point jedoch nicht auf diese Weise. Der drahtlose GUI-Assistent ist der richtige Weg.

Zero-Day-SSID-Bereitstellung

Stellen Sie eine Verbindung zur SSID "CiscoAirProvision" her, die vom AP mit dem **Kennwort** gesendet wird. Der Laptop erhält eine IP-Adresse aus dem Subnetz 192.168.1.0/24.
Falls Sie die SSID nicht übertragen sehen, besteht weiterhin die Möglichkeit, dass sich der Access Point in "

Erstellen Sie ein Admin-Konto auf dem Controller, indem Sie den Admin-Benutzernamen und das Kennwort angeben, und klicken Sie dann auf Start.

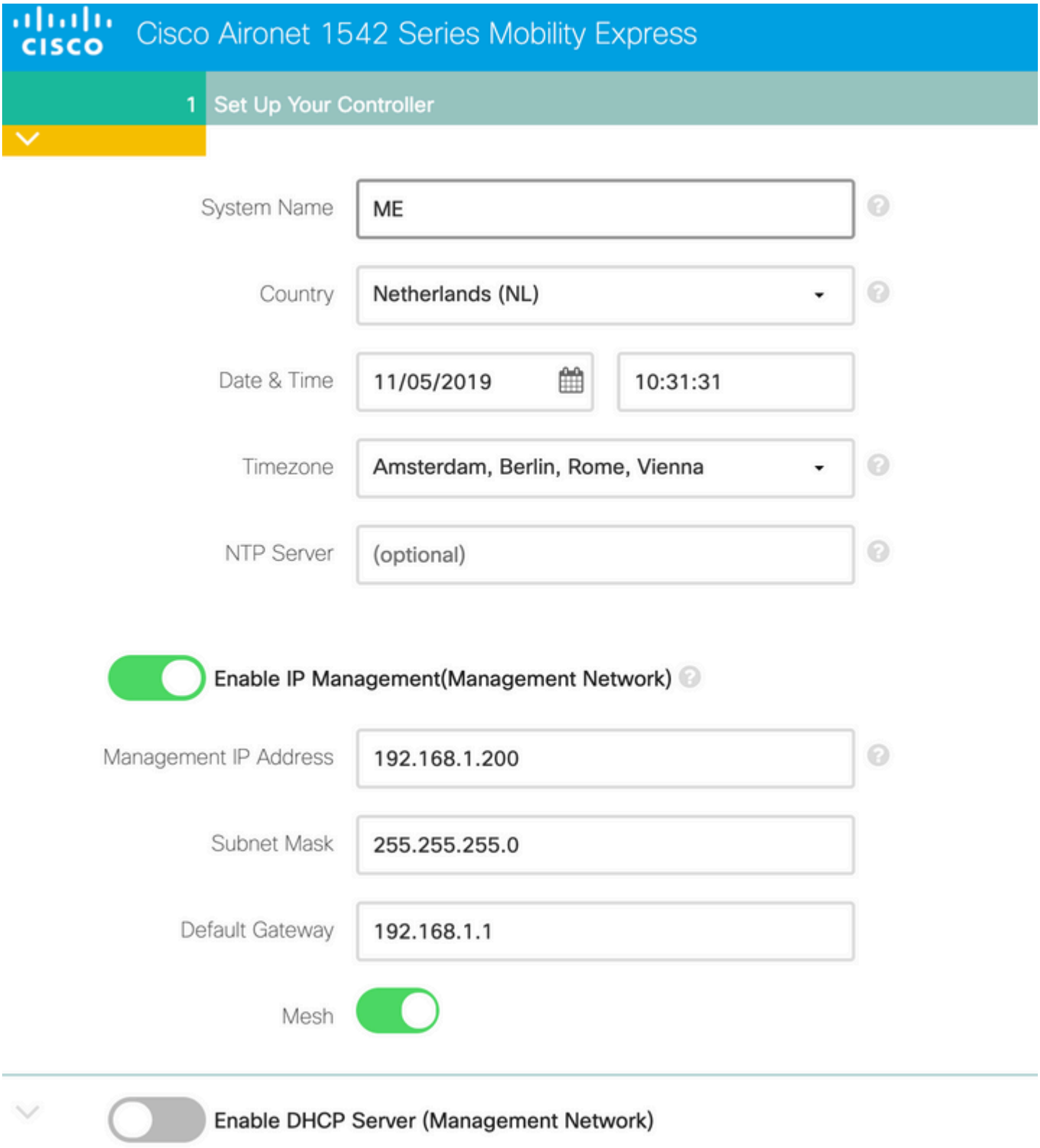


Im nächsten Schritt richten Sie den Controller durch die Angabe der Werte.

Feldname	**Beschreibung**
Systemname	Geben Sie den Systemnamen für den Mobility Express-Zugangspunkt ein. Beispiel:

	MobilityExpress-WLC
Land	Wählen Sie ein Land aus der Dropdown-Liste aus.
Datum und Uhrzeit	Wählen Sie das aktuelle Datum und die aktuelle Uhrzeit aus. **Hinweis:** Der Assistent versucht, die Uhreninformationen (Datum und Uhrzeit) mithilfe von JavaScript vom Computer zu importieren. Es wird dringend empfohlen, die Uhrzeiteinstellungen zu bestätigen, bevor Sie fortfahren. Die Zugangspunkte hängen von den Uhrzeiteinstellungen ab, die erforderlich sind, um dem WLC beizutreten.
Zeitzone	Wählen Sie die aktuelle Zeitzone aus.
NTP-Server	Geben Sie die NTP-Serverdetails ein.
Management-IP	Geben Sie die Management-IP-Adresse ein. HINWEIS: Sie muss sich von der IP-Adresse unterscheiden, die dem Access Point zugewiesen ist. In diesem Beispiel hat der Access Point zwar die IP .201 erhalten, im Konfigurationsassistenten wird jedoch die IP .200 zugewiesen. Beide werden verwendet.
Subnetzmaske	Geben Sie die Adresse der Subnetzmaske ein.
Standardgateway	Geben Sie das Standard-Gateway ein.

In dieser Konfiguration wird der DHCP-Server auf Switch 1 ausgeführt. Daher muss er nicht auf dem ME WLC aktiviert werden. Schieben Sie die Option Mesh nach **Aktivieren** und klicke auf "**Weiter"**.

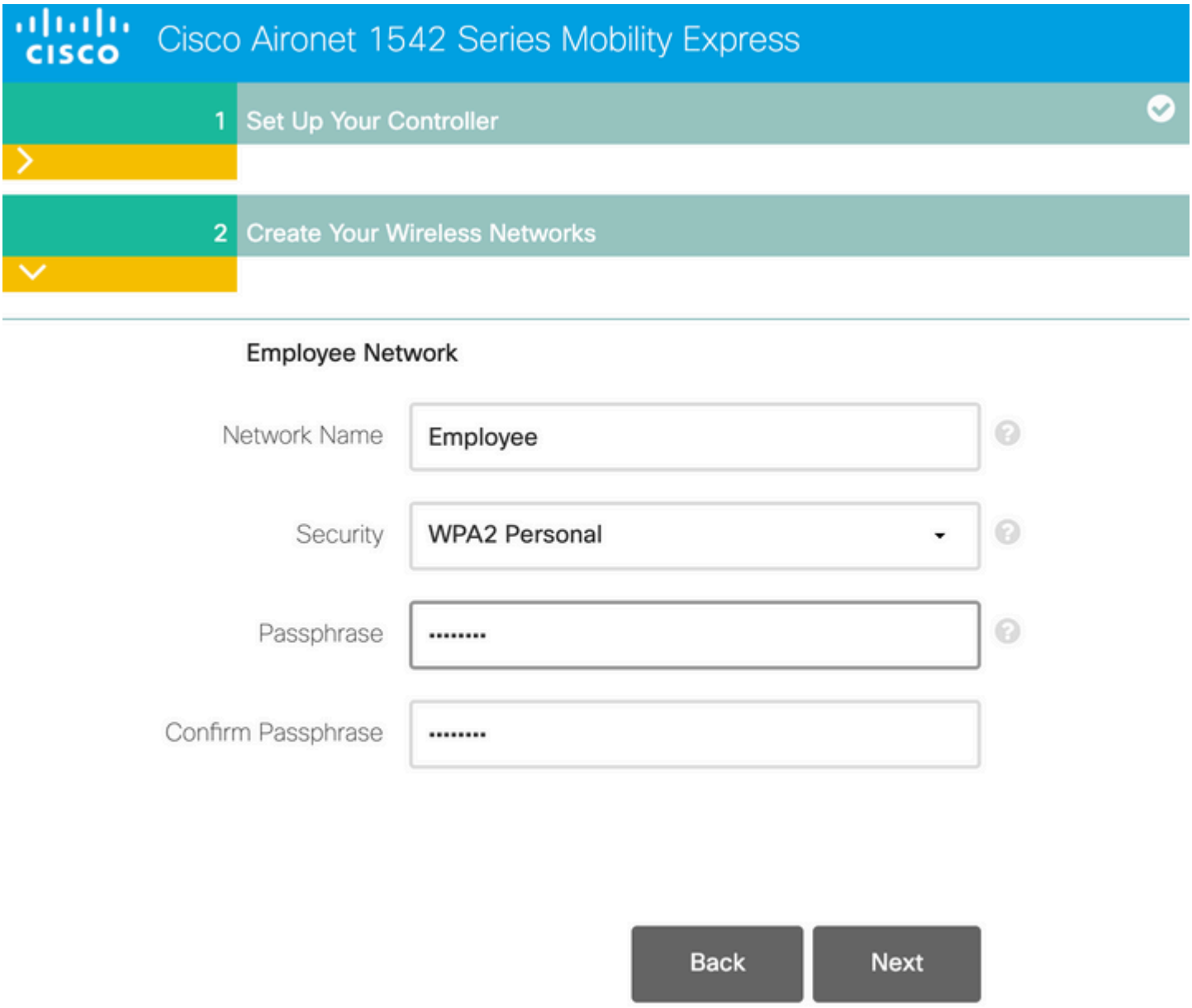


Im nächsten Schritt erstellen Sie das Wireless-Netzwerk, indem Sie die folgenden Felder angeben:

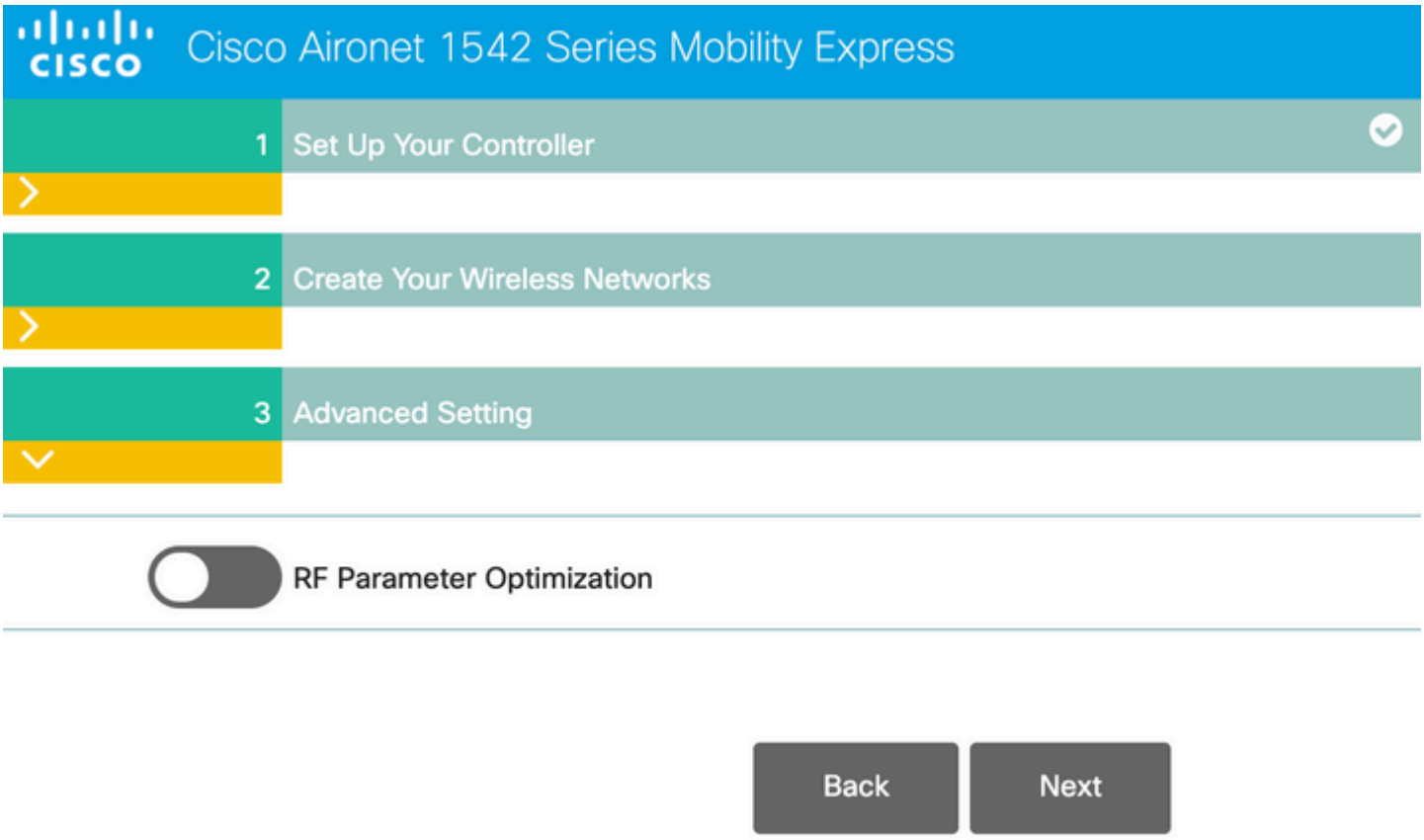
Feldname	**Beschreibung**
Netzwerkname	Geben Sie den Netzwerknamen ein.
Sicherheit	Wählen Sie **WPA2 Personal**-Sicherheitstyp aus der Dropdown-Liste.
Passphrase	Geben Sie den PSK (Pre-Shared Key) an.

Passphrase bestätigen	Geben Sie den Kennsatz erneut ein, und bestätigen Sie ihn.

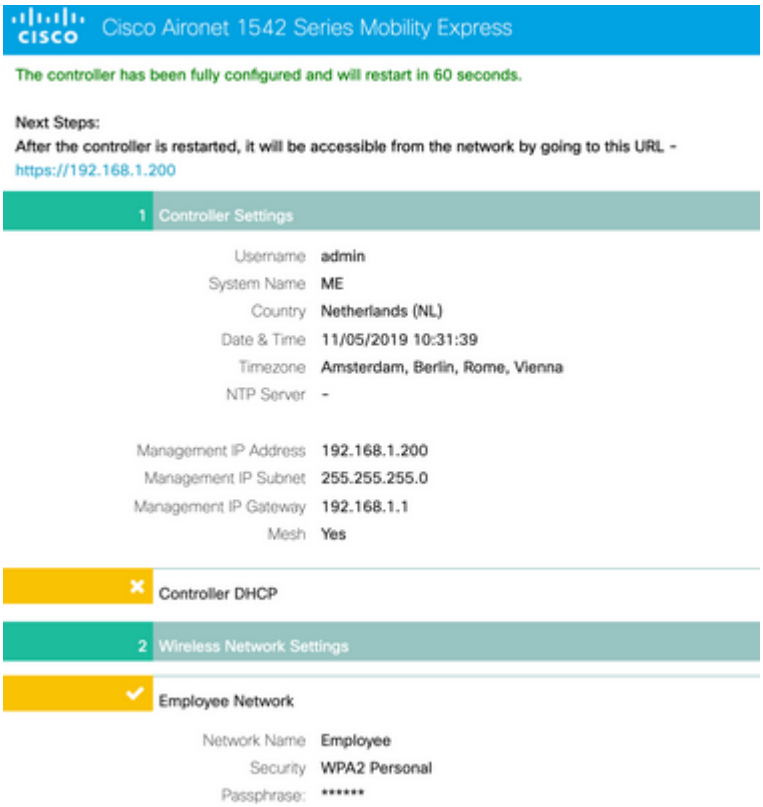
Dieses Netzwerk kann zu einem späteren Zeitpunkt deaktiviert werden.



Belassen Sie auf der Registerkarte Erweiterte Einstellungen die **Optimierung von RF-Parametern** Schieberegler deaktiviert und klicken Sie auf **Weiter**



Sobald die Einstellungen bestätigt wurden, startet der WLC neu:



Zusätzliche Mesh-Konfiguration

Vor der Herstellung der Mesh-Verbindung muss MAP in den Flex-Bridge-Modus umgewandelt werden. Der

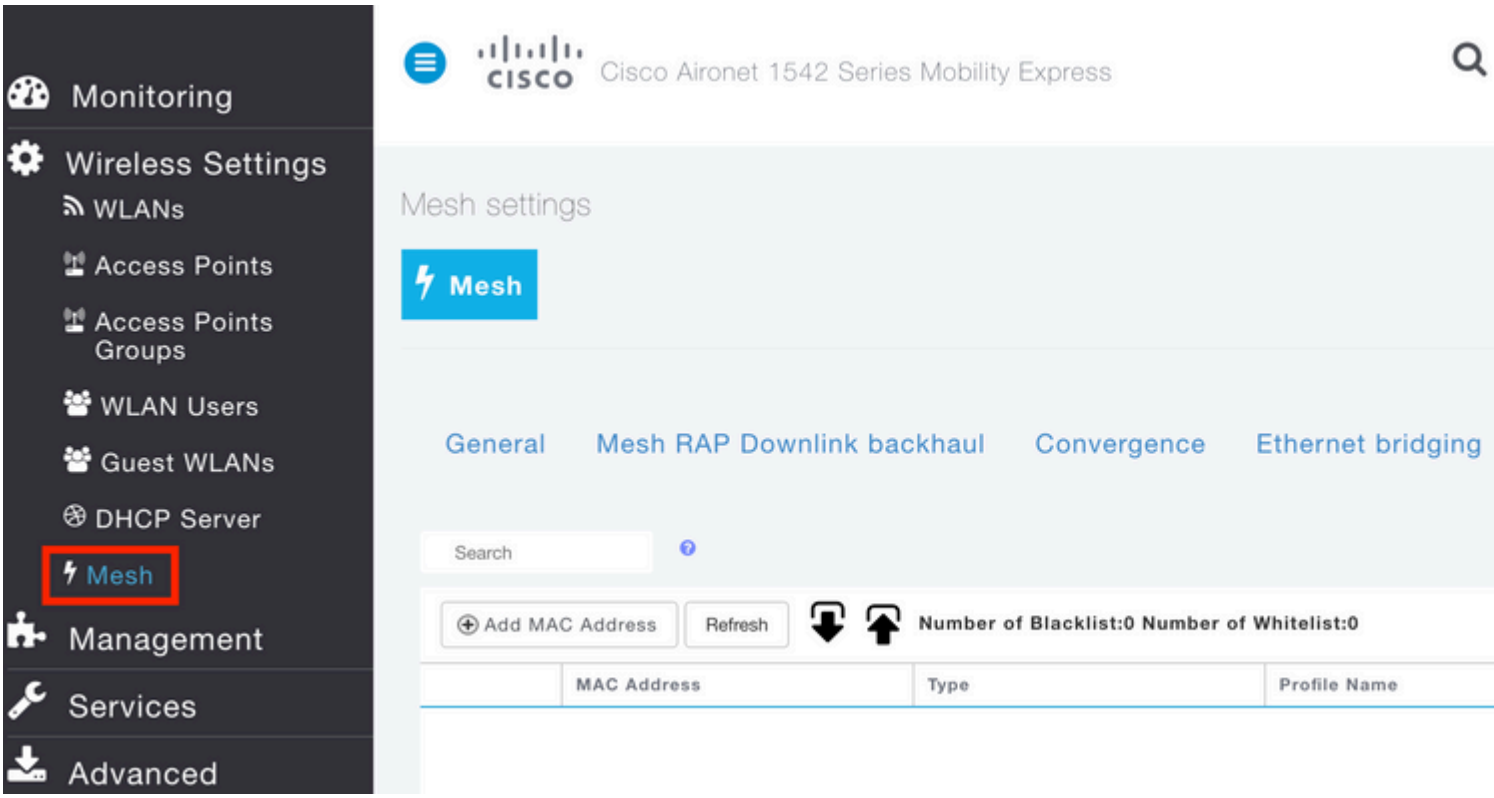
RAP befindet sich bereits im Flex-Bridge-Modus, wenn die Mesh-Option bei der Erstkonfiguration aktiviert wurde. Dies kann über die CLI durchgeführt werden:

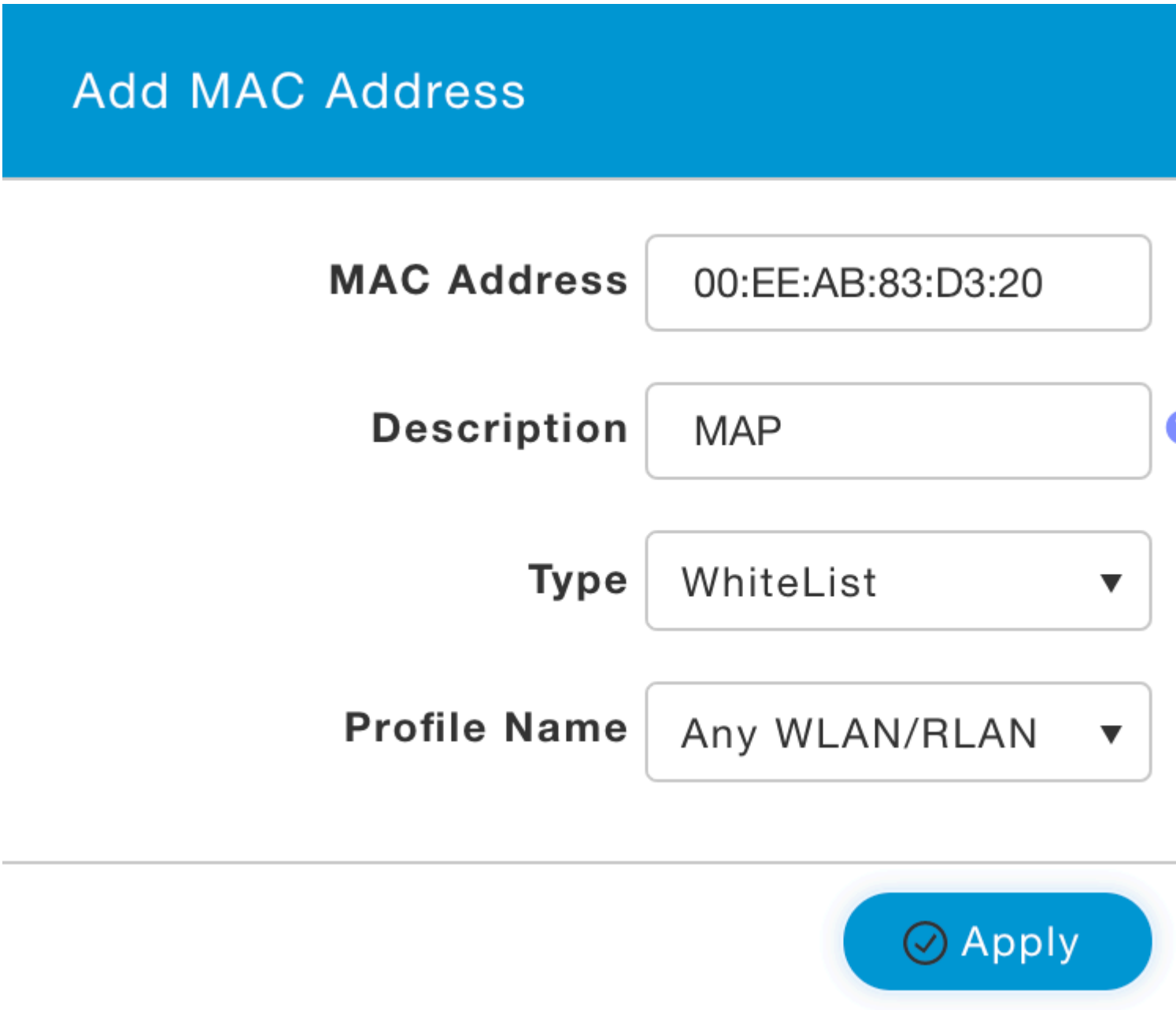
```
<#root>

MAP#

capwap ap mode flex-bridge


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

Damit MAP top mit dem ME Controller verbunden werden kann, muss es autorisiert werden. Suchen Sie auf MAP die MAC-Adresse seiner Ethernet-Schnittstelle:

```
<#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)
```

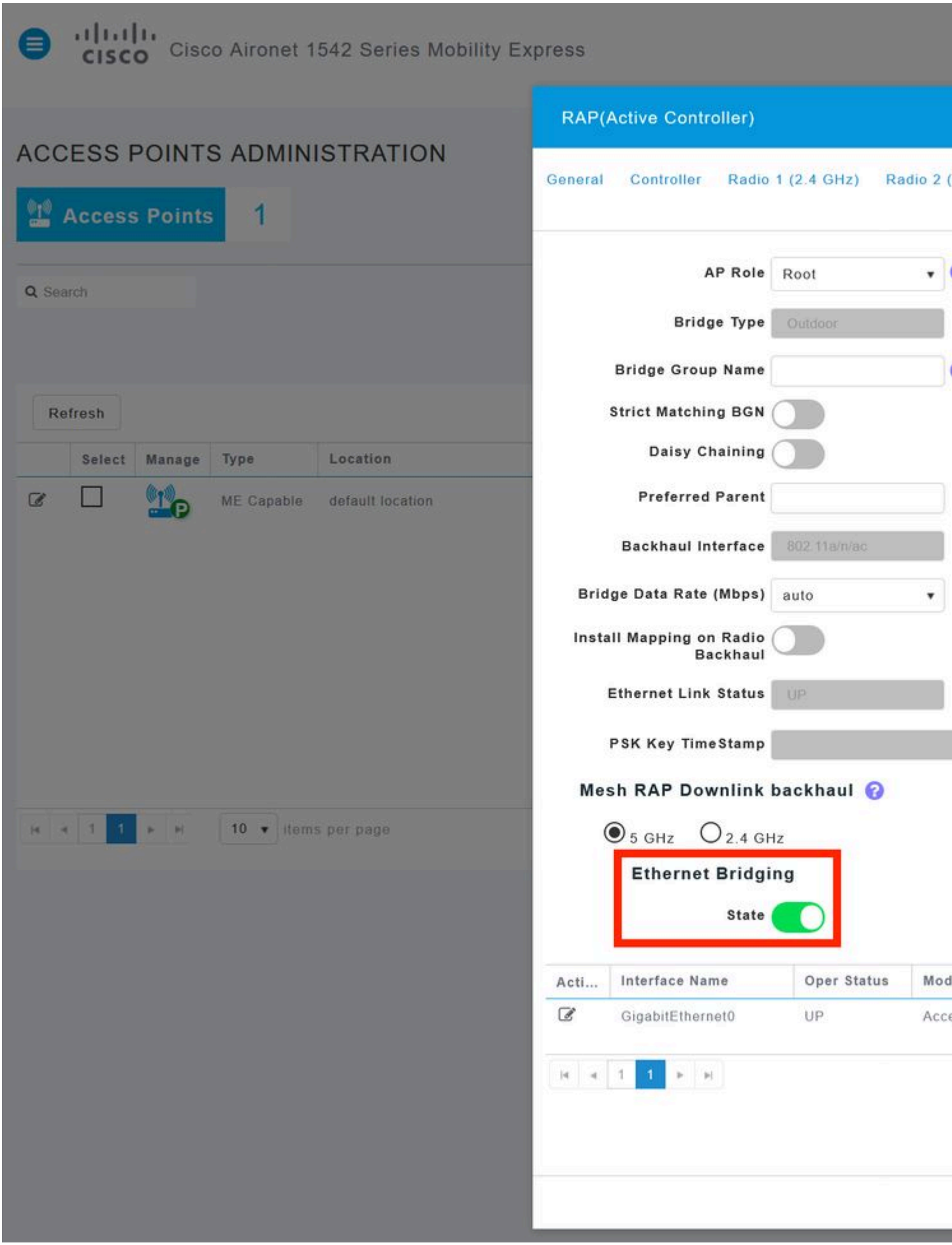
Rufen Sie von Laptop 1 aus die Web-Oberfläche des ME-Controllers über https://192.168.1.200 auf. Nachdem der Expertenmodus aktiviert wurde (obere rechte Ecke), wird unter den Wireless-Einstellungen eine Netzregisterkarte angezeigt. Fügen Sie unter MAC-Filterung die Ethernet-MAC-Adresse des MAP hinzu:


Monitoring
Wireless Settings
WLANs
Access Points
Access Points Groups
WLAN Users
Guest WLANs
DHCP Server
Mesh
Management
Services
Advanced
Cisco Aironet 1542 Series Mobility Express
Mesh settings
Mesh
General
Mesh RAP Downlink backhaul
Convergence
Ethernet bridging
Search
Add MAC Address
Refresh
Number of Blacklist:0 Number of Whitelist:0
MAC Address
Type
Profile Name

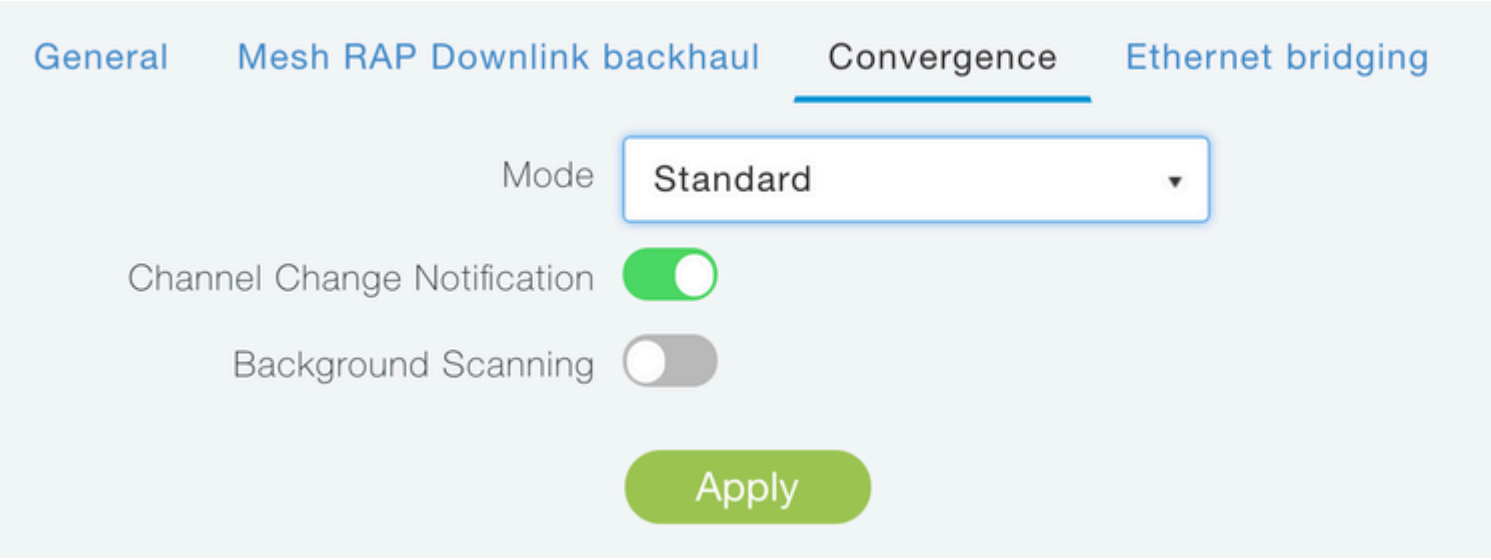


Hinweis: Alle nachfolgenden APs im Bridge- oder Flex-Bridge-Modus, die mit dem ME WLC verbunden werden, müssen ebenfalls autorisiert werden.

Nach der Einrichtung sollte eine Maschenverbindung hergestellt werden. Damit der kabelgebundene Client hinter dem MAP den Datenverkehr über die Mesh-Verbindung weiterleiten kann, muss Ethernet Bridging auf dem MAP unter **Wireless Settings (Wireless-Einstellungen) > Access Points (Zugriffspunkte) > MAP > Mesh (Netzwerk) aktiviert werden**:


Cisco Aironet 1542 Series Mobility Express
ACCESS POINTS ADMINISTRATION
Access Points
1
Search
Refresh
Select
Manage
Type
Location
ME Capable
default location
10
items per page
RAP(Active Controller)
General
Controller
Radio 1 (2.4 GHz)
Radio 2 (
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
Mesh RAP Downlink backhaul
5 GHz
2.4 GHz
Ethernet Bridging
State
Acti...
Interface Name
Oper Status
Mod
GigabitEthernet0
UP
Acce

Wenn die Mesh-Verbindung ein 5-GHz-Band verwendet, kann dies durch Radarsignaturen beeinflusst werden. Sobald der RAP ein Radarereignis erkennt, wechselt er zu einem anderen Kanal. Es wird empfohlen, die Kanaländerungsbenachrichtigung zu aktivieren, damit der RAP den MAP benachrichtigt, dass der Kanal gewechselt wird. Dadurch wird die Konvergenzzeit erheblich reduziert, da MAP nicht alle verfügbaren Kanäle abtasten muss:



Überprüfung

Wir können überprüfen, ob der MAP beigetreten ist, indem wir den Befehl show mesh ap summary ausführen:

<#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
```

Um zu testen, ob die Verbindung den Datenverkehr passiert, werden wir versuchen, einen Ping von Laptop 1 an Laptop 2 zu senden:

<#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
```

Hinweis: Sie können einen Ping an eine MAP- oder RAP-IP-Adresse senden, sobald die Mesh-Verbindung hergestellt wurde.

Fehlerbehebung

Auf MAP/RAP:

- `Debuggen von Mesh-Ereignissen`

Auf ME WLC:

- `debug capwap events enable`
- `debug capwap errors enable`
- `Aktivieren von Mesh-Ereignissen debuggen`

Beispiel eines erfolgreichen Teilnahmeprozesses, der von MAP beobachtet wurde (einige Nachrichten wurden entfernt, da sie nicht relevant sind):

<#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 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) b
[*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
[*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:
[*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 A
[*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, userna
[*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 05
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: EAP authentication is done, Parent(D4:78:9B:7B:DF:11) st
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Child(D4:E8:80:A0:D0:B1) generating keys to Parent D4:78
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_AUTH_RSP, Parent(D4:78:9B:7B:DF:11) state
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent D4:78:9B:7
[*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:DEVN
[*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:
[*11/05/2019 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
```

```
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load 1, AP i
[*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
[*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

!
```

Tipps, Tricks und häufige Fehler

- Durch ein Upgrade von MAP und RAP auf dieselbe Image-Version über das Kabel vermeiden wir, dass Bilder per Funk heruntergeladen werden (was in "schmutzigen" HF-Umgebungen problematisch sein kann).

- Eine Erhöhung der Kanalbreite der 5-GHz-Backhaul-Verbindung kann zu geringeren SNR- und falschen Radarerkennungen führen (hauptsächlich bei 80 MHz und 160 MHz).
- Die Mesh-Link-Konnektivität sollte nicht durch Pingen von MAP oder RAP getestet werden. Sie können nicht mehr gepingt werden, sobald die Mesh-Verbindung aktiv ist.
- Es wird dringend empfohlen, das Setup vor der Bereitstellung vor Ort in einer kontrollierten Umgebung zu testen.
- Wenn APs mit externen Antennen verwendet werden, überprüfen Sie im Bereitstellungsleitfaden, welche Antennen kompatibel sind und an welchen Port sie angeschlossen werden sollen.
- Um den Datenverkehr von verschiedenen VLANs über die Mesh-Verbindung zu überbrücken, muss die Funktion "VLAN Transparent" deaktiviert werden.
- Erwägen Sie einen lokalen Syslog-Server für die APs, da dieser sonst nur über eine Konsolenverbindung Debuginformationen bereitstellen kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.