Mobility Express APのイーサネットブリッジングを使用したポイントツーポイントメッシュリンクの設定

内容

概要

このドキュメントでは、Cisco Mobility Express(ME)ソフトウェアを使用して、イーサネットブリッジングを使用してポイントツーポイントメッシュリンク(PPP)を導入するプロセスについて説明します。

バージョン情報

このドキュメントでは、Cisco 1542屋外用アクセスポイントを使用しています。 Flex+Bridgeモードの屋内および屋外AP向けのMobility Expressソフトウェアでのメッシュサポートは、リリース8.10で導入されました。

次のAPモデルがサポートされています。

- MEルートAPとして：Cisco AireOS 1542、1562、1815s、3802s AP
- メッシュAPとして:Cisco AireOS 1542、1562、1815s、3802s AP

Mobility Express(ME)は、Autonomous APのモードとソフトウェアに代わるソリューションです。AireOSベースのワイヤレスLANコントローラ(WLC)ソフトウェアの軽量バージョンをアクセス

ポイント自体で実行できます。WLCとAPコードの両方がAPメモリの単一のパーティション内に格納されます。Mobility Expressの導入では、ライセンスファイルもライセンスのアクティベーションも不要です。

Mobility Express対応ソフトウェアを実行しているデバイスの電源を入れると、「AP部品」が最初に起動します。数分後、コントローラパーツも初期化されます。コンソールセッションが確立されると、ME対応デバイスにWLCプロンプトが表示されます。基盤となるAPシェルを入力するには、コマンドapciscoshellを使用できます。

```
<#root>

(Cisco Controller) >

apciscoshell

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

前提条件

使用するコンポーネント

- 1542D-EアクセスポイントX 2
- 3560-CX CiscoスイッチX 2
- ノートPC X 2
- 1xコンソールケーブル

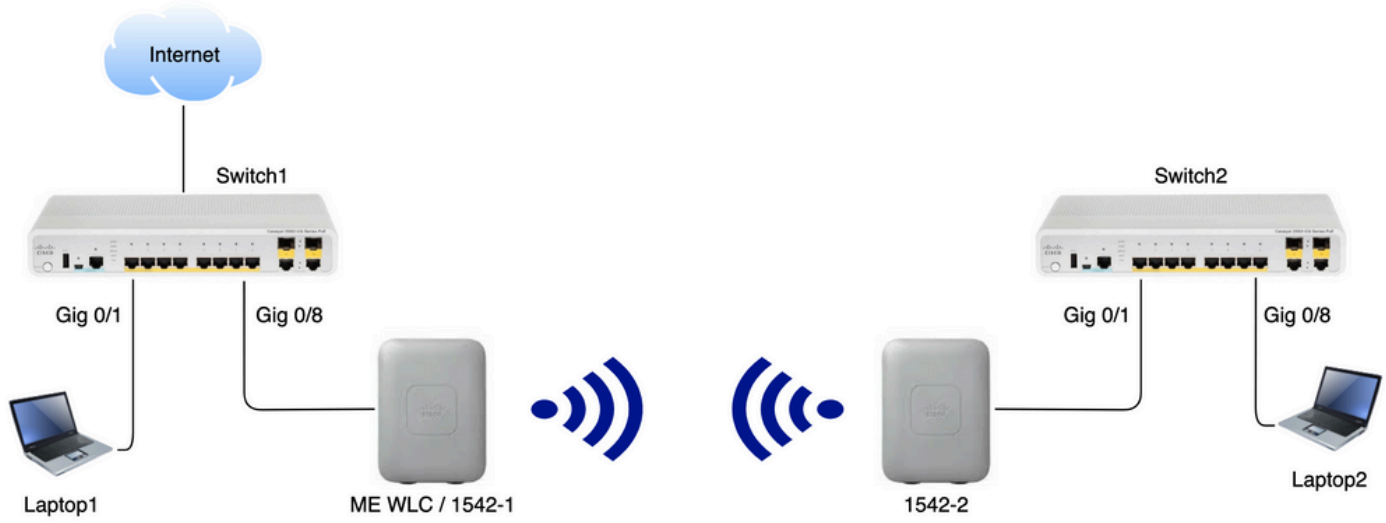
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

このネットワーク内のすべてのデバイスは、192.168.1.0/24サブネット内に配置されます。Mobility Express AP（コントローラ）の管理インターフェイスにはタグが付いていませんが、すべてのポートのネイティブVLANはVLAN 39です。AP 1542-1はコントローラおよびルートアクセスポイント(RAP)の役割を担い、AP 1542-2はメッシュアクセスポイント(MAP)の役割を担います。次の表に、ネットワーク内のすべてのデバイスのIPアドレスを示します。

注：管理インターフェイスにタグを付けると、内部WLCプロセスに参加するAPで問題が発生する可能性があります。管理インターフェイスにタグを付ける場合は、有線インフラストラクチャの部分が適切に設定されていることを確認します。

デバイス	IP アドレス
[Default Gateway]	192.168.1.1
ラップトップ1	192.168.1.100
ラップトップ2	192.168.1.101
Mobility Express WLC	192.168.1.200
1542-1(RAP)	192.168.1.201
1542-2（地図）	192.168.1.202



コンフィギュレーション

スイッチの設定

ラップトップが接続されているスイッチポートは、VLANが39に設定されたアクセスポートとして設定されます。

<#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
```

APが接続されているスイッチポートは、ネイティブVLANが39に設定されたトランクモードになります。

<#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
```

APの工場出荷時設定へのリセット

新しい導入を開始する前に、APを工場出荷時の状態にリセットすることを推奨します。これは、APのモード/リセットボタンを押し、電源を差し込んで、20秒以上保持し続けることによって実行できます。これにより、以前のすべての設定が消去されます。APには、コンソール接続を介してアクセスできます。デフォルトのユーザ名はCisco（大文字と小文字は区別されます）、パスワードはCisco（大文字と小文字は区別されます）です。

Mobility ExpressでAPがすでに実行されている場合は、工場出荷時のリセットによってAPがLightweightモードに戻るとは限りません。重要な手順は、APがLightweightイメージまたはMobility Expressイメージのどちらを実行しているかを特定することです。

APがLightweightの場合は、Mobility Expressコードをダウンロードして Mobility Expressに変換できます。APがすでにMobility Expressモードになっている場合は、アクセスポイント/コントローラのGUIでアップグレードプロセスに従って、ソフトウェアバージョンを変更する必要があります。

Lightweightイメージを実行するAPからのshow versionの例（図1を参照）:

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

次に、Mobility Expressソフトウェアですでに実行されているAPの例を示します（APがMobility Expressソフトウェアを実行している場合）。

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

Lightweight capwapイメージの1542-2(MAP)へのダウンロード

ラップトップ1はTFTPサーバとして使用されます。AP 1542-2をスイッチ1 Gig 0/8ポートに最初に接続するだけで、アップグレードを実行できます。software.cisco.comの1542 Lightweightイメージで、8.10.185のリリースイメージに対応する15.3.3-JJ1(フルネームap1g5-k9w8-tar.153-3.JK9.tar)をダウンロードします。最新のLightweight APイメージは、常に最新のMEバージョンに対応します。
イメージをTFTPルートフォルダに配置します。 コンソールケーブルを接続し、デフォルトのクレデンシャル(ユーザ名はCisco、パスワードもCisco)を使用してログインします。 APにIPアドレスを割り当て、次のコマンドを使用してアップグレードを実行します。

```
#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はアップグレードを実行してからリブートします。show versionコマンドを使用して、アップグレードが正常に行われたことを確認します。

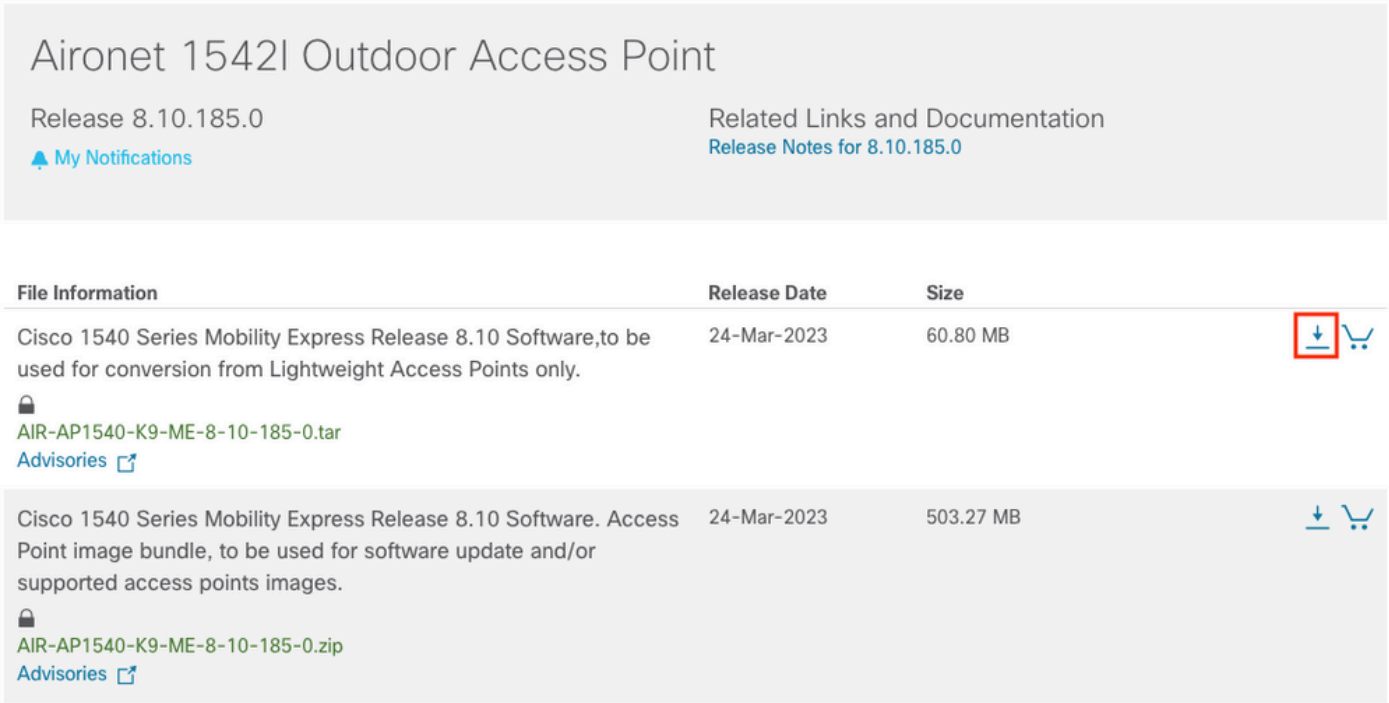
```
<#root>

MAP#

show version

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

APをスイッチ1から抜き、スイッチ2に接続し直す。

注:MAPのイメージを手動でアップグレードすることで、メッシュリンクが確立された後に地上波で行われるイメージのアップグレードプロセスを回避できます。

AP 1542-1(RAP)へのMobility Express対応イメージのダウンロード

1542 AP用のMobility Express 8.10.105リリースでは、.tarと.zipの2つの使用可能なファイルが表示されます。.tarファイルのダウンロード



.tarファイルのダウンロード

物理的なWLCとは異なり、MEアクセスポイントには、すべてのAPイメージを保存するのに十分なフラッシュメモリがありません。そのため、さらに別のAPをMobility Expressアクセスポイントに加入させる場合は、TFTPサーバに常にアクセス可能にしておくことが必要です。この例のようにAPを手動でアップグレードする場合、この手順は必要ありません。

アップグレードを実行するには、コンソールをAP 1542-1に接続し、IPアドレスを割り当てて、

イメージのアップグレードを実行します。

```
#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
```

アップグレードが完了すると、APがリブートします。APが起動するとすぐに、コントローラ部分も起動し始めます。まもなく、ゼロデイプロビジョニングSSID「CiscoAirProvision」がブロードキャストされるようになります。

コンソールを表示している場合は、CLIウィザードは表示されますが、APをそのように設定しないでください。Over-the-Air GUIウィザードを使用できます。

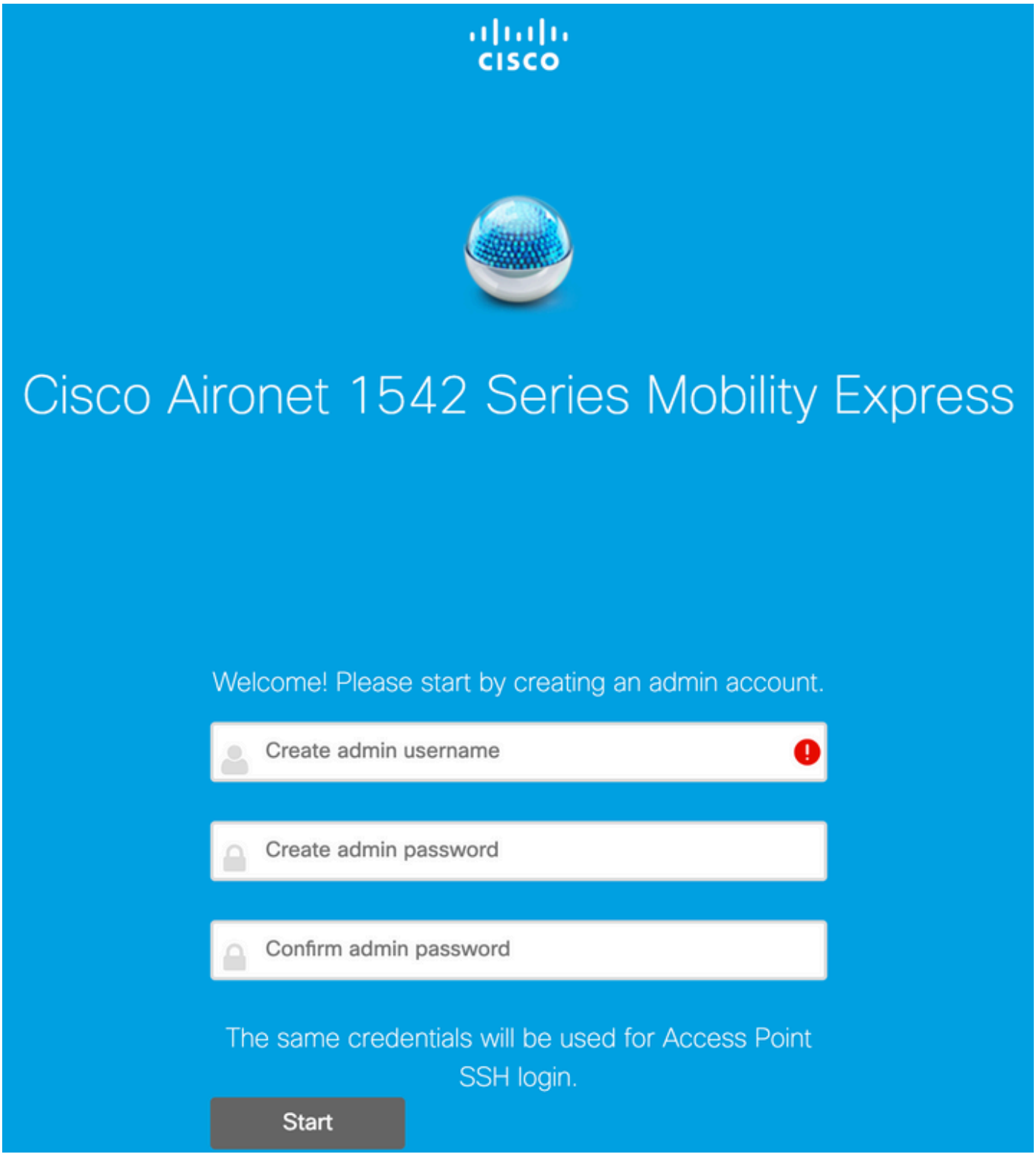
ゼロデイSSIDプロビジョニング

パスワードpasswordを使用して、APによってブロードキャストされる「CiscoAirProvision」SSIDに接続します。ラップトップは、サブネット192.168.1.0/24からIPアドレスを取得します。

SSIDがブロードキャストされない場合、APが「Mobility Express CAPABLE」であってもMobility Expressとして実行されていない可能性があります。その後、AP CLIに接続してap type mobility-expressを入力すると、APがリブートし、プロビジョニングSSIDがブロードキャストされます。

必要に応じて、このセットアップ中に「capwap ap mode local/flex-bridge」を使用して、ローカルモードとメッシュモードの間でAPを変換することもできます。

Webブラウザでアドレスhttp://192.168.1.1を開きます。 このページは、初期設定ウィザードにリダイレクトされます。 管理者ユーザ名とパスワードを指定してコントローラに管理者アカウントを作成し、Startをクリックします。

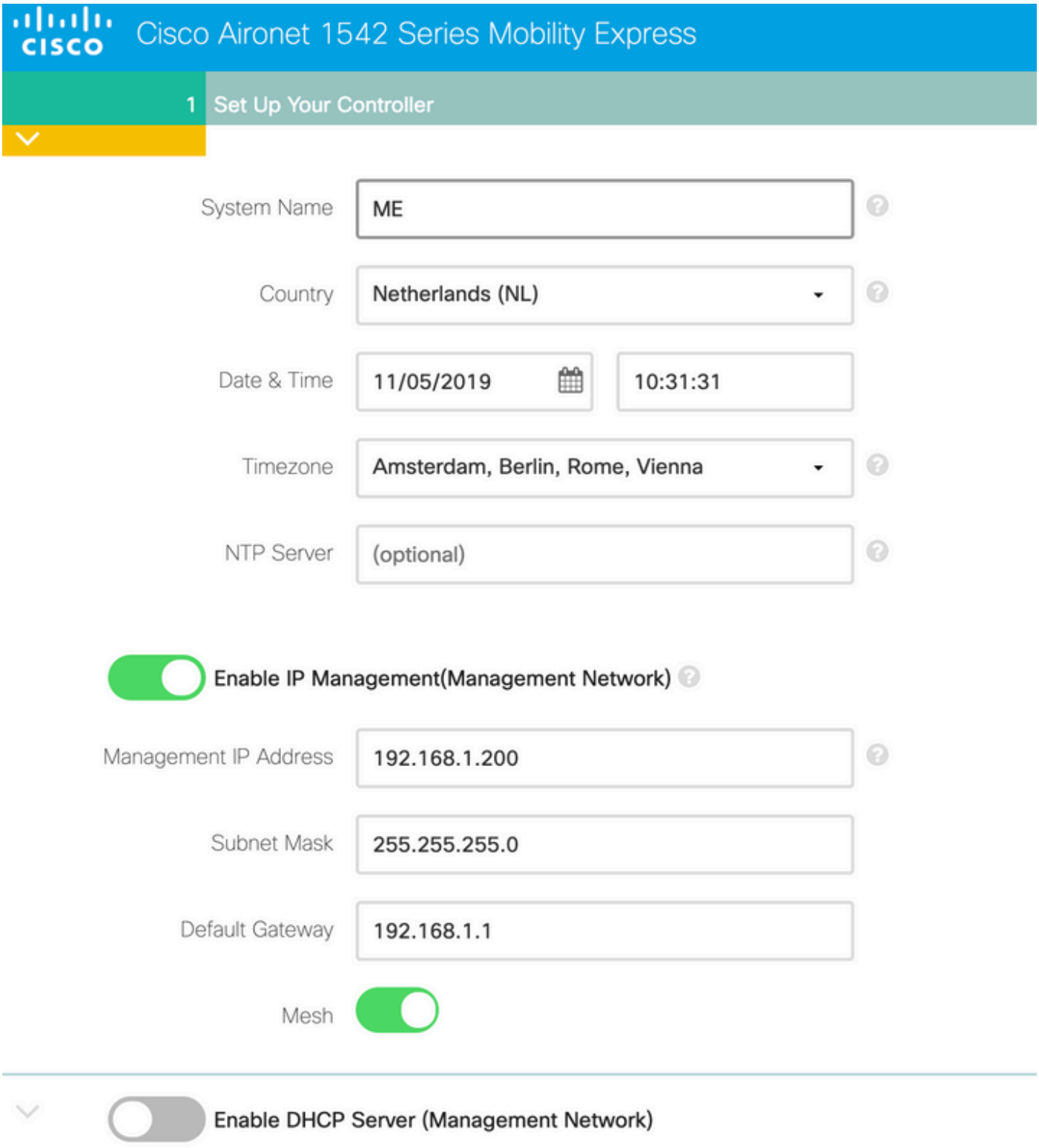


次の手順では、値を指定してコントローラを設定します。

フィールド名	説明
システム名	Mobility Express APのシステム名を入力します。例：MobilityExpress-WLC
Country	ドロップダウンリストから国を選択します。

日付/時刻	現在の日時を選択します。 注：ウィザードは、JavaScriptを使用してコンピュータからクロック情報（日付と時刻）をインポートしようとします。続行する前にクロック設定を確認することを強くお勧めします。アクセスポイントは、クロック設定に基づいてWLCに参加します。
TimeZone	現在のタイムゾーンを選択します。
NTP サーバ	NTPサーバの詳細を入力します。
Management IP	管理IPアドレスを入力します。注：アクセスポイントに割り当てられているIPとは異なるIPアドレスを指定する必要があります。この例では、APが。201 IPを取得している間に、設定ウィザードで。200を割り当てます。両方が使用されます。
サブネット マスク	サブネットマスクアドレスを入力します。
[Default Gateway]	デフォルトゲートウェイを入力します。

この設定では、DHCPサーバはスイッチ1で実行されるため、ME WLCで有効にする必要はありません。メッシュオプションをスライドして [Enable] Nextをクリックします。

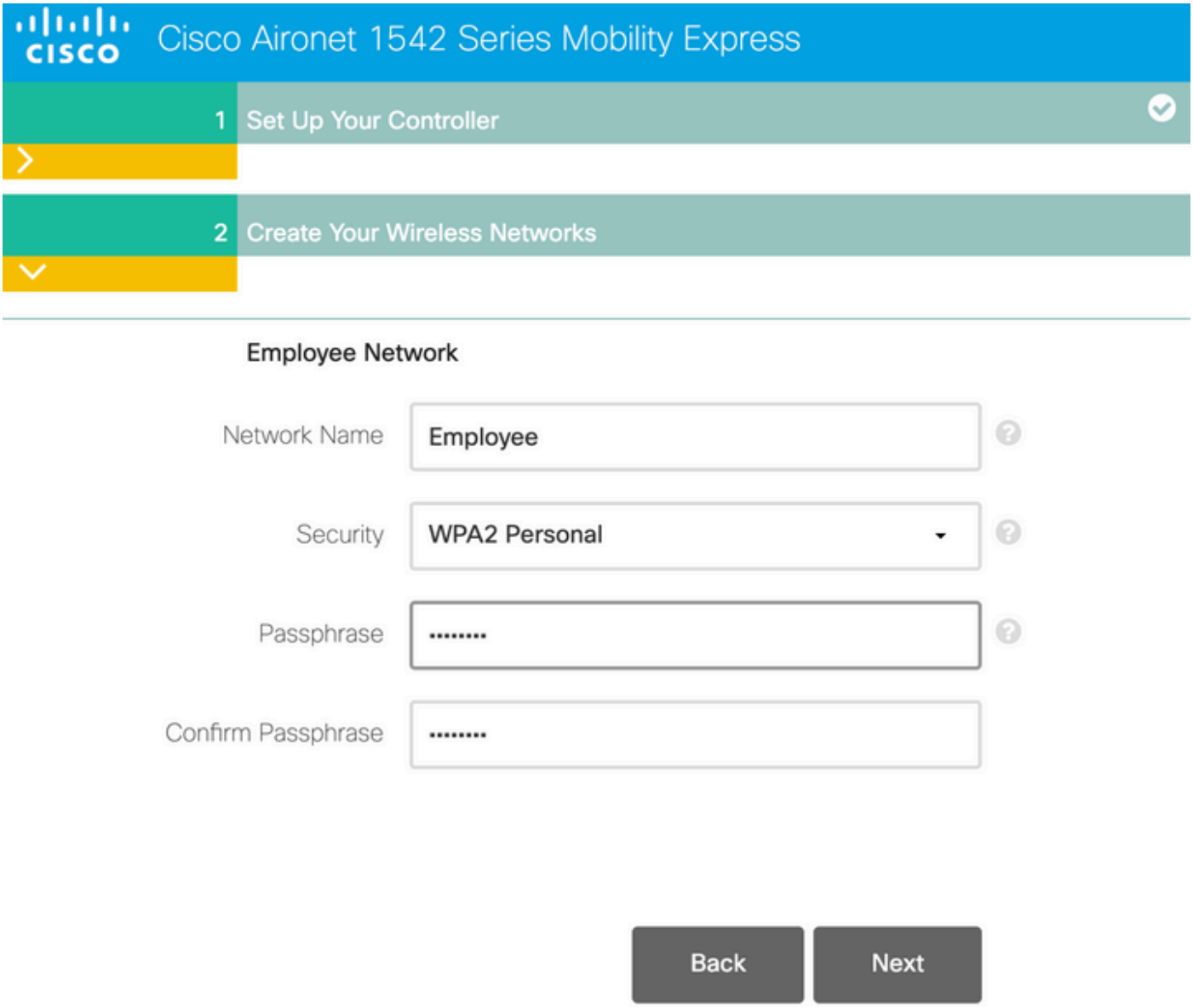


次の手順では、次のフィールドを指定してワイヤレスネットワークを作成します。

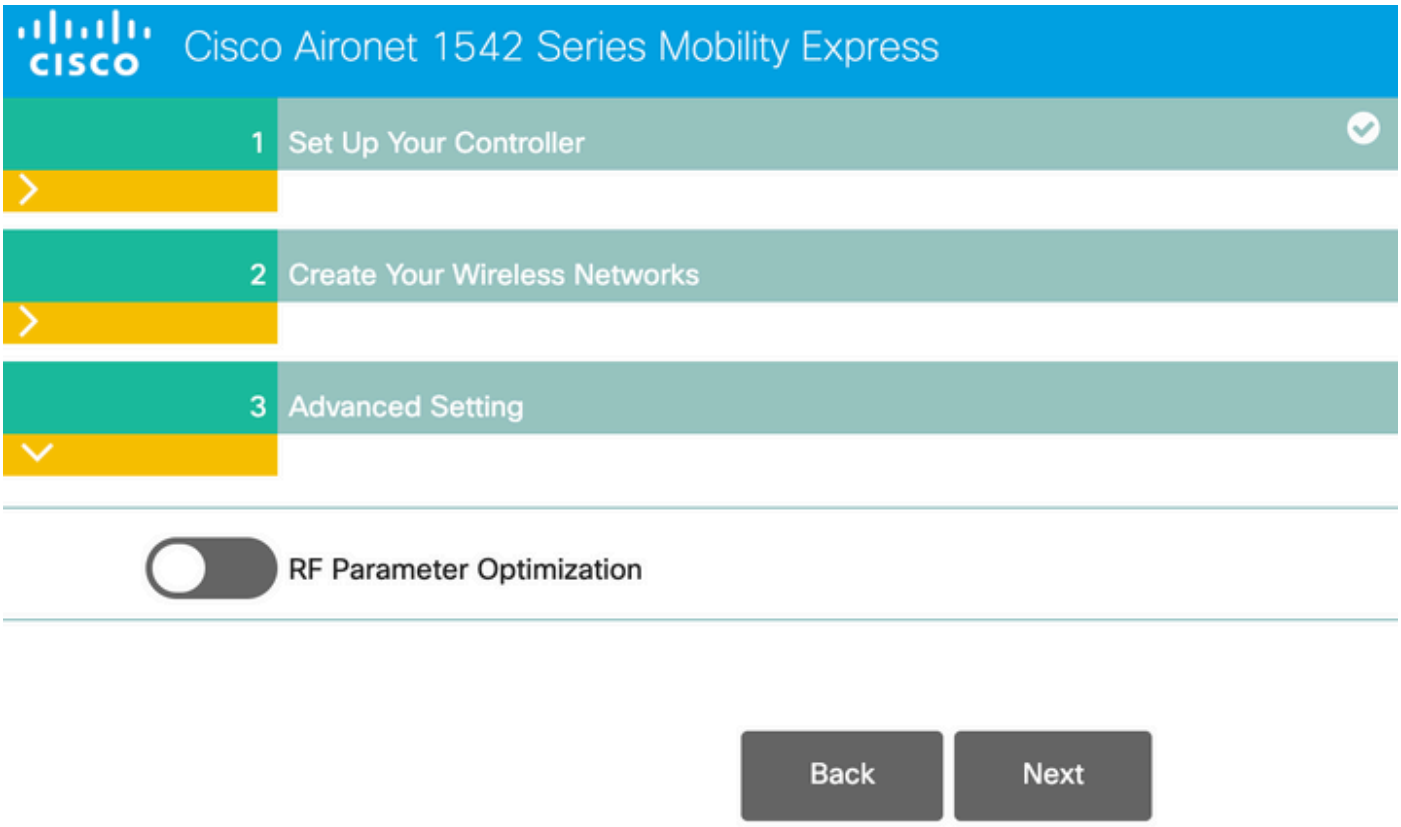
フィールド名	説明
ネットワーク名	ネットワーク名を入力します。
セキュリティ	次のいずれかを選択します WPA2 Personalセキュリティタイプをドロップダウンリストから選択します。
パスフレーズ	事前共有キー(PSK)を指定します。

パスフレーズの確認	パスフレーズを再入力して確認します。

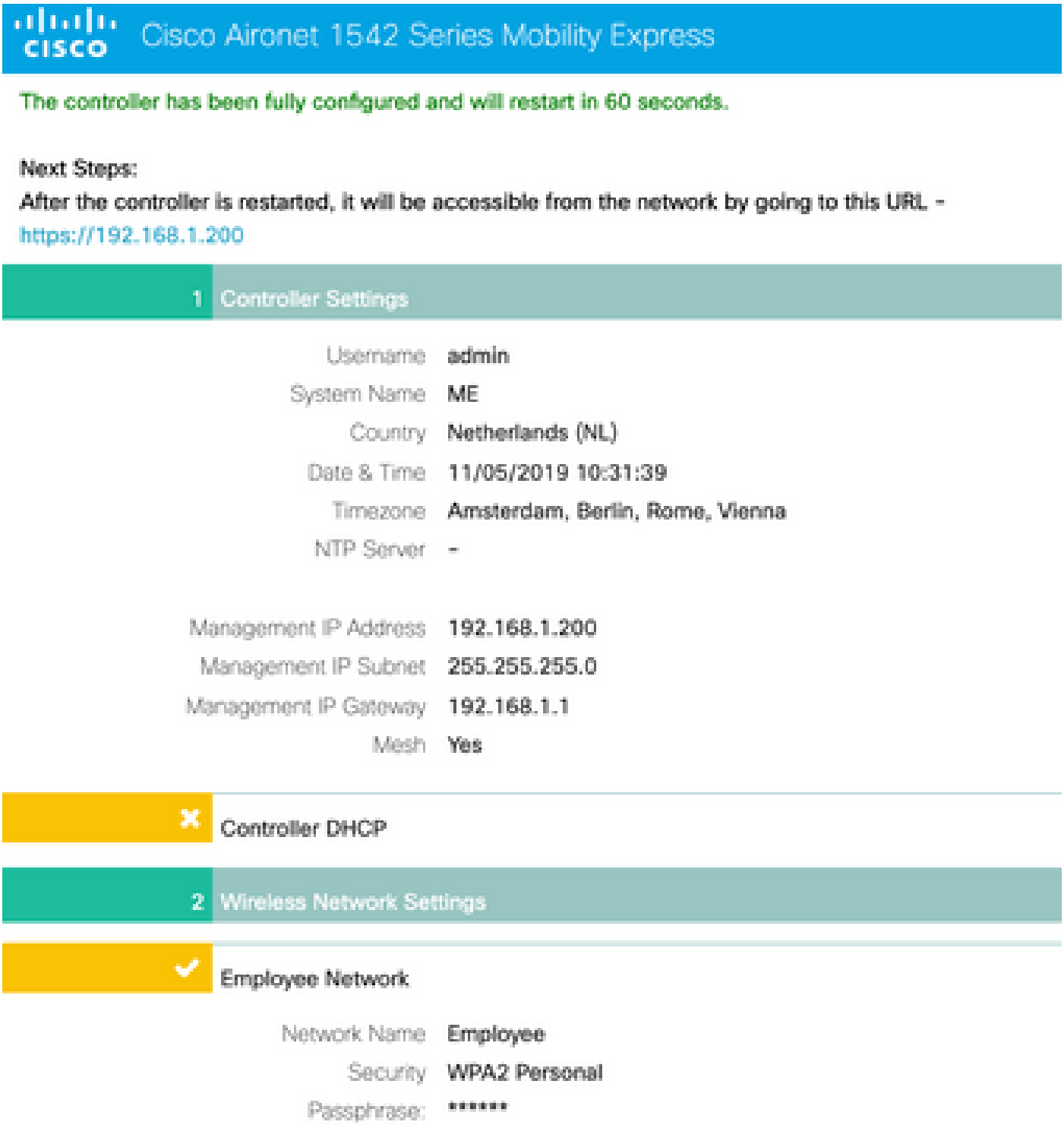
このネットワークは、後の段階で無効にできます。



[詳細設定]タブで、 RFパラメータの最適化 スライダを無効にし、「Next」をクリックします。



設定が確認されると、WLCがリブートします。



追加のメッシュ設定

メッシュリンクを確立する前に、MAPをフレックスブリッジモードに変換する必要があります。初期設定中にメッシュオプションが有効になっている場合、RAPはすでにflex-bridgeモードになっています。これはCLIから実行できます。

<#root>

MAP#

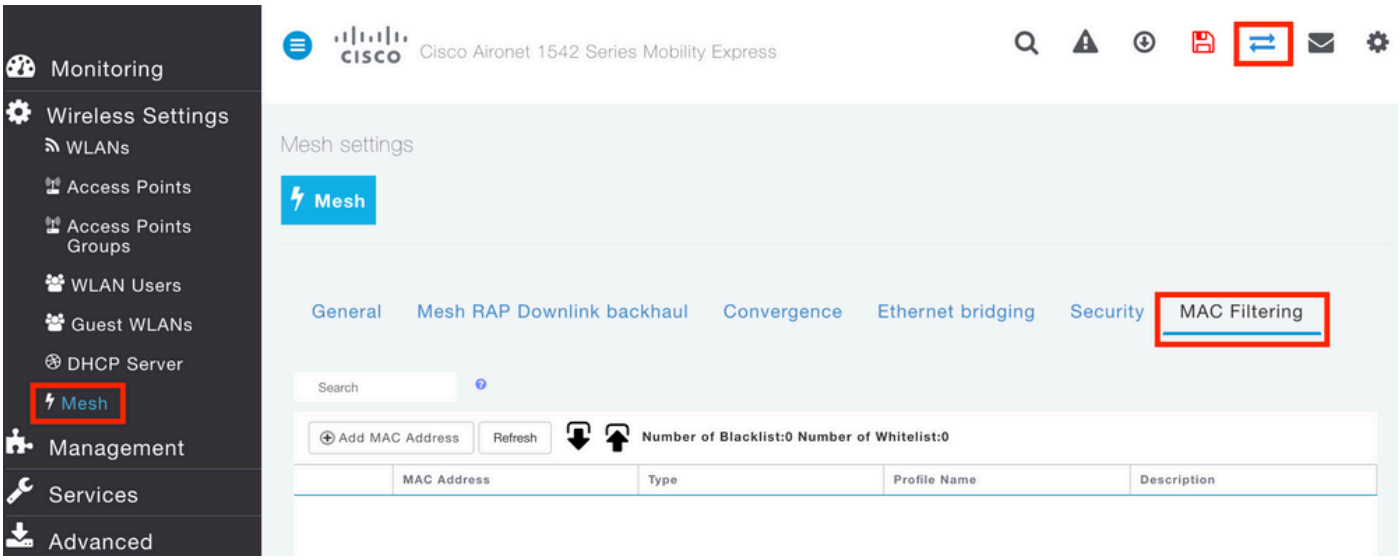
capwap ap mode flex-bridge

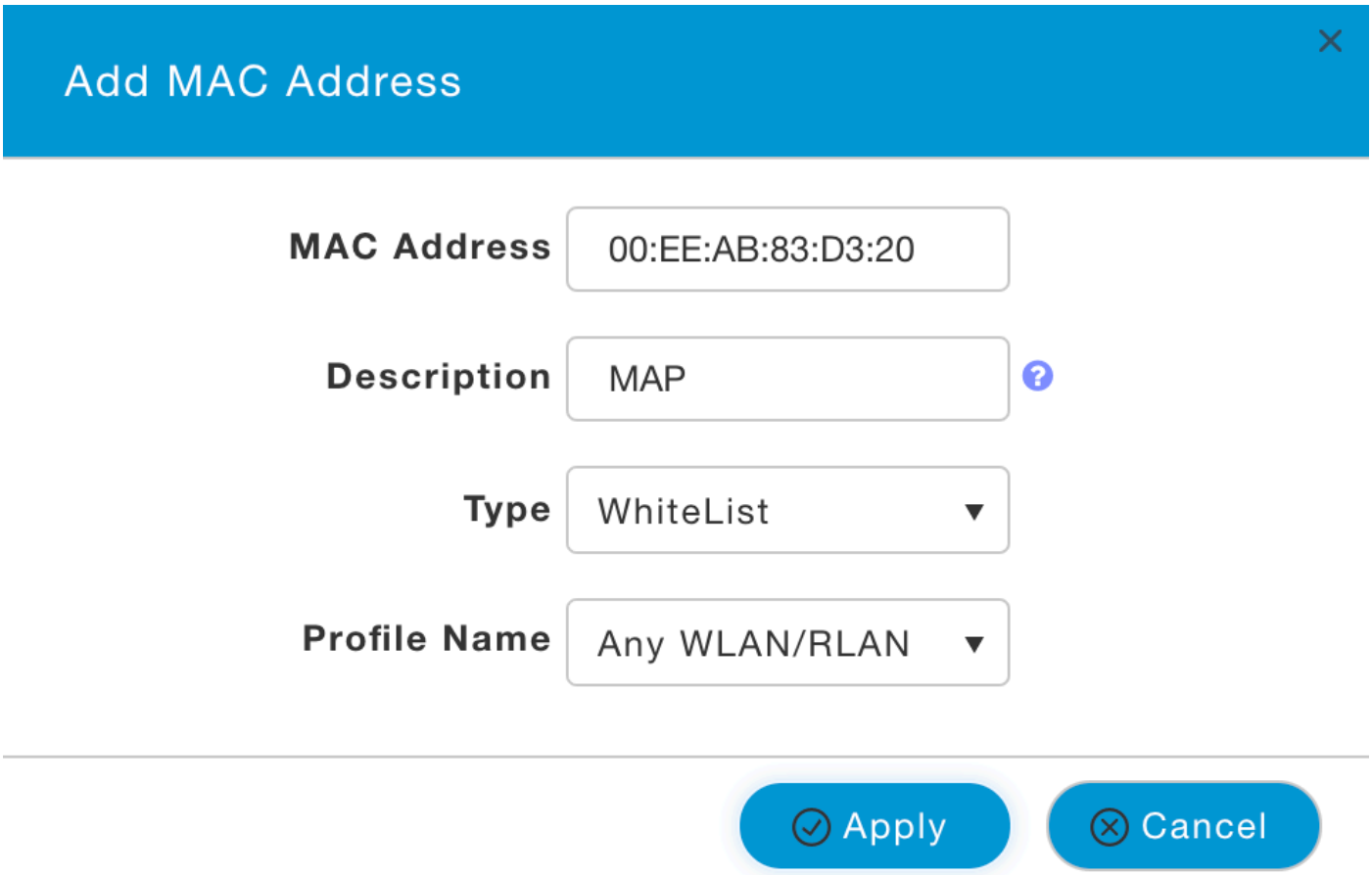
```
MAP#[*11/05/2019 18:26:28.1599] AP Rebooting: Reset Reason - AP mode changed
```

MAP top join the MEコントローラを許可する必要があります。MAPで、イーサネットインターフェイスのMACアドレスを見つけます。

```
<#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)
```

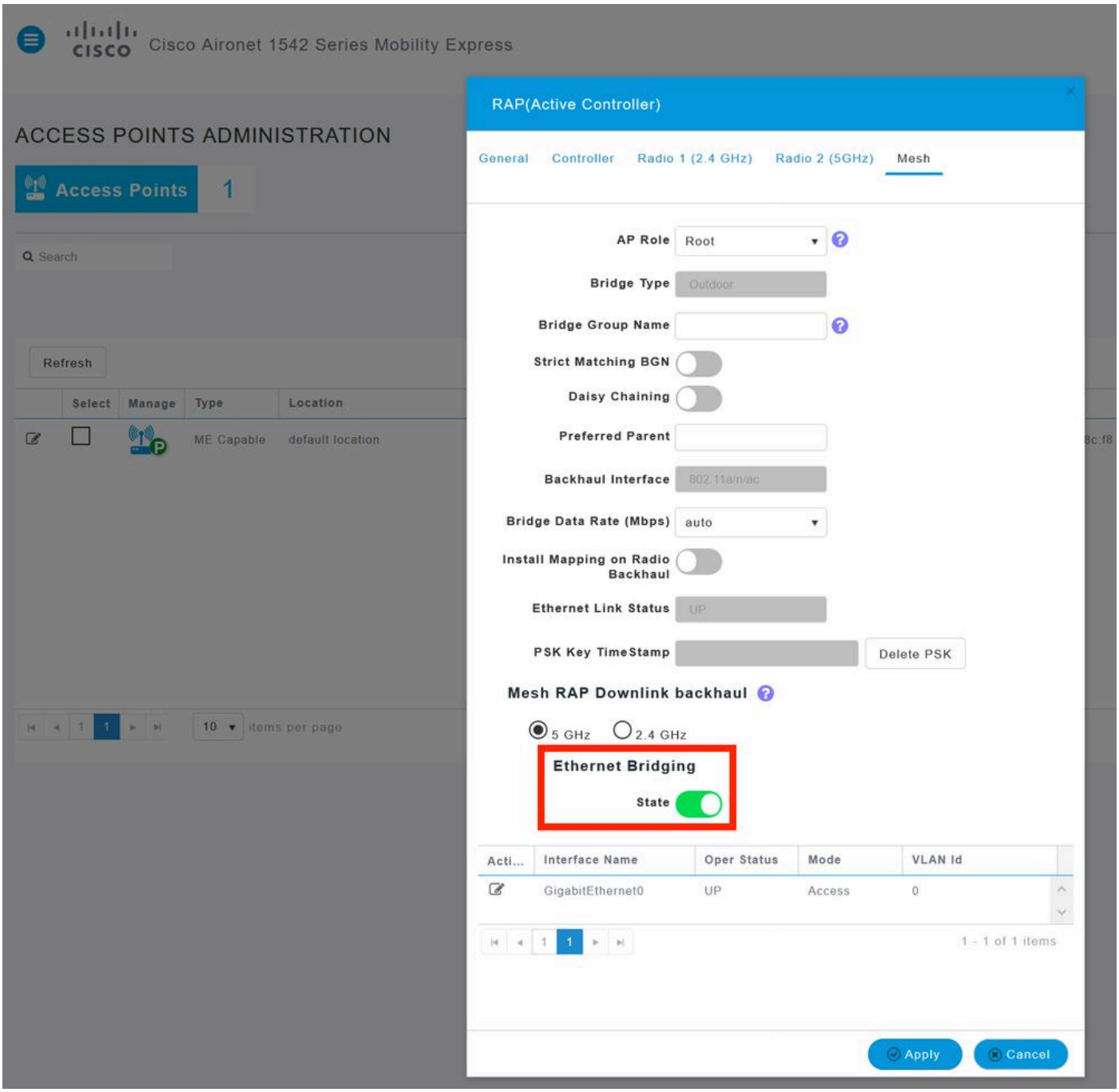
ラップトップ1から、https://192.168.1.200経由でMEコントローラのWebインターフェイスにアクセスします。エキスパートモードを有効にすると（右上隅）、ワイヤレス設定の下にメッシュタブが表示されます。MACフィルタリングで、MAPのイーサネットMACアドレスを追加します。



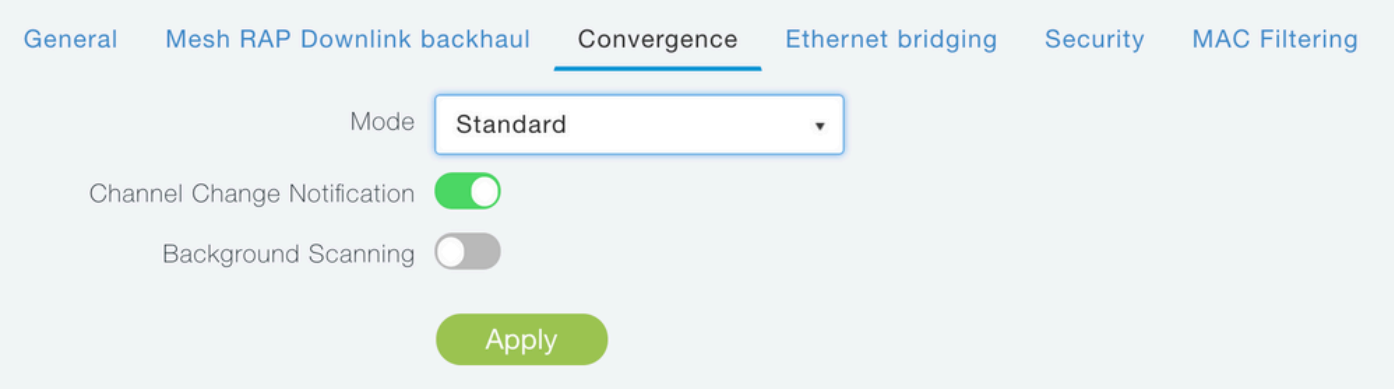


注:ME WLCに参加している、ブリッジモードまたはフレックスブリッジモードの後続のAPも承認される必要があります

これを設定した後、メッシュリンクを確立する必要があります。MAPの背後にある有線クライアントがメッシュリンクを介してトラフィックを渡すためには、MAPのWireless Settings > Access Points > MAP > Meshでイーサネットブリッジングを有効にする必要があります。



メッシュリンクが5 GHz帯域を使用している場合は、レーダーシグニチャの影響を受ける可能性があります。RAPは、レーダーイベントを検出すると、別のチャネルに切り替えます。チャネルが切り替えられることをRAPがMAPに通知するように、Channel Change Notification（CCN；チャネル変更通知）を有効にすることをお勧めします。これにより、MAPが使用可能なすべてのチャネルをスキャンする必要がなくなるため、コンバージェンス時間が大幅に短縮されます。



確認

show mesh ap summaryコマンドを実行して、MAPが結合されたことを確認できます。

<#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
```

リンクがトラフィックを通過しているかどうかをテストするために、ラップトップ1からラップトップ2にpingを実行してみます。

<#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
```

注:MAPまたはRAPのIPアドレスに対してpingを実行できるのは、メッシュリンクが確立さ

れた後だけです。

（「トラブルシューティング」）

MAP/RAPの場合：

- メッシュイベントのデバッグ

MEのWLC:

- `debug capwap events enable`
- `debug capwap errors enable`
- `debug mesh events enable`（メッシュイベントのデバッグの有効化）

MAPから確認された正常な参加プロセスの例（関連しないメッセージが修正されています）：

<#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)
[*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 2
[*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, usern
[*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) s
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Child(D4:E8:80:A0:D0:B1) generating keys to Parent D4:7
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_AUTH_RSP, Parent(D4:78:9B:7B:DF:11) stat
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent D4:78:9B:
[*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
[*11/05/2019 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, isIpv4OrIpv6Stati
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load 1, AP
[*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: 524
[*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

!
```

ヒント、コツ、よくある間違い

- MAPとRAPを有線で同じイメージバージョンにアップグレードすることで、無線でのイメージのダウンロードを回避できます（「ダーティ」RF環境では問題になる可能性があります）。
- 5GHzバックホールリンクのチャネル幅を拡大すると、SNRが低下し、誤ったレーダー検出が発生する可能性があります（主に80MHzと160MHz）。
- メッシュリンク接続は、MAPまたはRAPに対してpingを実行してテストしないでください。メッシュリンクが起動すると、pingは実行できません。
- サイトに導入する前に、制御された環境でセットアップをテストすることを強くお勧めしま

す。
- 外部アンテナを備えたAPを使用する場合は、導入ガイドを参照して、互換性のあるアンテナと接続する必要のあるポートを確認してください。
- メッシュリンクを介して異なるVLANからのトラフィックをブリッジするには、VLAN透過機能を無効にする必要があります。
- syslogサーバはデバッグ情報を提供できますが、それ以外の場合はコンソール接続でのみ利用可能なので、APに対してローカルにすることを検討してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。