

Konfigurieren einer Point-to-Point-Mesh-Verbindung mit Ethernet-Bridging auf Mobility Express-APs

Inhalt

[Einführung](#)

[Informationen zu Mobility Express](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Switch-Konfigurationen](#)

[Zurücksetzen der APs auf Werkseinstellungen](#)

[Herunterladen des Capwap-Bilds mit geringem Speicheraufkommen auf 1542-2 \(MAP\)](#)

[Herunterladen des Mobility Express-fähigen Image auf AP 1542-1 \(RAP\)](#)

[Zero-Day-SSID-Bereitstellung](#)

[Zusätzliche Mesh-Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Tipps, Tricks und häufige Fehler](#)

Einführung

In diesem Artikel wird der Prozess der Bereitstellung von Point-to-Point Mesh-Verbindungen mit Ethernet Bridging mithilfe der Cisco Mobility Express (ME)-Software für Cisco 1542 Access Points für den Außenbereich erläutert. Mesh-Unterstützung für Mobility Express-Software für Access Points in Innen- und Außenbereichen im Flex+Bridge-Modus wurde in Version 8.10 eingeführt.

Folgende AP-Modelle werden unterstützt:

- Als MIN-Root-AP: Cisco AireOS APs der Serien 1542, 1562, 1815, 3802
- Als Mesh-AP: Cisco AireOS APs 1542, 1562, 1815, 3802s

Informationen zu Mobility Express

Mobility Express (ME) ist eine Lösung, die den Autonomous AP-Modus und die Software ersetzt. Sie ermöglicht die Ausführung einer leichteren Version der AireOS-basierten WLC-Software (Wireless LAN Controller) auf dem Access Point selbst. 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, startet der "AP-Teil" zuerst. Einige Minuten später wird auch der Controller-Teil initialisiert. Sobald

eine Konsolensitzung erstellt wurde, zeigt ein ME-fähiges Gerät die WLC-Eingabeaufforderung an. Um die zugrunde liegende AP-Shell einzugeben, kann ein Befehl `apciscoshell` verwendet werden:

```
(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) >
```

Voraussetzungen

Verwendete Komponenten

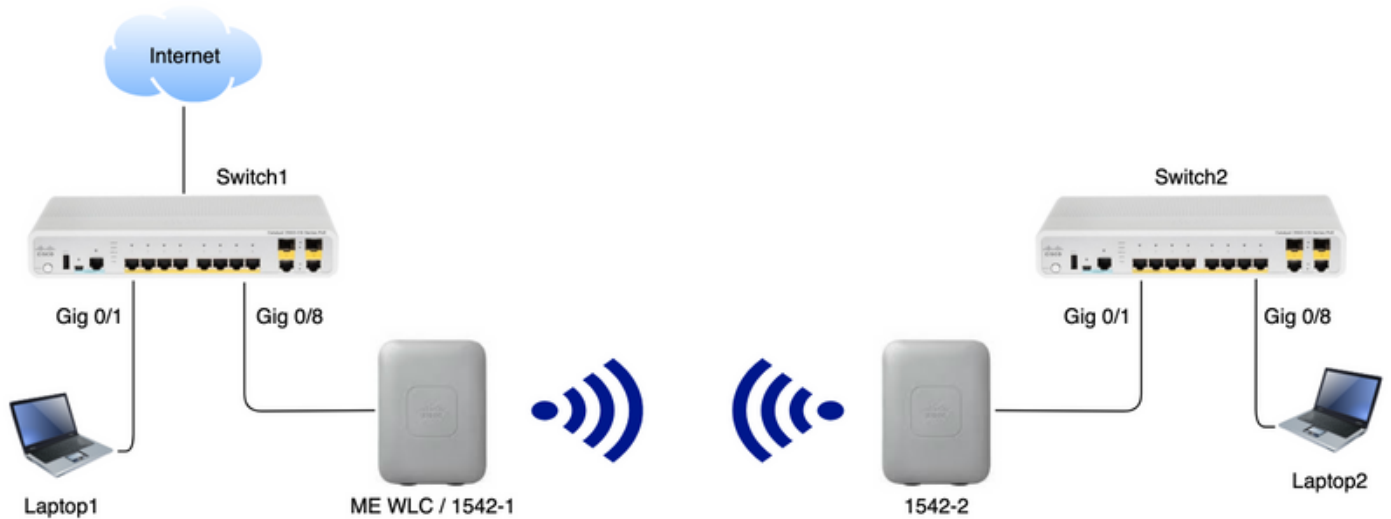
- 2 1542D-E Access Points
- 2 Cisco Switches der Serie 3560-CX
- 2 x Laptops
- 1 Konsolenkabel

Netzwerkdiagramm

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

Hinweis: Das Tagging der Verwaltungsschnittstelle kann Probleme mit dem AP verursachen, der dem internen WLC-Prozess beiträgt. Wenn Sie die Management-Schnittstelle markieren möchten, stellen Sie sicher, dass die kabelgebundene Infrastruktur entsprechend konfiguriert ist.

Gerät	IP-Adresse
Standard-Gateway	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 (MAP)	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:

```
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
```

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

```
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
```

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 Fortsetzen des Betriebs über 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 Kennwort von Cisco (Groß- und Kleinschreibung beachten).

Herunterladen des Capwap-Bilds mit geringem Speicheraufkommen auf 1542-2 (MAP)

Laptop 1 wird als TFTP-Server verwendet. Der AP 1542-2 kann zunächst an den Switch 1 Gig 0/8-Port angeschlossen werden, damit das Upgrade durchgeführt werden kann. Laden Sie auf software.cisco.com unter 1542 Lightweight Images die Version 15.3.3-JJ1 (vollständiger Name: *ap1g5-k9w8-tar.153-3.JK.tar*) herunter, die dem Image für die Version 8.10.105 entspricht. Das neueste Lightweight AP Image entspricht immer der neuesten ME Version. Legen Sie das Bild im TFTP-Stammordner ab. Verbinden Sie das Konsolenkabel, und melden Sie sich mit den Standardanmeldeinformationen an (Benutzername ist Cisco und Kennwort ist auch Cisco). Weisen Sie dem Access Point die IP-Adresse zu, und führen Sie das Upgrade 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.JK.tar
```

AP führt das Upgrade aus und startet dann neu. Vergewissern Sie sich, dass das Upgrade erfolgreich durchgeführt wurde, indem Sie den Befehl `show version` verwenden:

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

Der Access Point wird vom Switch 1 getrennt und wieder an den Switch 2 angeschlossen.

Hinweis: Indem wir das Image des MAP manuell aktualisieren, vermeiden wir, dass das Image-Upgrade ohne Benutzereingriff erfolgt, sobald die Mesh-Verbindung hergestellt wurde.

Herunterladen des Mobility Express-fähigen Image auf AP 1542-1 (RAP)

Unter Mobility Express 8.10.105-Versionen für den 1542 AP sehen wir 2 verfügbare Dateien: `.tar`

und .zip .zip-Paket herunterladen und extrahieren







Aironet 1542D Outdoor Access Point

Release 8.10.105.0














[▲ My Notifications](#)

[Related Links and Documentation](#)

[Release Notes for 8.10.105.0](#)

File Information	Release Date	Size	
Cisco 1540 Series Mobility Express Release 8.10 Software, to be used for conversion from Lightweight Access Points only. AIR-AP1540-K9-ME-8-10-105-0.tar	19-Oct-2019	56.50 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. AIR-AP1540-K9-ME-8-10-105-0.zip	19-Oct-2019	422.16 MB	  

Im Gegensatz zu einem physischen WLC verfügen ME Access Points nicht über genügend Flash-Speicher, um alle AP-Images zu speichern. Daher ist es erforderlich, einen jederzeit verfügbaren TFTP-Server bereitzustellen. Extrahieren Sie die ZIP-Datei, und kopieren Sie deren Inhalt in das Root des TFTP-Servers. Die extrahierte Datei enthält mehrere AP-Images:

Name
 ap_supp_list.inc
 ap1g1
 ap1g4
 ap1g4-capwap
 ap1g5
 ap1g6
 ap1g6a
 ap1g7
 ap3g2
 ap3g3
 apname_decoder.inc
 c3700
 version.info

Die Textdatei *apname_decoder.inc* enthält alle Namen der entsprechenden AP-Abbilder:

```

/*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)

```

Um das Upgrade durchzuführen, schließen Sie die Konsole an den AP 1542-1 an, weisen Sie der Konsole eine IP-Adresse zu, und führen Sie das Upgrade des Image 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/ap1g5
```

Nach Abschluss des Upgrades wird der Access Point neu gestartet. Kurz nach dem Start des Access Points wird auch der Startvorgang des Controllers gestartet. In Kürze wird die Zero-Day-Bereitstellung der SSID "CiscoAirProvision" übertragen.

Vergewissern Sie sich, dass das Upgrade erfolgreich durchgeführt wurde, indem Sie den Befehl `show version` verwenden:

```
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
```

Zero-Day-SSID-Bereitstellung

Stellen Sie mithilfe des **Kennworts** eine Verbindung zur vom Access Point gesendeten CiscoAirProvision-SSID her. Der Laptop erhält eine IP-Adresse aus dem Subnetz 192.168.1.0/24.

Falls die SSID nicht gesendet wird, ist es weiterhin möglich, dass der Access Point in "Mobility Express CAPABLE" (Mobility Express-fähig), jedoch nicht als Mobility Express ausgeführt wird. Anschließend müssen Sie eine Verbindung zur AP-CLI herstellen und **ap type mobility-express** eingeben und der Access Point sollte neu starten und die Provisioning SSID übertragen.

Öffnen Sie die Adresse <http://192.168.1.1> in einem Webbrowser. Diese Seite wird zum Assistenten zur Erstkonfiguration umgeleitet. Erstellen Sie ein Administratorkonto auf dem Controller, indem Sie Admin-Benutzername und -Kennwort angeben, und klicken Sie dann auf 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.

Richten Sie im nächsten Schritt den Controller durch Angeben der Werte ein.

Feldname

Systemname

Land

Datum und Uhrzeit

Beschreibung

Geben Sie den Systemnamen für den Mobility Express Access Point ein. Beispiel: MobilitätExpress-WLAN
Wählen Sie aus der Dropdown-Liste ein Land aus.
Wählen Sie das aktuelle Datum und die aktuelle Uhrzeit aus.

Hinweis: Der Assistent versucht, die Uhreninformationen (Datum und Uhrzeit) mithilfe

JavaScript vom Computer zu importieren. Es wird dringend empfohlen, die Uhreinstellungen zu bestätigen, bevor Sie fortfahren. Die Access Point-Konfiguration ist von den Uhreinstellungen abhängig, um dem Netzwerk beizutreten.

Wählen Sie die aktuelle Zeitzone aus.

Geben Sie die NTP-Serverdetails ein.

Geben Sie die Management-IP-Adresse ein. HINWEIS:

Sie muss sich von der IP-Adresse des Access Points unterscheiden. In diesem Beispiel wurde dem Access Point zwar die IP-Adresse .201 zugewiesen, im Konfigurationsassistenten jedoch die Adresse .202. Beide werden verwendet.

Geben Sie die Adresse der Subnetzmaske ein.

Geben Sie das Standard-Gateway ein.

Zeitzone

NTP-Server

Management-IP

Subnetzmaske

Standard-Gateway

In dieser Konfiguration wird der DHCP-Server auf Switch 1 ausgeführt, sodass die Aktivierung auf dem ME WLC nicht erforderlich ist. Verschieben Sie die Option Mesh zu **Aktivieren** und klicken Sie auf **Weiter**.

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)

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

Feldname

Netzwerkname

Sicherheit

Passphrase

Passphrase bestätigen

Beschreibung

Geben Sie den Netzwerknamen ein.

Wählen Sie **Persönlicher WPA2-Sicherheitstyp** aus der **Dropdown-Liste**.

Geben Sie den PSK (Pre-Shared Key) an.

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

Dieses Netzwerk kann zu einem späteren Zeitpunkt deaktiviert werden.



1 Set Up Your Controller 



2 Create Your Wireless Networks



Employee Network

Network Name 

Security 

Passphrase 

Confirm Passphrase

Back

Next

Belassen Sie auf der Registerkarte Erweiterte Einstellungen die **Optimierung von Funkparametern** deaktiviert ist, und klicken Sie auf **Weiter**.



1 Set Up Your Controller



2 Create Your Wireless Networks



3 Advanced Setting



RF Parameter Optimization

Back

Next

Nach Bestätigung der Einstellungen wird der WLC neu gestartet:



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

✘ Controller DHCP

2 Wireless Network Settings

✔ Employee Network

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

Zusätzliche Mesh-Konfiguration

Vor dem Herstellen der Mesh-Verbindung muss der MAP in den Flex-Bridge-Modus konvertiert werden. Der RAP befindet sich bereits im Flex-Bridge-Modus, wenn die Mesh-Option während der Erstkonfiguration aktiviert wurde. Dies kann über die CLI erfolgen:

```
MAP# capwap ap mode flex-bridge
```

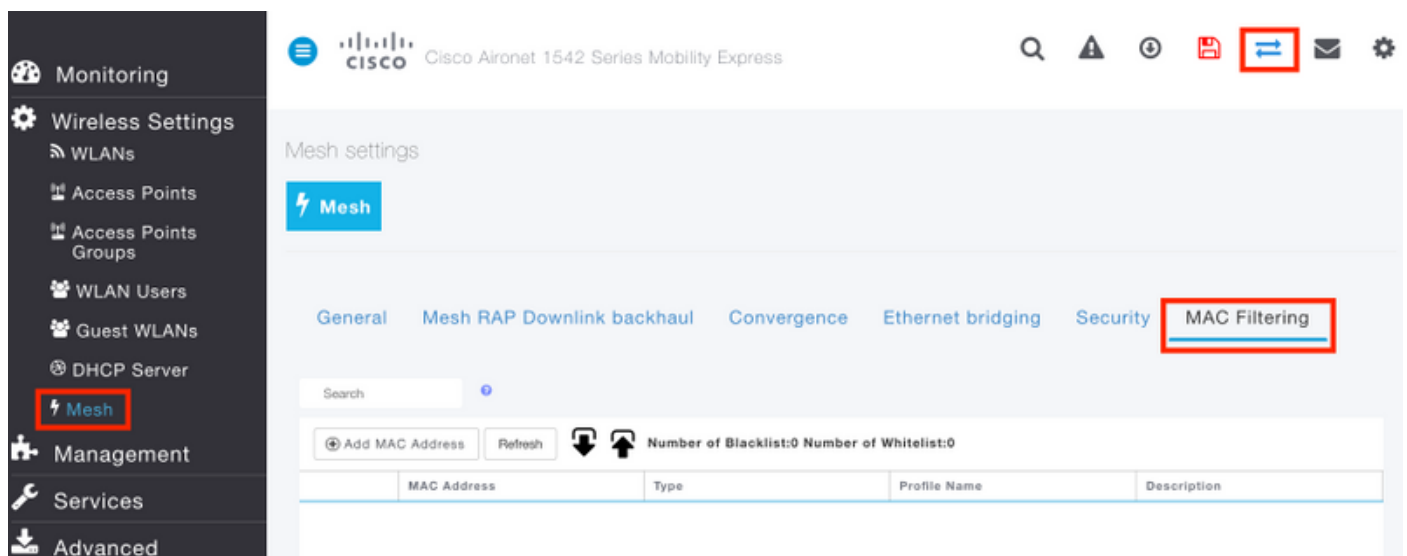
```
MAP#[*11/05/2019 18:26:28.1599] AP Rebooting: Reset Reason - AP mode changed
```

Damit MAP top dem ME-Controller beitreten kann, muss er autorisiert werden. Auf MAP finden Sie die MAC-Adresse der Ethernet-Schnittstelle:

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)
```

Greifen Sie von Laptop 1 über <https://192.168.1.200> auf die Webschnittstelle des ME Controllers zu. Nachdem der Expertenmodus aktiviert wurde (oben rechts), wird unter Wireless-Einstellungen eine Mesh-Registerkarte angezeigt. Fügen Sie unter MAC-Filterung die Ethernet-MAC-Adresse des MAP hinzu:



Add MAC Address

MAC Address

Description ?

Type ▼

Profile Name ▼

Hinweis: Alle nachfolgenden Access Points im Bridge- oder Flex-Bridge-Modus, die dem ME WLC hinzugefügt werden, müssen ebenfalls autorisiert werden.

Nach der Einrichtung sollte eine Mesh-Verbindung eingerichtet werden. Damit kabelgebundene Clients hinter dem MAP den Datenverkehr über die Mesh-Verbindung weiterleiten können, muss Ethernet-Bridging auf der MAP unter **Wireless Settings > Access Points > MAP > Mesh** aktiviert sein:

The screenshot shows the configuration page for a RAP (Active Controller) in the Mesh tab. The 'Ethernet Bridging' toggle is highlighted with a red box and is turned on. The 'Mesh RAP Downlink backhaul' section shows the 5 GHz radio selected. Below the configuration fields is a table with one entry for the GigabitEthernet0 interface.

Acti...	Interface Name	Oper Status	Mode	VLAN id
	GigabitEthernet0	UP	Access	0

Wenn der Mesh-Link ein 5-GHz-Band verwendet, kann dies durch Radarsignaturen beeinträchtigt werden. Sobald der RAP ein Radarereignis erkennt, wechselt er zu einem anderen Kanal. Es wird empfohlen, die Channel Change Notification zu aktivieren, damit RAP dem MAP mitteilt, dass der Kanal gewechselt wird. Dadurch wird die Konvergenzzeit erheblich reduziert, da MAP nicht alle verfügbaren Kanäle scannen muss:

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

Mode

Channel Change Notification

Background Scanning

Überprüfen

Sie können überprüfen, ob der MAP beigetreten ist, indem Sie den Befehl `show Mesh ap summary` ausführen:

(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

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

VAPERОВI:~ 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 MAP- oder RAP-IP-Adressen nur dann pingen, wenn der Mesh-Link eingerichtet wurde.

Fehlerbehebung

Auf MAP/RAP:

- Mesh-Debugereignisse

Auf ME WLC:

- Debug-CAWAP-Ereignisse aktivieren
- Debug Capwap-Fehler aktivieren
- debuggen Mesh-Ereignisse aktivieren

Beispiel für einen erfolgreichen Join-Prozess, der über den MAP beobachtet wurde (einige Meldungen wurden korrigiert, da sie nicht relevant sind):

```
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) 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!

```

Tipps, Tricks und häufige Fehler

- Durch die Aktualisierung von MAP und RAP auf dieselbe Image-Version über das Kabel vermeiden wir den Download von Bildern über die Luft (was in "schmutzigen" Funkumgebungen problematisch sein kann).
- Eine Erhöhung der Kanalbreite der 5-GHz-Backhaul-Verbindung kann zu einer geringeren SNR- und falschen Radarerkennung 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 pingeln, sobald die Mesh-Verbindung hergestellt ist.
- Es wird dringend empfohlen, die Konfiguration in einer kontrollierten Umgebung zu testen, bevor sie vor Ort bereitgestellt wird.
- Wenn APs mit externen Antennen verwendet werden, überprüfen Sie im Bereitstellungsleitfaden, welche Antennen kompatibel sind und welchen Anschluss sie anschließen sollen.
- Um den Datenverkehr verschiedener VLANs über die Mesh-Verbindung zu überbrücken, muss die VLAN Transparent-Funktion deaktiviert werden.
- Erwägen Sie, einen Syslog-Server für die APs lokal zu verwenden, da dieser Debugging-Informationen bereitstellen kann, die ansonsten nur über eine Konsolenverbindung verfügbar sind.