

Mobility Express AP에서 이더넷 브리징을 사용하여 Point-to-Point 메시 링크 구성

목차

[소개](#)

[Mobility Express 정보](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[설정](#)

[스위치 구성](#)

[AP의 공장 초기화](#)

[1542-2\(MAP\)에 경량형 capwap 이미지 다운로드](#)

[AP 1542-1\(RAP\)에 Mobility Express 지원 이미지 다운로드](#)

[제로 데이 SSID 프로비저닝](#)

[추가 메시 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[팁, 요령 및 일반적인 실수](#)

소개

이 문서는 Cisco ME(Mobility Express) 소프트웨어를 사용하여 이더넷 브리징을 사용하여 Point-to-Point 메시 링크를 구축하는 프로세스에 대해 설명합니다.

Mobility Express 정보

이 문서에서는 Cisco 1542 실외 액세스 포인트를 사용합니다. Flex+Bridge 모드의 실내 및 실외 AP에 대한 Mobility Express 소프트웨어에 대한 메시 지원은 릴리스 8.10에 도입되었습니다.

다음 AP 모델이 지원됩니다.

- ME 루트 AP: Cisco AireOS 1542, 1562, 1815s, 3802s AP
- 메시 AP 역할: Cisco AireOS 1542, 1562, 1815s, 3802s AP

ME(Mobility Express)는 자동 AP 모드 및 소프트웨어를 대체하는 솔루션입니다. 액세스 포인트 자체에서 더 가벼운 버전의 AireOS 기반 WLC(Wireless LAN Controller) 소프트웨어를 실행할 수 있습니다. WLC와 AP 코드는 모두 AP 메모리의 단일 파티션 내에 저장됩니다. Mobility Express 구축에는 라이선스 파일 또는 라이선스 활성화가 필요하지 않습니다.

Mobility Express 지원 소프트웨어를 실행하는 디바이스의 전원이 켜지면 "AP 부품"이 먼저 부팅됨

니다. 몇 분 후 컨트롤러 부분도 초기화됩니다. 콘솔 세션이 설정되면 ME 지원 디바이스에서 WLC 프롬프트를 표시합니다. 기본 AP 셸에 들어가려면 `apciscoshell` 명령을 사용할 수 있습니다.

```
<#root>
```

```
(Cisco Controller) >
```

```
apciscoshell
```

```
!!Warning!!: You are entering ap shell. This will stop you from establishing new telnet/SSH/Web session.  
Also the existing sessions will be suspended till you exit the ap shell.  
To exit the ap shell, use 'logout'
```

```
User Access Verification
```

```
Username:
```

```
admin
```

```
Password:
```

```
*****
```

```
RAP>
```

```
logout
```

```
(Cisco Controller) >
```

사전 요구 사항

사용되는 구성 요소

- 2x 1542D-E 액세스 포인트
- 3560-CX Cisco 스위치 2개
- 2x 노트북
- 콘솔 케이블 1개

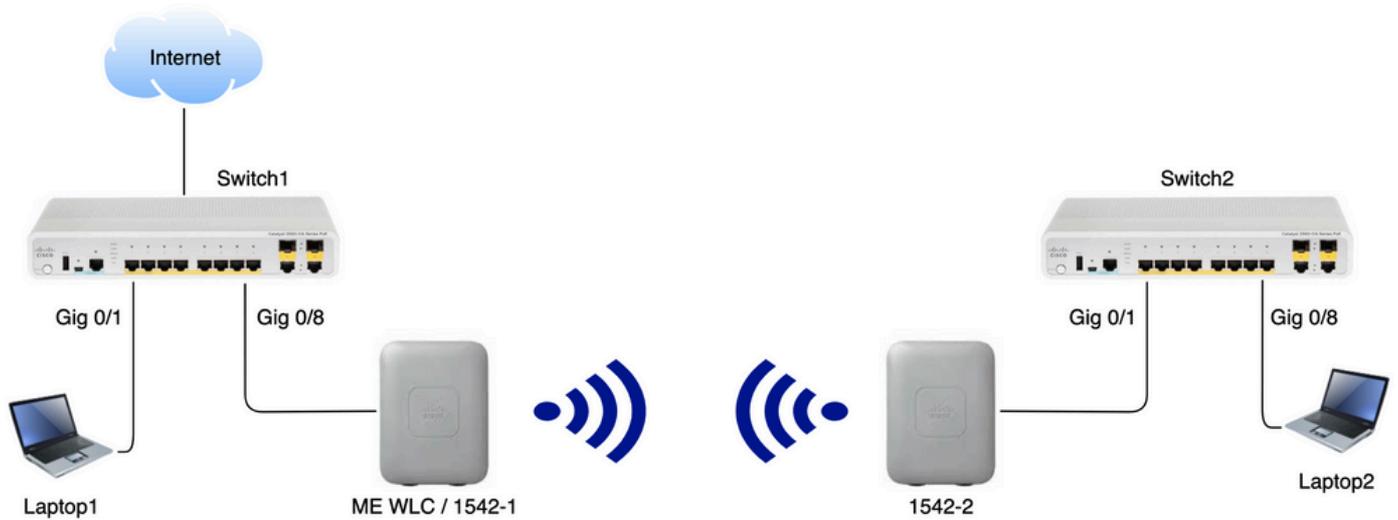
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 네트워크의 모든 디바이스는 192.168.1.0/24 서브넷 내에 있습니다. Mobility Express AP(컨트롤러)의 관리 인터페이스는 태그가 지정되지 않지만 모든 포트의 기본 VLAN은 VLAN 39가 됩니다. AP 1542-1은 컨트롤러 및 RAP(Root Access Point)의 역할을 하며, AP 1542-2는 MAP(Mesh Access Point)의 역할을 합니다. 이 표에는 네트워크에 있는 모든 디바이스의 IP 주소가 포함되어 있습니다.

참고: 관리 인터페이스에 태그를 지정하면 내부 WLC 프로세스에 참여하는 AP에 문제가 발생할 수 있습니다. 관리 인터페이스에 태그를 지정하기로 결정한 경우 유선 인프라 부분이 적절하게 구성되었는지 확인합니다.

디바이스	IP 주소
기본 게이트웨이	192.168.1.1
랩톱 1	192.168.1.100
랩톱 2	192.168.1.101
Mobility Express WLC	192.168.1.200
1542-1(RAP)	192.168.1.201
1542-2 (지도)	192.168.1.202



설정

스위치 구성

랩톱이 연결되는 스위치 포트는 VLAN이 39로 설정된 액세스 포트 구성됩니다.

```
<#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
```

AP가 연결된 스위치 포트는 기본 VLAN이 39로 설정된 트렁크 모드가 됩니다.

```
<#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
```

AP의 공장 초기화

새 구축을 시작하기 전에 AP의 공장 재설정을 수행하는 것이 좋습니다. 이 작업은 AP의 모드/재설정 버튼을 누르고 전원을 연결한 다음 20초 이상 계속 유지하면 수행할 수 있습니다. 이렇게 하면 이전 컨피그레이션이 모두 초기화됩니다. AP는 콘솔 연결을 통해 기본 사용자 이름 Cisco와 비밀번호 Cisco(대/소문자 구분)로 액세스할 수 있습니다.

AP가 Mobility Express에서 이미 실행 중인 경우 출고 시 재설정이 반드시 AP를 경량 모드로 다시 이동하지는 않습니다. 중요한 단계는 AP에서 경량 이미지 또는 Mobility Express 이미지를 실행 중인지 확인하는 것입니다.

AP가 경량인 경우 mobility express 코드를 다운로드하여 Mobility Express로 변환할 수 있습니다. AP가 이미 mobility express 모드에 있는 경우, 소프트웨어 버전을 변경하려면 액세스 포인트/컨트롤러의 GUI에서 업그레이드 프로세스를 수행해야 합니다.

경량 이미지를 실행하는 AP의 show 버전 예:

```
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
```

다음은 Mobility Express 소프트웨어에서 이미 실행 중인 AP의 예입니다.

```
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
```

1542-2(MAP)에 경량형 capwap 이미지 다운로드

랩톱 1이 TFTP 서버로 사용됩니다. AP 1542-2는 업그레이드를 수행할 수 있도록 처음에 스위치 1Gig 0/8 포트에 연결할 수 있습니다. software.cisco.com의 1542 LDS(Lightweight) 이미지에서 8.10.185 릴리스 이미지에 해당하는 15.3.3-JJ1(전체 이름 ap1g5-k9w8-tar.153-3.JK9.tar)을 다운로드합니다. 최신 경량 AP 이미지는 항상 최신 ME 버전과 일치합니다.

이미지를 TFTP 루트 폴더에 저장합니다. 콘솔 케이블을 연결하고 기본 자격 증명을 사용하여 로그인합니다(사용자 이름은 Cisco이고 비밀번호도 Cisco). AP에 IP 주소를 할당하고 다음 명령을 사용하여 업그레이드를 수행합니다.

```
#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
```

AP가 업그레이드를 수행한 다음 재부팅합니다. show version 명령을 사용하여 업그레이드가 성공했는지 확인합니다.

```
<#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
```

AP가 스위치 1에서 분리되고 스위치 2에 다시 연결됩니다.

참고: MAP의 이미지를 수동으로 업그레이드함으로써 메시 링크가 설정된 후 이미지 업그레이드 프로세스가 OTA(over-the-air)로 진행되는 것을 방지합니다.

AP 1542-1(RAP)에 Mobility Express 지원 이미지 다운로드

1542 AP용 Mobility Express 8.10.105 릴리스에서는 .tar 및 .zip의 2가지 파일을 볼 수 있습니다.
.tar 파일 다운로드

Aironet 1542I Outdoor Access Point

Release 8.10.185.0

[My Notifications](#)

Related Links and Documentation

[Release Notes for 8.10.185.0](#)

File Information	Release Date	Size	
Cisco 1540 Series Mobility Express Release 8.10 Software, to be used for conversion from Lightweight Access Points only.  AIR-AP1540-K9-ME-8-10-185-0.tar Advisories 	24-Mar-2023	60.80 MB	 
Cisco 1540 Series Mobility Express Release 8.10 Software. Access Point image bundle, to be used for software update and/or supported access points images.  AIR-AP1540-K9-ME-8-10-185-0.zip Advisories 	24-Mar-2023	503.27 MB	 

.tar 파일 다운로드

물리적 WLC와 달리 ME 액세스 포인트에는 플래시 메모리가 부족하여 모든 AP 이미지를 저장할 수 없으므로 Mobility Express 액세스 포인트에 추가 AP를 연결하려는 경우 항상 TFTP 서버에 액세스할 수 있어야 합니다. 이 예제와 같이 AP를 수동으로 업그레이드하는 경우에는 이 단계가 필요하지 않습니다.

업그레이드를 수행하려면 콘솔을 AP 1542-1에 연결하고 IP 주소를 할당한 다음 이미지 업그레이드를 수행합니다.

```
#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
```

업그레이드가 완료되면 AP가 재부팅됩니다. AP가 켜진 후 곧 컨트롤러 파트도 부팅하기 시작합니다. 곧 제로 데이 프로비저닝 SSID "CiscoAirProvision"이 브로드캐스트되는 것을 볼 수 있습니다.

콘솔에 있는 경우 CLI 마법사를 볼 수 있지만 AP를 이와 같이 구성하지 않습니다. Over-the-air GUI 마법사를 사용하면 됩니다.

제로 데이 SSID 프로비저닝

비밀번호 비밀번호를 사용하여 AP에서 브로드캐스트하는 "CiscoAirProvision" SSID에 연결합니다. 노트북 컴퓨터는 서브넷 192.168.1.0/24에서 IP 주소를 가져옵니다.

브로드캐스트되는 SSID가 표시되지 않는 경우에도 AP가 "Mobility express CAPABLE"에 있지만 mobility express로 실행되지 않을 수 있습니다. 그런 다음 AP CLI에 연결하고 ap type mobility-express를 입력해야 하며 AP가 재부팅되고 프로비저닝 SSID를 브로드캐스트합니다.

이 설정 중에 필요한 경우 "capwap ap mode local/flex-bridge"를 사용하여 로컬 모드와 메시 모드 간에 AP를 변환할 수도 있습니다.

웹 브라우저에서 <http://192.168.1.1> 주소를 엽니다. 이 페이지는 초기 컨피그레이션 마법사로 리디렉션됩니다. 관리자 사용자 이름 및 비밀번호를 지정하고 Start(시작)를 클릭하여 컨트롤러에서 관리자 계정을 생성합니다.



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.

다음 단계에서는 값을 지정하여 컨트롤러를 설정합니다.

필드 이름	설명
시스템 이름	Mobility Express AP의 시스템 이름을 입력합니다. 예: MobilityExpress-WLC
국가	드롭다운 목록에서 국가를 선택합니다.

날짜 및 시간	<p>현재 날짜 및 시간을 선택합니다.</p> <p>참고: 마법사는 JavaScript를 사용하여 컴퓨터에서 시계 정보(날짜 및 시간)를 가져오려고 시도합니다. 계속하기 전에 시계 설정을 확인하는 것이 좋습니다. 액세스 포인트는 클럭 설정에 따라 WLC에 조인합니다.</p>
시간대	현재 표준 시간대를 선택합니다.
NTP 서버	NTP 서버 세부사항을 입력합니다.
관리 IP	관리 IP 주소를 입력합니다. 참고: 액세스 포인트에 할당된 IP와 달라야 합니다. 이 예에서는 AP가 .201 IP를 가져오는 동안 컨피그레이션 마법사에서 .200을 할당합니다. 둘 다 사용됩니다.
서브넷 마스크	서브넷 마스크 주소를 입력합니다.
기본 게이트웨이	기본 게이트웨이를 입력합니다.

이 설정에서는 DHCP 서버가 스위치 1에서 실행되므로 ME WLC에서 활성화할 필요가 없습니다. 메쉬 옵션을 다음으로 밀기 사용 다음을 클릭합니다.

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)

다음 단계에서는 다음 필드를 지정하여 무선 네트워크를 만듭니다.

필드 이름	설명
네트워크 이름	네트워크 이름을 입력합니다.
보안	다음을 선택합니다. 드롭다운 목록의 WPA2 개인 보안 유형
암호	PSK(Pre-Shared Key)를 지정합니다.
암호 확인	암호를 다시 입력하고 확인합니다.

이 네트워크는 나중 단계에서 비활성화할 수 있습니다.

The image shows the Cisco Aironet 1542 Series Mobility Express setup interface. At the top, the Cisco logo and product name are displayed. Below this, there are two main steps: '1 Set Up Your Controller' and '2 Create Your Wireless Networks'. Step 2 is currently active. Underneath, the 'Employee Network' configuration section is shown with four input fields: 'Network Name' (containing 'Employee'), 'Security' (set to 'WPA2 Personal'), 'Passphrase' (masked with dots), and 'Confirm Passphrase' (also masked with dots). Each field has a help icon to its right. At the bottom of the form, there are two buttons: 'Back' and 'Next'.

고급 설정 탭에서 RF 매개변수 최적화 슬라이더가 비활성화되고 Next(다음)를 클릭합니다.



1 Set Up Your Controller 



2 Create Your Wireless Networks



3 Advanced Setting



RF Parameter Optimization

Back

Next

설정이 확인되면 WLC가 재부팅됩니다.



The controller has been fully configured and will restart in 60 seconds.

Next Steps:

After the controller is restarted, it will be accessible from the network by going to this URL -

<https://192.168.1.200>

1 Controller Settings

Username	admin
System Name	ME
Country	Netherlands (NL)
Date & Time	11/05/2019 10:31:39
Timezone	Amsterdam, Berlin, Rome, Vienna
NTP Server	-
Management IP Address	192.168.1.200
Management IP Subnet	255.255.255.0
Management IP Gateway	192.168.1.1
Mesh	Yes

x Controller DHCP

2 Wireless Network Settings

✓ Employee Network

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

추가 메시 컨피그레이션

메시 링크를 설정하기 전에 MAP를 flex-bridge 모드로 변환해야 합니다. 초기 컨피그레이션 중에 메시 옵션이 활성화된 경우 RAP는 이미 flex-bridge 모드에 있습니다. 이 작업은 CLI에서 수행할 수 있습니다.

```
<#root>
```

```
MAP#
```

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

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

MAP top이 ME 컨트롤러에 조인하려면 권한이 있어야 합니다. MAP에서 이더넷 인터페이스의 mac 주소를 찾습니다.

<#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)
```

랩톱 1에서 https://192.168.1.200을 통해 ME 컨트롤러 웹 인터페이스에 [액세스합니다](https://192.168.1.200). Expert 모드가 활성화되면(오른쪽 상단) Wireless settings(무선 설정) 아래에 메시 탭이 나타납니다. mac filtering 아래에서 MAP의 이더넷 MAC 주소를 추가합니다.

The screenshot shows the Cisco Aironet 1542 Series Mobility Express web interface. The left sidebar contains a navigation menu with 'Monitoring', 'Wireless Settings', 'WLANs', 'Access Points', 'Access Points Groups', 'WLAN Users', 'Guest WLANs', 'DHCP Server', 'Mesh' (highlighted with a red box), 'Management', 'Services', and 'Advanced'. The main content area is titled 'Mesh settings' and features a 'Mesh' button. Below this, there are tabs for 'General', 'Mesh RAP Downlink backhaul', 'Convergence', 'Ethernet bridging', 'Security', and 'MAC Filtering' (highlighted with a red box). The 'MAC Filtering' page includes a search bar, an 'Add MAC Address' button, a 'Refresh' button, and a table with columns for 'MAC Address', 'Type', 'Profile Name', and 'Description'. The table is currently empty, and the status shows 'Number of Blacklist:0' and 'Number of Whitelist:0'.



Add MAC Address

MAC Address

00:EE:AB:83:D3:20

Description

MAP



Type

WhiteList



Profile Name

Any WLAN/RLAN



✓ Apply

✗ Cancel

참고: ME WLC에 조인되는 브리지 또는 플렉스 브리지 모드의 모든 후속 AP에도 권한이 부여되어야 합니다

이를 설정한 후에는 메쉬 링크를 설정해야 합니다. MAP 뒤에 있는 유선 클라이언트가 메쉬 링크를 통해 트래픽을 전달하려면 MAP의 Wireless Settings(무선 설정) > Access Points(액세스 포인트) > MAP > Mesh(메시)에서 Ethernet Bridging(이더넷 브리징)을 활성화해야 합니다.

Cisco Aironet 1542 Series Mobility Express

ACCESS POINTS ADMINISTRATION

Access Points 1

Q Search

Refresh

Select	Manage	Type	Location
<input type="checkbox"/>		ME Capable	default location

10 Items per page

RAP(Active Controller)

General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) **Mesh**

AP Role: Root

Bridge Type: Outdoor

Bridge Group Name:

Strict Matching BGN:

Daisy Chaining:

Preferred Parent:

Backhaul Interface: 802.11a/n/ac

Bridge Data Rate (Mbps): auto

Install Mapping on Radio Backhaul:

Ethernet Link Status: UP

PSK Key TimeStamp: Delete PSK

Mesh RAP Downlink backhaul

5 GHz 2.4 GHz

Ethernet Bridging

State

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

1 - 1 of 1 items

Apply Cancel

메시 링크가 5GHz 대역을 사용하는 경우 레이더 시그니처의 영향을 받을 수 있습니다. RAP가 레이더 이벤트를 탐지하면 다른 채널로 전환됩니다. RAP가 MAP에 채널이 전환될 것임을 알리도록 채널 변경 알림을 활성화하는 것이 좋습니다. 이렇게 하면 MAP에서 사용 가능한 모든 채널을 검사할 필요가 없으므로 통합 시간이 크게 단축됩니다.

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

Mode: Standard

Channel Change Notification:

Background Scanning:

Apply

다음을 확인합니다.

show mesh ap summary 명령을 실행하여 MAP가 조인되었는지 확인할 수 있습니다.

```
<#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
```

링크가 트래픽을 통과하는지 테스트하기 위해 랩톱 1에서 랩톱 2로 ping을 시도합니다.

```
<#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
```

참고: 메시 링크가 설정된 경우에만 MAP 또는 RAP IP 주소를 ping할 수 있습니다.

문제 해결

MAP/RAP에서

- 메시 이벤트 디버그

내 WLC:

- debug capwap events enable
- 디버그 capwap 오류 활성화

- 디버그 메시 이벤트 활성화

MAP에서 관찰된 성공적인 조인 프로세스의 예(일부 메시지는 관련이 없으므로 수정됨):

<#root>

MAP#debug mesh events

Enabled all mesh event debugs

[*11/05/2019 18:28:24.5699] EVENT-MeshRadioBackhaul[1]: Sending SEEK_START to Channel Manager
[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]:

Starting regular seek

[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: channels to be sought: 100
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[0]: start scanning on channel 1.
[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[1]: start scanning on channel 100.
[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADD_LINK to MeshLink
[*11/05/2019 18:28:06.5699] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: AWPP adjacency added channel(100)
[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADJ_FOUND to Channel Manager 0x64
[*11/05/2019 18:28:06.5699] EVENT-MeshChannelMgr[1]: Adj found on channel 100.
[*11/05/2019 18:28:07.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:08.5499] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[0]: continue scanning on channel 2.
[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:09.0399] EVENT-MeshChannelMgr[1]: continue scanning on channel 104.
[*11/05/2019 18:28:09.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:10.7899] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:11.0199] EVENT-MeshChannelMgr[0]: continue scanning on channel 3.
[*11/05/2019 18:28:11.0399] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:11.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:11.3099] EVENT-MeshChannelMgr[1]: continue scanning on channel 108.
[*11/05/2019 18:28:13.0199] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:13.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:13.2499] EVENT-MeshChannelMgr[0]: continue scanning on channel 4.
[*11/05/2019 18:28:13.3099] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:13.5599] EVENT-MeshChannelMgr[1]: continue scanning on channel 112.
[*11/05/2019 18:28:15.2099] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:15.2499] EVENT-MeshChannelMgr[0]: scanning timer expires.
[*11/05/2019 18:28:15.5099] EVENT-MeshChannelMgr[0]: continue scanning on channel 5.
[*11/05/2019 18:28:15.5599] EVENT-MeshChannelMgr[1]: scanning timer expires.
[*11/05/2019 18:28:15.8099] EVENT-MeshChannelMgr[1]: continue scanning on channel 116.
.
..
.
[*11/05/2019 18:28:35.7999] EVENT-MeshChannelMgr[1]: Mesh BH requests to switch to channel 100, width 20 MHz
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: abort scanning.
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: Set to configured channel 1, width 20 MHz
[*11/05/2019 18:28:36.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:37.5099] EVENT-MeshRadioBackhaul[1]: Sending LINK_UP to MeshLink
[*11/05/2019 18:28:37.5099] CRIT-MeshLink: Set Root port Mac: D4:78:9B:7B:DF:11 BH Id: 2 Port:54 Device:11:11:11:11:11:11
[*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 AUTHENTICATING
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: Opening wpas socket
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: start socket to WPA supplicant
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: MeshSecurity::wpas_init my_mac=00:EE:AB:83:D3:20, user=11:11:11:11:11:11
[*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 successfully 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

!

팁, 요령 및 일반적인 실수

- MAP와 RAP를 유선 상의 동일한 이미지 버전으로 업그레이드함으로써 공중으로 전달되는 이미지 다운로드를 피하고 있습니다("더티(dirty)" RF 환경에서는 문제가 될 수 있음).
- 5GHz 백홀 링크의 채널 폭을 늘리면 SNR이 낮아지고 레이더 탐지가 잘못될 수 있습니다(주로 80MHz 및 160MHz).
- MAP 또는 RAP를 ping하여 메시 링크 연결을 테스트해서는 안 됩니다. 메시 링크가 표시되면 ping할 수 없습니다.
- 사이트에 구축하기 전에 제어된 환경에서 설정을 테스트하는 것이 좋습니다.
- 외부 안테나가 있는 AP를 사용하는 경우 구축 설명서를 참조하여 어떤 안테나가 호환되는지 그리고 어떤 포트에 연결해야 하는지 확인하십시오.
- 메시 링크를 통해 서로 다른 VLAN의 트래픽을 브리징하려면 VLAN 투명 기능을 비활성화해야 합니다.
- syslog 서버가 AP에 로컬인 경우를 고려하십시오. 그렇지 않으면 콘솔 연결에서만 사용할 수 있는 디버그 정보를 제공할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.