# 무선 LAN 컨트롤러 메시 네트워크 컨피그레이션 예

## 목차



## 소개

이 문서에서는 메시 네트워크 솔루션을 사용하여 포인트-투-포인트 브리징 링크를 설정하는 방법에 대한 기본 컨피그레이션 예를 제공합니다.이 예에서는 두 개의 경량 액세스 포인트(LAP)를 사용합니다. 한 LAP는 RAP(Roof-Top Access Point)로 작동하고 다른 LAP는 PAP(Pole-Top Access Point)로 작동하며 Cisco WLAN(Wireless LAN) Controller(WLC)에 연결됩니다. RAP는 Cisco Catalyst 스위치를 통해 WLC에 연결됩니다.

WLC 릴리스 5.2 이상 버전에서는 Wireless LAN Controller Mesh Network Configuration Example for Releases 5.2 이상을 참조하십시오.

## 사전 요구 사항

- WLC는 기본 작업을 위해 구성됩니다.
- WLC는 레이어 3 모드로 구성됩니다.
- WLC에 대한 스위치가 구성됩니다.

## 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- LAP 및 Cisco WLC의 컨피그레이션에 대한 기본 지식
- LWAPP(Lightweight AP Protocol)에 대한 기본 지식
- 외부 DHCP 서버 및/또는 DNS(Domain Name Server) 컨피그레이션 지식
- Cisco 스위치에 대한 기본 구성 지식

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 3.2.150.6을 실행하는 Cisco 4402 Series WLC
- Cisco Aironet 1510 Series LAP 2개
- Cisco Layer 2 스위치

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

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# 배경 정보

## Cisco Aironet 1510 Series Lightweight 실외형 메시 AP

Cisco Aironet 1510 Series Lightweight 실외형 메시 AP는 무선 클라이언트 액세스 및 포인트-투-포인트 브리징, 포인트-투-멀티포인트 브리징 및 포인트-투-멀티포인트 메시 무선 연결을 위해 설계된 무선 장치입니다.실외 액세스 포인트는 벽 또는 돌출부, 옥상 기둥 또는 가로등 기둥에 장착할 수 있는 독립형 장치입니다.

AP1510은 컨트롤러와 함께 작동하여 중앙 집중화되고 확장 가능한 관리, 높은 보안 및 모빌리티를 제공합니다.제로 컨피그레이션 구축을 지원하도록 설계된 AP1510은 메시 네트워크에 쉽고 안전하게 연결되며 컨트롤러 GUI 또는 CLI를 통해 네트워크를 관리하고 모니터링할 수 있습니다.

AP1510에는 두 개의 동시 작동 무선 장치가 장착되어 있습니다.클라이언트 액세스에 사용되는 2.4GHz 무선 장치 및 다른 AP1510에 대한 데이터 백홀에 사용되는 5GHz 무선 장치무선 LAN 클라이언트 트래픽은 AP의 백홀 라디오를 통과하거나 컨트롤러 이더넷 연결에 도달할 때까지 다른 AP1510을 통해 릴레이됩니다.

## RAP(Roof-top Access Point)

RAP는 Cisco WLC에 유선 연결을 제공합니다.이들은 백홀 무선 인터페이스를 사용하여 인접 PAP와 통신합니다.RAP는 브리징 또는 메시 네트워크에 대한 상위 노드이며 브리지 또는 메시 네트워크를 유선 네트워크에 연결합니다.따라서 브리징 또는 메시 네트워크 세그먼트에는 하나의 RAP만 있을 수 있습니다.

**참고:** LAN-to-LAN 브리징에 메시 네트워킹 솔루션을 사용할 때는 RAP를 Cisco WLC에 직접 연결하지 마십시오.Cisco WLC는 LWAPP 지원 포트에서 오는 이더넷 트래픽을 전달하지 않으므로 Cisco WLC와 RAP 간의 스위치 또는 라우터가 필요합니다.RAP는 레이어 2 또는 레이어 3 LWAPP 모드에서 작동할 수 있습니다.

## PAP(Pole-top Access Point)

PAP는 Cisco WLC에 유선 연결이 없습니다.완전히 무선이 가능하며 다른 PAP 또는 RAP와 통신하는 클라이언트를 지원하거나 주변 장치 또는 유선 네트워크에 연결하는 데 사용할 수 있습니다.이더넷 포트는 보안상의 이유로 기본적으로 비활성화되지만 PAP에 대해 활성화해야 합니다.

**참고:** Cisco Aironet 1030 Remote Edge LAP는 단일 홉의 구축을 지원하는 반면 Cisco Aironet 1500 Series Lightweight 실외 AP는 단일 홉과 다중 홉의 구축을 모두 지원합니다.따라서 Cisco Aironet 1500 Series Lightweight 실외형 AP는 Cisco WLC에서 하나 이상의 홉에 대해 옥상 AP로, PAP로 사용할 수 있습니다.

## 메시 네트워크에서 지원되지 않는 기능

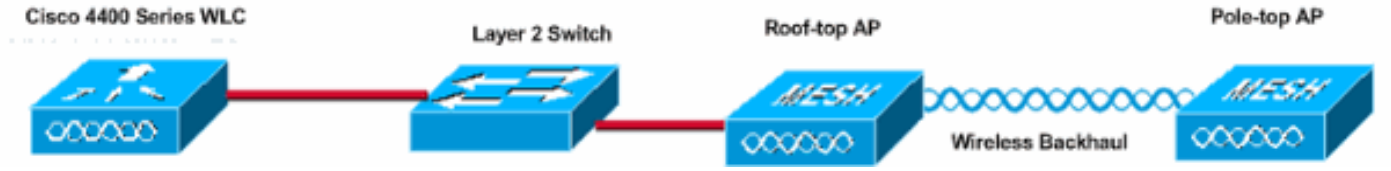
이러한 컨트롤러 기능은 메시 네트워크에서 지원되지 않습니다.

- 복수 국가 지원
- 로드 기반 CAC(메시 네트워크는 대역폭 기반 또는 고정 CAC만 지원)
- 고가용성(빠른 하트비트 및 기본 검색 조인 타이머)
- EAP-FASTv1 및 802.1X 인증
- EAP-FASTv1 및 802.1X 인증
- 로컬에서 중요한 인증서
- 위치 기반 서비스

## 액세스 포인트 시작 시퀀스

이 목록에서는 RAP 및 PAP가 시작될 때 수행되는 작업을 설명합니다.

- 모든 트래픽은 RAP와 Cisco WLC를 거쳐 LAN으로 전송됩니다.
- RAP가 나타나면 PAP가 자동으로 연결됩니다.
- 연결된 링크는 공유 암호를 사용하여 링크에 대한 AES(Advanced Encryption Standard)를 제공하는 데 사용되는 키를 생성합니다.
- 원격 PAP가 RAP에 연결되면 메시 AP가 데이터 트래픽을 전달할 수 있습니다.
- 사용자는 Cisco CLI(Command Line Interface), 컨트롤러의 Cisco 웹 사용자 인터페이스 또는 Cisco WCS(Wireless Control System)를 사용하여 공유 암호를 변경하거나 메시 AP를 구성할 수 있습니다. 공유 암호를 수정할 것을 권장합니다.




# 구성

포인트-투-포인트 브리징을 위한 WLC 및 AP를 구성하려면 다음 단계를 완료합니다.

1. WLC에서 제로 터치 컨피그레이션을 활성화합니다.
2. AP 권한 부여 목록에 MIC를 추가합니다.
3. AP에 대한 브리징 매개변수를 구성합니다.
4. 컨피그레이션을 확인합니다.

## 제로 터치 컨피그레이션 사용(기본적으로 사용)

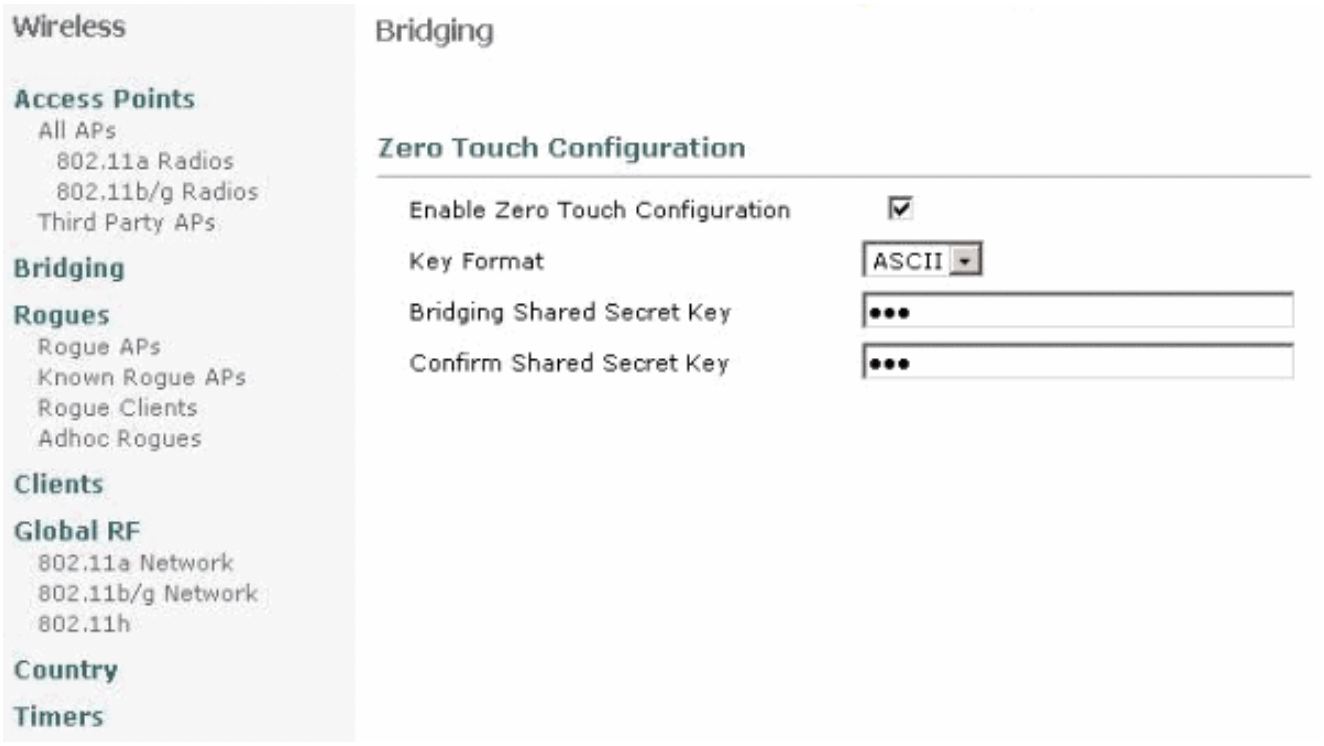
### GUI 컨피그레이션

Enable Zero Touch Configuration(제로 터치 컨피그레이션 활성화)을 사용하면 AP가 WLC에 등록할 때 컨트롤러에서 공유 비밀 키를 가져올 수 있습니다.이 확인란을 선택하지 않으면 컨트롤러는 공유 비밀 키를 제공하지 않으며 AP는 보안 통신에 기본 사전 공유 키를 사용합니다.기본값은 enabled(활성화) 또는 checked(선택)입니다. WLC GUI에서 다음 단계를 완료합니다.

**참고:** WLC 버전 4.1 이상에서는 Zero-Touch 컨피그레이션에 대한 프로비저닝이 없습니다.

1. Wireless(**무선) > Bridging(브리징)**을 선택하고 **Enable Zero Touch Configuration(제로 터치 컨피그레이션 활성화)을 클릭합니다**.
2. 키 형식을 선택합니다.
3. 브리징 공유 비밀 키를 입력합니다.
4. Confirm Shared Secret Key(공유 비밀 키 확인)에 Bridging Shared Secret Key(브리징 공유 비밀 키)를 다시 입력합니다

.




### CLI 컨피그레이션

CLI에서 다음 단계를 완료합니다.

1. 제로 터치 컨피그레이션을 활성화하려면 **config network zero-config enable** 명령을 실행합니다.

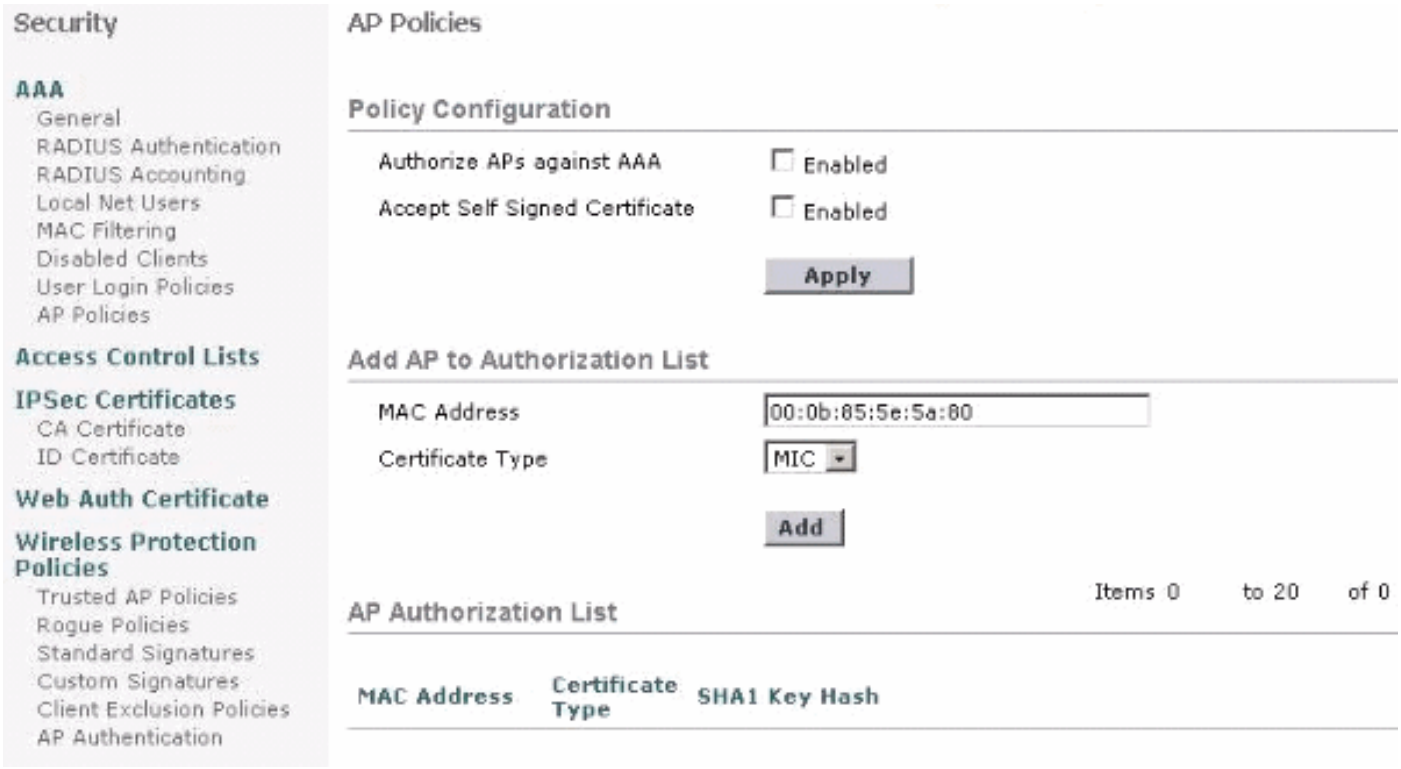
```
(Cisco Controller) >config network zero-config enable
```

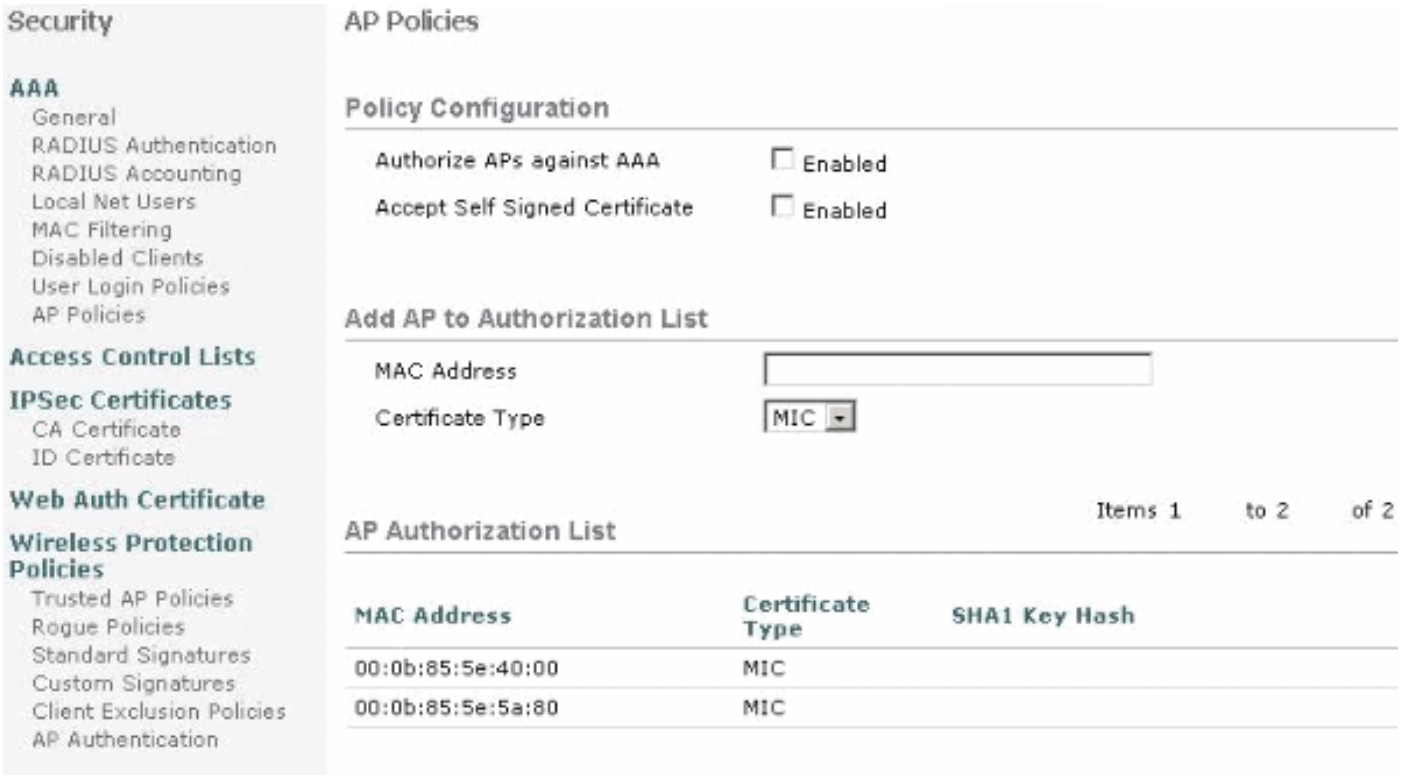
2. 브리징 공유 비밀 키를 추가하려면 **config network bridging-shared-secret <string>** 명령을 실행합니다.

```
(Cisco Controller) >config network bridging-shared-secret Cisco
```

## AP 권한 부여 목록에 MIC 추가

다음 단계는 WLC의 권한 부여 목록에 AP를 추가하는 것입니다.이렇게 하려면 Security(**보안) > AP Policies(AP 정책)**를 선택하고 Add AP to Authorization List(권한 부여 목록에 AP 추가) 아래에 AP MAC 주소를 입력하고 Add(추가)를 **클릭합니다**.






이 예에서는 두 AP(RAP 및 PAP)가 모두 컨트롤러의 AP 권한 부여 목록에 추가됩니다.

### CLI 컨피그레이션

MIC를 권한 부여 목록에 추가하려면 config auth-list add mic <AP mac> 명령을 실행합니다.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

## 구성

이 문서에서는 다음 구성을 사용합니다.

**Cisco WLC 4402**

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
Switch Description..............................  Cisco
Controller
Machine Model.....................................
WLC4402-12
Serial Number.....................................
FLS0943H005
Burned-in MAC Address.............................
00:0B:85:40:CF:A0
Crypto Accelerator 1.............................  Absent
Crypto Accelerator 2.............................  Absent
Power Supply 1...................................  Absent
Power Supply 2.....................................
Present, OK
```

```
Press Enter to continue Or <Ctl Z> to abort

System Information
Manufacturer's Name.............................. Cisco
Systems, Inc
Product Name..................................... Cisco
Controller
Product Version.................................
3.2.150.6
RTOS Version....................................
3.2.150.6
Bootloader Version..............................
3.2.150.6
Build Type....................................... DATA +
WPS

System Name.....................................
lab120wlc4402ip100
System Location.................................
System Contact..................................
System ObjectID.................................
1.3.6.1.4.1.14179.1.1.4.3
IP Address......................................
192.168.120.100
System Up Time................................... 0 days
1 hrs 4 mins 6 secs

Configured Country............................... United
States
Operating Environment...........................
Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to
65 C
Internal Temperature............................. +42 C

State of 802.11b Network........................
Disabled
State of 802.11a Network........................
Disabled
Number of WLANs.................................. 1
3rd Party Access Point Support..................
Disabled
Number of Active Clients......................... 0

Press Enter to continue Or <Ctl Z> to abort

Switch Configuration
802.3x Flow Control Mode........................
Disable
Current LWAPP Transport Mode..................... Layer
3
LWAPP Transport Mode after next switch reboot.... Layer
3
FIPS prerequisite features......................
Disabled

Press Enter to continue Or <Ctl Z> to abort

Network Information
RF-Network Name.............................. airespacerf
Web Mode..................................... Enable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
```

```
Telnet..................................... Enable
Ethernet Multicast Mode..................... Disable
Mode: Ucast
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Enable
Bridge AP Zero Config....................... Enable
Bridge Shared Secret.......................
youshouldsetme
Allow Old Bridging Aps To Authenticate...... Disable
Over The Air Provisioning of AP's........... Disable
Mobile Peer to Peer Blocking................ Disable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled

Press Enter to continue Or <Ctl Z> to abort

Port Summary
           STP   Admin   Physical   Physical   Link
Link    Mcast
Pr  Type   Stat   Mode     Mode      Status   Status
Trap   Appliance   POE
-- ------- ---- ------- ---------- ---------- ------ ---
---- --------- -------
1  Normal  Forw Enable  Auto       1000 Full  Up
Enable  Enable     N/A
2  Normal  Forw Enable  Auto       1000 Full  Up
Enable  Enable     N/A

Mobility Configuration
Mobility Protocol Port...................... 16666
Mobility Security Mode.....................
Disabled
Default Mobility Domain.....................
airespacerf
Mobility Group members configured.............. 3

Switches configured in the Mobility Group
 MAC Address          IP Address         Group Name
 00:0b:85:33:a8:40    192.168.5.70       <local>
 00:0b:85:40:cf:a0    192.168.120.100    <local>
 00:0b:85:43:8c:80    192.168.5.40       airespacerf

Interface Configuration
Interface Name.............................. ap-
manager
IP Address..................................
192.168.120.101
IP Netmask..................................
255.255.255.0
IP Gateway..................................
192.168.120.1
VLAN........................................
untagged
Active Physical Port........................ 1
Primary Physical Port....................... 1
Backup Physical Port.....................
Unconfigured
Primary DHCP Server.....................
192.168.1.20
```

```
Secondary DHCP Server.....................
Unconfigured
ACL.......................................
Unconfigured
AP Manager.................................. Yes

Interface Name............................
management
MAC Address...............................
00:0b:85:40:cf:a0
IP Address................................
192.168.120.100
IP Netmask................................
255.255.255.0
IP Gateway................................
192.168.120.1
VLAN......................................
untagged
Active Physical Port..................... 1
Primary Physical Port..................... 1
Backup Physical Port.....................
Unconfigured
Primary DHCP Server.......................
192.168.1.20
Secondary DHCP Server.....................
Unconfigured
ACL.......................................
Unconfigured
AP Manager.................................. No

Interface Name............................
service-port
MAC Address...............................
00:0b:85:40:cf:a1
IP Address................................
192.168.250.100
IP Netmask................................
255.255.255.0
DHCP Protocol.............................
Disabled
AP Manager.................................. No

Interface Name............................
virtual
IP Address................................
1.1.1.1
Virtual DNS Host Name.....................
Disabled
AP Manager.................................. No

WLAN Configuration

WLAN Identifier.............................. 1
Network Name (SSID).......................
lab120wlc4402ip100
Status....................................
Enabled
MAC Filtering.............................
Enabled
Broadcast SSID............................
Enabled
AAA Policy Override.......................
Disabled
Number of Active Clients..................... 0
```

```
Exclusionlist Timeout.......................... 60
seconds
Session Timeout................................ 1800
seconds
Interface.....................................
management
WLAN ACL......................................
unconfigured
DHCP Server...................................
Default
Quality of Service............................. Silver
(best effort)
WMM...........................................
Disabled
802.11e.......................................
Disabled
Dot11-Phone Mode (7920).......................
Disabled
Wired Protocol................................. None
IPv6 Support..................................
Disabled
Radio Policy................................... All
Radius Servers
   Authentication.............................
192.168.1.20 1812
Security

   802.11 Authentication:....................... Open
System
   Static WEP Keys.............................
Enabled
        Key Index:.....................................
1
        Encryption:....................................
104-bit WEP
   802.1X........................................
Disabled
   Wi-Fi Protected Access (WPA1).................
Disabled
   Wi-Fi Protected Access v2 (WPA2).............
Disabled
   IP Security...................................
Disabled
   IP Security Passthru..........................
Disabled
   L2TP..........................................
Disabled
   Web Based Authentication.....................
Disabled
   Web-Passthrough...............................
Disabled
   Auto Anchor...................................
Disabled
   Cranite Passthru..............................
Disabled
   Fortress Passthru.............................
Disabled

RADIUS Configuration
Vendor Id Backward Compatibility.................
Disabled
Credentials Caching...........................
Disabled
Call Station Id Type........................... IP
```

```
Address
Administrative Authentication via RADIUS.....
Enabled
Keywrap.....................................
Disabled

Load Balancing Info
Aggressive Load Balancing.....................
Enabled
Aggressive Load Balancing Window.............. 0
clients

Signature Policy
  Signature Processing.........................
Enabled

Spanning Tree Switch Configuration

STP Specification..................... IEEE 802.1D
STP Base MAC Address...................
00:0B:85:40:CF:A0
Spanning Tree Algorithm............... Disable
STP Bridge Priority................... 32768
STP Bridge Max. Age (seconds)......... 20
STP Bridge Hello Time (seconds)........ 2
STP Bridge Forward Delay (seconds)..... 15

Spanning Tree Port Configuration

STP Port ID............................... 8001
STP Port State............................ Forwarding
STP Port Administrative Mode.............. 802.1D
STP Port Priority......................... 128
STP Port Path Cost........................ 4
STP Port Path Cost Mode................... Auto


STP Port ID............................... 8002
STP Port State............................ Forwarding
STP Port Administrative Mode.............. 802.1D
STP Port Priority......................... 128
STP Port Path Cost........................ 4
STP Port Path Cost Mode................... Auto
```

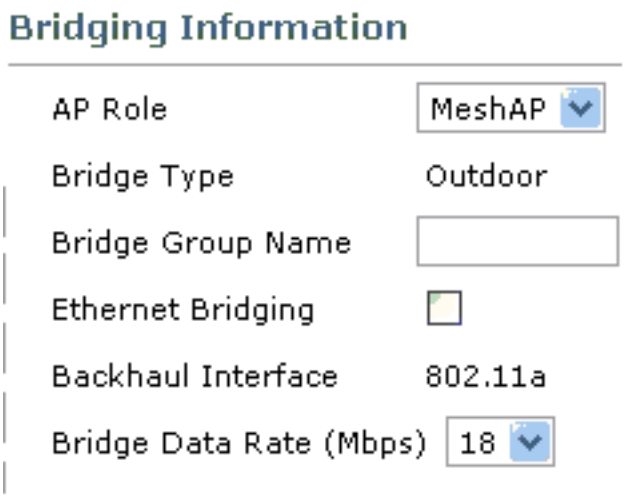
## AP에 대한 브리징 매개변수 구성

이 섹션에서는 메시 네트워크에서 AP의 역할을 구성하는 방법 및 관련 브리징 매개변수를 제공합니다.GUI 또는 CLI를 사용하여 이러한 매개변수를 구성할 수 있습니다.

1. Wireless(**무선**)를 클릭한 다음 **Access** Points(액세스 포인트) 아래의 All APs(모든 AP)를 클릭합니다.All APs 페이지가 나타납니다.
2. All APs(모든 **AP**) > Details(세부사항) 페이지에 액세스하려면 AP1510에 대한 Detail(세부사항) 링크를 클릭합니다.

이 페이지에서 일반 아래의 AP 모드는 AP1510과 같은 브리지 기능이 있는 AP에 대해 브리지로 자동 설정됩니다. 이 페이지에는 브리징 정보 아래의 이 정보도 표시됩니다.메시 네트워크에서 이 AP의 역할을 지정하려면 Bridging Information(브리징 정보)에서 다음 옵션 중 하나를 선택합니다.

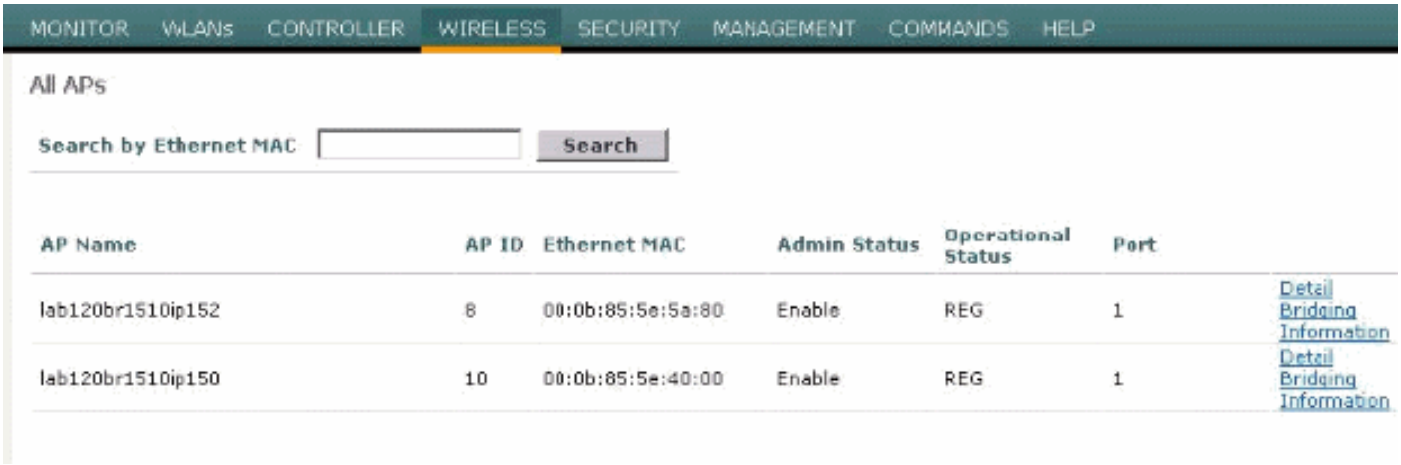
- **MeshAP** - AP1510에서 컨트롤러에 대한 무선 연결이 있는 경우 이 옵션을 선택합니다.
- **RootAP** - AP1510이 컨트롤러에 유선 연결이 있는 경우 이 옵션을 선택합니다.




## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

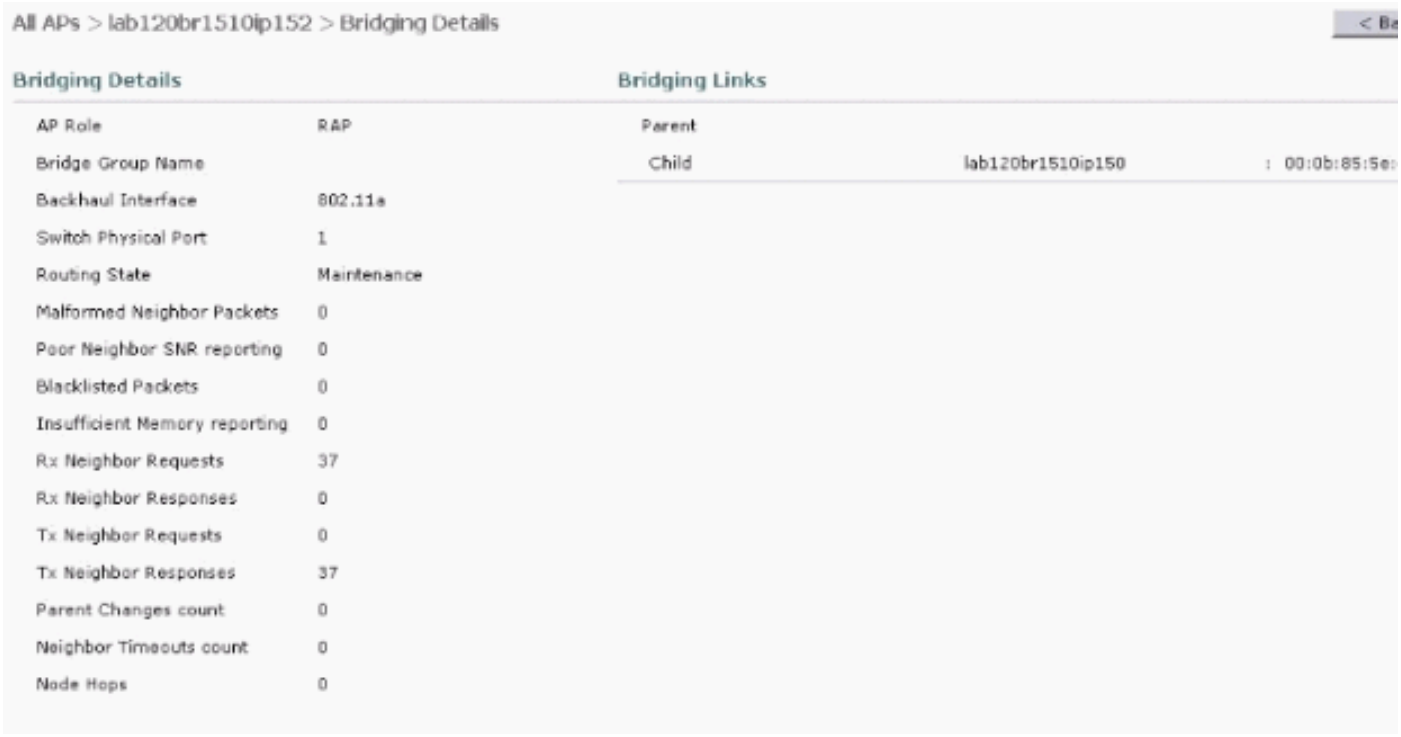
AP가 WLC에 등록되면 WLC의 GUI 상단의 Wireless(무선) 탭에서 볼 수 있습니다.




CLI에서 **show ap summary** 명령을 사용하여 WLC에 등록된 AP를 확인할 수 있습니다.

```
(Cisco Controller) >show ap summary

AP Name             Slots  AP Model     Ethernet MAC       Location         Port

------------------  -----  ----------  -----------------  ----------------  ----

lab120br1510ip152    2     OAP1500     00:0b:85:5e:5a:80   default_location  1

lab120br1510ip150    2     OAP1500     00:0b:85:5e:40:00   default_location  1


(Cisco Controller) >
```

AP의 역할을 확인하려면 GUI에서 Bridging Details를 클릭합니다.




CLI에서 **show mesh path <Cisco AP>** 및 **show mesh neigh <Cisco AP>** 명령을 사용하여 WLC에 등록된 AP를 확인할 수 있습니다.

```
(Cisco Controller) >show mesh path lab120br1510ip152
00:0B:85:5E:5A:80 is RAP

(Cisco Controller) >show mesh neigh lab120br1510ip152

AP MAC : 00:0B:85:5E:40:00

FLAGS : 160 CHILD

worstDv 255, Ant 0, channel 0, biters 0, ppiters 10

Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0

adjustedEase 0, unadjustedEase 0

txParent 0, rxParent 0

poorSnr  0

lastUpdate   1150103792 (Mon Jun 12 09:16:32 2006)

parentChange 0

Per antenna smoothed snr values: 0 0 0 0

Vector through 00:0B:85:5E:40:00

(Cisco Controller) >
```

# 문제 해결

AP WLC 것은 메시 구축에서 가장 일반적인 문제 중 하나입니다.다음 검사를 완료합니다.

1. 액세스 포인트의 MAC 주소가 WLC의 Mac Filter 목록에 추가되었는지 확인합니다.이는

Security(보안) > **Mac Filtering(Mac 필터링)에서 확인할** 수 있습니다.

2. RAP와 MAP 간의 공유 암호를 확인합니다.WLC에서 키가 일치하지 않는 경우 이 메시지를 볼 수 있습니다.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, BRIDGE AP 00:0b:85:68:c1:d0"` **참고**: 버전에 사용 가능한 경우 항상 **Enable Zero Touch Configuration** 옵션을 사용하십시오.이렇게 하면 메시 AP의 키가 자동으로 구성되며 컨피그레이션 오류가 발생하지 않습니다.
3. RAP는 라디오 인터페이스에서 브로드캐스트 메시지를 전달하지 않습니다.따라서 MAP에서 RAP로 전달된 IP 주소를 가져올 수 있도록 유니캐스트를 통해 IP 주소를 전송하도록 DHCP 서버를 구성합니다.그렇지 않으면 MAP에 고정 IP를 사용합니다.
4. Bridge Group Name(브리지 그룹 이름)을 기본값으로 유지하거나, Bridge Group Names(브리지 그룹 이름)가 MAP과 해당 RAP에서 정확히 동일하게 구성되었는지 확인하십시오.

이는 메시 액세스 포인트와 관련된 문제입니다.WLC와 액세스 포인트 간에 공통된 연결 문제는 Troubleshoot a Lightweight Access Point Not Join a Wireless LAN Controller를 참조하십시오.

## 문제 해결 명령

**참고:** debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

다음 debug 명령을 사용하여 WLC의 문제를 해결할 수 있습니다.

- **debug pem state enable** - 액세스 정책 관리자 디버그 옵션을 구성하는 데 사용됩니다.
- **debug pem events enable** - 액세스 정책 관리자 디버그 옵션을 구성하는 데 사용됩니다.
- **debug dhcp message enable**—DHCP 서버와 주고받는 DHCP 메시지의 디버그를 표시합니다.
- **debug dhcp packet enable**—DHCP 서버에서 보내고 받는 DHCP 패킷 세부 정보의 디버그를 표시합니다.

트러블슈팅에 사용할 수 있는 몇 가지 추가 **debug** 명령은 다음과 같습니다.

- **debug lwapp errors enable** - LWAPP 오류의 디버그를 표시합니다.
- **debug pm pki enable** - AP와 WLC 간에 전달되는 인증서 메시지의 디버그를 표시합니다.

이 **디버그 lwapp 이벤트는 WLC** 명령 출력을 활성화하여 LAP가 WLC에 등록되었음을 보여줍니다.

```
(Cisco Controller) >debug lwapp events enable

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST
from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1'

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce
00:0B:85:40:CF:A0 rxNonce  00:0B:85:5E:40:00

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for
AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223,
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop
MAC: 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of
LWAPP Join-Reply to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
```

**00:0b:85:5e:40:00 slot 1**

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 **Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:5e:40:00** to 00:0b:85:40:cf:a3

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00 -- static 1, 192.168.120.150/255.255.255.0, gtw 192.168.120.1

Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -A

Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -A

Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Config-Message to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID 'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated. Last AP failure was due to Link Failure, reason: STATISTICS_INFO_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 0!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 1!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00

## 관련 정보

- Cisco Mesh Networking 솔루션 구축 설명서
- 빠른 시작 가이드:Cisco Aironet 1500 Series Lightweight 실외 메시 액세스 포인트
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems