Beispiel für eine Mesh-Netzwerkkonfiguration eines Wireless LAN-Controllers

Inhalt

Einführung

Dieses Dokument enthält ein einfaches Konfigurationsbeispiel für die Einrichtung einer Punkt-zu-Punkt-Verbindung mithilfe der Mesh Network-Lösung. In diesem Beispiel werden zwei Lightweight Access Points (LAPs) verwendet. Eine LAP fungiert als RAP (Dach-Top Access Point), die andere LAP als PAP (PAP) und ist mit einem Cisco Wireless LAN (WLAN) Controller (WLC) verbunden. Der RAP ist über einen Cisco Catalyst Switch mit dem WLC verbunden.

Weitere Informationen zu den Versionen 5.2 und WLC 5.2 und höher finden Sie im Konfigurationsbeispiel für ein drahtloses LAN-Controller-Mesh-Netzwerk.

Voraussetzungen

- Der WLC ist für den Basisbetrieb konfiguriert.
- Der WLC wird im Layer-3-Modus konfiguriert.
- Der Switch für den WLC wird konfiguriert.

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von LAPs und Cisco WLCs
- Grundkenntnisse des Lightweight AP Protocol (LWAPP).
- Kenntnis der Konfiguration eines externen DHCP-Servers und/oder Domain Name Server (DNS)
- Grundkenntnisse der Konfiguration von Cisco Switches

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 4402 mit Firmware 3.2.150.6
- Zwei (2) Cisco Aironet LAPs der Serie 1510
- Cisco Layer-2-Switch

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Cisco Aironet 1510 Lightweight Outdoor Mesh AP

Der Lightweight Outdoor Mesh AP der Cisco Aironet Serie 1510 ist ein Wireless-Gerät, das für Wireless-Client-Zugriff, Punkt-zu-Punkt-Bridging, Punkt-zu-Mehrpunkt-Bridging und Point-to-Multipoint-Mesh-Verbindungen entwickelt wurde. Der Access Point für den Außenbereich ist eine Standalone-Einheit, die an einer Wand oder einem Überhang, an einem Pol auf dem Dach oder an einem Laternenmast angebracht werden kann.

Der AP1510 arbeitet mit Controllern zusammen, um eine zentrale und skalierbare Verwaltung, hohe Sicherheit und Mobilität zu ermöglichen. Der AP1510 ist auf die Unterstützung von Zero-Configuration-Bereitstellungen ausgelegt. Er ist einfach und sicher in das Mesh-Netzwerk integriert und für die Verwaltung und Überwachung des Netzwerks über die grafische Benutzeroberfläche oder Kommandozeile des Controllers verfügbar.

Der AP1510 ist mit zwei gleichzeitig betriebenen Funkmodulen ausgestattet: ein 2,4-GHz-Funkmodul für den Client-Zugriff und ein 5-GHz-Funkmodul für das Daten-Backhaul zu anderen AP1510-Geräten. Der Wireless LAN-Client-Datenverkehr durchläuft das Backhaul-Funkmodul des AP oder wird über andere AP1510 weitergeleitet, bis er die Ethernet-Verbindung des Controllers

erreicht.

RAP (Roof-Top Access Point)

RAPs verfügen über eine kabelgebundene Verbindung zu einem Cisco WLC. Sie verwenden die Wireless-Backhaul-Schnittstelle, um mit benachbarten PAPs zu kommunizieren. RAPs sind der übergeordnete Knoten für ein Bridging- oder Mesh-Netzwerk und verbinden eine Bridge oder ein Mesh-Netzwerk mit dem kabelgebundenen Netzwerk. Daher kann für jedes Bridge- oder Mesh-Netzwerksegment nur ein RAP vorhanden sein.

Hinweis: Wenn Sie die Mesh-Netzwerklösung für das LAN-to-LAN-Bridging verwenden, verbinden Sie keinen RAP direkt mit einem Cisco WLC. Ein Switch oder Router zwischen dem Cisco WLC und dem RAP ist erforderlich, da Cisco WLCs keinen Ethernet-Datenverkehr weiterleiten, der von einem LWAPP-fähigen Port stammt. RAPs können im Layer-2- oder Layer-3-LWAPP-Modus verwendet werden.

PAP (Pole-Top Access Point)

PAPs verfügen über keine kabelgebundene Verbindung zu einem Cisco WLC. Sie können vollständig drahtlos sein und Clients unterstützen, die mit anderen PAPs oder RAPs kommunizieren, oder sie können für die Verbindung mit Peripheriegeräten oder einem kabelgebundenen Netzwerk verwendet werden. Der Ethernet-Port ist aus Sicherheitsgründen standardmäßig deaktiviert. Sie sollten ihn jedoch für PAPs aktivieren.

Hinweis: Cisco Aironet Remote Edge LAPs der Serie 1030 unterstützen Single-Hop-Bereitstellungen, während Lightweight Outdoor APs der Cisco Aironet Serie 1500 sowohl Single- als auch Multi-Hop-Bereitstellungen unterstützen. Daher können die Cisco Aironet APs der Serie 1500 für den Außenbereich als Access Points auf dem Dach und als PAPs für einen oder mehrere Hops vom Cisco WLC verwendet werden.

Funktionen, die von Mesh-Netzwerken nicht unterstützt werden

Diese Controller-Funktionen werden in Mesh-Netzwerken nicht unterstützt:

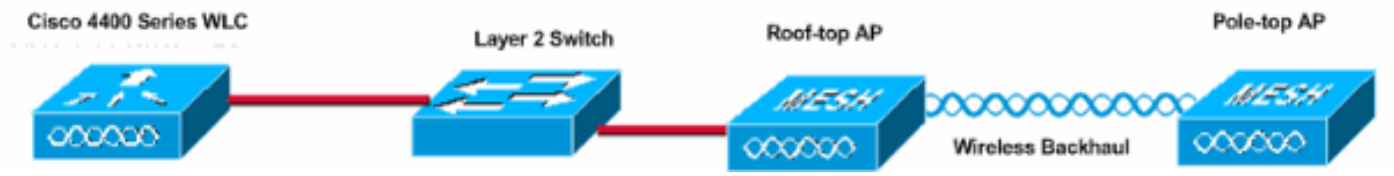
- Unterstützung mehrerer Länder
- Lastenbasierte CAC (Mesh-Netzwerke unterstützen nur bandbreitenbasierte oder statische CACs)
- Hohe Verfügbarkeit (schneller Heartbeat- und primärer Discovery Join-Timer)
- EAP-FASTv1- und 802.1X-Authentifizierung
- EAP-FASTv1- und 802.1X-Authentifizierung
- Lokal bedeutendes Zertifikat
- Standortbasierte Services

Startsequenz des Access Points

Diese Liste beschreibt, was beim Starten des RAP und des PAP geschieht:

- Der gesamte Datenverkehr wird über den RAP und den Cisco WLC geleitet, bevor er an das LAN gesendet wird.
- Wenn der RAP aktiviert wird, werden die PAPs automatisch mit dem RAP verbunden.

- Die verbundene Verbindung verwendet einen gemeinsamen geheimen Schlüssel, um einen Schlüssel zu generieren, der den Advanced Encryption Standard (AES) für die Verbindung bereitstellt.
- Sobald der Remote-PAP mit dem RAP verbunden ist, können die Mesh-APs Datenverkehr weiterleiten.
- Benutzer können den gemeinsamen geheimen Schlüssel ändern oder die Mesh-APs über die Cisco Befehlszeilenschnittstelle (CLI), die Cisco Web-Benutzeroberfläche des Controllers oder das Cisco Wireless Control System (Cisco WCS) konfigurieren. Cisco empfiehlt, den gemeinsamen geheimen Schlüssel zu ändern.



Konfigurieren

Führen Sie diese Schritte aus, um den WLC und die APs für das Punkt-zu-Punkt-Bridging zu konfigurieren.

1. Aktivieren der Konfiguration ohne Benutzereingriff auf dem WLC.
2. Fügen Sie das MIC der AP-Autorisierungsliste hinzu.
3. Konfigurieren Sie Bridging-Parameter für die APs.
4. Überprüfen Sie die Konfiguration.

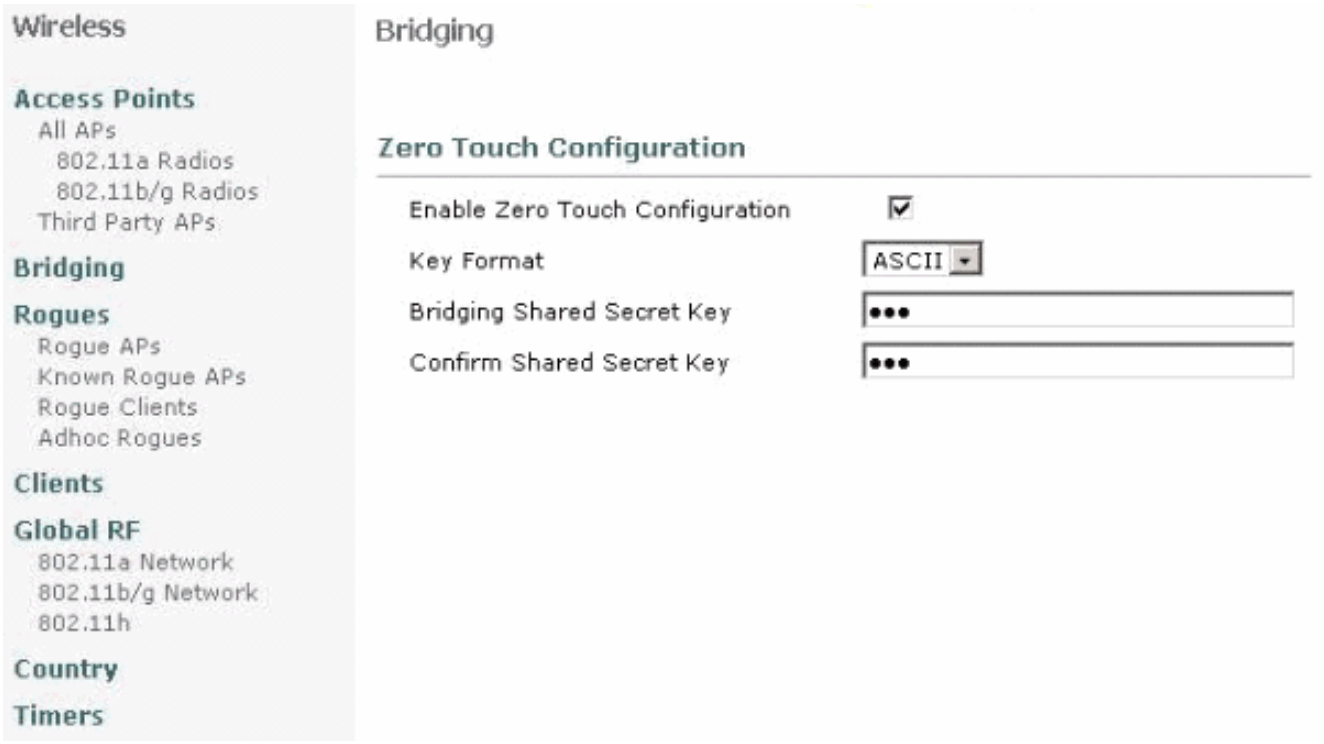
Konfiguration ohne Benutzereingriff aktivieren (standardmäßig aktiviert)

GUI-Konfiguration

Mit der Funktion "Zero Touch Configuration" (Zero-Touch-Konfiguration aktivieren) können APs den gemeinsamen geheimen Schlüssel vom Controller abrufen, wenn er beim WLC registriert wird. Wenn Sie das Kontrollkästchen deaktivieren, stellt der Controller den gemeinsamen geheimen Schlüssel nicht bereit, und die APs verwenden einen vorinstallierten Standardschlüssel für die sichere Kommunikation. Der Standardwert ist aktiviert (oder aktiviert). Gehen Sie wie folgt vor:

Hinweis: In WLC Version 4.1 und höher ist keine Konfiguration ohne Benutzereingriff vorgesehen.

1. Wählen Sie **Wireless > Bridging aus**, und klicken Sie auf **Konfiguration ohne Benutzereingriff aktivieren**.
2. Wählen Sie das Schlüsselformat aus.
3. Geben Sie den gemeinsamen geheimen Schlüssel Bridging ein.
4. Geben Sie den gemeinsamen geheimen Schlüssel Bridging erneut in den Schlüssel zur Bestätigung des gemeinsamen geheimen Schlüssels ein.



CLI-Konfiguration

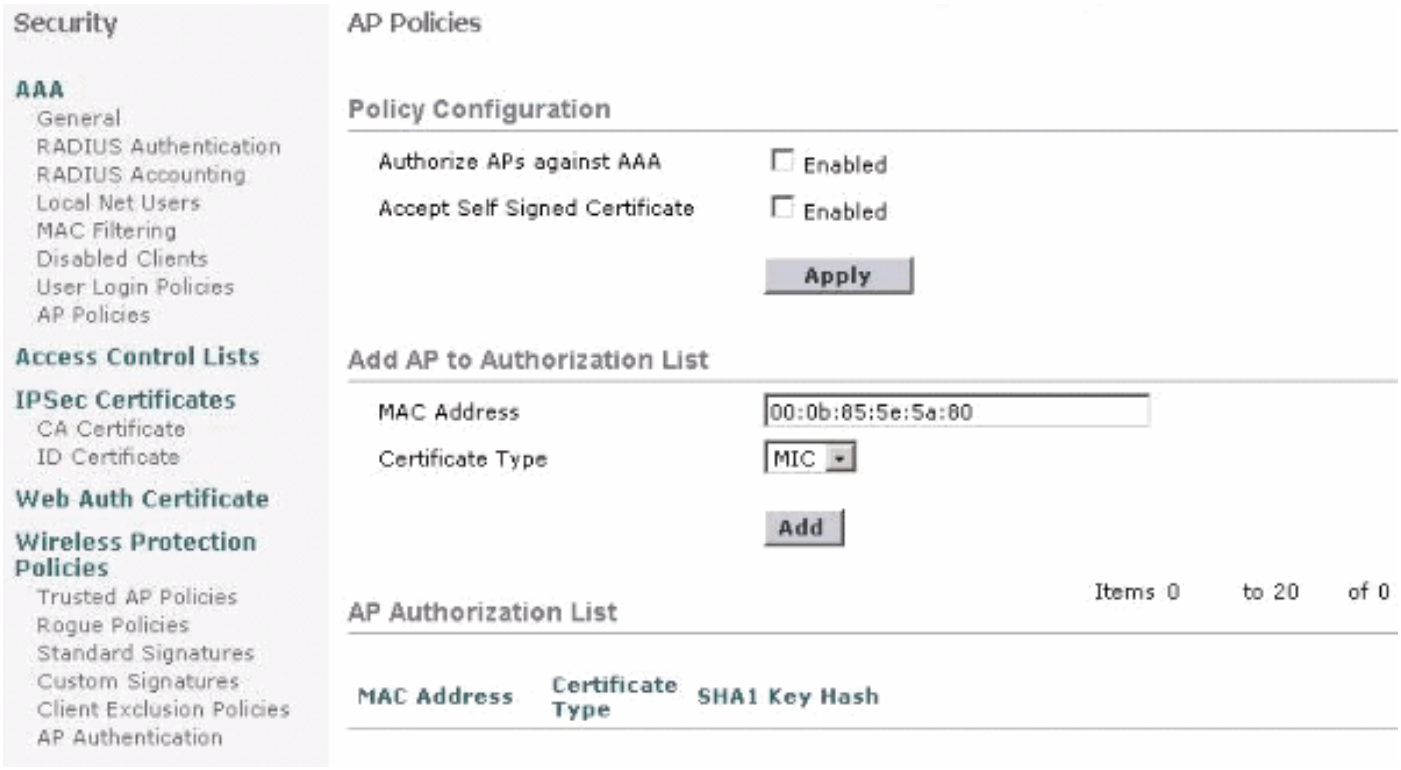
Gehen Sie wie folgt von der CLI aus:

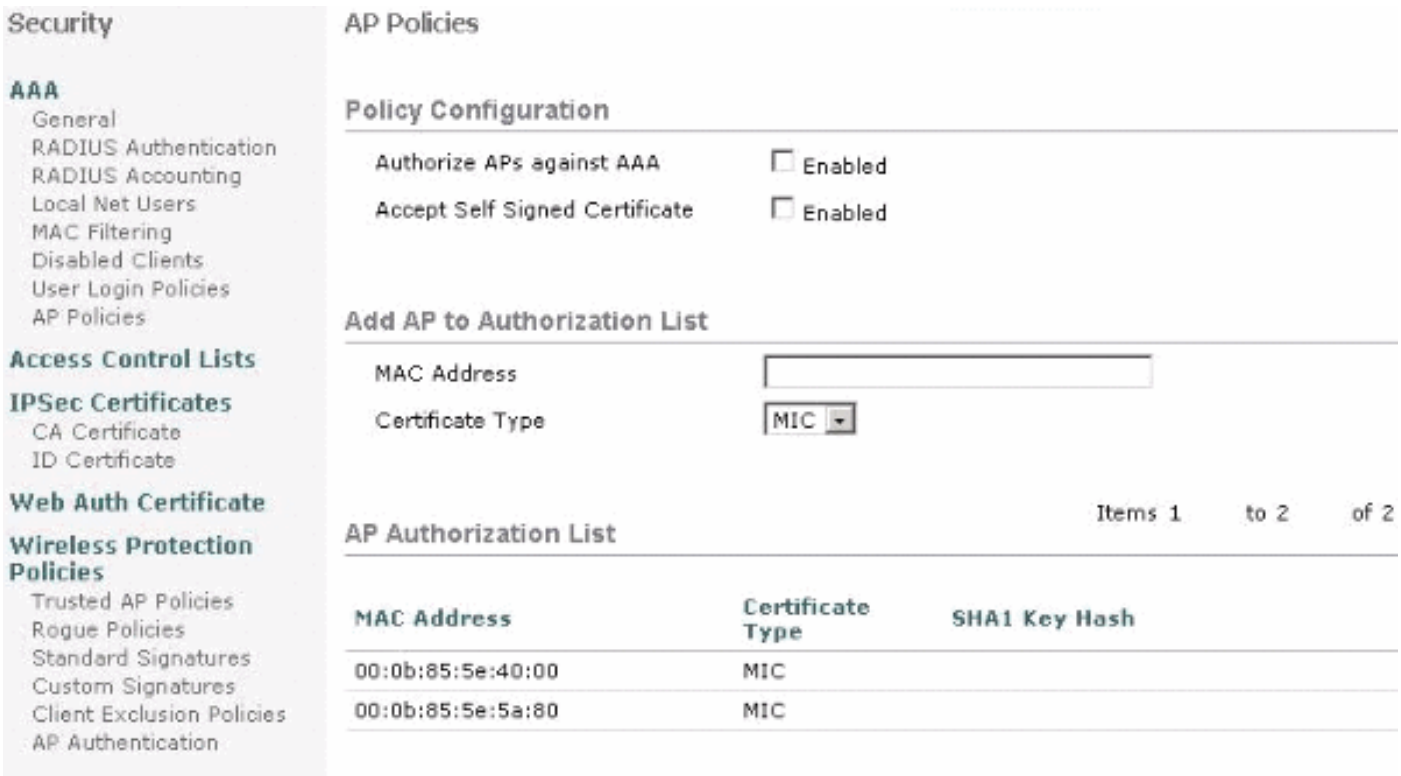
1. Geben Sie den Befehl **config network zero-config enable** ein, um die Konfiguration ohne Benutzereingriff zu aktivieren.
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. Geben Sie den Befehl **config network bridging-shared-secret <string>** ein, um den gemeinsamen geheimen Bridging-Schlüssel hinzuzufügen.
   ```
   (Cisco Controller) >config network bridging-shared-secret Cisco
   ```

Hinzufügen des MIC zur AP-Autorisierungsliste

Der nächste Schritt besteht darin, den Access Point der Autorisierungsliste des WLC hinzuzufügen. Wählen Sie dazu **Security > AP Policies (Sicherheit > AP-Richtlinien) aus**, geben Sie die AP-MAC-Adresse unter Add AP to Authorization List (AP zur Autorisierungsliste hinzufügen) ein, und klicken Sie auf **Add**.





In diesem Beispiel werden beide APs (der RAP und der PAP) der AP-Autorisierungsliste auf dem Controller hinzugefügt.

CLI-Konfiguration

Geben Sie den Befehl **config auth-list add mic <AP mac>** ein, um die MIC der Autorisierungsliste hinzuzufügen.

```
(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
```

Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

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
```

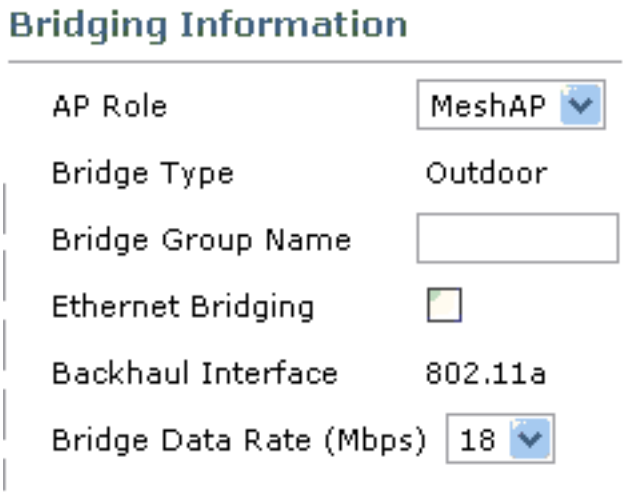
Konfigurieren der Bridging-Parameter für die APs

Dieser Abschnitt enthält Anweisungen zur Konfiguration der Rolle des Access Points im Mesh-Netzwerk und der zugehörigen Bridging-Parameter. Sie können diese Parameter entweder über die GUI oder die CLI konfigurieren.

1. Klicken Sie auf **Wireless** und dann auf **All APs** unter Access Points. Die Seite Alle APs wird angezeigt.
2. Klicken Sie auf den Link **Detail** für Ihren AP1510, um die Seite All APs > Details aufzurufen.

Auf dieser Seite wird unter Allgemein der AP-Modus automatisch auf Bridge für APs festgelegt, die Bridge-Funktionen aufweisen, z. B. den AP1510. Diese Seite zeigt diese Informationen auch unter Bridging Information (Bridging-Informationen) an. Wählen Sie unter Bridging Information (Bridging-Informationen) eine der folgenden Optionen aus, um die Rolle dieses Access Points im Mesh-Netzwerk anzugeben:

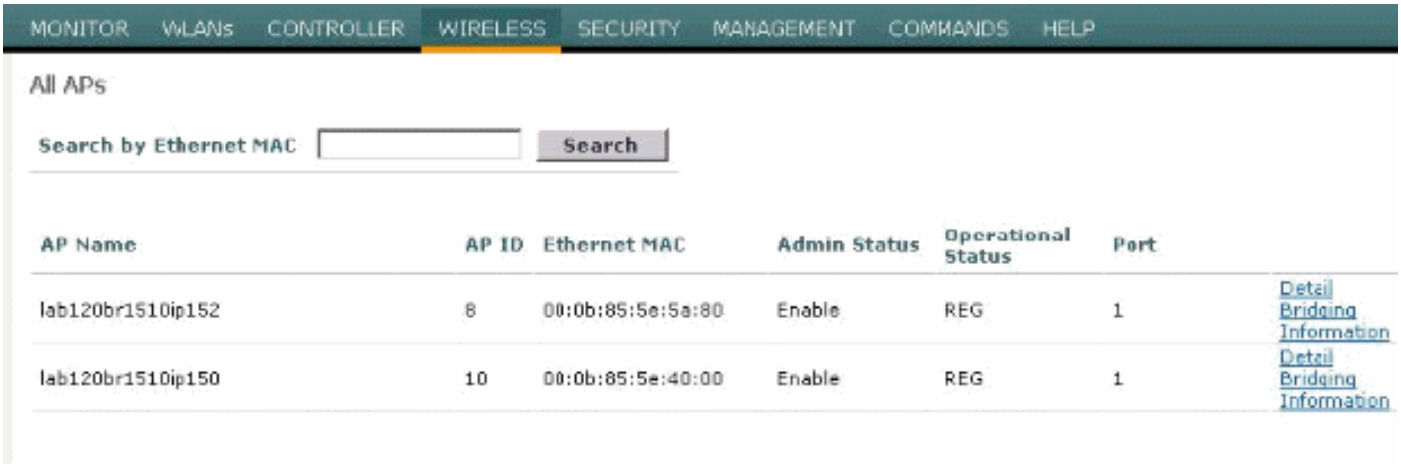
- **MeshAP**: Wählen Sie diese Option aus, wenn der AP1510 über eine Wireless-Verbindung mit dem Controller verfügt.
- **RootAP**: Wählen Sie diese Option aus, wenn der AP1510 über eine Kabelverbindung mit dem Controller verfügt.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

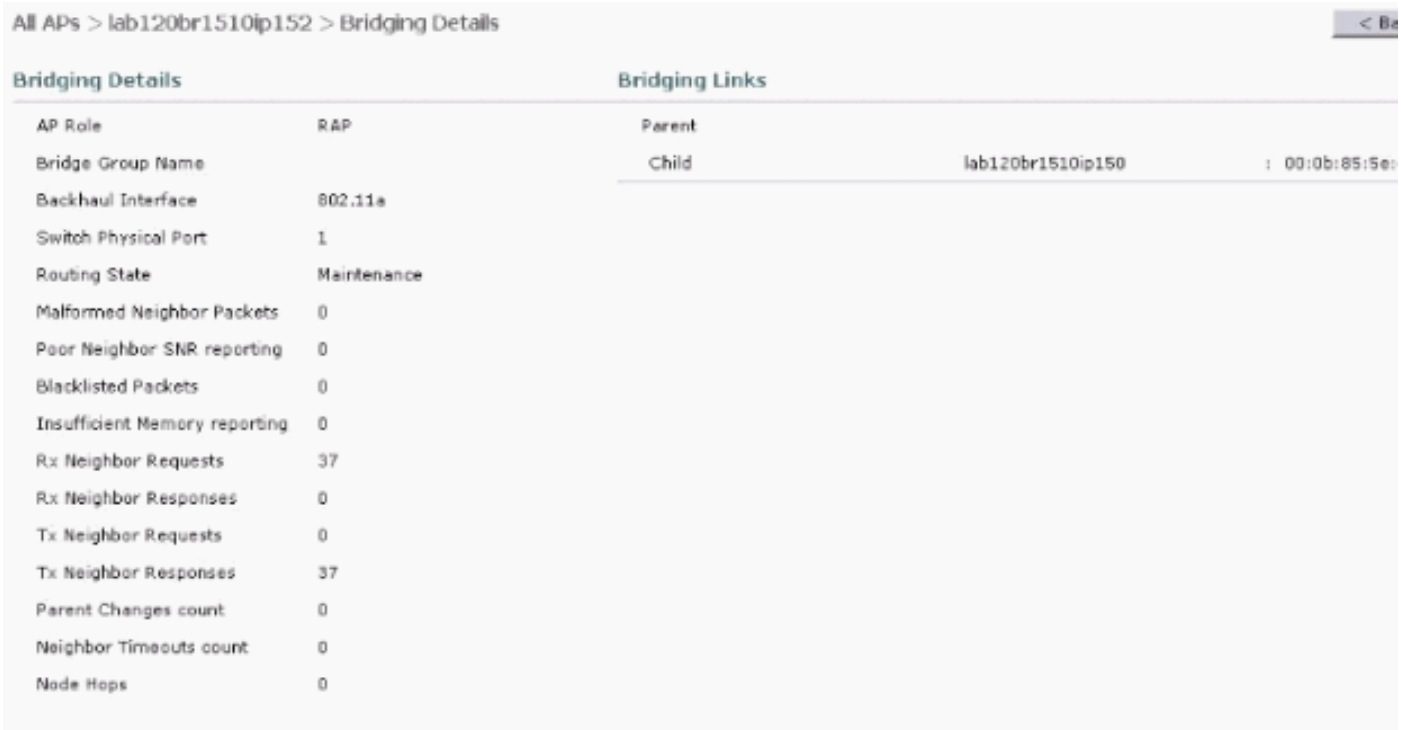
Nachdem sich die APs beim WLC registriert haben, können Sie sie auf der Registerkarte Wireless (Wireless) oben in der GUI des WLC anzeigen:



Auf der CLI können Sie den Befehl **show ap summary** verwenden, um zu überprüfen, ob die beim WLC registrierten APs:

```
(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) >
```

Klicken Sie in der GUI auf **Bridging Details**, um die Rolle des Access Points zu überprüfen:



In der CLI können Sie mithilfe der Befehle **show Mesh path <Cisco AP>** und **show Mesh** neben **<Cisco AP>**-Befehlen überprüfen, ob die beim WLC registrierten Access Points:

```
(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) >
```

Fehlerbehebung

`Mesh-APs stellen keine Verbindung zum WLC her`, was bei der Mesh-Bereitstellung am häufigsten auftrat. Führen Sie diese Prüfungen durch:

1. Überprüfen Sie, ob die MAC-Adresse des Access Points in der MAC-Filterliste des WLC hinzugefügt wurde. Dies wird unter **Sicherheit > Mac-Filterung** angezeigt.
2. Prüfen Sie den gemeinsamen geheimen Schlüssel zwischen RAP und MAP. Diese Meldung wird im WLC angezeigt, wenn der Schlüssel nicht übereinstimmt.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, invalid BRIDGE key Hash AP 00:0b:85:68:c1:d0"` **Hinweis:** Versuchen Sie immer, die Option **Konfiguration ohne Benutzereingriff aktivieren** zu verwenden, wenn diese für eine Version verfügbar ist. Dadurch wird der Schlüssel für die Mesh-APs automatisch konfiguriert und Fehlkonfigurationen vermieden.
3. RAPs leiten keine Broadcast-Nachrichten über ihre Funkschnittstelle weiter. Konfigurieren Sie den DHCP-Server so, dass er IP-Adressen über Unicast sendet, sodass MAP ihre IP-Adressen von RAP weiterleiten kann. Andernfalls verwenden Sie eine statische IP für den MAP.
4. Lassen Sie entweder den Bridge-Gruppennamen auf Standardwerte zurück, oder stellen Sie sicher, dass die Bridge-Gruppennamen auf MAPs und dem zugehörigen RAPs genau gleich konfiguriert sind.

Diese Probleme sind spezifisch für Mesh Access Points. Informationen zu Verbindungsproblemen, die zwischen dem WLC und einem Access Point häufig auftreten, finden Sie unter Fehlerbehebung bei einem Lightweight Access Point Not Joining a Wireless LAN Controller (Kein WLAN-Controller).

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Sie können die folgenden Debugbefehle verwenden, um eine Fehlerbehebung für den WLC durchzuführen:

- debug pem state enable - Wird zum Konfigurieren der Debugoptionen für den Zugriffsrichtlinien-Manager verwendet.
- debug pem events enable - Wird zum Konfigurieren der Debugoptionen für den Zugriffsrichtlinien-Manager verwendet.
- debug dhcp message enable (DHCP-Fehlermeldung aktivieren) - Zeigt das Debuggen von DHCP-Meldungen an, die an den DHCP-Server und von diesem gesendet werden.
- debug dhcp packet enable (DHCP-Paketaktivierung): Zeigt das Debuggen von DHCP-Paketdetails, die an den und vom DHCP-Server gesendet werden.

Einige zusätzliche **Debugbefehle**, die Sie zur Fehlerbehebung verwenden können, sind:

- **debug lwapp errors enable**: Zeigt das Debuggen von LWAPP-Fehlern.
- **debug pm pki enable**: Zeigt das Debuggen von Zertifikatsmeldungen an, die zwischen dem Access Point und dem WLC übergeben werden.

Diese **Debug-Lwapp-Ereignisse aktivieren die** Ausgabe des WLC-Befehls, zeigt, dass die LAP beim WLC registriert wird:

```
(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
```

Zugehörige Informationen

- Implementierungsleitfaden für die Cisco Mesh Networking-Lösung
- Schnellstartanleitung: Cisco Aironet 1500 Lightweight Outdoor Mesh Access Points
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0
- Wireless-Support-Seite

- Technischer Support und Dokumentation - Cisco Systems