無線LAN控制器Mesh網路組態範例

目錄

簡介

本文提供如何使用網狀網解決方案建立點對點橋接連結的基本組態範例。此範例使用兩個輕量型存取點(LAP)。 一個LAP作為頂蓋接入點(RAP)運行，另一個LAP作為頂蓋接入點(PAP)運行，並且它們連線到思科無線區域網(WLAN)控制器(WLC)。 RAP通過Cisco Catalyst交換機連線到WLC。

有關WLC 5.2版及更新版本，請參閱無線LAN控制器MAP網路組態範例（5.2版及更新版本）

必要條件

- WLC已配置為基本操作。
- WLC設定在第3層模式下。
- 已設定WLC的交換器。

需求

嘗試此組態之前，請確保符合以下要求：

- LAP和Cisco WLC配置的基本知識
- 輕量AP協定(LWAPP)基礎知識。
- 瞭解外部DHCP伺服器和/或域名伺服器(DNS)的配置
- 思科交換機的基本配置知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 4402系列WLC（執行韌體3.2.150.6）
- 兩(2)個Cisco Aironet 1510系列LAP
- 思科第2層交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

Cisco Aironet 1510系列輕量型室外網狀AP

Cisco Aironet 1510系列輕量型室外網狀AP是一種無線裝置，專用於無線客戶端訪問和點對點橋接、點對多點橋接以及點對多點網狀無線連線。室外接入點是一個獨立的單元，可以安裝在牆壁或懸垂處、屋頂柱或街燈柱上。

AP1510與控制器一起運行，可提供集中且可擴展的管理、高安全性和移動性。AP1510旨在支援零配置部署，可輕鬆、安全地加入網狀網路，並可通過控制器GUI或CLI管理和監控網路。

AP1510配備了兩個同時運行的無線電：用於客戶端訪問的2.4 GHz無線電和用於向其他AP1510傳輸資料的5 GHz無線電訊號。無線LAN使用者端流量會通過AP的回程無線電或通過其他AP1510中繼，直到到達控制器乙太網路連線。

屋頂式存取點(RAP)

RAP具有到Cisco WLC的有線連線。它們使用回傳無線介面與相鄰PAP通訊。RAP是任何橋接或網狀網路的父節點，將網橋或網狀網路連線到有線網路。因此，任何橋接或網狀網段只能有一個RAP。

注意：使用網狀網路解決方案進行LAN到LAN橋接時，請勿將RAP直接連線到Cisco WLC。Cisco WLC和RAP之間需要交換器或路由器，因為Cisco WLC不會轉送來自啟用LWAPP的埠的乙太網流量。RAP可以在第2層或第3層LWAPP模式下工作。

極頂式存取點(PAP)

PAP沒有到Cisco WLC的有線連線。它們可以是完全無線的，並支援與其他PAP或RAP通訊的客戶端，或者可用於連線外圍裝置或有線網路。出於安全原因，乙太網埠預設處於禁用狀態，但您應該為PAP啟用它。

注意：Cisco Aironet 1030遠端邊緣LAP支援單躍點部署，而Cisco Aironet 1500系列輕量型室外AP支援單躍點和多躍點部署。因此，Cisco Aironet 1500系列輕量型室外AP可用作屋頂AP，也可作為Cisco WLC一個或多個躍點的PAP。

網狀網路不支援的功能

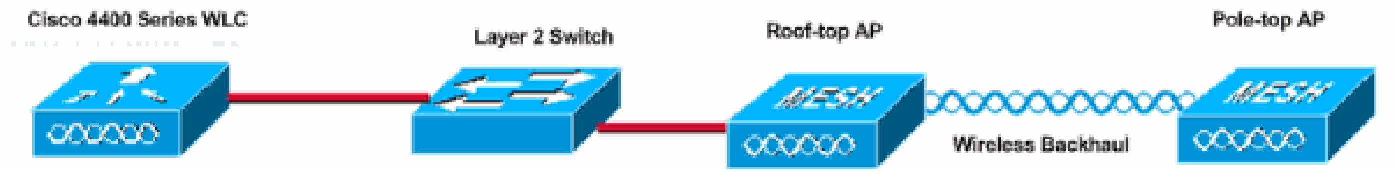
網狀網路不支援以下控制器功能：

- 多國支援
- 基於負載的CAC（網狀網路僅支援基於頻寬或靜態CAC。）
- 高可用性（快速心跳和主發現加入計時器）
- EAP-FASTv1和802.1X身份驗證
- EAP-FASTv1和802.1X身份驗證
- 本地有效證書
- 基於位置的服務

接入點啟動順序

以下清單描述了RAP和PAP啟動時會發生的情況：

- 所有流量在傳送到LAN之前都會通過RAP和Cisco WLC。
- 當RAP啟動時，PAP自動連線到它。
- 連線的鏈路使用共用金鑰生成用於為鏈路提供高級加密標準(AES)的金鑰。
- 一旦遠端PAP連線到RAP，網格AP就可以傳遞資料流量。
- 使用者可以使用思科命令列介面(CLI)、控制器的Cisco Web使用者介面或思科無線控制系統(Cisco WCS)更改共用金鑰或配置網格AP。 思科建議您修改共用金鑰。



設定

完成這些步驟，設定WLC和AP以進行點對點橋接。

1. 在WLC上啟用零接觸配置。
2. 將MIC新增到AP授權清單中。
3. 配置AP的橋接引數。
4. 驗證設定.

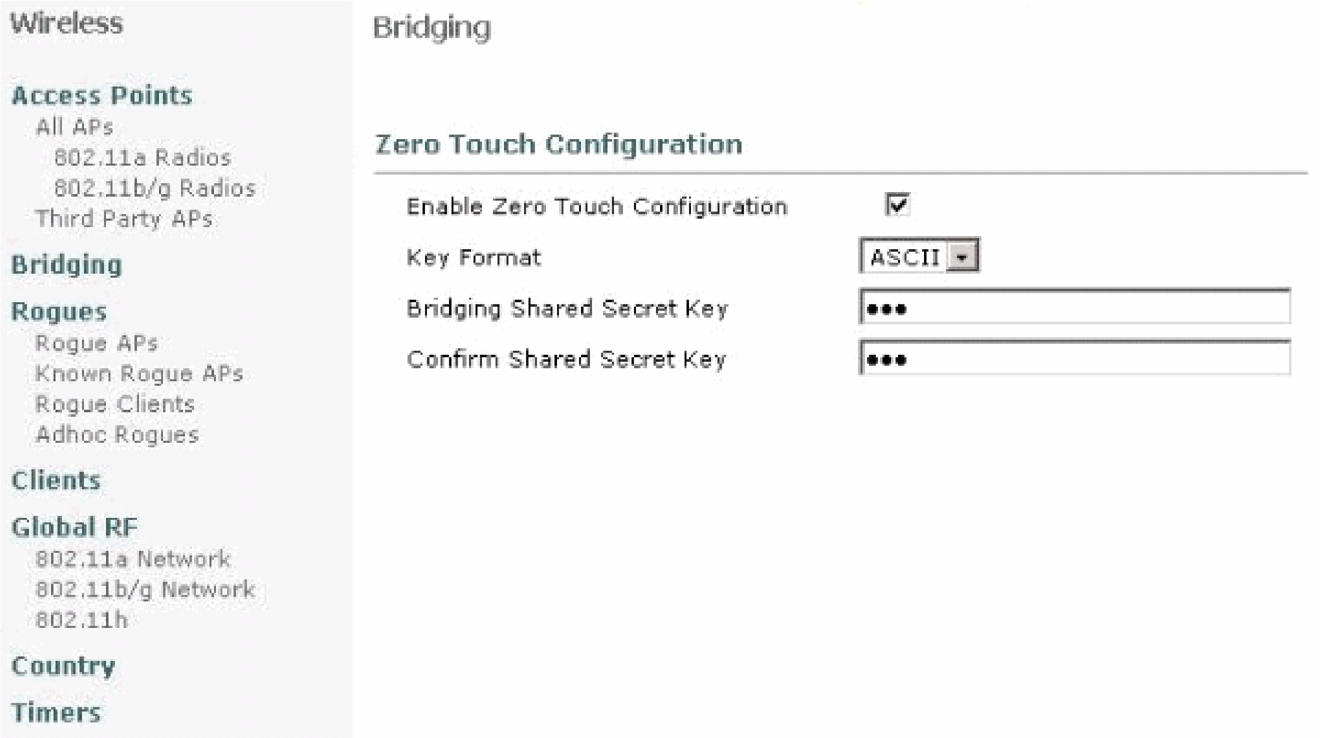
啟用零接觸配置（預設啟用）

GUI配置

啟用零接觸組態會使AP在控制器註冊到WLC時從控制器獲取共用金鑰。如果取消選中此框，則控制器不提供共用金鑰，並且AP使用預設預共用金鑰進行安全通訊。預設值已啟用（或已檢查）。 在WLC GUI上完成以下步驟：

註：WLC 4.1版及更新版本中沒有零接觸配置的配置。

1. 選擇**Wireless > Bridging**，然後按一下**Enable Zero Touch Configuration**。
2. 選擇金鑰格式。
3. 輸入橋接共用金鑰。
4. 在確認共用金鑰中再次輸入橋接共用金鑰。



Enable Zero Touch Configuration ☑

Key Format ASCII

Bridging Shared Secret Key •••

Confirm Shared Secret Key •••

CLI組態

從CLI完成以下步驟：

1. 發出**config network zero-config enable**命令，以啟用零接觸設定。

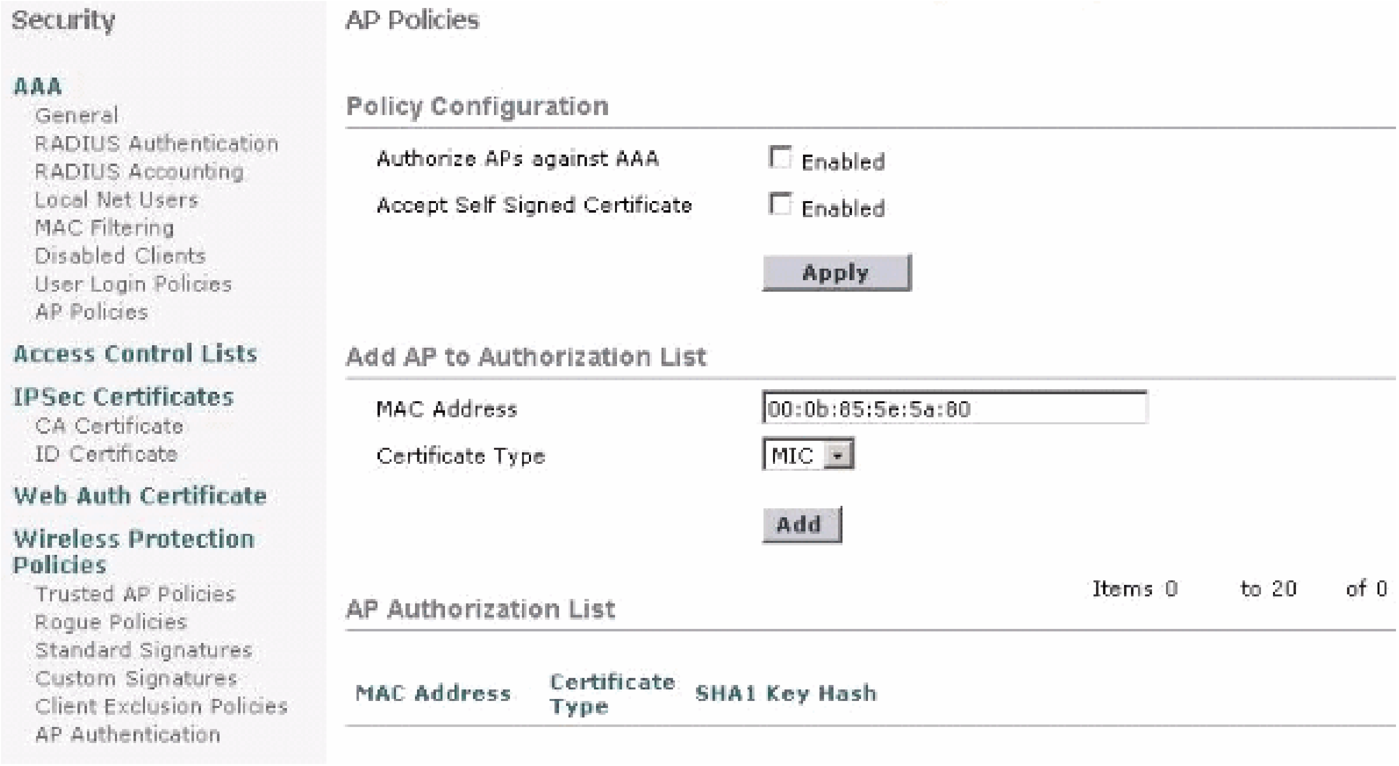
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. 發出**config network bridging-shared-secret <string>**命令以新增橋接共用金鑰。

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

將MIC新增到AP授權清單

下一步是將AP新增到WLC上的授權清單中。為此，請選擇**Security > AP Policies**，在Add AP to Authorization List下輸入AP MAC地址，然後按一下**Add**。



AP Policies

Policy Configuration

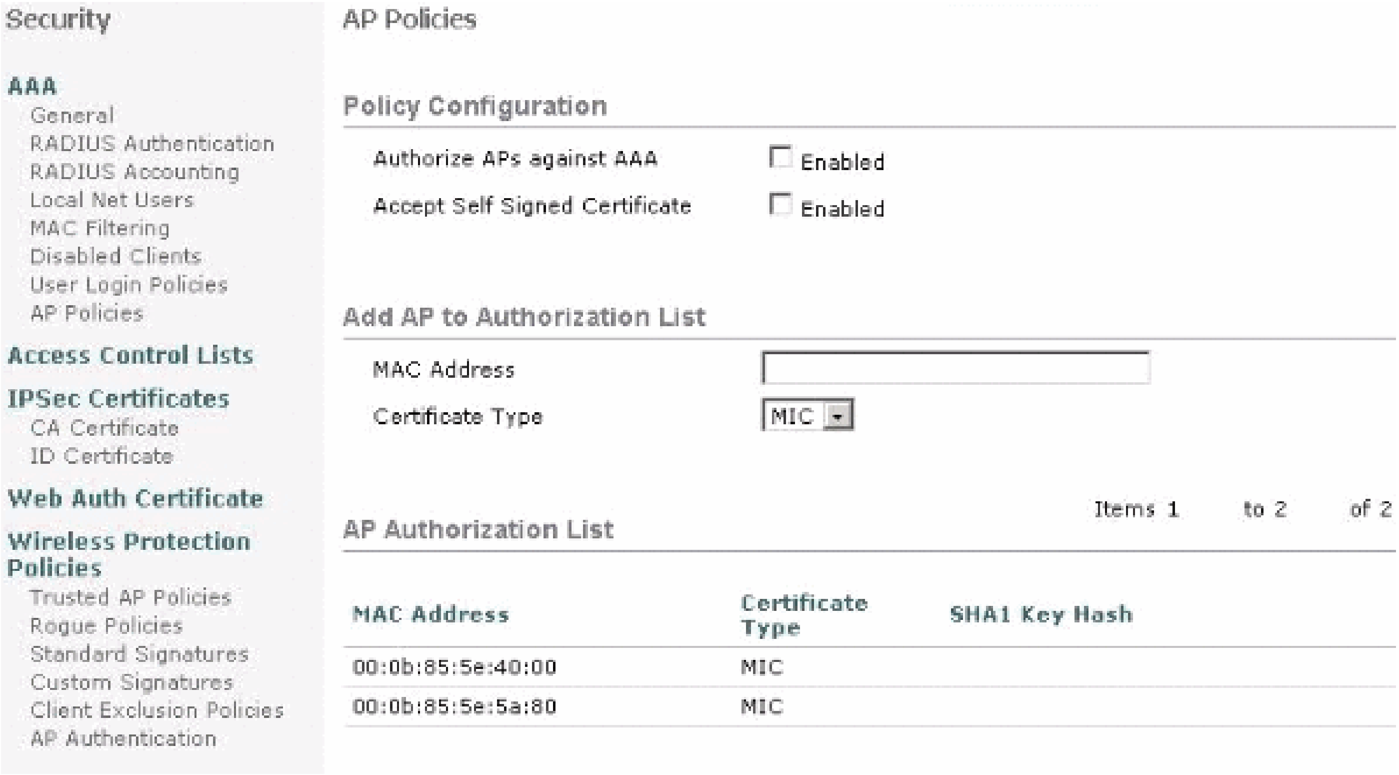
Authorize APs against AAA	□ Enabled
Accept Self Signed Certificate	□ Enabled

Add AP to Authorization List

MAC Address	00:0b:85:5e:5a:80
Certificate Type	MIC

AP Authorization List — Items 0 to 20 of 0

MAC Address	Certificate Type	SHA1 Key Hash



AP Policies

Policy Configuration

Authorize APs against AAA	□ Enabled
Accept Self Signed Certificate	□ Enabled

Add AP to Authorization List

MAC Address	
Certificate Type	MIC

AP Authorization List — Items 1 to 2 of 2

MAC Address	Certificate Type	SHA1 Key Hash
00:0b:85:5e:40:00	MIC	
00:0b:85:5e:5a:80	MIC	

在本範例中，兩個AP（RAP和PAP）都會新增到控制器上的AP授權清單中。

CLI組態

發出**config auth-list add mic <AP mac>**命令，將MIC新增到授權清單。

```
(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
```

組態

本檔案會使用以下設定：

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
```

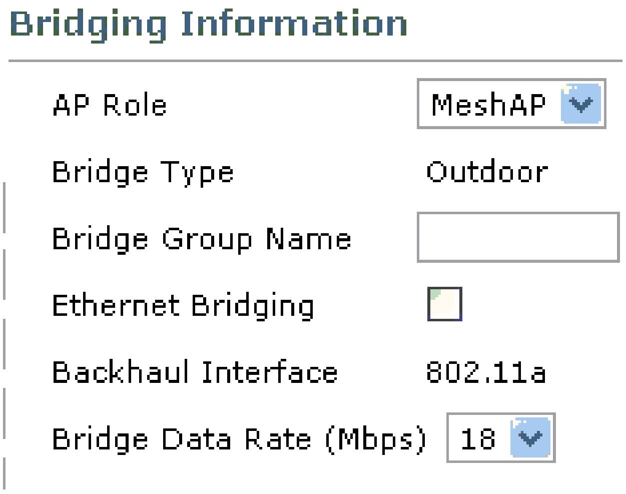
配置AP的橋接引數

本節提供如何配置AP在網狀網路中的角色和相關橋接引數的說明。您可以使用GUI或CLI配置這些引數。

1. 按一下**Wireless**，然後按一下**Access Points**下的All APs。系統將顯示All APs頁面。
2. 按一下AP1510的**Detail**連結以訪問All APs > Details頁面

在此頁面上，對於具有網橋功能的AP（例如AP1510），「常規」(General)下的AP模式自動設定為「網橋」(Bridge)。此頁還在「橋接資訊」(Bridging Information)下顯示此資訊。在Bridging Information下，選擇以下選項之一以指定此AP在網狀網中的角色：

- **MeshAP** — 如果AP1510與控制器有無線連線，請選擇此選項。
- **RootAP** — 如果AP1510與控制器有有線連線，請選擇此選項。



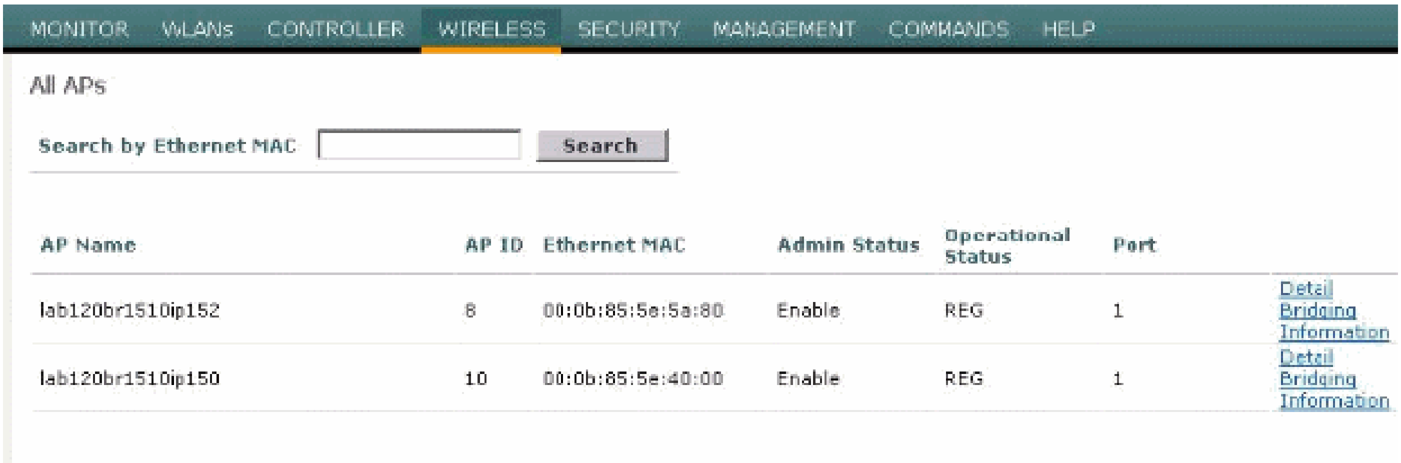
Bridging Information

AP Role	MeshAP
Bridge Type	Outdoor
Bridge Group Name	
Ethernet Bridging	□
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	18

驗證

使用本節內容，確認您的組態是否正常運作。

AP向WLC註冊後，您可以在WLC GUI頂部的Wireless頁籤下檢視它們：



All APs

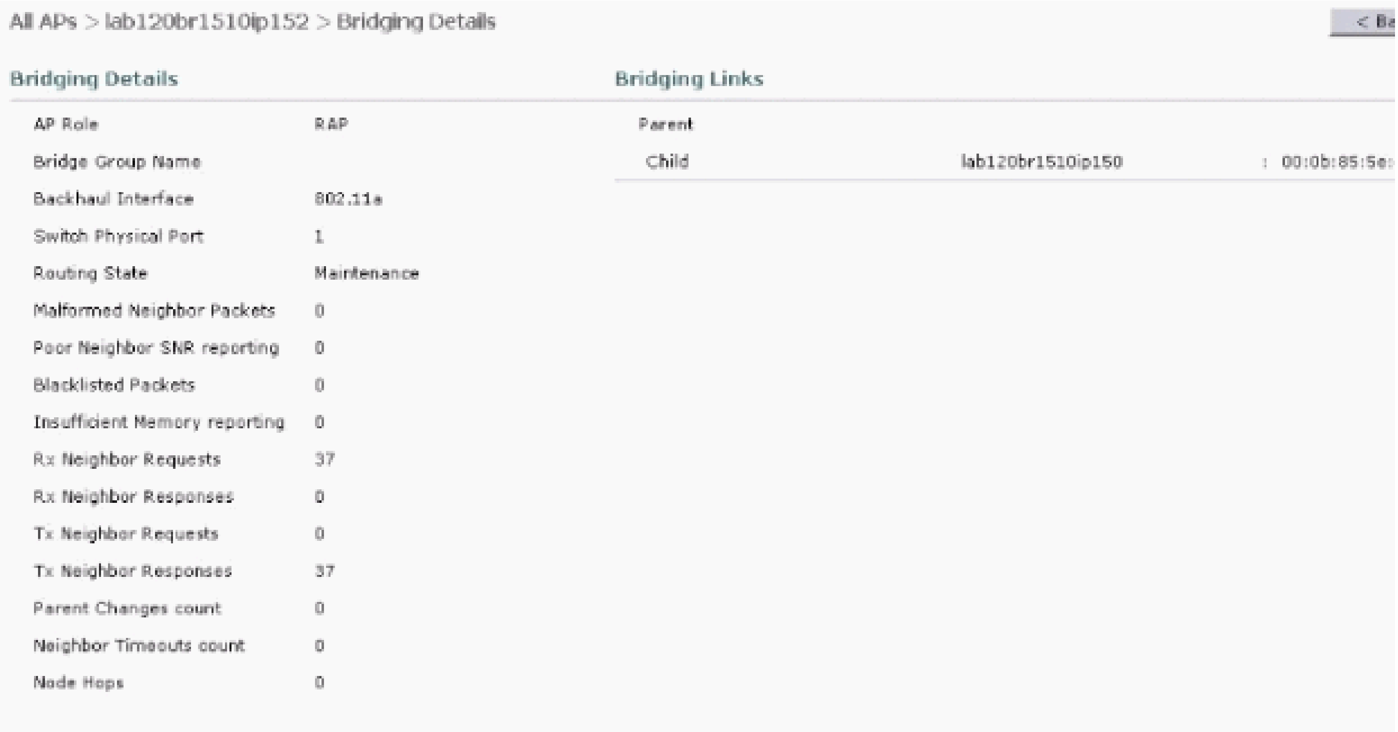
Search by Ethernet MAC

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
lab120br1510ip152	8	00:0b:85:5e:5a:80	Enable	REG	1	Detail Bridging Information
lab120br1510ip150	10	00:0b:85:5e:40:00	Enable	REG	1	Detail Bridging Information

在CLI上，可以使用**show ap summary**命令驗證已在WLC中註冊的AP:

```
(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) >
```

在GUI中按一下**Bridging Details**以驗證AP的角色：



All APs > lab120br1510ip152 > Bridging Details

Bridging Details

AP Role	RAP
Bridge Group Name	
Backhaul Interface	802.11a
Switch Physical Port	1
Routing State	Maintenance
Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	0
Blacklisted Packets	0
Insufficient Memory reporting	0
Rx Neighbor Requests	37
Rx Neighbor Responses	0
Tx Neighbor Requests	0
Tx Neighbor Responses	37
Parent Changes count	0
Neighbor Timeouts count	0
Node Hops	0

Bridging Links

Parent		
Child	lab120br1510ip150	: 00:0b:85:5e:

在CLI上，您可以使用**show mesh path <Cisco AP>**和**show mesh neigh neigh <Cisco AP>**指令驗證是否已向WLC註冊AP:

```
(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) >
```

疑難排解

APWLC是網狀部署中最常見的問題之一。完成以下檢查：

1. 檢查存取點的MAC位址是否已新增到WLC的Mac過濾器清單中。可從**Security > Mac Filtering**下看到這種情況。
2. 檢查RAP和MAP之間的共用金鑰。當金鑰不相符時，您可以在WLC中看到此訊息。`" LWAPP Join-Request AUTH_STRING_PAYLOAD invalid BRIDGE key hash AP 00:0b:85:68:c1:d0"` **附註：** 如果版本可用，請始終嘗試使用**啟用零接觸配置**選項。這樣可自動配置網狀AP的金鑰並避免配置錯誤。
3. RAP不會在其無線電介面上轉發任何廣播消息。因此，將DHCP伺服器配置為通過單播傳送IP地址，以便MAP可以通過RAP獲得轉發的IP地址。否則，請對MAP使用靜態IP。
4. 將Bridge Group Name保留為預設值，或者確保在MAP和相應的RAP上配置完全相同的網橋組名稱。

這些是網狀無線接入點特有的問題。有關WLC和存取點之間常見的連線問題，請參閱排解輕量存取點未加入無線LAN控制器的疑難問題。

疑難排解指令

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

您可以使用以下debug命令來排除WLC故障：

- **debug pem state enable** — 用於配置訪問策略管理器調試選項。
- **debug pem events enable** — 用於配置訪問策略管理器調試選項。
- **debug dhcp message enable** — 顯示與DHCP伺服器交換的DHCP消息的調試。
- **debug dhcp packet enable** — 顯示傳送到DHCP伺服器以及從DHCP伺服器傳送的DHCP資料包詳細資訊的調試。

您可以用來排解疑難問題的其他**debug**命令如下：

- **debug lwapp errors enable** — 顯示LWAPP錯誤的調試。
- **debug pm pki enable** — 顯示在AP和WLC之間傳遞的證書消息的調試。

此**debug lwapp events enable** WLC命令輸出顯示LAP已註冊到WLC:

```
(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
```

相關資訊

- 思科網狀網路解決方案部署指南
- 快速入門手冊：Cisco Aironet 1500系列輕量型室外網狀存取點
- 思科無線LAN控制器組態設定指南4.0版
- 無線支援頁面
- 技術支援與文件 - Cisco Systems