无线局域网控制器网状网络配置示例

目录

简介

本文档提供有关如何使用网状网络解决方案建立点对点桥接链路的基本配置示例。此示例使用两个轻量接入点 (LAP)。一个 LAP 充当屋顶接入点 (RAP)，另一个 LAP 充当杆顶接入点 (PAP)，并且这两者连接到一个 Cisco 无线 LAN (WLAN) 控制器 (WLC)。RAP 通过 Cisco Catalyst 交换机连接到 WLC。

[版本5.2及以上版本的](#)请参考的[无线局域网控制器网状网络配置示例](#)WLC版本5.2及以上版本版本的

先决条件

- 针对基本操作配置了 WLC。
- 以第 3 层模式配置了 WLC。
- 配置了 WLC 的交换机。

要求

尝试进行此配置之前，请确保满足以下要求：

- 有关 LAP 和 Cisco WLC 配置的基本知识
- 基本了解轻量 AP 协议 (LWAPP)。
- 了解外部 DHCP 服务器和/或域名服务器 (DNS) 配置方面的知识
- 了解 Cisco 交换机配置方面的基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 3.2.150.6 的 Cisco 4402 系列 WLC
- 两 (2) 个 Cisco Aironet 1510 系列 LAP
- Cisco 第 2 层交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

Cisco Aironet 1510 系列轻量室外网状 AP

Cisco Aironet 1510 系列轻量室外网状 AP 是一种专为无线客户端访问和点对点桥接、点对多点桥接以及点对多点网状无线连接而设计的无线设备。室外接入点是一种可以安装在墙壁或突出物、屋顶桅杆或者路灯桅杆上的独立单元。

AP1510 与控制器一起运行，以提供集中和可扩展的管理、高安全性和移动性。AP1510 旨在支持零配置部署，可轻易而安全地加入网状网络，并且可用于通过控制器 GUI 或 CLI 管理和监控网络。

AP1510 配备两种同时运行的无线：客户端访问使用 2.4-GHz 无线，到其他 AP1510 的数据回程使用 5-GHz 无线。无线 LAN 客户端流量通过 AP 的回程无线电进行传递，或通过其他 AP1510 进行中继，直至抵达控制器的以太网连接为止。

屋顶接入点 (RAP)

RAP 与 Cisco WLC 具有有线连接。这些 RAP 使用回程无线接口与相邻的 PAP 通信。RAP 是任何桥接或网状网络的父节点，它将桥接或网状网络连接到有线网络。因此，对于任何桥接网段或网状网络网段，只能有一个 RAP。

注意： 对 LAN 到 LAN 桥接使用网状网络解决方案时，不要将 RAP 直接连接到 Cisco WLC。Cisco WLC 与 RAP 之间必须有交换机或路由器，因为 Cisco WLC 不转发来自启用了 LWAPP 的端口的以太网流量。RAP 可工作在第 2 层或第 3 层 LWAPP 模式下。

杆顶接入点 (PAP)

PAP 没有通往 Cisco WLC 的有线连接。这些 PAP 可以完全采用无线方式，并支持与其他 PAP 或 RAP 通信的客户端，也可以用于连接到外围设备或有线网络。默认情况下，出于安全原因禁用了以太网端口，但您需要为 PAP 启用此端口。

注意： Cisco Aironet 1030 远程边缘 LAP 支持单跃点部署，而 Cisco Aironet 1500 系列轻量室外 AP 支持单跃点和多跃点部署。就本身而论，Cisco Aironet 1500 系列轻量室外 AP 可用作屋顶 AP，还可用作距 Cisco WLC 一个或多个跃点的 PAP。

网状网络中不支持的功能

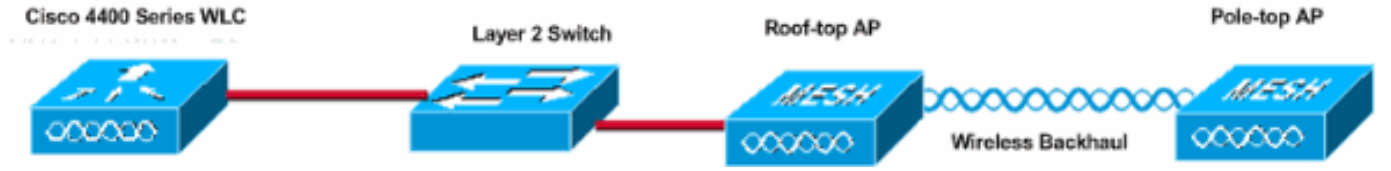
网状网络中不支持以下这些控制器功能：

- 多国家/地区支持
- 基于负载的 CAC（网状网络仅支持基于带宽的 CAC，即静态 CAC。）
- 高可用性（快速检测信号和主发现加入计时器）
- EAPFASTv1 和 802.1X 身份验证
- EAPFASTv1 和 802.1X 身份验证
- 本地签名证书
- 基于位置的服务

接入点启动顺序

下面这个列表介绍启动 RAP 和 PAP 时发生什么情况：

- 所有流量通过 RAP 和 Cisco WLC，然后再发送到 LAN。
- RAP 启动时，PAP 自动与其连接。
- 连链路使用一共享机密生成使用为链路提供高级加密标准(AES)的密钥。
- 远程 PAP 连接到 RAP 后，网状 AP 即可传输数据流量。
- 使用Cisco命令行界面(CLI)，用户能更改共享机密或配置mesh AP，控制器的Cisco网页用户界面或者思科无线控制系统(Cisco WCS)。Cisco 建议您修改共享密钥。



配置

完成以下这些步骤，为点对点桥接配置 WLC 和 AP。

1. 在 WLC 上启用零接触配置。
2. 向 AP 授权列表添加 MIC。
3. 配置 AP 的桥接参数。
4. 验证配置。

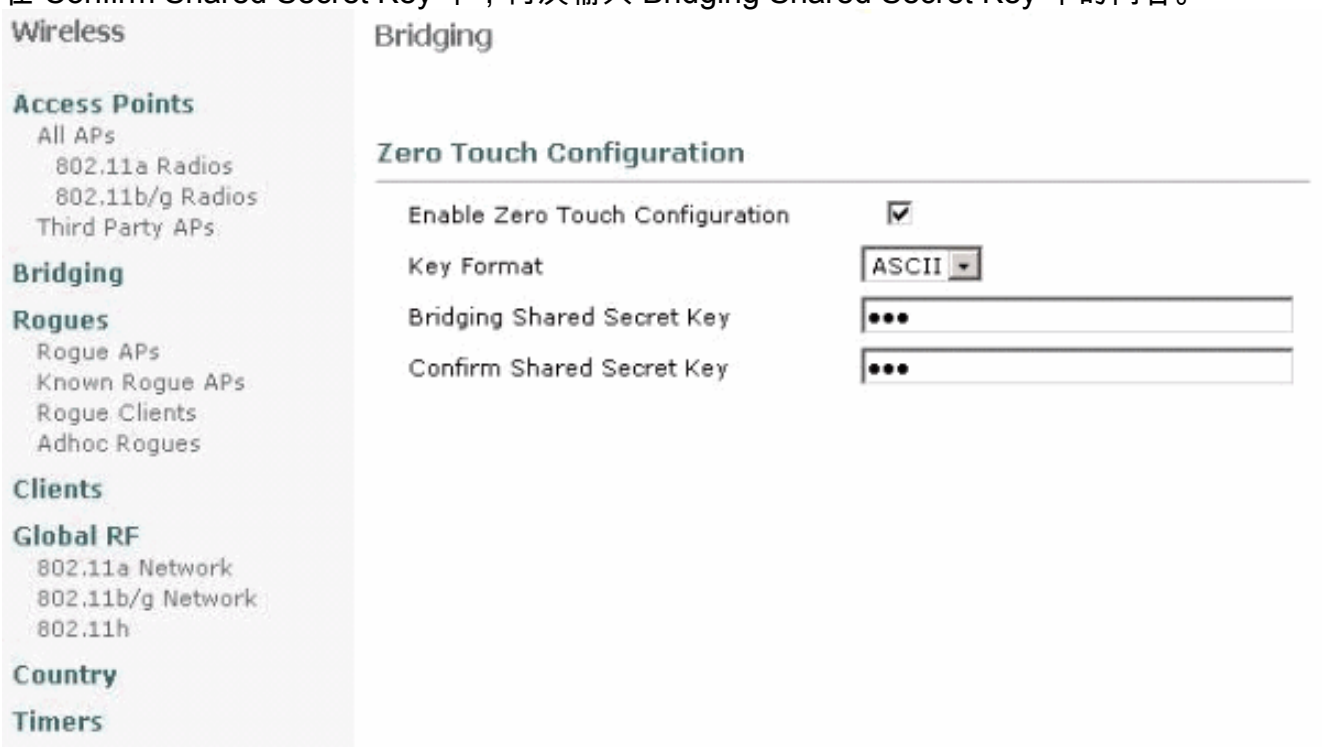
启用零接触配置（默认情况下启用）

GUI 配置

Enable Zero Touch Configuration 使 AP 在其注册到 WLC 后即可从控制器获得共享密钥。如果取消选中此框，则控制器不提供共享密钥，而 AP 使用默认的预先共享密钥进行安全通信。默认值为启用（即选中）。从 WLC GUI 中完成以下这些步骤：

注意： WLC 4.1 版及更高版本中未设置零接触配置。

1. 选择 **Wireless > Bridging**，然后单击 Enable Zero Touch Configuration。
2. 选择 Key Format。
3. 输入 Bridging Shared Secret Key。
4. 在 Confirm Shared Secret Key 中，再次输入 Bridging Shared Secret Key 中的内容。



CLI 配置

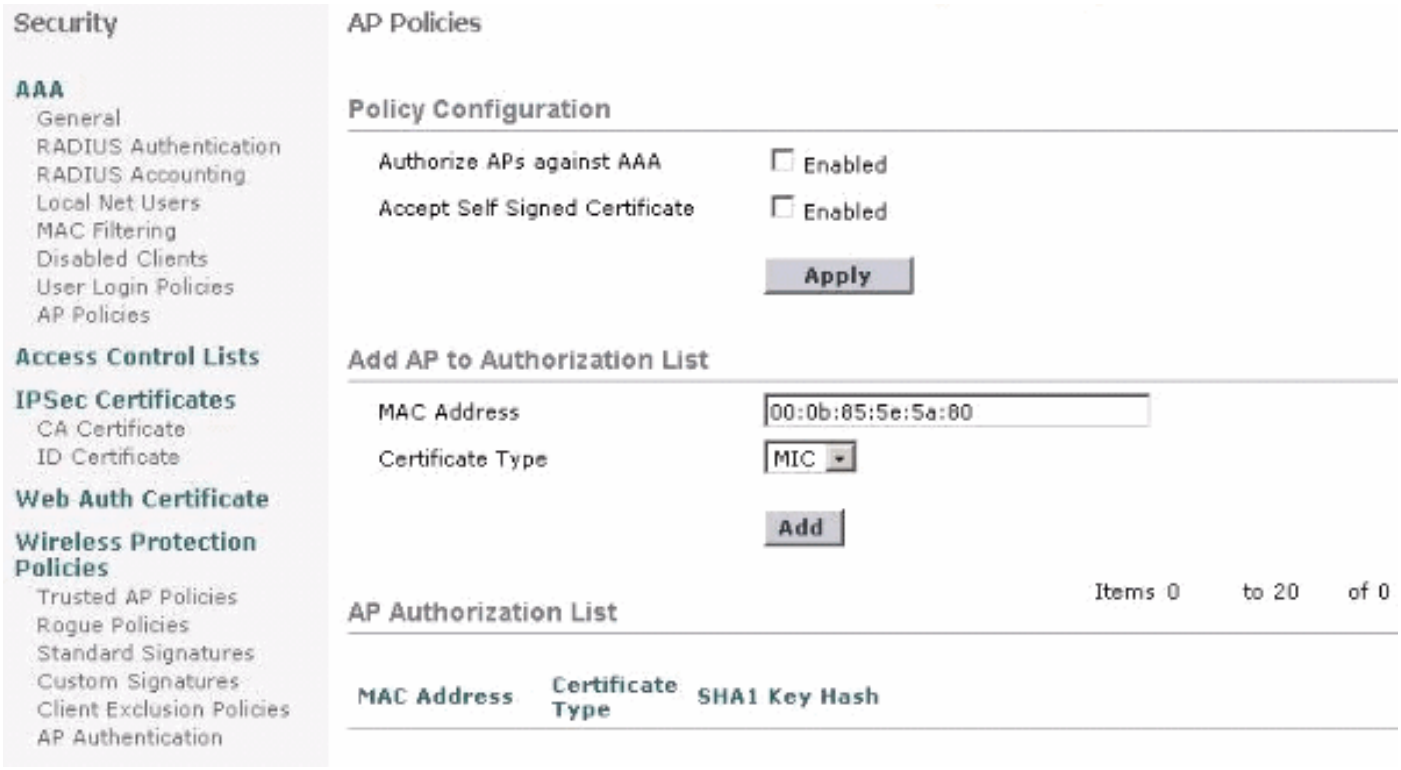
从 CLI 中完成以下这些步骤：

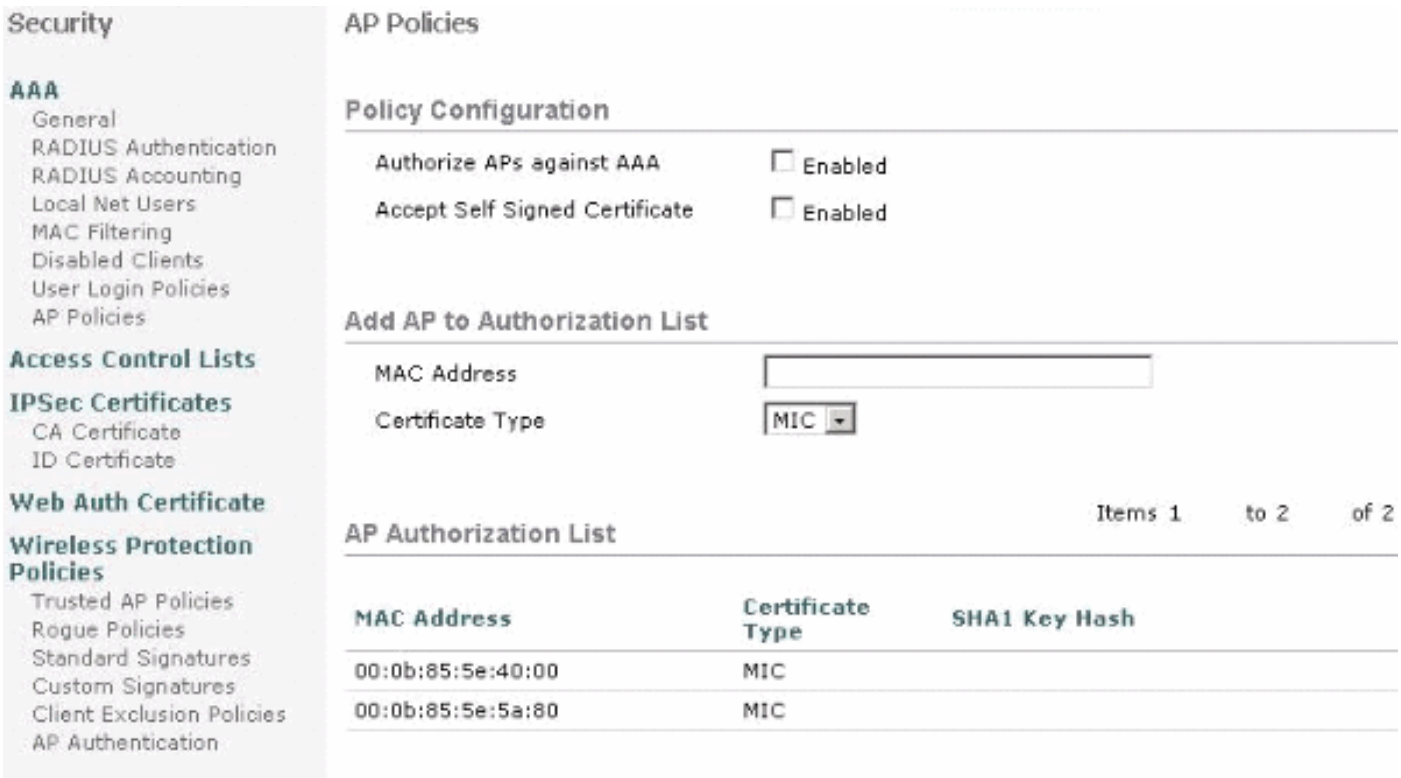
1. 发出 **config network zero-config enable** 命令以启用零接触配置。
```
(Cisco Controller) >config network zero-config enable
```

2. 发出 **config network bridging-shared-secret <字符串>** 命令以添加桥接共享密钥。
```
(Cisco Controller) >config network bridging-shared-secret Cisco
```

向 AP 授权列表添加 MIC

下一步是向 WLC 上的授权列表添加 AP。要执行此操作，请选择 **Security > AP Policies**，在 Add AP to Authorization List 下输入 AP 的 MAC 地址，然后单击 Add。





在本例中，将这两个 AP（RAP 和 PAP）都添加到控制器上的 AP 授权列表。

CLI 配置

发出 **config auth-list add mic <AP mac>** 命令以向授权列表添加 MIC。

```
(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
```

[配置](#)

本文档使用以下配置：

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
```

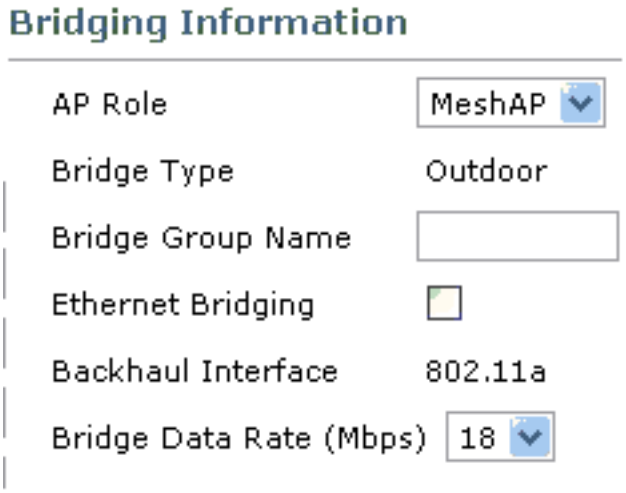
配置 AP 的桥接参数

此部分介绍如何配置 AP 在网状网络中的角色以及相关的桥接参数。可以使用 GUI 或 CLI 配置这些参数。

1. 单击 **Wireless**，然后单击 Access Points 下的 All APs。此时将显示 All APs 页。
2. 单击 AP1510 的 **Detail** 链接以访问 All APs > Details 页

在此页上，对于具有网桥功能的 AP（如 AP1510）总是将 General 下的 AP Mode 自动设置为 Bridge。此页还在 Bridging Information 下显示这些信息。在 Bridging Information 下，选择以下这些选项之一以指定此 AP 在网状网络中的角色：

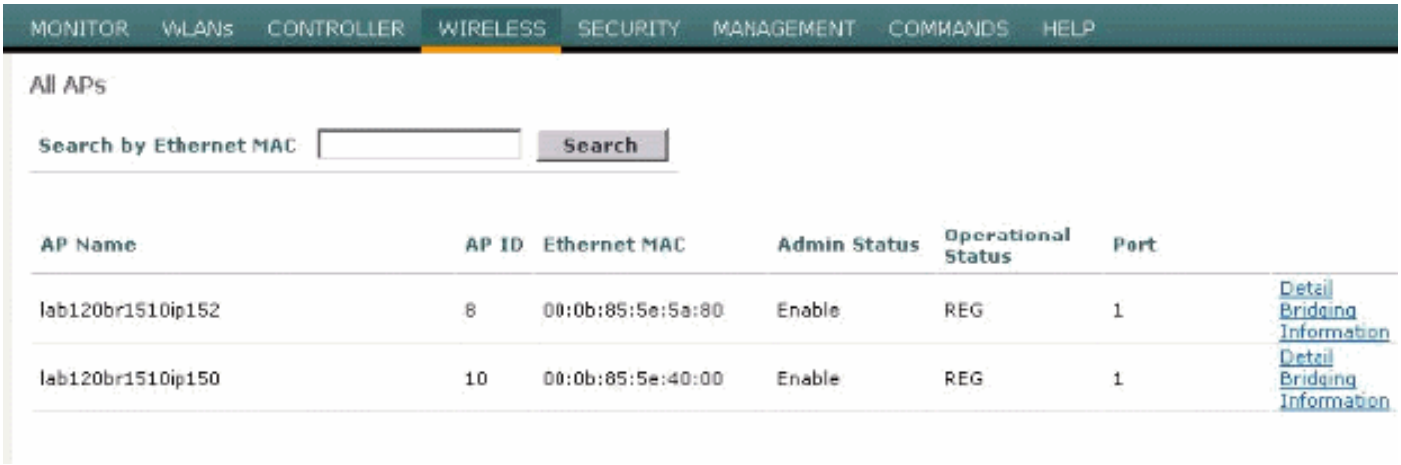
- **MeshAP** — 如果 AP1510 通过无线连接与控制器相连，则选择此选项。
- **RootAP** — 如果 AP1510 通过有线连接与控制器相连，则选择此选项。



验证

使用本部分可确认配置能否正常运行。

将 AP 注册到 WLC 之后，可以在 WLC 的 GUI 顶部的 Wireless 选项卡下查看这些 AP：



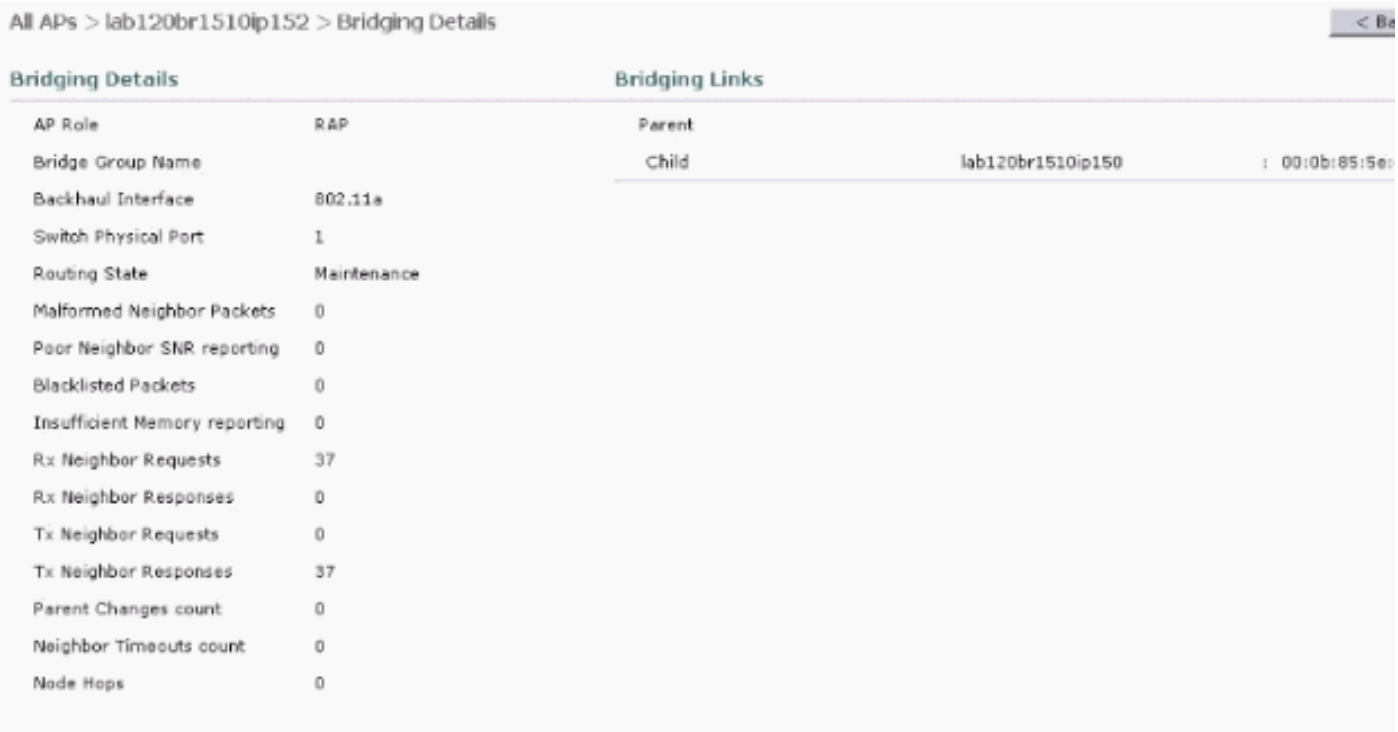
在 CLI 中，可以使用 **show ap summary** 命令验证 AP 是否已注册到 WLC：

```
(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) >
```

单击 GUI 中的 **Bridging Details** 以验证 AP 的角色：



在 CLI 中，可以使用 **show mesh path <Cisco AP>** 和 show mesh neigh <Cisco AP> 命令验证 AP 是否已注册到 WLC：

```
(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) >
```

故障排除

Mesh APs doesn't associate to the WLC 是网状部署中最常见的问题之一。完成以下这些检查：

1. 检查接入点的 MAC 地址是否已添加到 WLC 的 Mac Filter 列表中。在 **Security > Mac Filtering** 下可以看到这一点。
2. 检查 RAP 与 MAP 之间的共享密钥。当密钥中出现不匹配的情况时会在 WLC 中看到此消息。“LWAPPAUTH_STRING_PAYLOADAP 00:0b:85:68:c1:d0"**注意：** 请始终尝试使用 **Enable Zero Touch Configuration** 选项（如果某个版本中有此选项）。这将自动配置网状 AP 的密钥，从而避免错误配置。
3. RAP 不转发其无线接口上的任何广播消息。因此，配置 DHCP 服务器以通过单播发送 IP 地址，以使 MAP 可以让 RAP 转发其 IP 地址。否则，对 MAP 使用静态 IP。
4. 将 Bridge Group Name 保留为默认值，或确保在 MAP 和相应 RAP 上将 Bridge Group Name 配置得刚好相同。

这些是网状接入点所特有的问题。有关 WLC 与接入点之间所共有的连接问题，请参阅排除轻量接入点无法加入无线 LAN 控制器的故障。

故障排除命令

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

可以使用以下这些 debug 命令排除 WLC 的故障：

- debug pem state enable — 用于配置访问策略管理器的调试选项。
- debug pem events enable — 用于配置访问策略管理器的调试选项。
- debug dhcp message enable — 显示与 DHCP 服务器相互交换的 DHCP 消息的调试。
- debug dhcp packet enable — 显示与 DHCP 服务器相互往来的 DHCP 数据包详细信息的调试。

可用于排除故障的另一些 **debug** 命令为：

- **debug lwapp errors enable** — 显示 LWAPP 错误的调试。
- **debug pm pki enable** — 显示 AP 与 WLC 之间传递的证书消息的调试。

此 **debug lwapp events enable** WLC 命令输出表示 LAP 已注册到 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
```

相关信息

- Cisco 网状网络解决方案部署指南
- 快速入门指南：Cisco Aironet 1500 系列轻量室外网状接入点
- Cisco 无线 LAN 控制器配置指南 4.0 版
- 无线支持页
- 技术支持和文档 - Cisco Systems