Exemplo de configuração de rede em malha da controladora Wireless LAN

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações de Apoio](#)
[AP de malha externa leve Cisco Aironet 1510 Series](#)
[Ponto de acesso de telhado (RAP)](#)
[Ponto de acesso de vara (PAP)](#)
[Recursos não suportados em redes em malha](#)
[Sequência de inicialização do ponto de acesso](#)
[Configurar](#)
[Habilitar configuração zero-touch (Habilitado por padrão)](#)
[Adicione o MIC à lista de autorização do AP](#)
[Configurar parâmetros de bridging para os APs](#)
[Verificar](#)
[Troubleshoot](#)
[Comandos para Troubleshooting](#)
[Informações Relacionadas](#)

Introduction

Este documento fornece um exemplo da configuração básica que mostra como estabelecer um link ponto a ponto usando a solução de rede de malha. Este exemplo usa dois pontos de acesso leves (LAP). Um LAP opera como um ponto de acesso de telhado (RAP), o outro LAP opera como um ponto de acesso de montagem em poste (PAP), e são conectados a um Controlador de LAN Wireless (WLC) da Cisco. O RAP é conectado ao WLC através de um switch Cisco Catalyst.

Consulte o Exemplo de Configuração de Rede em Malha da Controladora Wireless LAN para as Versões 5.2 e posteriores para a WLC versão 5.2 e versões posteriores.

Prerequisites

- A WLC está configurada para operação básica.
- A WLC está configurada no modo de Camada 3.
- O switch para a WLC está configurado.

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração dos LAPs e dos WLCs da Cisco
- Conhecimento básico do Lightweight AP Protocol (LWAPP).
- Conhecimento da configuração de um servidor DHCP externo e/ou servidor de nome de domínio (DNS)
- Conhecimento de configuração básica de switches Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC Cisco 4402 Series que executa o firmware 3.2.150.6
- Dois (2) LAPs Cisco Aironet 1510 Series
- Switch Cisco de Camada 2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

AP de malha externa leve Cisco Aironet 1510 Series

O AP de malha externa leve Cisco Aironet 1510 Series é um dispositivo sem fio projetado para acesso de cliente sem fio e bridging ponto a ponto, bridging ponto a multiponto e conectividade sem fio ponto a multiponto. O ponto de acesso externo é uma unidade autônoma que pode ser montada em uma parede ou em uma tomada, em um poste de telhado ou em um poste de luz de rua.

O AP1510 opera com controladores para fornecer gerenciamento centralizado e escalável, alta segurança e mobilidade. Projetado para suportar implantações de configuração zero, o AP1510 se une de forma fácil e segura à rede em malha e está disponível para gerenciar e monitorar a rede através da GUI ou CLI do controlador.

O AP1510 é equipado com dois rádios operacionais simultaneamente: um rádio de 2,4 GHz usado para acesso do cliente e um rádio de 5 GHz usado para backhaul de dados para outros AP1510s. O tráfego do cliente de LAN sem fio passa pelo rádio de backhaul do AP ou é retransmitido através de outros AP1510s até alcançar a conexão Ethernet do controlador.

Ponto de acesso de telhado (RAP)

Os RAPs têm uma conexão com fio com um Cisco WLC. Eles usam a interface sem fio de

backhaul para se comunicar com PAPs vizinhos. Os RAPs são o nó pai de qualquer rede de bridging ou de malha e conectam uma bridge ou uma rede de malha à rede com fio. Consequentemente, pode haver somente um RAP para qualquer segmento em bridge ou de rede em malha.

Observação: ao usar a solução de rede em malha para bridging de LAN para LAN, não conecte um RAP diretamente a um Cisco WLC. Um switch ou roteador entre o Cisco WLC e o RAP é necessário porque as WLCs da Cisco não encaminham o tráfego Ethernet proveniente de uma porta habilitada para LWAPP. Os RAPs podem funcionar no modo LWAPP da camada 2 ou da camada 3.

Ponto de acesso de vara (PAP)

Os PAPs não têm conexão com fio com um Cisco WLC. Eles podem ser completamente sem fio e comportar clientes que se comunicam com outros PAPs ou RAPs, ou podem ser usados para se conectar a dispositivos periféricos ou a uma rede com fio. A porta Ethernet é desabilitar por padrão por razões de segurança, mas você deve habilitá-la para os PAPs.

Observação: os LAPs de borda remota Cisco Aironet 1030 suportam implantações de salto único, enquanto os APs externos Lightweight Cisco Aironet 1500 Series suportam implantações de salto único e de vários saltos. Como tal, os APs Lightweight Externo Cisco Aironet 1500 Series podem ser usados como APs de telhado e como PAPs para um ou mais saltos do Cisco WLC.

Recursos não suportados em redes em malha

Esses recursos do controlador não são suportados em redes de malha:

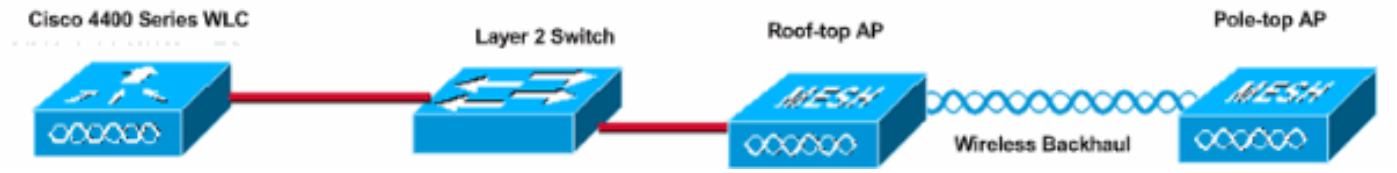
- Suporte em vários países
- CAC baseado em carga (as redes em malha suportam somente CAC baseada em largura de banda ou estática).
- Alta disponibilidade (pulsação rápida e temporizador de junção de descoberta primária)
- Autenticação EAP-FASTv1 e 802.1X
- Autenticação EAP-FASTv1 e 802.1X
- Certificado localmente significativo
- Serviços baseados no local

Sequência de inicialização do ponto de acesso

Esta lista descreve o que acontece quando o RAP e o PAP são iniciados:

- Todo o tráfego viaja através do RAP e do Cisco WLC antes de ser enviado para a LAN.
- Quando o RAP é ativado, os PAPs se conectam automaticamente a ele.
- O link conectado usa um segredo compartilhado para gerar uma chave que é usada para fornecer AES (Advanced Encryption Standard) para o link.
- Quando o PAP remoto se conecta ao RAP, os APs de malha podem passar o tráfego de dados.
- Os usuários podem alterar o segredo compartilhado ou configurar os APs em malha usando a interface de linha de comando (CLI) da Cisco, a interface de usuário da Web da Cisco do controlador ou o Cisco Wireless Control System (Cisco WCS). A Cisco recomenda que você

modifique o segredo compartilhado.



Configurar

Conclua estes passos para configurar a WLC e os APs para o bridging ponto-a-ponto.

1. Ative a configuração zero-touch na WLC.
2. Adicione o MIC à lista de autorização do AP.
3. Configure parâmetros de bridging para os APs.
4. Verificar a configuração.

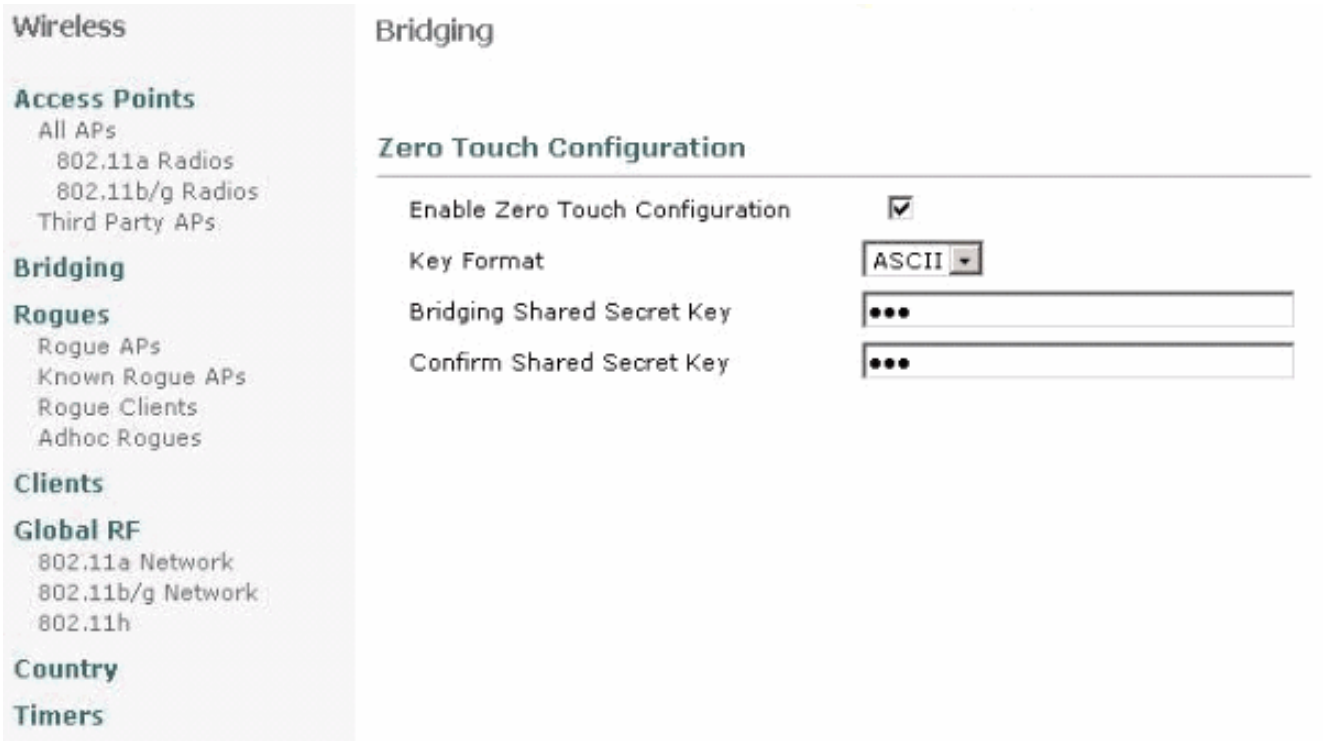
Habilitar configuração zero-touch (Habilitado por padrão)

Configuração de GUI

Habilitar Configuração Zero Touch permite que os APs obtenham a chave secreta compartilhada do controlador quando ele se registra no WLC. Se você desmarcar essa caixa, o controlador não fornecerá a chave secreta compartilhada e os APs usarão uma chave pré-compartilhada padrão para comunicação segura. O valor padrão está ativado (ou marcado). Conclua estes passos da GUI do WLC:

Observação: não há provisão para configuração Zero-Touch na versão 4.1 do WLC ou posterior.

1. Escolha **Wireless > Bridging** e clique em **Enable Zero Touch Configuration**.
2. Selecione o formato da chave.
3. Insira a chave secreta compartilhada de ponte.
4. Insira novamente a Chave secreta compartilhada de ponte na caixa Confirmar chave secreta compartilhada.



Configuração de CLI

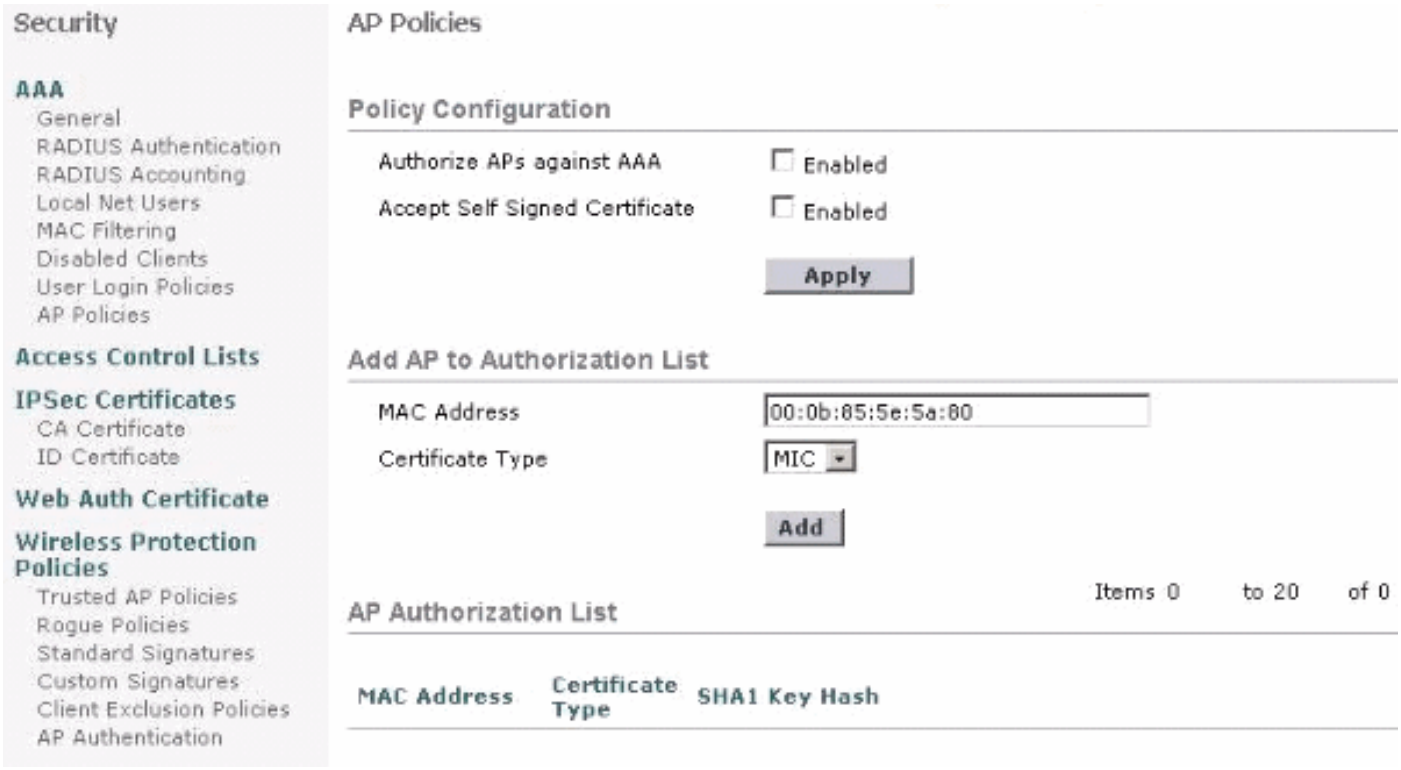
Conclua estes passos da CLI:

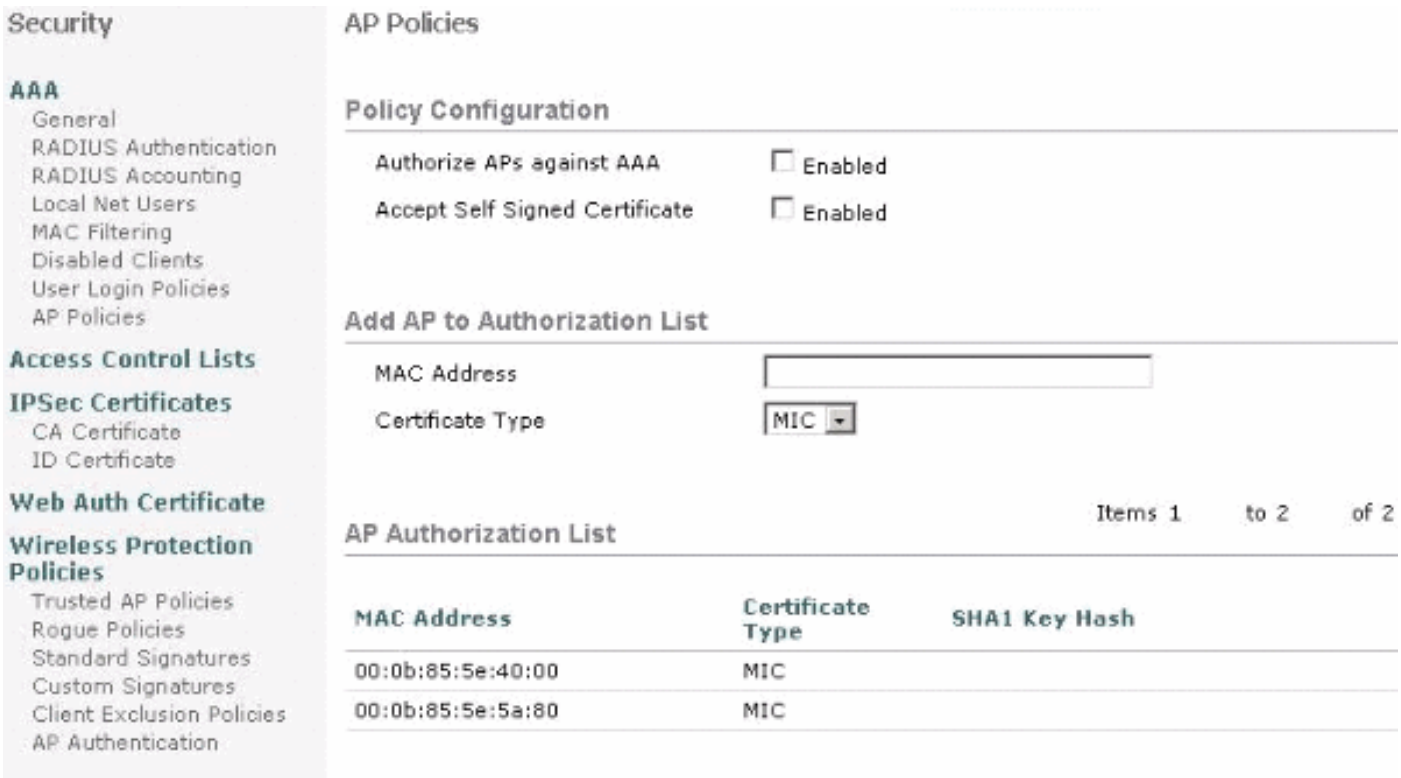
1. Execute o comando **config network zero-config enable** para ativar a configuração de toque zero.
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. Execute o comando **config network bridging-shared-secret <string>** para adicionar a chave secreta compartilhada de bridging.
   ```
   (Cisco Controller) >config network bridging-shared-secret Cisco
   ```

Adicione o MIC à lista de autorização do AP

A próxima etapa é adicionar o AP à lista de autorização na WLC. Para fazer isso, escolha **Security > AP Policies**, insira o endereço MAC do AP em Add AP to Authorization List e clique em **Add**.





Neste exemplo, ambos os APs (o RAP e o PAP) são adicionados à lista de autorização do AP no controlador.

Configuração de CLI

Emita o **comando config auth-list add mic <AP mac>** para adicionar o MIC à lista de autorização.

```
(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
```

Configuração

Este documento utiliza esta configuração:

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
```

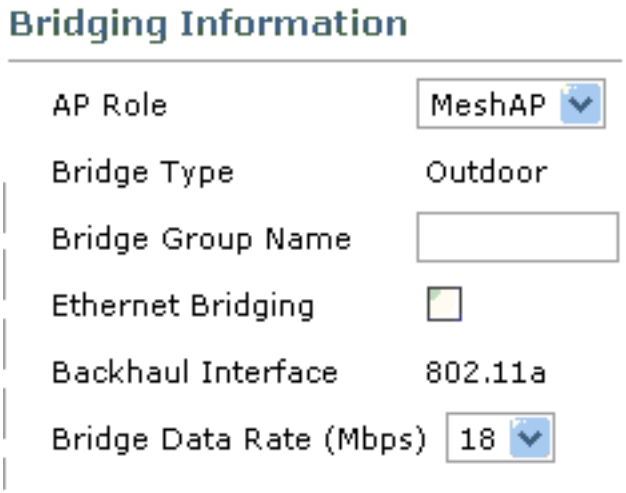
Configurar parâmetros de bridging para os APs

Esta seção fornece instruções sobre como configurar a função do AP na rede de malha e parâmetros de bridging relacionados. Você pode configurar esses parâmetros usando a GUI ou a CLI.

1. Clique em **Wireless** e em **All APs** em Access Points. A página Todos os APs é exibida.
2. Clique no link **Detalhe** do seu AP1510 para acessar a página Todos os APs > Detalhes

Nesta página, o Modo AP em Geral é automaticamente definido como Bridge para APs que têm funcionalidade de bridge, como o AP1510. Esta página também mostra essas informações em Bridging Information. Em Bridging Information, escolha uma destas opções para especificar a função deste AP na rede de malha:

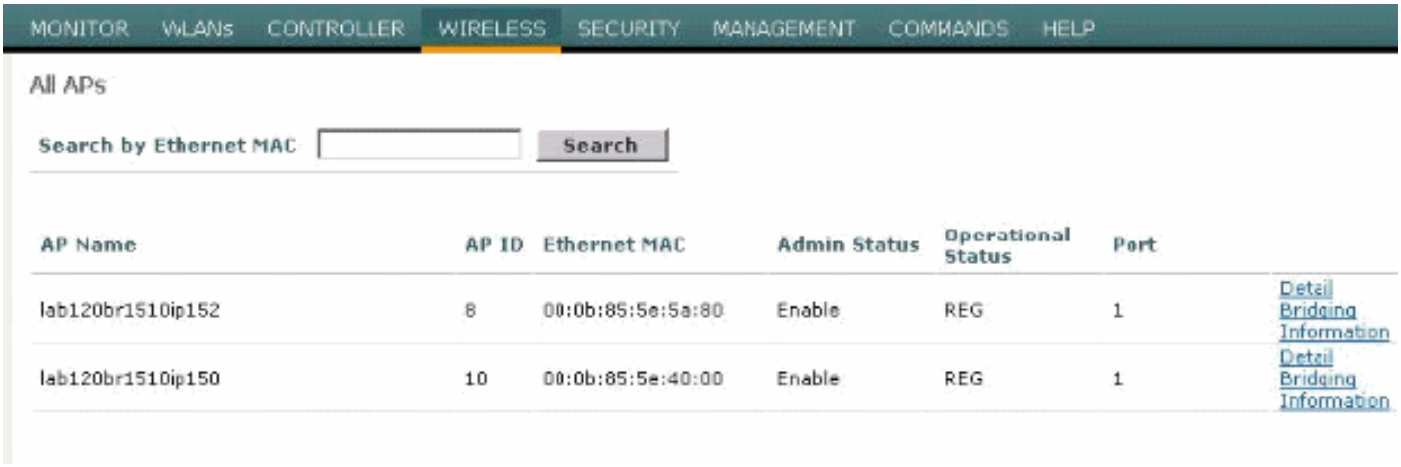
- **MeshAP** —Escolha esta opção se o AP1510 tiver uma conexão sem fio com a controladora.
- **RootAP** —Escolha esta opção se o AP1510 tiver uma conexão com fio com o controlador.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

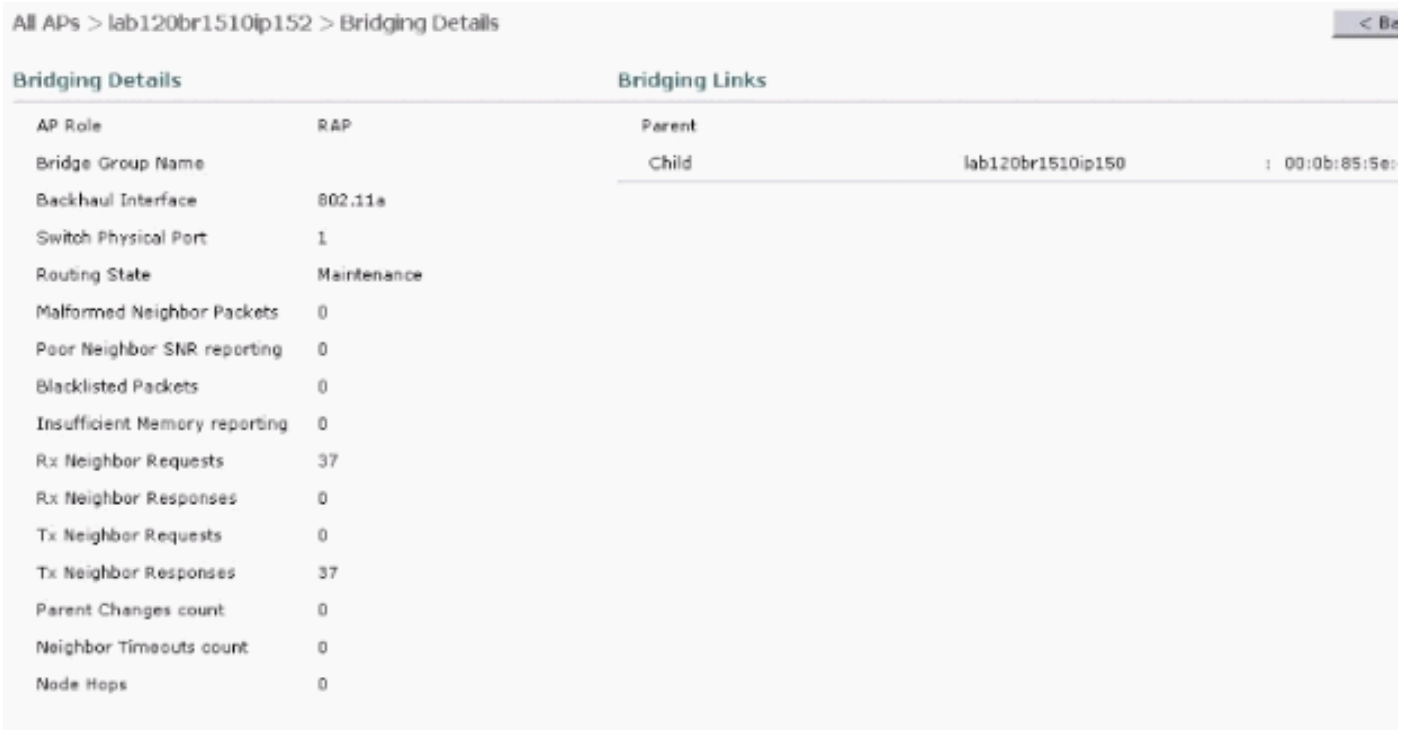
Depois que os APs se registrarem na WLC, você poderá visualizá-los na guia Wireless (Sem fio) na parte superior da GUI da WLC:



Na CLI, você pode usar o comando **show ap summary** para verificar se os APs estão registrados na 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) >
```

Clique em **Bridging Details** na GUI para verificar a função do AP:



Na CLI, você pode usar os comandos **show mesh path <Cisco AP>** e **show mesh neigh <Cisco AP>** para verificar se os APs estão registrados na 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) >
```

Troubleshoot

`Os APs em malha não se associam à WLC` é um dos problemas mais comuns observados na implantação da malha. Conclua estas verificações:

1. Verifique se o endereço MAC do ponto de acesso é adicionado na lista Filtro Mac na WLC. Isso pode ser visto em **Security > Mac Filtering**.
2. Verifique o segredo compartilhado entre o RAP e o MAP. Você pode ver essa mensagem na WLC quando há uma incompatibilidade na chave.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, hash de chave BRIDGE inválido AP 00:0b:85:68:c1:d0"` **Observação:** sempre tente usar a opção **Ativar configuração zero** se disponível para uma versão. Isso configura automaticamente a chave para os APs em malha e evita configurações incorretas.
3. Os RAPs não encaminham nenhuma mensagem de broadcast em sua interface de rádio. Portanto, configure o servidor DHCP para enviar endereços IP através de unicast para que o MAP possa obter seus endereços IP encaminhados pelo RAP. Caso contrário, use um IP estático para o MAP.
4. Deixe o nome do grupo de bridge em valores padrão ou certifique-se de que os nomes dos grupos de bridge estejam configurados exatamente como os mesmos em MAPs e no RAP correspondente.

Esses são problemas específicos dos pontos de acesso em malha. Para problemas de conectividade comuns entre a WLC e um ponto de acesso, consulte Solução de problemas de um ponto de acesso leve que não se une a um controlador de LAN sem fio.

Comandos para Troubleshooting

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Você pode usar estes comandos debug para solucionar problemas do WLC:

- **debug pem state enable** —Usado para configurar as opções de depuração do access policy manager.
- **debug pem events enable** —Usado para configurar as opções de depuração do access policy manager.
- **debug dhcp message enable** —Mostra a depuração de mensagens DHCP que são trocadas de e para o servidor DHCP.
- **debug dhcp packet enable** —Mostra a depuração dos detalhes do pacote DHCP que são enviados de e para o servidor DHCP.

Alguns comandos **debug** adicionais que você pode usar para solucionar problemas são:

- **debug lwapp errors enable** — Mostra a depuração de erros LWAPP.
- **debug pm pki enable** —Mostra a depuração de mensagens de certificado que são passadas entre o AP e a WLC.

Esta saída do comando **debug lwapp events enable** WLC mostra que o LAP é registrado no 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
```

Informações Relacionadas

- Guia de implantação da solução de rede em malha da Cisco
- Guia de início rápido: Pontos de acesso de malha externa leve Cisco Aironet 1500 Series
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems