Exemple de configuration de réseau à maillage de contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document propose un exemple de configuration de base pour établir une liaison en pont de point à point à l'aide de la solution de réseau maillé. Cet exemple utilise deux points d'accès allégés (LAP). Un LAP fonctionne comme un point d'accès de toit (RAP), l'autre LAP fonctionne comme un point d'accès de mât (PAP), et ils sont connectés à un contrôleur de réseau local sans fil de Cisco. Le point d'accès RAP est connecté au contrôleur de réseau local sans fil par un commutateur Cisco Catalyst.

Reportez-vous à [Exemple de configuration de réseau maillé de contrôleur de réseau local sans fil pour les versions 5.2 et ultérieures](#) pour les versions 5.2 et ultérieures du WLC

Conditions préalables

- Le WLC est configuré pour le fonctionnement de base.
- Le WLC est configuré en mode de couche 3.

- Le commutateur du WLC est configuré.

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de base de la configuration des LAP et des WLC Cisco
- Connaissance de base du protocole LWAPP (Lightweight AP Protocol).
- La connaissance de la configuration d'un server DHCP externe et/ou d'un domain name server (DNS)
- La connaissance de base de la configuration des commutateurs Cisco

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 4402 qui exécute le firmware 3.2.150.6
- Deux (2) LAP de la gamme Cisco Aironet 1510
- Commutateur de couche 2 Cisco

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Point d'accès extérieur léger pour réseau maillé de la gamme Cisco Aironet 1510

Le point d'accès extérieur léger pour réseau maillé de la gamme Cisco Aironet 1510 est un périphérique sans fil conçu pour l'accès client sans fil et le pontage point à point, le pontage point à multipoint et la connectivité sans fil maillée point à multipoint. Le point d'accès extérieur est une unité autonome qui peut être montée sur un mur ou un mur, sur un poteau sur le toit ou sur un poteau de lampadaire.

L'AP1510 fonctionne avec des contrôleurs pour fournir une gestion centralisée et évolutive, une sécurité élevée et la mobilité. Conçu pour prendre en charge des déploiements sans configuration, le point d'accès AP1510 se connecte facilement et en toute sécurité au réseau maillé et est disponible pour gérer et surveiller le réseau via l'interface graphique utilisateur ou l'interface de ligne de commande du contrôleur.

L'AP1510 est équipé de deux radios en fonctionnement simultané : une radio 2,4 GHz utilisée pour l'accès client et une radio 5 GHz utilisée pour la liaison de données vers d'autres AP1510. Le trafic client LAN sans fil passe par la radio de liaison du point d'accès ou est relayé par d'autres points d'accès 1510 jusqu'à ce qu'il atteigne la connexion Ethernet du contrôleur.

Point d'accès sur le toit (RAP)

Les RAP ont une connexion câblée à un WLC Cisco. Ils utilisent l'interface sans fil de liaison pour communiquer avec les PAP voisins. Les RAP sont le noeud parent vers tout réseau de pontage ou de maillage et connectent un pont ou un réseau maillé au réseau câblé. Par conséquent, il peut seulement y avoir un RAP pour tout segment de pont ou de réseau maillé.

Remarque : lorsque vous utilisez la solution de réseau maillé pour le pontage LAN à LAN, ne connectez pas un RAP directement à un WLC Cisco. Un commutateur ou un routeur entre le WLC Cisco et le RAP est requis car les WLC Cisco ne transmettent pas le trafic Ethernet provenant d'un port compatible LWAPP. Les RAP peuvent fonctionner en mode LWAPP de couche 2 ou de couche 3.

Point d'accès au sommet du pôle (PAP)

Les PAP n'ont pas de connexion câblée à un WLC Cisco. Ils peuvent être entièrement sans fil et prendre en charge les clients qui communiquent avec d'autres PAP ou RAP, ou ils peuvent être utilisés pour se connecter à des périphériques ou à un réseau câblé. Le port Ethernet est désactivé par défaut pour des raisons de sécurité, mais vous devez l'activer pour les PAP.

Remarque : Les LAP de périphérie distante Cisco Aironet 1030 prennent en charge les déploiements à un saut tandis que les AP extérieurs légers Cisco Aironet 1500 prennent en charge les déploiements à un et plusieurs sauts. Ainsi, les points d'accès extérieurs légers de la gamme Cisco Aironet 1500 peuvent être utilisés comme points d'accès sur le toit et comme points d'accès pour un ou plusieurs sauts du WLC Cisco.

Fonctionnalités non prises en charge sur les réseaux maillés

Ces fonctionnalités de contrôleur ne sont pas prises en charge sur des réseaux maillés :

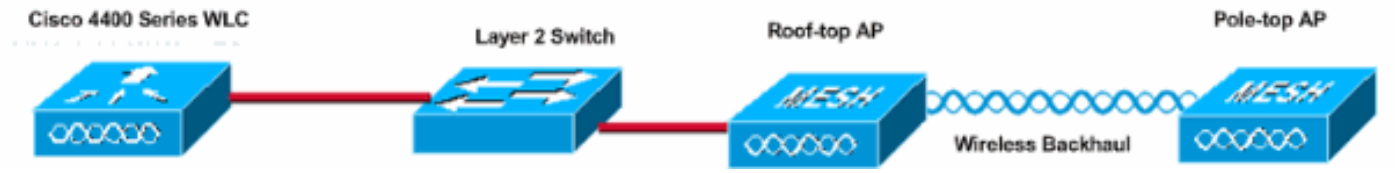
- Prise en charge multinationale
- CAC basé sur la charge (les réseaux maillés prennent en charge uniquement les CAC basés sur bande passante ou statiques.)
- Haute disponibilité (pulsation rapide et temporisateur de détection de connexion primaire)
- Authentification EAP-FASTv1 et 802.1x
- Authentification EAP-FASTv1 et 802.1x
- Certificat important localement
- Services de localisation

Séquence de démarrage du point d'accès

Cette liste décrit ce qui se passe au démarrage du RAP et du PAP :

- Tout le trafic traverse le RAP et le WLC Cisco avant d'être envoyé au LAN.
- Lorsque le RAP apparaît, les PAP s'y connectent automatiquement.
- La liaison connectée utilise un secret partagé pour générer une clé utilisée pour fournir la norme AES (Advanced Encryption Standard) de la liaison.
- Une fois que le PAP distant se connecte au RAP, les points d'accès maillés peuvent transmettre le trafic de données.

- Les utilisateurs peuvent modifier le secret partagé ou configurer les points d'accès maillés à l'aide de l'interface de ligne de commande (CLI) Cisco, de l'interface utilisateur Web Cisco du contrôleur ou du système de contrôle sans fil Cisco (Cisco WCS). Cisco vous recommande de modifier le secret partagé.



Configuration

Complétez ces étapes afin de configurer le WLC et les AP pour le pontage point à point.

1. Activez la configuration automatique sur le WLC.
2. Ajoutez le MIC à la liste d'autorisations du point d'accès.
3. Configurez les paramètres de pontage pour les points d'accès.
4. Vérifier la configuration

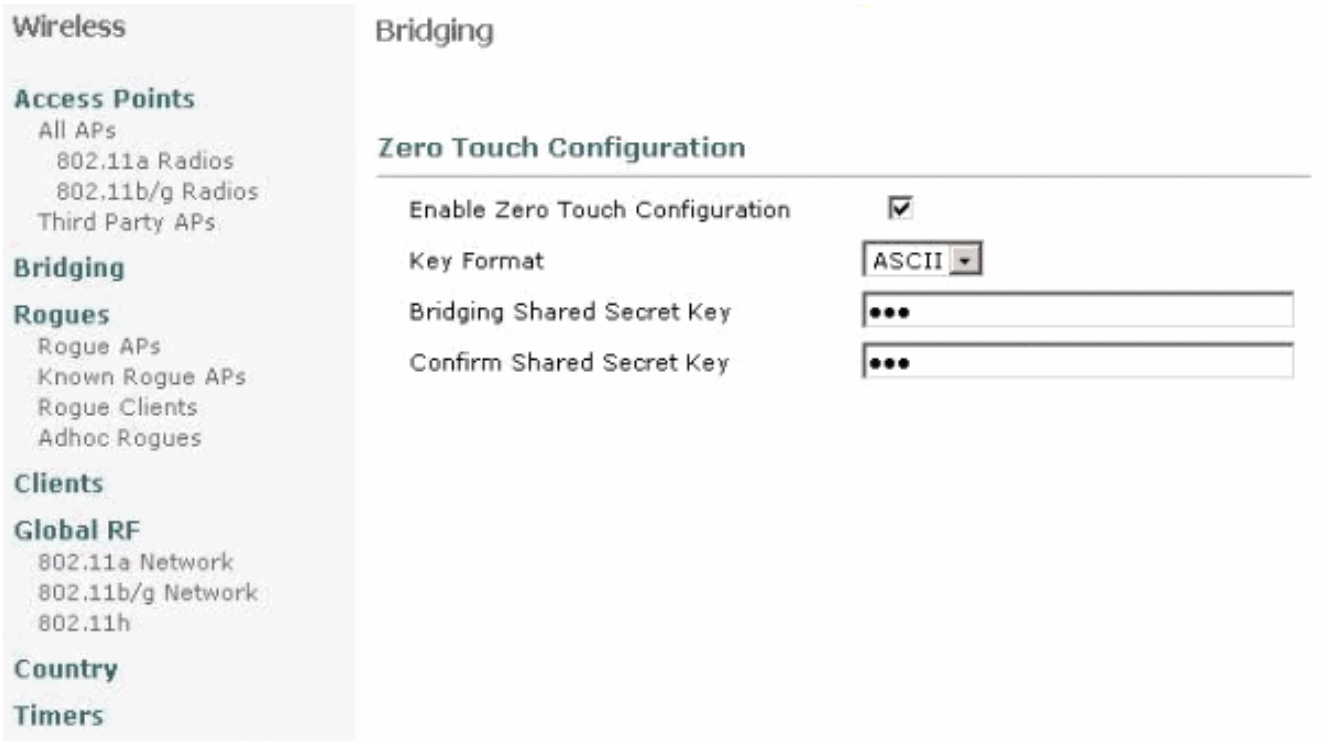
Activer la configuration automatique (activée par défaut)

Configuration de la GUI

Enable Zero Touch Configuration permet aux AP d'obtenir la clé secrète partagée du contrôleur lorsqu'il s'enregistre auprès du WLC. Si vous décochez cette case, le contrôleur ne fournit pas la clé secrète partagée, et les AP utilisent une clé pré-partagée par défaut pour la communication sécurisée. La valeur par défaut est activée (ou cochée). Complétez ces étapes à partir de l'interface graphique du WLC :

Remarque : Il n'existe aucune disposition pour la configuration Zero-Touch dans les versions 4.1 et ultérieures du WLC.

1. Choisissez **Wireless > Bridging** et cliquez sur **Enable Zero Touch Configuration**.
2. Sélectionnez le format de clé.
3. Saisissez la clé secrète partagée de pontage.
4. Saisissez à nouveau la clé secrète partagée de pontage dans Confirmer la clé secrète partagée.



Configuration CLI

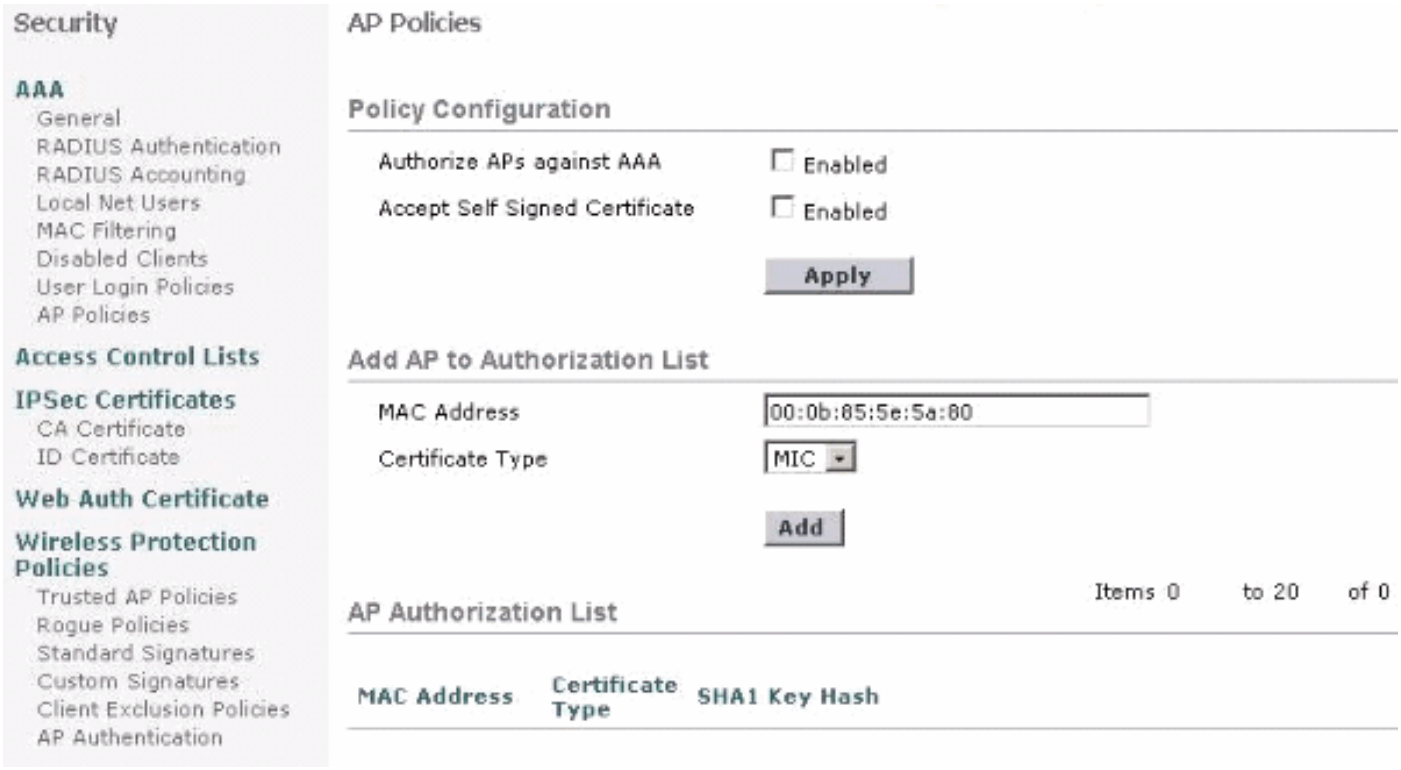
Effectuez ces étapes à partir de l'interface de ligne de commande :

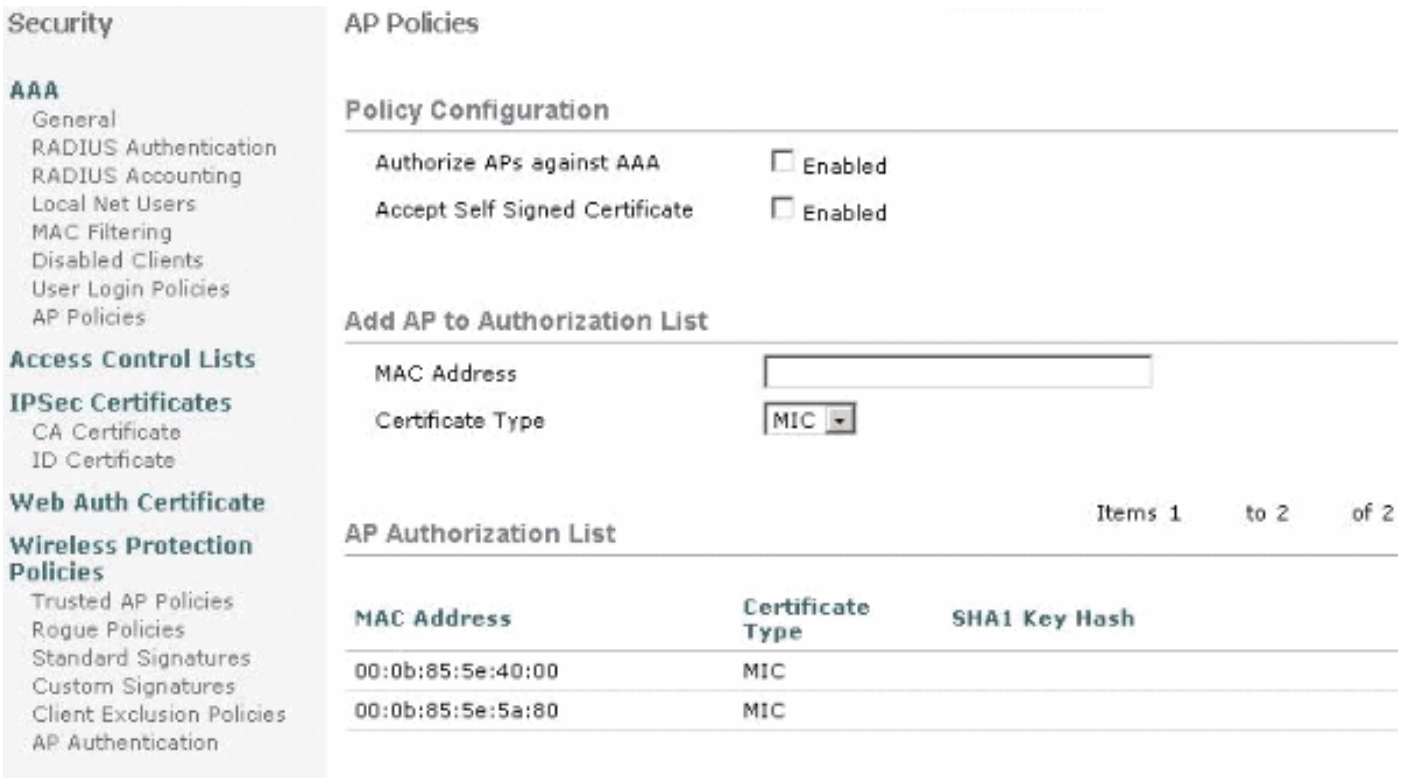
1. Émettez la commande **config network zero-config enable** afin d'activer la configuration zero touch.
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. Émettez la commande **config network bridging-shared-secret <string>** afin d'ajouter la clé secrète partagée de pontage.
   ```
   (Cisco Controller) >config network bridging-shared-secret Cisco
   ```

Ajouter le MIC à la liste d'autorisation du point d'accès

L'étape suivante consiste à ajouter l'AP à la liste d'autorisation sur le WLC. Pour ce faire, choisissez **Security > AP Policies**, saisissez l'adresse MAC de l'AP sous Add AP to Authorization List et cliquez sur **Add**.





Dans cet exemple, les deux points d'accès (RAP et PAP) sont ajoutés à la liste d'autorisation AP sur le contrôleur.

Configuration CLI

Émettez la commande **config auth-list add mic <AP mac>** afin d'ajouter le MIC à la liste d'autorisation.

```
(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
```

Configuration

Ce document utilise la configuration suivante :

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
```

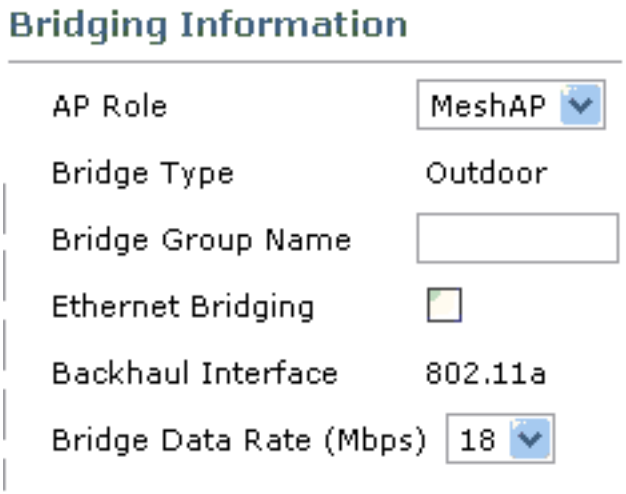
Configurer les paramètres de pontage des points d'accès

Cette section fournit des instructions sur la façon de configurer le rôle du point d'accès dans le réseau maillé et les paramètres de pontage associés. Vous pouvez configurer ces paramètres à l'aide de l'interface utilisateur graphique ou de l'interface de ligne de commande.

1. Cliquez sur **Sans fil**, puis sur **Tous les points d'accès** sous Points d'accès. La page Tous les AP s'affiche.
2. Cliquez sur le lien **Detail** pour votre AP1510 afin d'accéder à la page All APs > Details.

Sur cette page, le mode AP sous Général est automatiquement défini sur Bridge pour les AP qui ont une fonctionnalité de pont, comme AP1510. Cette page affiche également ces informations sous Bridging Information. Sous Bridging Information, choisissez l'une des options suivantes afin de spécifier le rôle de ce point d'accès dans le réseau maillé :

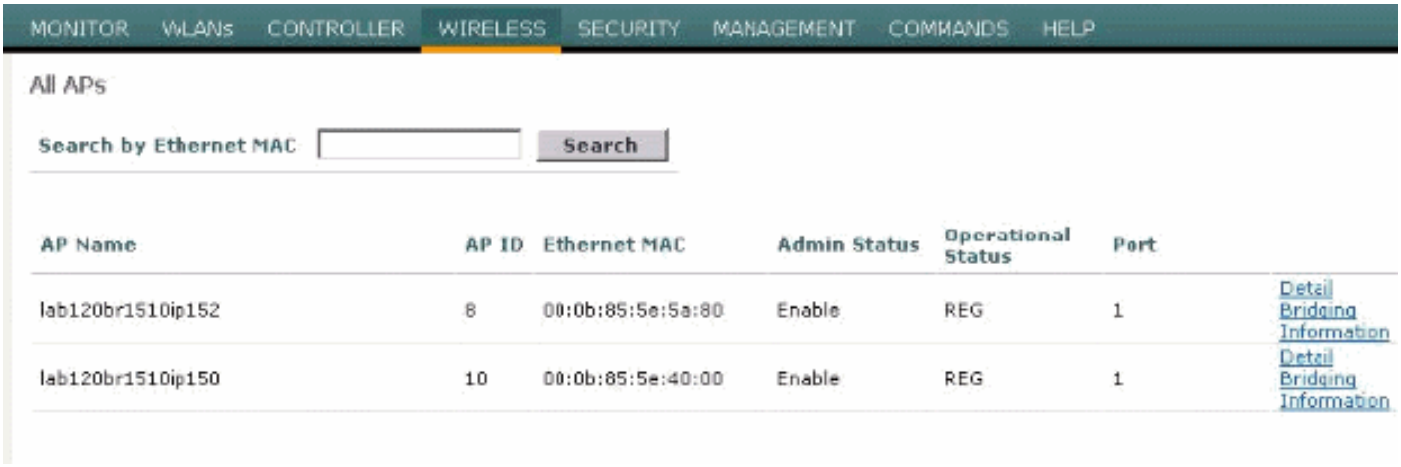
- **MeshAP** : sélectionnez cette option si l'AP1510 dispose d'une connexion sans fil au contrôleur.
- **RootAP** : sélectionnez cette option si l'AP1510 dispose d'une connexion câblée au contrôleur.



Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

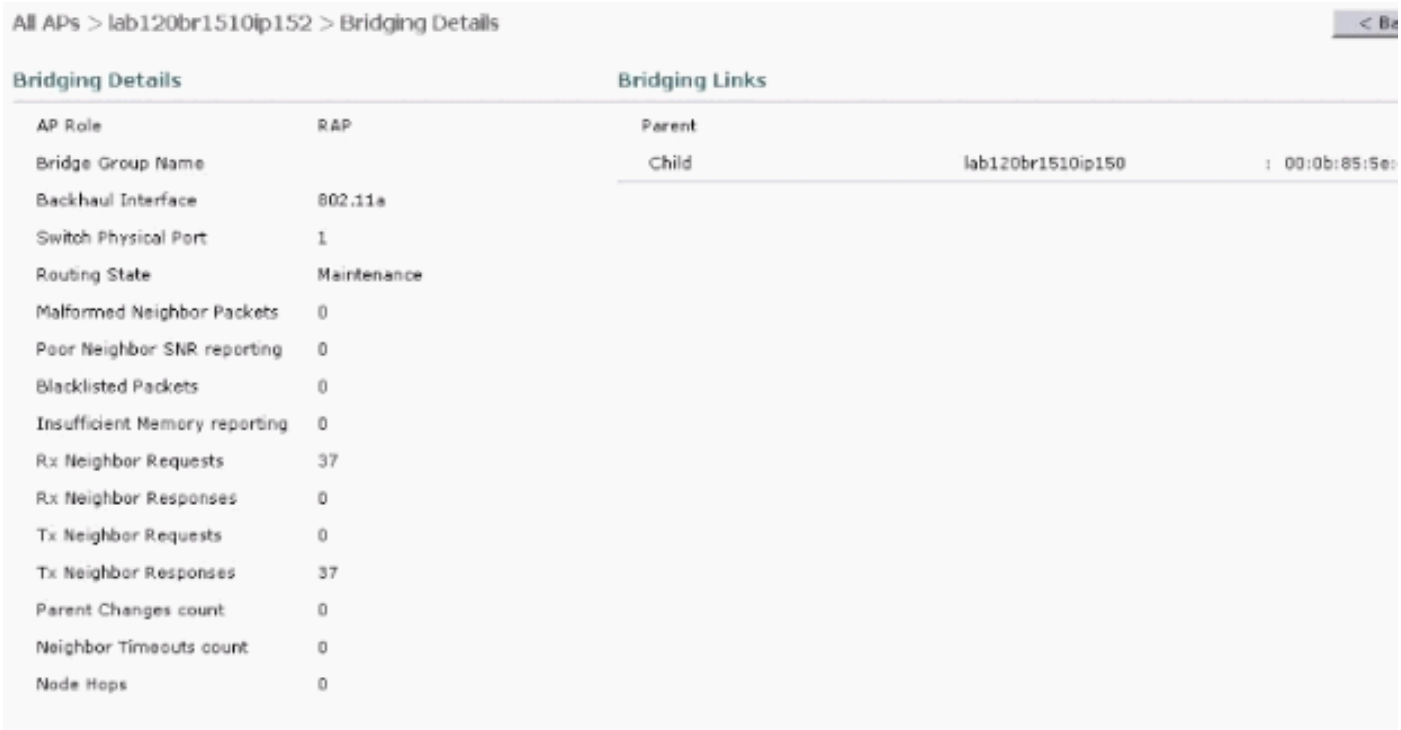
Après l'enregistrement des AP avec le WLC, vous pouvez les afficher sous l'onglet Wireless en haut de l'interface utilisateur graphique du WLC :



Sur la CLI, vous pouvez utiliser la commande **show ap summary** afin de vérifier que les AP enregistrés auprès du 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) >
```

Cliquez sur **Bridging Details** dans l'interface graphique afin de vérifier le rôle du point d'accès :



Sur la CLI, vous pouvez utiliser les commandes **show mesh path <Cisco AP>** et **show mesh neigh <Cisco AP>** afin de vérifier que les AP enregistrés auprès du 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) >
```

Dépannage

`Les points d'accès maillés ne s'associent pas au WLC` est l'un des problèmes les plus courants observés dans le déploiement maillé. Effectuez ces vérifications :

1. Vérifiez que l'adresse MAC du point d'accès est ajoutée dans la liste des filtres Mac du WLC. Ceci peut être vu sous **Sécurité > Filtrage Mac**.
2. Vérifiez le secret partagé entre le RAP et le MAP. Vous pouvez voir ce message dans le WLC lorsqu'il y a une non-correspondance dans la clé.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, point d'accès de clé PONT non valide 00:0b:85:68:c1:d0 »` **Remarque :** essayez toujours d'utiliser l'option **Activer la configuration automatique** si elle est disponible pour une version. Cela configure automatiquement la clé pour les AP maillés et évite les erreurs de configuration.
3. Les RAP ne transmettent aucun message de diffusion sur leur interface radio. Configurez donc le serveur DHCP pour envoyer des adresses IP par monodiffusion afin que MAP puisse faire transférer leurs adresses IP par RAP. Sinon, utilisez une adresse IP statique pour le MAP.
4. Laissez le nom du groupe de ponts aux valeurs par défaut ou assurez-vous que les noms des groupes de ponts sont configurés exactement de la même manière sur les MAP et le RAP correspondant.

Il s'agit de problèmes spécifiques aux points d'accès maillés. Pour les problèmes de connectivité courants entre le WLC et un point d'accès, référez-vous à Dépannage d'un point d'accès léger ne se connectant pas à un contrôleur de réseau local sans fil.

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Vous pouvez utiliser ces commandes de débogage pour dépanner le WLC :

- **debug pem state enable** —Utilisé pour configurer les options de débogage du gestionnaire de stratégies d'accès.
- **debug pem events enable** —Utilisé pour configurer les options de débogage du gestionnaire de stratégies d'accès.
- **debug dhcp message enable** - Affiche le débogage des messages DHCP échangés vers et depuis le serveur DHCP.
- **debug dhcp packet enable** - Affiche le débogage des détails des paquets DHCP envoyés au serveur DHCP et en provenance de celui-ci.

Les commandes **debug** supplémentaires que vous pouvez utiliser pour le dépannage sont les suivantes :

- **debug lwapp errors enable** - Affiche le débogage des erreurs LWAPP.
- **debug pm pki enable** - Affiche le débogage des messages de certificat qui sont passés entre l'AP et le WLC.

Cette sortie de commande **debug lwapp events enable** WLC montre que le LAP est inscrit au 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
```

Informations connexes

- Guide de déploiement de la solution de réseau maillé Cisco
- Guide de démarrage rapide : Points d'accès extérieur légers pour réseau maillé de la gamme Cisco Aironet 1500
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems