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.

Veuillez se référer à l'exemple Sans fil de configuration réseau de maille de contrôleur LAN pour des versions 5.2 et ultérieures pour des versions de version 5.2 et ultérieures WLC

Conditions préalables

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

- Le commutateur pour le 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

Composants utilisés

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

- Gamme Cisco 4402 WLC qui exécute des micrologiciels 3.2.150.6
- Deux (2) recouvrements de gamme 1510 de Cisco Aironet
- Cisco posent le commutateur 2

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Maille extérieure légère AP de gamme 1510 de Cisco Aironet

La maille extérieure légère AP de gamme 1510 de Cisco Aironet est un périphérique Sans fil conçu pour l'accès client Sans fil et la transition point par point, la transition point-à-multipoint, et la Connectivité point-à-multipoint de radio de maille. Le Point d'accès extérieur est une unité autonome qui peut être montée sur un mur ou un surplomb, sur un poteau de dessus de toit, ou sur un poteau de réverbère.

L'AP1510 fonctionne avec des contrôleurs pour fournir la Gestion centralisée et extensible, la sécurité élevée, et la mobilité. A conçu pour prendre en charge des déploiements de zéro-configuration, l'AP1510 facilement et joint sécurisé le réseau maillé et est disponible pour gérer et surveiller le réseau par le GUI ou le CLI de contrôleur.

L'AP1510 est équipé de deux radios simultanément de fonctionnement : un 2.4-GHz transmet par radio utilisé pour l'accès client et un 5-GHz transmet par radio utilisé pour la liaison de données à l'autre AP1510s. Le trafic Sans fil de client de RÉSEAU LOCAL traverse la radio de liaison d'AP ou est transmis par relais par l'autre AP1510s jusqu'à ce qu'il atteigne la connexion Ethernet de

contrôleur.

Point d'accès de dessus de toit (RAP)

Les coups secs et durs ont une connexion câblée à un Cisco WLC. Ils emploient l'interface Sans fil de liaison pour communiquer avec les mamelons voisins. Les coups secs et durs sont le noeud de parent à toute transition ou réseau maillé et connectent une passerelle 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: Quand vous utilisez la solution réseau de maille pour l'entre réseaux locaux jetant un pont sur, ne connectez pas un RAP directement à un Cisco WLC. Un commutateur ou un routeur entre le Cisco WLC et le RAP est exigé parce que les Cisco WLC n'expédient pas le trafic Ethernet qui provient un port LWAPP-activé. Les coups secs et durs peuvent fonctionner en mode de la couche 2 ou de la couche 3 LWAPP.

Point d'accès au dessus du polonais (PAP)

Les mamelons n'ont aucune connexion câblée à un Cisco WLC. Ils peuvent être complètement Sans fil, et prennent en charge les clients qui communiquent avec d'autres mamelons ou coups secs et durs, ou ils peuvent être utilisés pour se connecter aux dispositifs 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: Cisco Aironet 1030 recouvrements à distance de périphérie prennent en charge des déploiements de simple-saut tandis que le Gamme Cisco Aironet 1500 aps extérieurs légers prend en charge des déploiements simples et de multi-alimentation. En soi, le Gamme Cisco Aironet 1500 aps extérieurs légers peut être utilisé comme dessus de toit aps et comme mamelons pour un ou plusieurs sauts du Cisco WLC.

Caractéristiques non prises en charge sur des 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

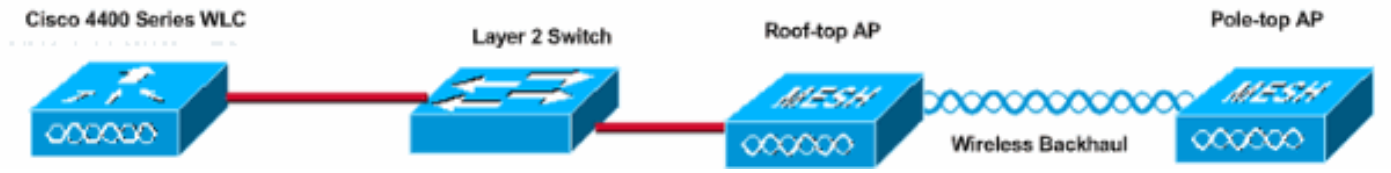
Séquence de démarrage de Point d'accès

Cette liste décrit ce qui se produit quand le RAP et le PAP démarrent :

- Tout le trafic voyage par le RAP et le Cisco WLC avant qu'il soit envoyé au RÉSEAU LOCAL.
- Quand le RAP monte, les mamelons se connectent automatiquement à lui.
- Le lien connecté emploie un secret partagé pour générer une clé qui est utilisée pour fournir le

Norme AES (Advanced Encryption Standard) pour le lien.

- Une fois que le distant PAP se connecte au RAP, la maille aps peut passer le trafic de données.
- Les utilisateurs peuvent changer le secret partagé ou configurer la maille aps utilisant l'interface de ligne de commande Cisco (CLI), l'interface utilisateur d'utilisateur web de Cisco du contrôleur, ou le Système de contrôle sans fil Cisco (Cisco WCS). Cisco recommande que vous modifiiez le secret partagé.



Configurez

Terminez-vous ces étapes afin de configurer le WLC et les aps pour la transition point par point.

1. Enable zéro configurations de toucher sur le WLC.
2. Ajoutez la MIC à la liste d'autorisation AP.
3. Configure jetant un pont sur des paramètres pour les aps.
4. Vérifier la configuration

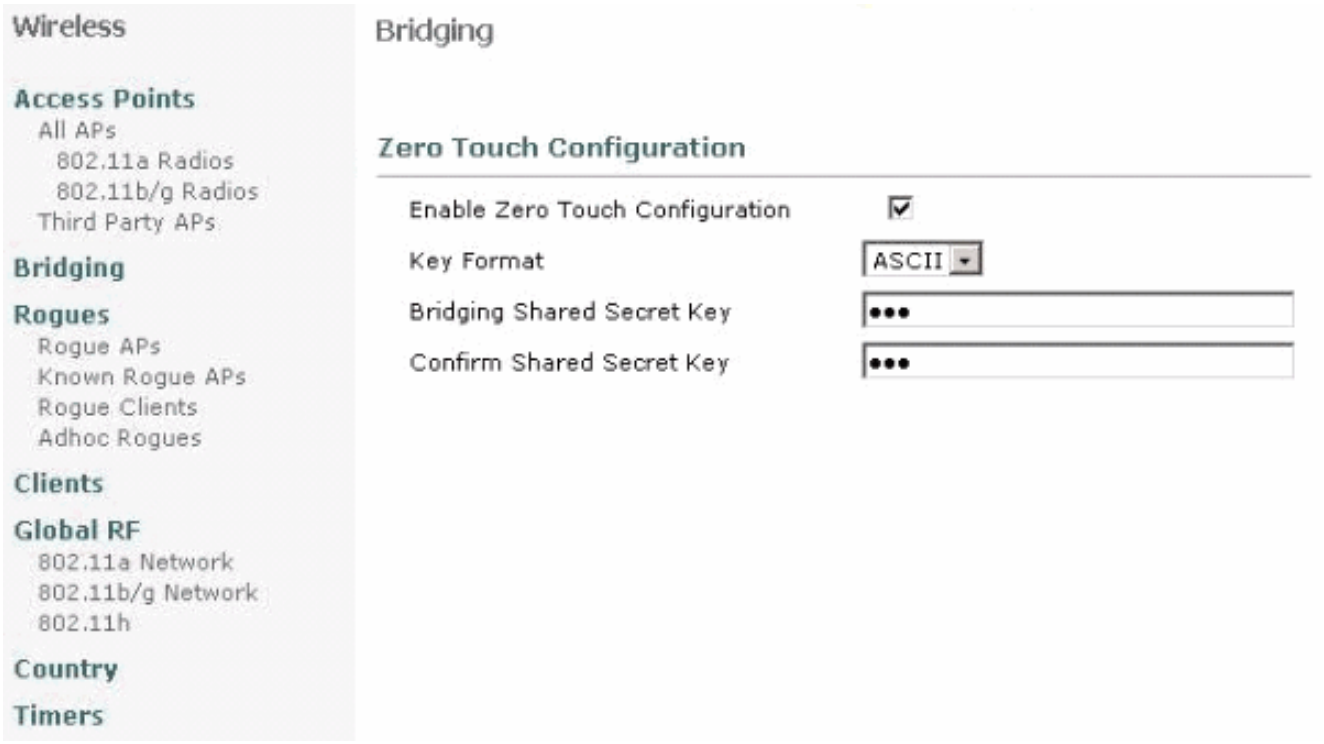
Enable zéro configurations de toucher (activées par défaut)

Configuration de la GUI

Activez la configuration zéro de toucher permet aux aps d'obtenir la clé secrète partagée du contrôleur quand elle s'inscrit au WLC. Si vous décochez la cette case, le contrôleur ne fournit pas la clé secrète partagée, et les aps utilisent une clé pré-partagée par défaut pour la communication protégée. La valeur par défaut est activée (ou coché). Terminez-vous ces étapes du GUI WLC :

Remarque: Il n'y a aucune disposition pour la configuration de Zéro-toucher dans la version 4.1 et ultérieures WLC.

1. Choisissez la **radio > en jetant un pont sur** et cliquez sur la **configuration zéro de toucher d'enable**.
2. Sélectionnez le format principal.
3. Introduisez la clé secrète partagée traversière.
4. Introduisez la clé secrète partagée traversière de nouveau dans la clé secrète partagée par confirmer.



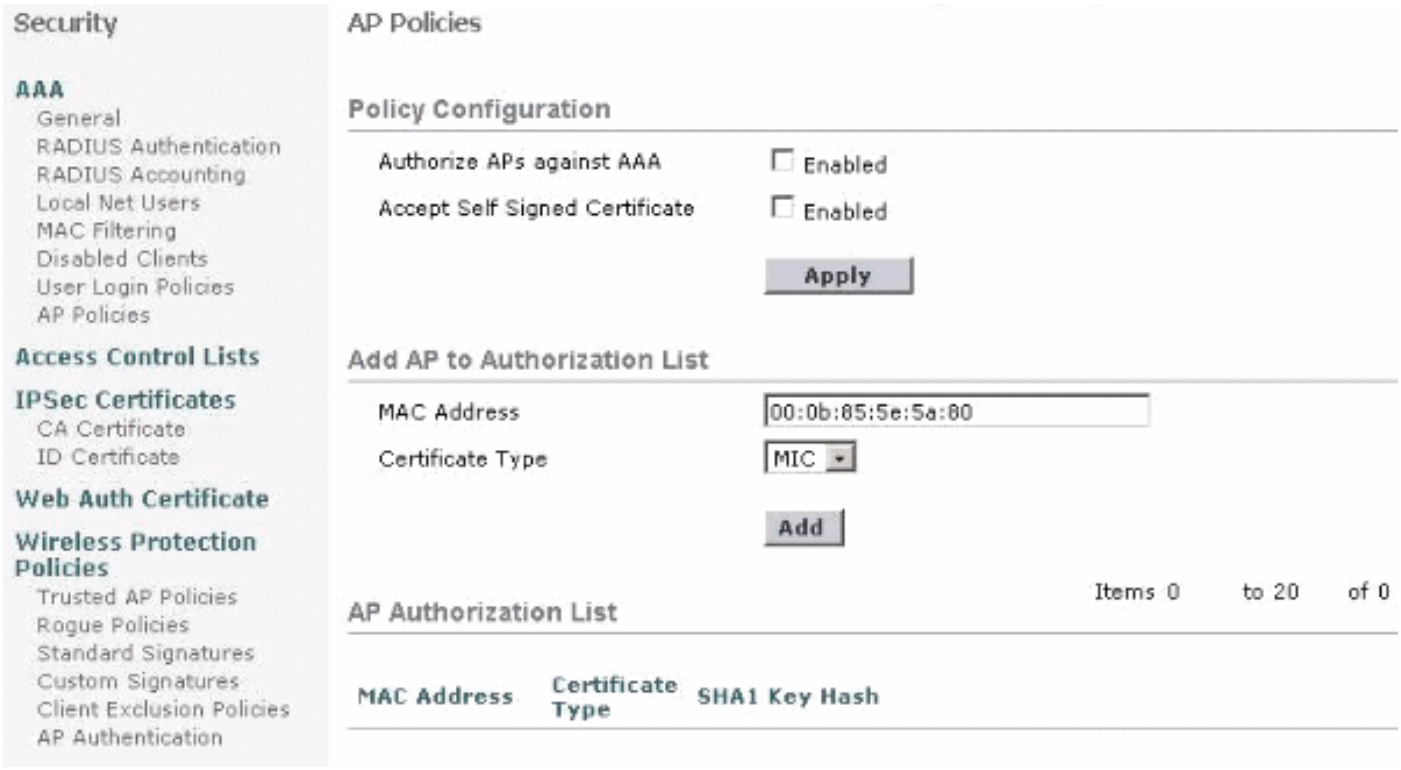
Configuration CLI

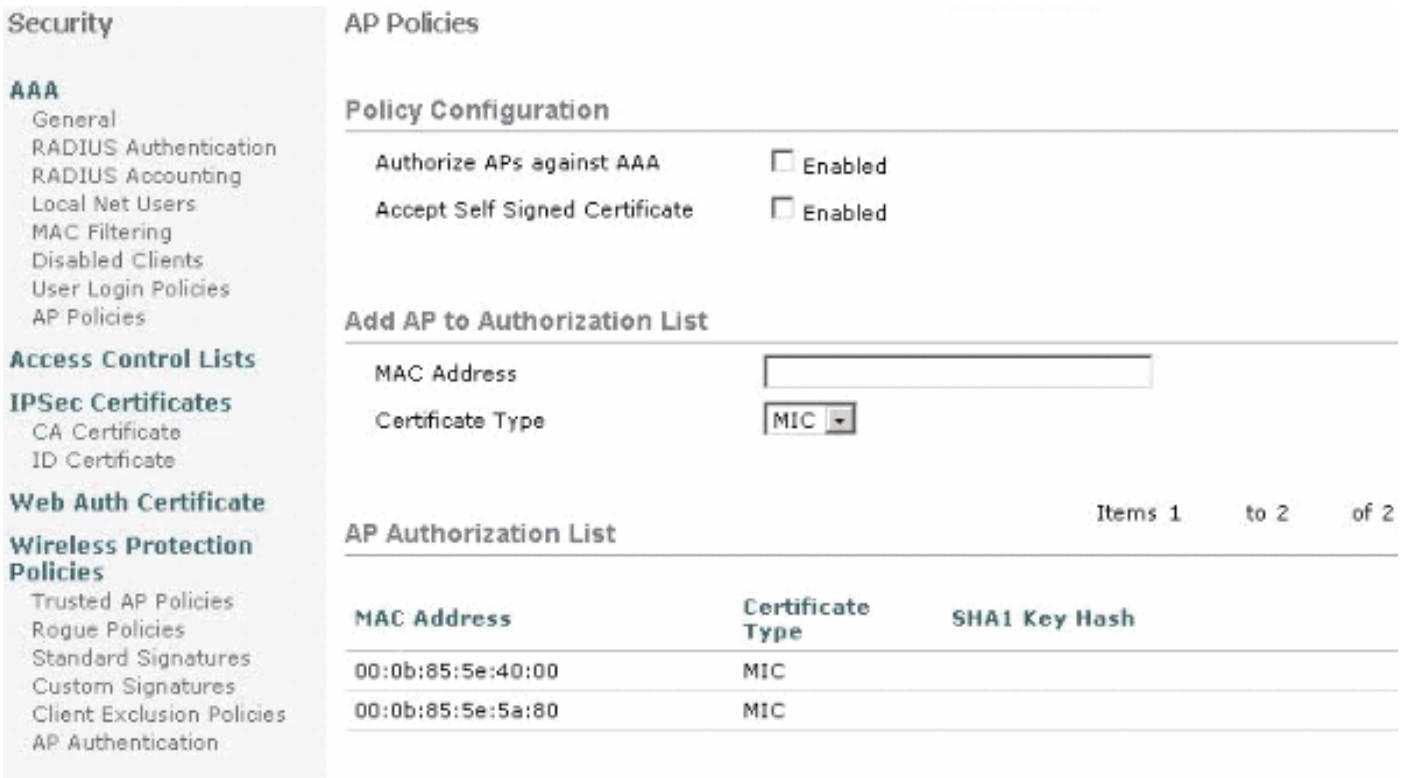
Terminez-vous ces étapes du CLI :

1. Émettez la commande d'**enable de config network zero-config** afin d'activer la configuration zéro de toucher.`(Cisco Controller) >`**`config network zero-config enable`**
2. Émettez la commande de **<string> de config network bridging-shared-secret** afin d'ajouter la clé secrète partagée traversière.`(Cisco Controller) >`**`config network bridging-shared-secret Cisco`**

Ajoutez la MIC à la liste d'autorisation AP

L'étape suivante est d'ajouter AP à la liste d'autorisation sur le WLC. Afin de faire ceci, choisissez le **Security > AP Policies**, écrivez l'adresse MAC AP dessous ajoutent AP à la liste d'autorisation et cliquent sur Add.





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

Configuration CLI

Émettez la commande de **mac> du config auth-list add MIC <AP** afin d'ajouter la 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
```

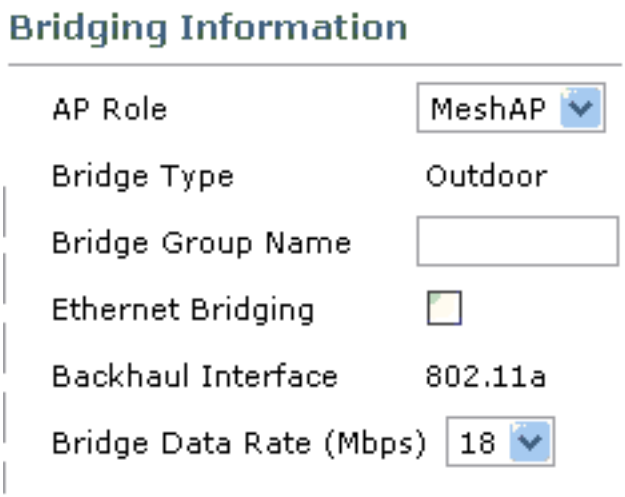
Configurez jeter un pont sur des paramètres pour les aps

Cette section fournit des instructions sur la façon dont configurer le rôle d'AP dans le réseau maillé et associé jetant un pont sur des paramètres. Vous pouvez configurer ces paramètres utilisant le GUI ou le CLI.

1. Cliquez sur la **radio** et puis **tous les aps aux** Points d'accès. La toute la page aps paraît.
2. Cliquez sur le lien de **détail** pour votre AP1510 afin d'accéder à la page d'All APs > Details

Àcette page, le mode AP sous le général est automatiquement placé pour jeter un pont sur pour les aps qui ont la fonctionnalité de passerelle, telle que l'AP1510. Cette page affiche également ces informations sous jeter un pont sur les informations. Sous jeter un pont sur les informations, choisissez une de ces options afin de spécifier le rôle de cet AP dans le réseau maillé :

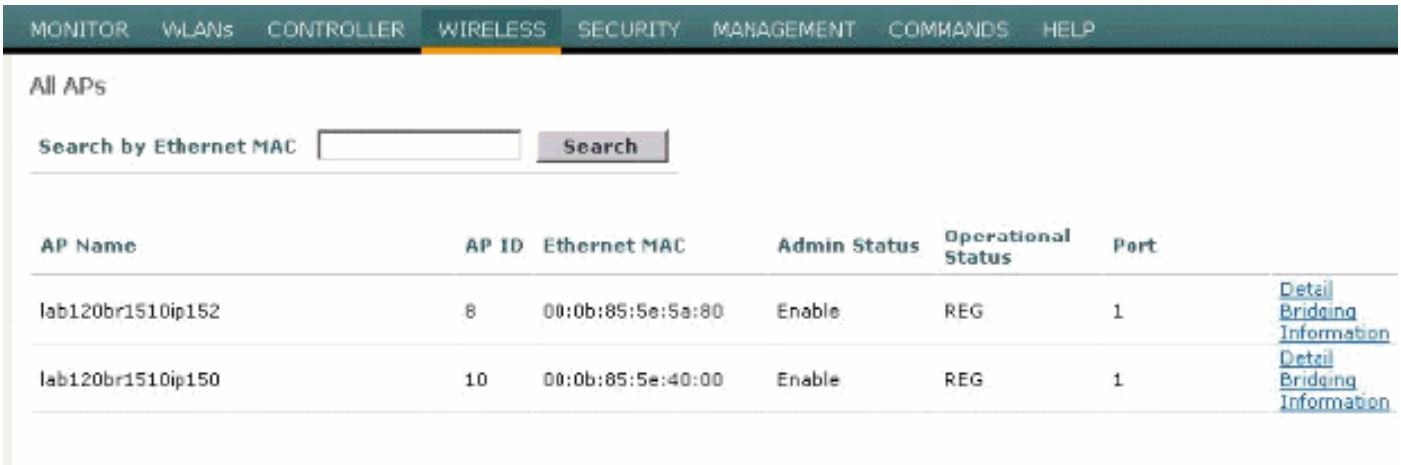
- **MeshAP** — Choisissez cette option si l'AP1510 a une connexion Sans fil au contrôleur.
- **RootAP** — Choisissez cette option si l'AP1510 a une connexion câblée au contrôleur.



Vérifiez

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

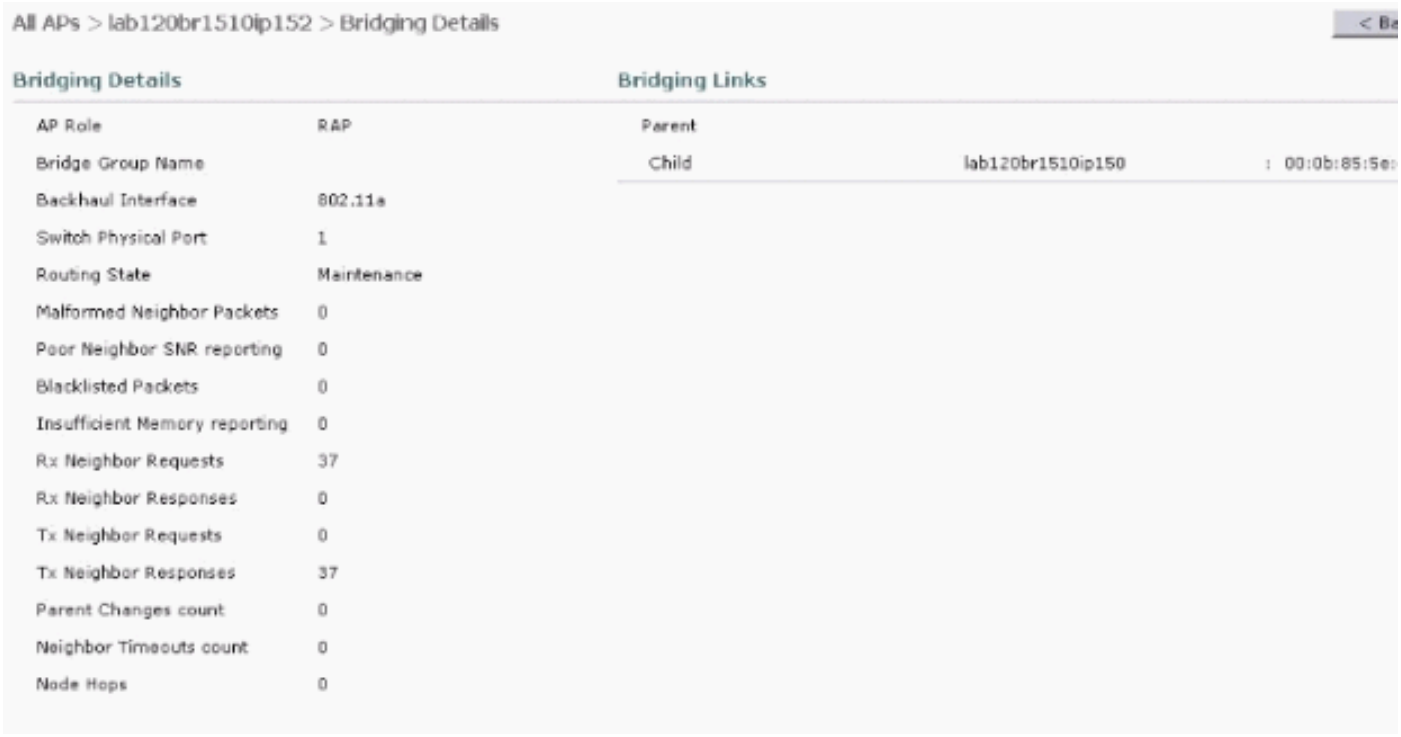
Après que les aps s'inscrivent au WLC, vous pouvez les visualiser sous l'onglet sans fil en haut du GUI du WLC :



Sur le CLI, vous pouvez employer la commande de **show ap summary** afin de vérifier que les aps se sont inscrits au 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 **en jetant un pont sur des détails** dans le GUI afin de vérifier le rôle d'AP :



Sur le CLI, vous pouvez employer le **<Cisco AP> de show mesh path** et des commandes du **<Cisco AP> de show mesh neigh** afin de vérifier que les aps se sont inscrits au 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) >
```

Dépannez

`La maille aps ne s'associe pas au WLC` est l'un des la plupart des problèmes courants vus dans le déploiement de maille. Terminez-vous ces contrôles :

1. Vérifiez que l'adresse MAC du Point d'accès est ajoutée dans la liste de filtre de MAC dans le WLC. Ceci peut être vu sous la **Sécurité > le filtrage de MAC**.
2. Vérifiez le secret partagé entre le RAP et la MAP. Vous pouvez voir ce message dans le WLC quand il y a une non-concordance dans la clé.`« Demande de jonction AUTH_STRING_PAYLOAD LWAPP, informations parasites non valides AP 00:0b:85:68:c1:d0" de clé de PASSERELLE` **Remarque:** Toujours essai pour utiliser l'**enable** option de **configuration nulle de toucher** si disponible pour une version. Ceci configure automatiquement la clé pour la maille aps et évite des mauvaises configurations.
3. Les coups secs et durs n'expédient aucun message de diffusion sur leur interface par radio. Configurez ainsi le serveur DHCP pour envoyer des adresses IP par l'unicast de sorte que la MAP puisse obtenir leurs adresses IP expédiées par RAP. Autrement utilisez un IP statique pour la MAP.
4. Laissez le nom de groupe de passerelle aux valeurs par défaut ou assurez-vous que des noms de groupe de passerelle sont configurés exactement les mêmes sur des cartes et le RAP correspondant.

Ce sont des questions qui sont spécifiques pour engrener des Points d'accès. Pour les problèmes de connectivité qui sont communs entre le WLC et un Point d'accès, référez-vous dépannent un

point d'accès léger ne joignant pas un contrôleur LAN Sans fil.

Dépannage des commandes

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

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

- enable d'état de debug pem — Utilisé pour configurer le gestionnaire de stratégie d'accès mettez au point les options.
- enable d'événements de debug pem — Utilisé pour configurer le gestionnaire de stratégie d'accès mettez au point les options.
- enable de message de debug dhcp — Affiche le débogage des messages DHCP qui sont permutés à et du serveur DHCP.
- enable de paquet de debug dhcp — Affiche le débogage des détails de paquet DHCP qui sont envoyés à et du serveur DHCP.

Quelques commandes de **débogage** supplémentaires que vous pouvez employer pour dépanner sont :

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

Cette sortie de commande de l'**enable** WLC d'**événements de debug lwapp** prouve que le RECOUVREMENT obtient enregistré 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

- Cisco engrènent le guide de déploiement de solution réseau
- Guide de démarrage rapide : Points d'accès extérieurs légers de maille de 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