Exemple de configuration de l'autorisation des points d'accès légers (LAP) dans un réseau sans fil unifié Cisco

Contenu

Introduction

Ce document explique comment configurer les contrôleurs de réseau local sans fil pour autoriser les points d'accès allégés en fonction de leur adresse MAC.

Conditions préalables

Conditions requises

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

- Connaissance de base de la façon configurer un Cisco Secure Access Control Server (ACS) pour authentifier des clients sans fil
- La connaissance de la configuration des recouvrements et des Cisco WLC de Cisco Aironet
- La connaissance des solutions de sécurité de Cisco Unified Wireless

Composants utilisés

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

- Gamme Cisco 4400 WLC qui exécute la version 5.0.148.0

- Recouvrements de Gamme Cisco Aironet 1000
- Recouvrements de Gamme Cisco Aironet 1200
- Version 4.2 de serveur de Cisco Secure ACS

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.

Autorisation de point d'accès léger (LAP)

Pendant la procédure d'enregistrement de RECOUVREMENT, les recouvrements et le WLCs authentifient mutuellement utilisant les Certificats X.509.

Les Certificats X.509 sont gravés dans l'éclair protégé sur le Point d'accès (AP) et WLC à l'usine par Cisco. Sur AP, des Certificats d'origine s'appellent la fabrication les Certificats installés (MIC). Tout le Cisco aps a fabriqué après juillet 18, 2005 ont MICs.

Les aps de Cisco Aironet 1200, 1130, et 1240 ont fabriqué avant juillet 18, 2005, qui ont été mis à jour de l'IOS autonome à l'IOS de Protocol de point d'accès léger (LWAPP), génèrent un certificat auto-signé (SSC) pendant le processus de mise à niveau. Pour les informations sur la façon dont gérer des aps avec SSCs, référez-vous à améliorer les Points d'accès autonomes de Cisco Aironet au mode léger.

En plus de cette authentification mutuelle qui se produit pendant la procédure d'enregistrement, le WLCs peut également limiter les recouvrements qui s'inscrivent à eux ont basé sur l'adresse MAC du RECOUVREMENT.

Le manque d'un mot de passe fort en employant l'adresse MAC du RECOUVREMENT ne devrait pas être une question parce que le contrôleur emploie la MIC pour authentifier AP avant d'autoriser AP par le serveur de RAYON. L'utilisation de la MIC fournit l'authentification poussée.

L'autorisation de RECOUVREMENT peut être exécutée de deux manières :

- Utilisant la liste interne d'autorisation sur le WLC
- Utilisant la base de données d'adresse MAC sur un serveur d'AAA

Les comportements des recouvrements diffèrent basé sur le certificat utilisé :

- Enroule avec SSCs — Le WLC utilisera seulement la liste interne d'autorisation et ne fera pas suivre à une demande un serveur de RAYON pour ces recouvrements.
- Enroule avec MICs — WLC peut utiliser la liste interne d'autorisation configurée sur le WLC ou utiliser un serveur de RAYON pour autoriser les recouvrements

Ce document discute l'autorisation de RECOUVREMENT utilisant chacun des deux la liste interne d'autorisation et le serveur d'AAA.

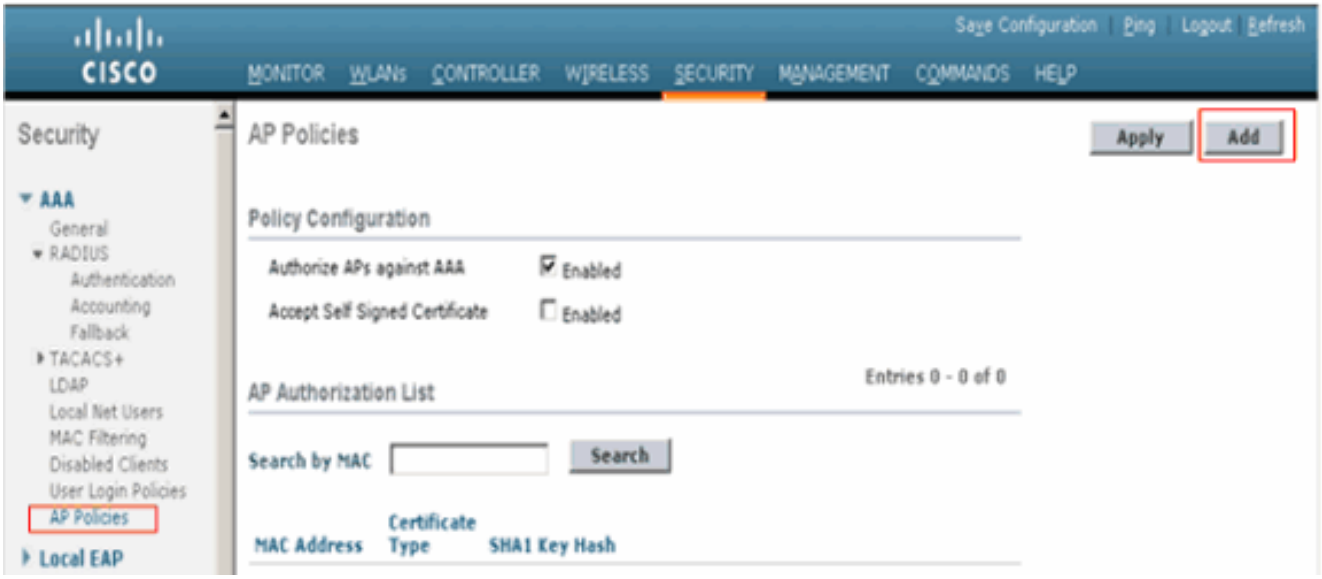
Utilisant la liste interne d'autorisation sur le WLC

Sur le WLC, employez la liste d'autorisation AP pour limiter des recouvrements basés sur leur adresse MAC. La liste d'autorisation AP est disponible sous le **Security > AP Policies** dans le GUI WLC.

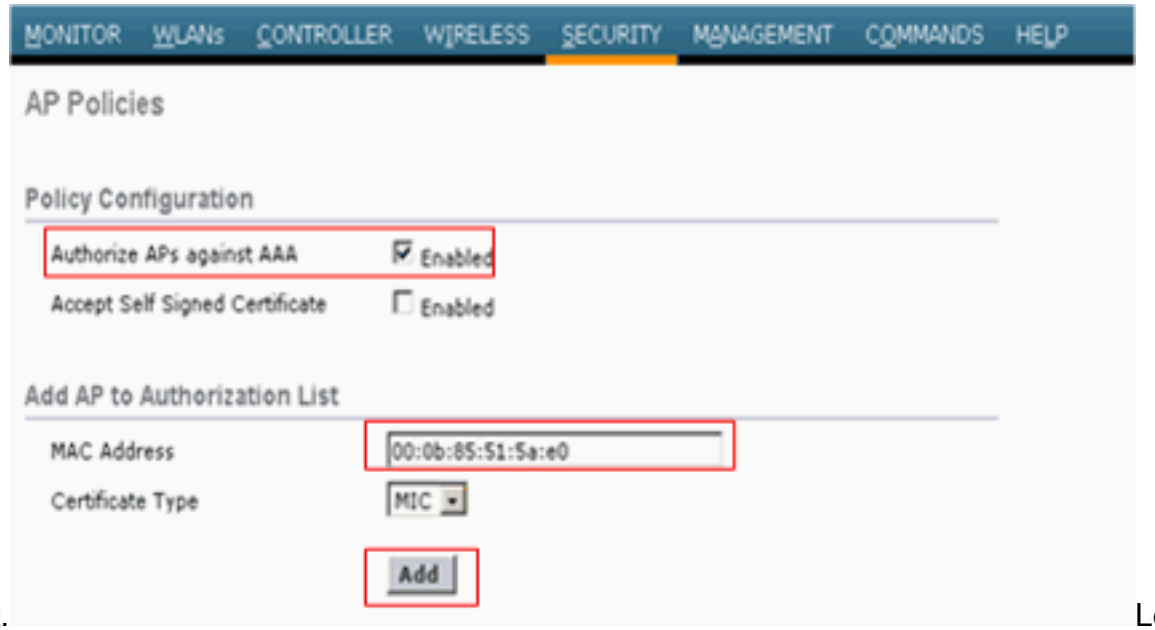
Cet exemple affiche comment ajouter le RECOUVREMENT avec l'adresse MAC **00:0b:85:5b:fb:d0**.

Procédez comme suit :

1. Du GUI de contrôleur WLC, cliquez sur Security **> des stratégies AP**.La page de stratégies AP paraît.
2. Sous la configuration de politique, cochez la case pour **Authorize aps contre l'AAA**.Quand ce paramètre est sélectionné, le WLC vérifie la liste locale d'autorisation d'abord. Si le MAC du RECOUVREMENT n'est pas présent, il vérifie le serveur de RAYON.
3. Cliquez sur le bouton d'**ajouter du** côté droit de l'écran.



4. Sous ajoutez AP à la liste d'autorisation, écrivent l'adresse MAC AP. Puis, choisissez le type de certificat et cliquez sur Add.Dans cet exemple, un RECOUVREMENT avec le certificat MIC est ajouté.**Remarque:** Pour des recouvrements avec SSCs, choisissez **SSC** sous le type de



certificat. Le RECOUVREMENT est ajouté à la liste d'autorisation AP et est répertorié sous la **liste d'autorisation**

AP.

Vérifiez

Afin de vérifier cette configuration, vous devez connecter le RECOUVREMENT à l'adresse MAC 00:0b:85:51:5a:e0 au réseau et au moniteur. Utilisez l'**enable** et le **debug aaa d'événements de debug lwapp toutes les** commandes d'**enable** d'exécuter ceci.

Cette sortie affiche que met au point quand l'adresse MAC de RECOUVREMENT n'est pas présente dans la liste d'autorisation AP :

Remarque: Certaines des lignes dans la sortie ont été déplacées à la deuxième ligne due aux contraintes de l'espace.

```
debug lwapp events enable Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:39 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12
17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12
17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0 debug
aaa all enable Wed Sep 12 17:56:26 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:26 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:26 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:26 2007:
```

```
proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:26 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0 Wed Sep 12 17:56:26 2007: AuthorizationResponse:
0xbadff7d4 Wed Sep 12 17:56:26 2007: structureSize...................28 Wed Sep 12 17:56:26
2007: resultCode.....................-7 Wed Sep 12 17:56:26 2007:
protocolUsed.....................0xffffffff Wed Sep 12 17:56:26 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 0 AVPs: Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:31 2007:
Callback.....................0x8108e2c Wed Sep 12 17:56:31 2007:
protocolType.....................0x00000001 Wed Sep 12 17:56:31 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:31 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0
```

Cette exposition de sortie met au point quand l'adresse MAC du RECOUVREMENT est ajoutée à la liste d'autorisation AP :

Remarque: Certaines des lignes dans la sortie ont été déplacées à la deuxième ligne due aux contraintes de l'espace.

```
debug lwapp events enable Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:43:59 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12
17:44:10 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12
17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index
58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP
Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0
Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed Sep 12 17:44:10 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 debug aaa all enable Wed
Sep 12 17:57:44 2007: User 000b85515ae0 authenticated Wed Sep 12 17:57:44 2007:
00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0) for mobile 00:0b:85:51:5a:e0 Wed Sep 12
17:57:44 2007: AuthorizationResponse: 0xbadff96c Wed Sep 12 17:57:44 2007:
structureSize...................70 Wed Sep 12 17:57:44 2007: resultCode.....................0
Wed Sep 12 17:57:44 2007: protocolUsed.....................0x00000008 Wed Sep 12 17:57:44 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:57:44 2007: Packet
contains 2 AVPs: Wed Sep 12 17:57:44 2007: AVP[01] Service-Type.............................
0x00000065 (101) (4 bytes) Wed Sep 12 17:57:44 2007: AVP[02] Airespace / WLAN-
Identifier.............. 0x00000000 (0) (4 bytes)
```

Autorisation AP contre un serveur d'AAA

Vous pouvez également configurer WLCs pour utiliser des serveurs de RAYON pour autoriser des aps utilisant MICs. Le WLC utilise l'adresse MAC d'un RECOUVREMENT en tant que chacun des deux le nom d'utilisateur et mot de passe en envoyant les informations à un serveur de RAYON. Par exemple, si l'adresse MAC d'AP est 000b85229a70, chacun des deux le nom d'utilisateur et mot de passe utilisé par le contrôleur pour autoriser AP sont 000b85229a70.

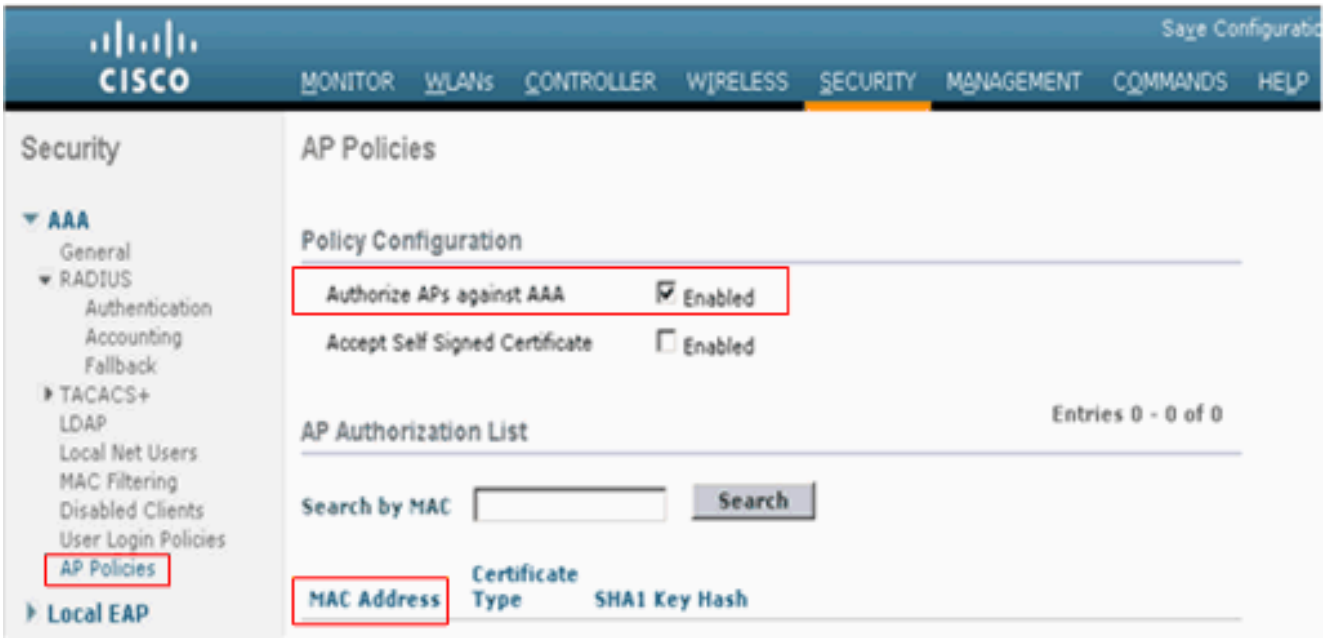
Remarque: Si vous utilisez l'adresse MAC comme nom d'utilisateur et mot de passe pour l'authentification AP sur un serveur d'AAA de RAYON, n'utilisez pas le même serveur d'AAA pour l'authentification client. La raison pour ceci est si les pirates informatiques découvrent l'adresse MAC AP, alors ils peuvent utiliser ce MAC comme qualifications de nom d'utilisateur et mot de

passe pour obtenir sur le réseau.

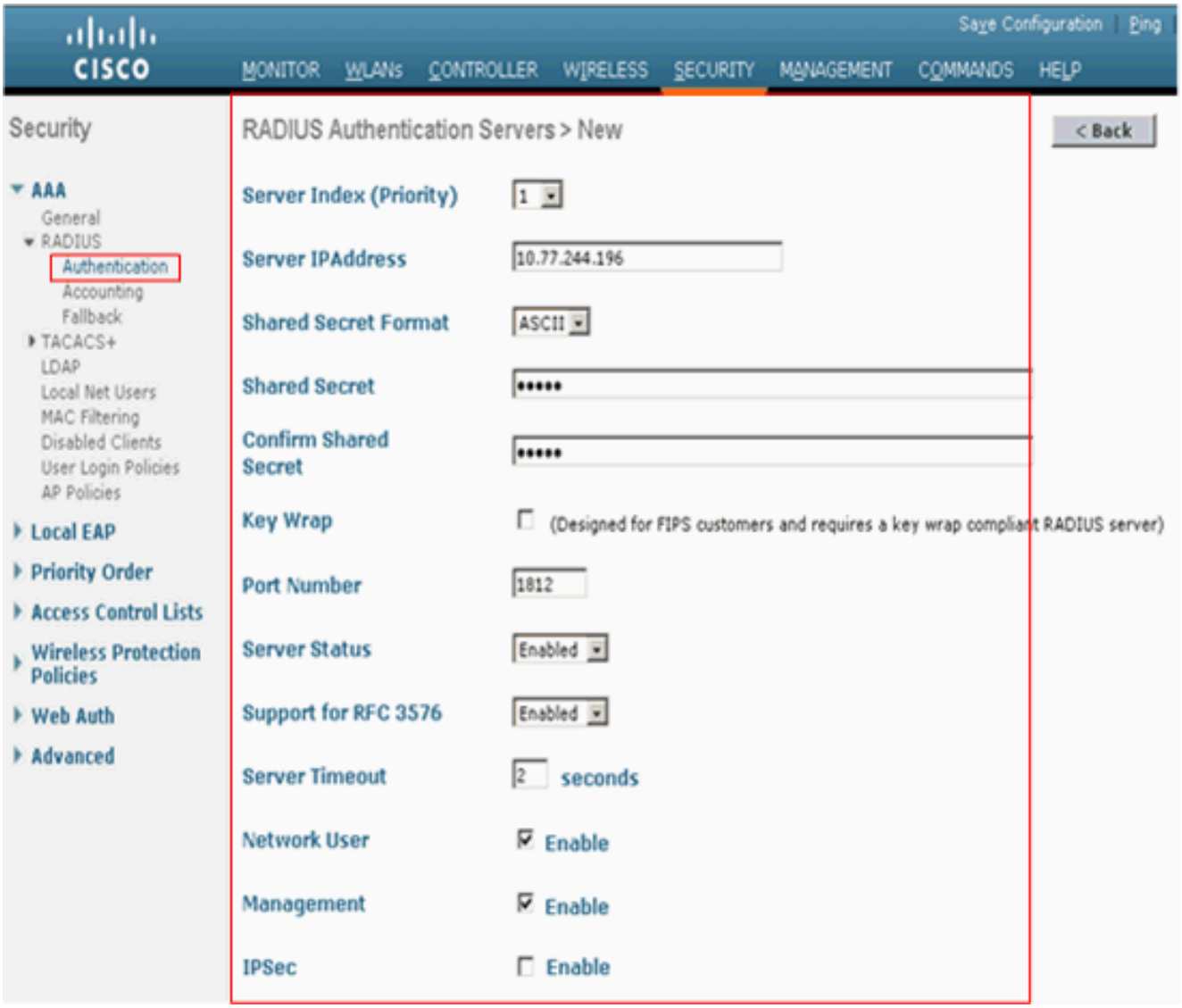
Cet exemple affiche comment configurer le WLCs pour autoriser des recouvrements utilisant le Cisco Secure ACS.

Terminez-vous ces étapes sur le WLC :

1. Du GUI de contrôleur WLC, cliquez sur Security **> des stratégies AP**.La page de stratégies AP paraît.
2. Sous la configuration de politique, cochez la case pour **Authorize aps contre l'AAA**.Quand ce paramètre est sélectionné, le WLC vérifie la base de données locale de MAC d'abord. Pour cette raison, assurez-vous que la base de données locale est vide en effaçant les adresses MAC sous la liste d'autorisation AP. Si l'adresse MAC de RECOUVREMENT n'est pas présente, elle vérifie alors le serveur de
RAYON.



3. Cliquez sur Security et **authentification de RAYON du** GUI de contrôleur pour afficher la page de serveurs d'authentification RADIUS. Puis, cliquez sur New afin de définir un serveur de RAYON.



4. Définissez les paramètres de serveur de RAYON sur le **RADIUS Authentication Servers > New page**. Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur.Cet exemple utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 10.77.244.196.
5. Cliquez sur **Apply**.

Configurez le Cisco Secure ACS pour autoriser des recouvrements

Afin de permettre au Cisco Secure ACS d'autoriser des recouvrements, vous devez se terminer ces étapes :

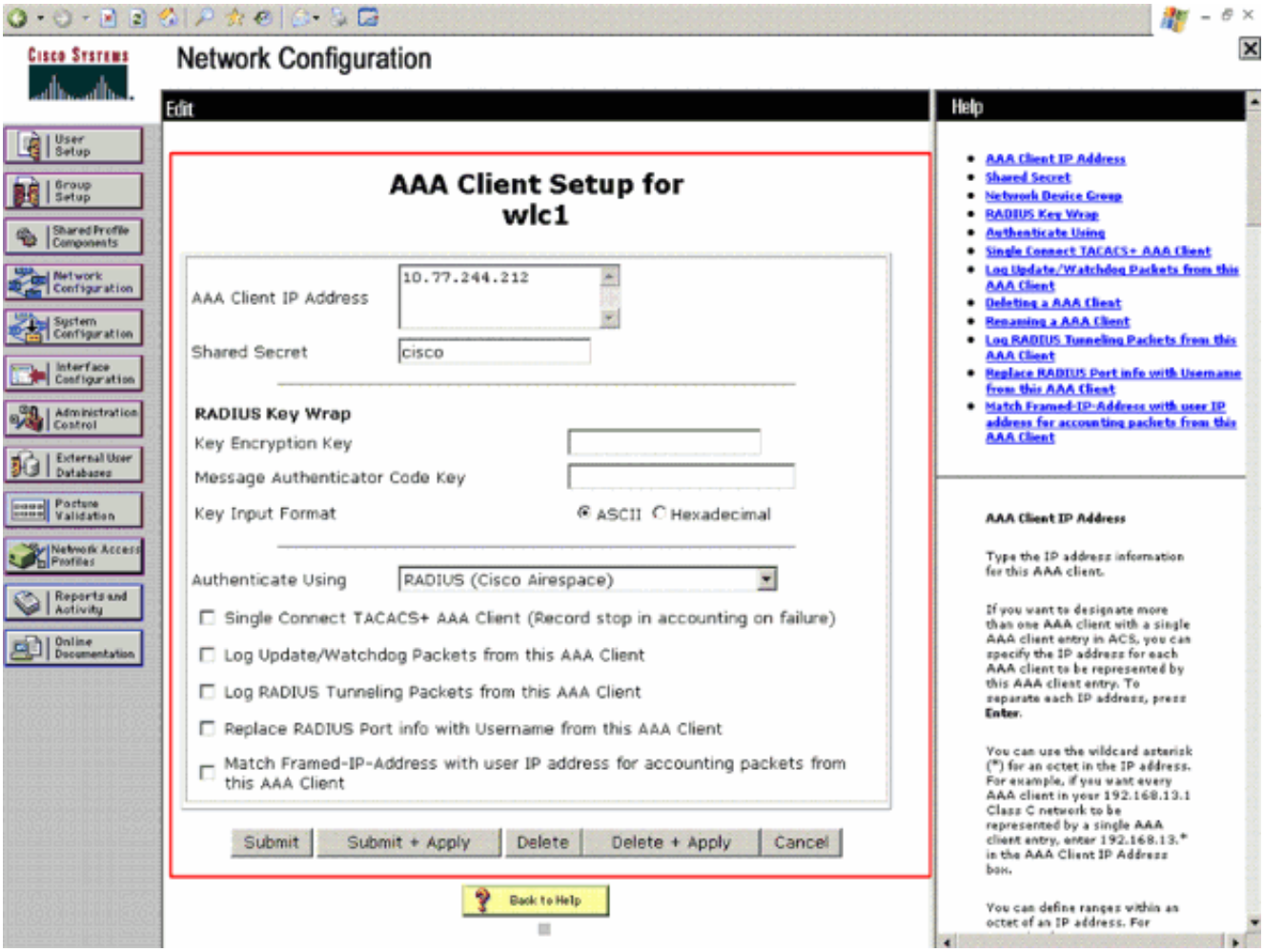
1. Configurez le WLC en tant que client d'AAA sur le Cisco Secure ACS
2. Ajoutez les adresses MAC de RECOUVREMENT à la base de données utilisateur sur le Cisco Secure ACS

Configurez le WLC en tant que client d'AAA sur le Cisco Secure ACS

Terminez-vous ces étapes afin de configurer le WLC en tant que client d'AAA sur le Cisco Secure ACS :

1. Cliquez sur Network Configuration **> ajoutez le client d'AAA**.La page de client d'AAA d'ajouter paraît.

2. Àcette page, définissez le nom de système WLC, adresse IP d'interface de gestion, secret partagé, et l'authentifiez utilisant le RAYON Airespace.**Remarque:** Alternativement, vous pouvez essayer l'option d'authentifier utilisant l'Aironet de RAYON.Voici un exemple :

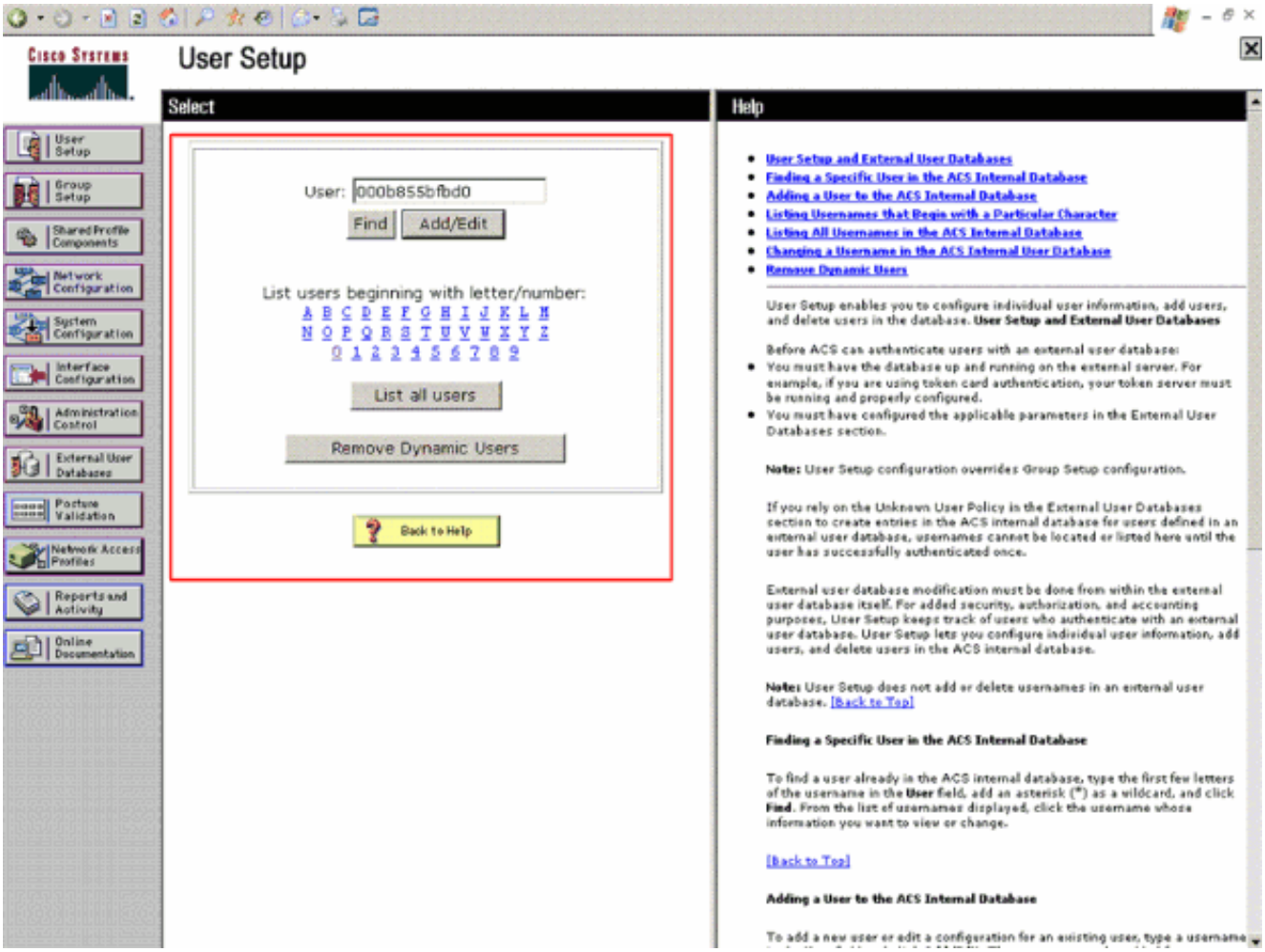


3. Cliquez sur Submit **+ appliquez**.

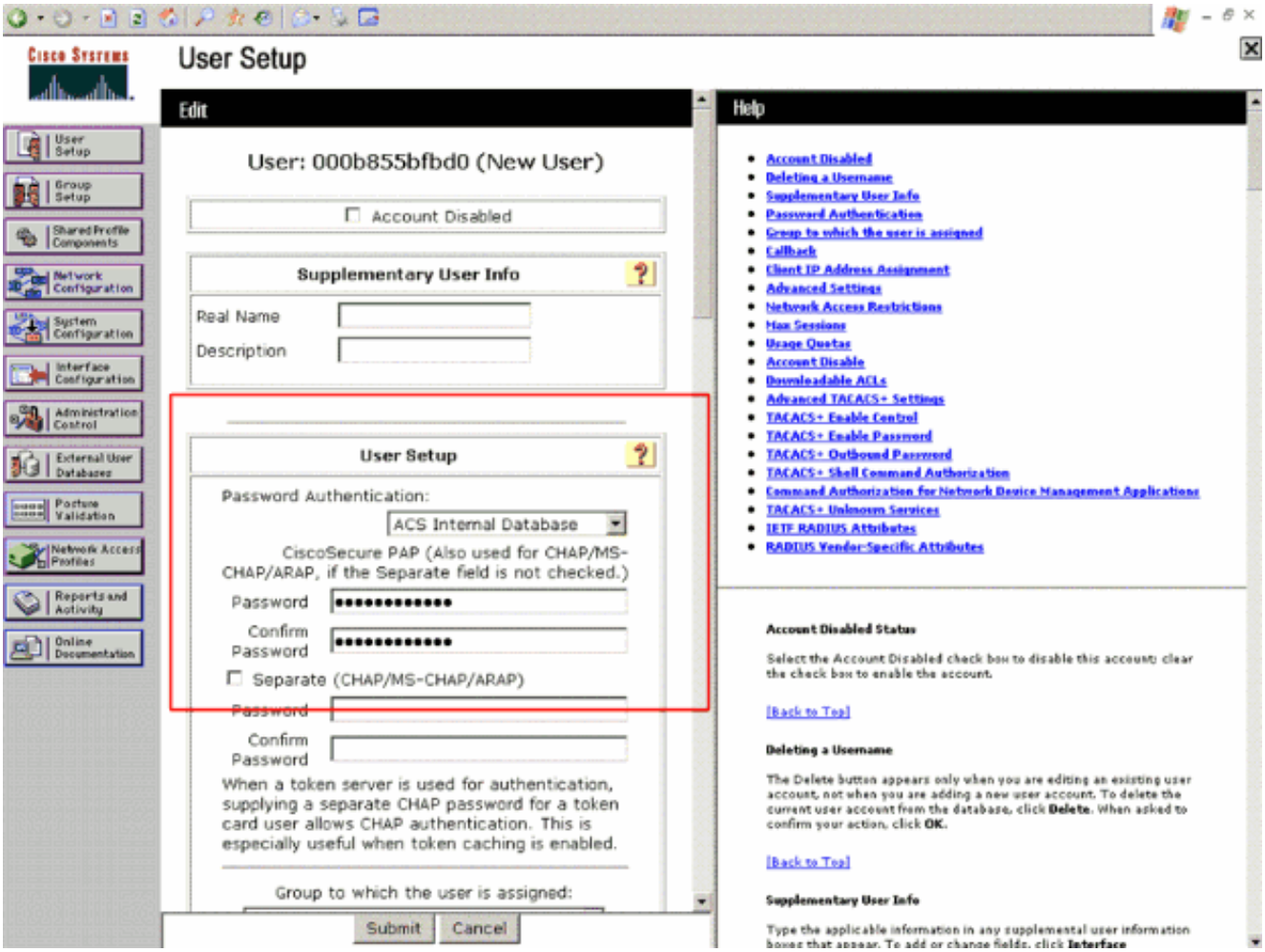
Ajoutez les adresses MAC de RECOUVREMENT à la base de données utilisateur sur le Cisco Secure ACS

Terminez-vous ces étapes afin d'ajouter les adresses MAC de RECOUVREMENT au Cisco Secure ACS :

1. Choisissez **User Setup** depuis l'interface graphique ACS, entrez le nom d'utilisateur et cliquez sur **Add/Edit**.Le nom d'utilisateur devrait être l'adresse MAC du RECOUVREMENT que vous voulez autoriser. L'adresse MAC ne doit pas contenir des deux points ou des traits d'union.Dans cet exemple, le RECOUVREMENT est ajouté avec l'adresse MAC **000b855bfbd0** :



2. Quand la page d'installation utilisateur paraît, définissez le mot de passe pour ce RECOUVREMENT dans le domaine de mot de passe comme affiché.Le mot de passe devrait également être l'adresse MAC du RECOUVREMENT. Dans cet exemple, c'est **000b855bfbd0**.



3. Cliquez sur **Submit**.
4. Répétez cette procédure pour ajouter plus de recouvrements à la base de données de Cisco Secure ACS.

Vérifiez

Afin de vérifier cette configuration, vous devez connecter le RECOUVREMENT à l'adresse MAC 00:0b:85:51:5a:e0 au réseau et au moniteur. Employez l'**enable** et le **debug aaa d'événements de debug lwapp toutes les** commandes d'**enable** afin d'exécuter ceci.

Comme vu du met au point, le WLC passé sur l'adresse MAC de RECOUVREMENT au serveur 10.77.244.196 de RAYON, et le serveur a avec succès authentifié le RECOUVREMENT. Le LAP s'enregistre alors auprès du contrôleur.

Remarque: Certaines des lignes dans la sortie ont été déplacées à la deuxième ligne due aux contraintes de l'espace.

```
debug aaa all enable Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778 Thu Sep 13
13:54:39 2007: Callback.....................0x8108e2c Thu Sep 13 13:54:39 2007:
protocolType.....................0x00000001 Thu Sep 13 13:54:39 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:39 2007: Packet
contains 8 AVPs (not shown) Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission
of Authentication Packet (id 123) to 10.77.244.196:1812, proxy state 00:0b:85:51:5a:e0-85:51 Thu
Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00 .{.r............
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
......000b85515a Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33
33 2d e0..00-0b-85-33- Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62
```

```
2d 38 35 2d 52-80..00-0b-85- Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06
00 00 00 01 04 06 51-5a-e0..... Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c
63 31 02 12 03 04 0e 12 .M....wlc1..... Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40
2a be 9d 38 42 91 06 06 00 00 ....c@*..8B..... Thu Sep 13 13:54:39 2007: 00000070: 00 0a .. Thu
Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd .{.0..@K.:3..\0.
Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53
..n.........CACS Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34
2f 31 :0/977/a4df4d4/1 Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response
code=2 Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2 Thu Sep 13
13:54:40 2007: 00:0b:85:51:5a:e0 Access-Accept received from RADIUS server 10.77.244.196 for
mobile 00:0b:85:51:5a:e0 receiveId = 0 Thu Sep 13 13:54:40 2007: AuthorizationResponse:
0x9845500 Thu Sep 13 13:54:40 2007: structureSize.....................84 Thu Sep 13 13:54:40
2007: resultCode.....................0 Thu Sep 13 13:54:40 2007:
protocolUsed.....................0x00000001 Thu Sep 13 13:54:40 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:40 2007: Packet
contains 2 AVPs: Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address.............. 0xffffffff
(-1) (4 bytes) Thu Sep 13 13:54:40 2007: AVP[02] Class.....................
CACS:0/977/a4df4d4/1 (20 bytes) debug lwapp events enable Thu Sep 13 14:01:51 2007:
00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful
transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:01:51
2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to
ff:ff:ff:ff:ff:ff on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful
transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:02:02
2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Thu Sep 13
14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index
57)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP
Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0
Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 13 14:02:02 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

Dépannez

Utilisez ces commandes de dépanner votre configuration :

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

- **enable d'événements de debug lwapp** — Configures mettent au point des événements et des erreurs LWAPP.
- **enable de paquet de debug lwapp** — Configures mettent au point du tracé de paquets LWAPP.
- **le debug aaa tout activent** — Configures mettent au point de tous les messages d'AAA.

Informations connexes

- Passer les points d'accès autonomes de Cisco Aironet au mode léger
- Conseils de dépannage de l'outil de mise à niveau LWAPP
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems