Exemple de configuration de pontage Ethernet dans un réseau à maillage sans fil point à point

Contenu

Introduction

Ce document présente un exemple de configuration simple pour l'établissement d'un pont Ethernet sur un réseau maillé sans fil d'extérieur. Ce document explique l'établissement d'un pont Ethernet point à point entre les points d'accès (AP) des technologies sans fil d'extérieur maillées.

Conditions préalables

- Le contrôleur LAN sans fil (WLC) est configuré pour un 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 points d'accès légers (LAP) et des WLC Cisco

- Connaissances de base sur la solution de réseau maillé sans fil
- Avoir une connaissance de base du protocole LWAPP (Lightweight AP Protocol)
- 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 2000 qui exécute le microprogramme 4.0.217.0
- 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

La solution de réseau maillé, qui fait partie de la solution de réseau sans fil unifié Cisco, permet à deux points d'accès maillé léger Cisco Aironet (ci-après appelés points d'accès maillés) de communiquer entre eux sur un ou plusieurs sauts sans fil pour rejoindre plusieurs réseaux locaux ou étendre la couverture sans fil 802.11b. Les points d'accès maillés Cisco sont configurés, surveillés et exploités à partir et via tout contrôleur LAN sans fil Cisco déployé dans la solution de réseau maillé.

Les déploiements de solutions de réseau maillé pris en charge sont de trois types généraux :

- Déploiement point à point
- Déploiement point à multipoint
- Déploiement maillé

Ce document se concentre sur la façon de configurer le déploiement de maillage point à point et le pontage Ethernet sur le même. Dans le déploiement de maillage point à point, les points d'accès maillés fournissent un accès sans fil et une liaison aux clients sans fil. Ils peuvent également prendre en charge le pontage entre un LAN et une terminaison vers un périphérique Ethernet distant ou un autre LAN Ethernet.

Référez-vous à Déploiements de solutions de réseau maillé pour obtenir des informations détaillées sur chacun de ces types de déploiement.

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 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.

Vous pouvez utiliser les points d'accès légers de périphérie distante Cisco Aironet 1510 et les points d'accès extérieurs légers de la gamme Cisco Aironet 1500 dans l'un des rôles suivants :

- Point d'accès sur le toit (RAP)
- Point d'accès maillé (MAP), également appelé PAP (Point d'accès au sommet du pôle)

Les RAP ont une connexion filaire à un contrôleur LAN sans fil Cisco. Ils utilisent l'interface sans fil de liaison pour communiquer avec les MAP voisines. Les RAP sont le noeud parent d'un réseau de pontage ou de maillage et connectent un pont ou un réseau maillé au réseau câblé, de sorte qu'il ne peut y avoir qu'un seul RAP pour un segment de réseau maillé ou ponté.

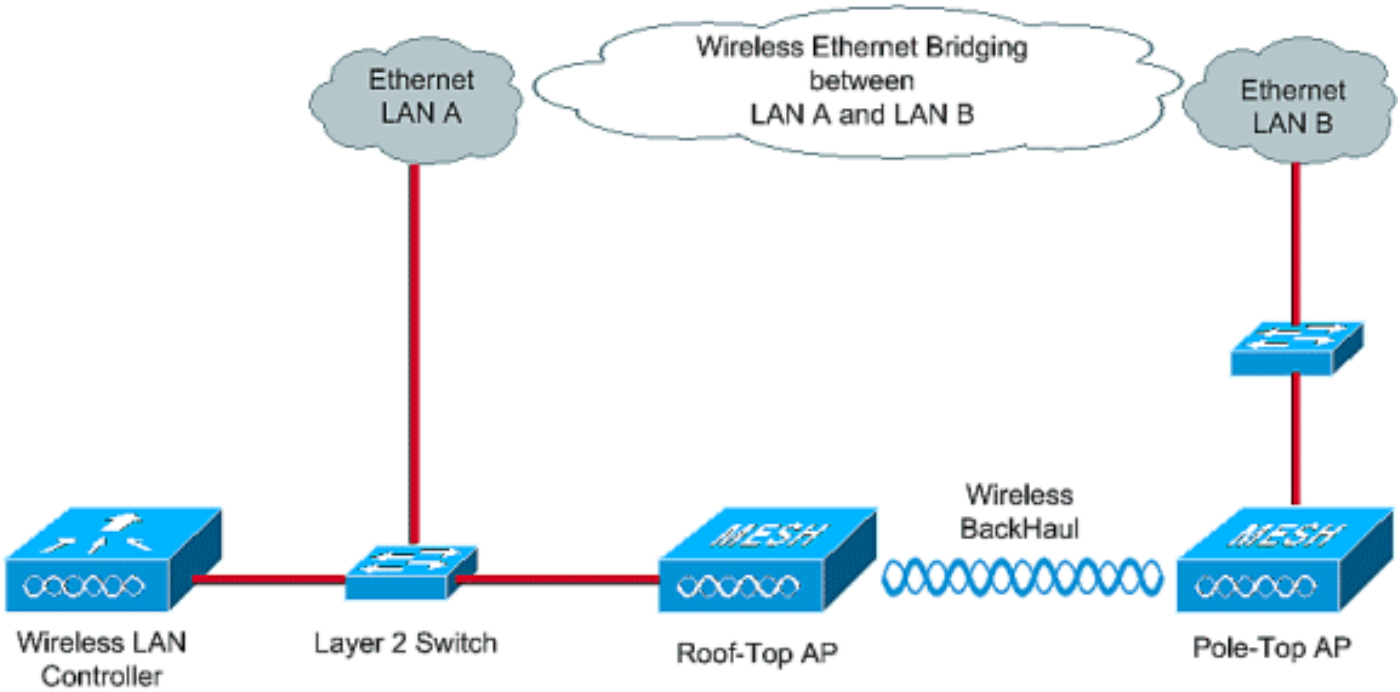
Les MAP n'ont pas de connexion câblée à un contrôleur LAN sans fil Cisco. Ils peuvent être entièrement sans fil et prendre en charge des clients qui communiquent avec d'autres MAP ou RAP, ou ils peuvent être utilisés pour se connecter à des périphériques ou à un réseau câblé. Le port Ethernet est désactivé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

Configuration

Cet exemple de configuration explique comment configurer le pontage Ethernet entre deux points d'accès à maillage extérieur léger de la gamme 1510 avec un point d'accès qui agit en tant que RAP et l'autre qui agit en tant que MAP.

Dans cette configuration, le point d'accès avec l'adresse MAC 00:0B:85:7F:47:00 est configuré en tant que RAP, et le point d'accès avec l'adresse MAC 00:0B:85:71:1B:00 est configuré en tant que MAP. Un LAN Ethernet local A est connecté à l'extrémité RAP et un LAN Ethernet B est connecté au MAP.

Diagramme du réseau



Afin de configurer des points d'accès 1510 maillés prêts à l'emploi pour le pontage Ethernet, procédez comme suit :

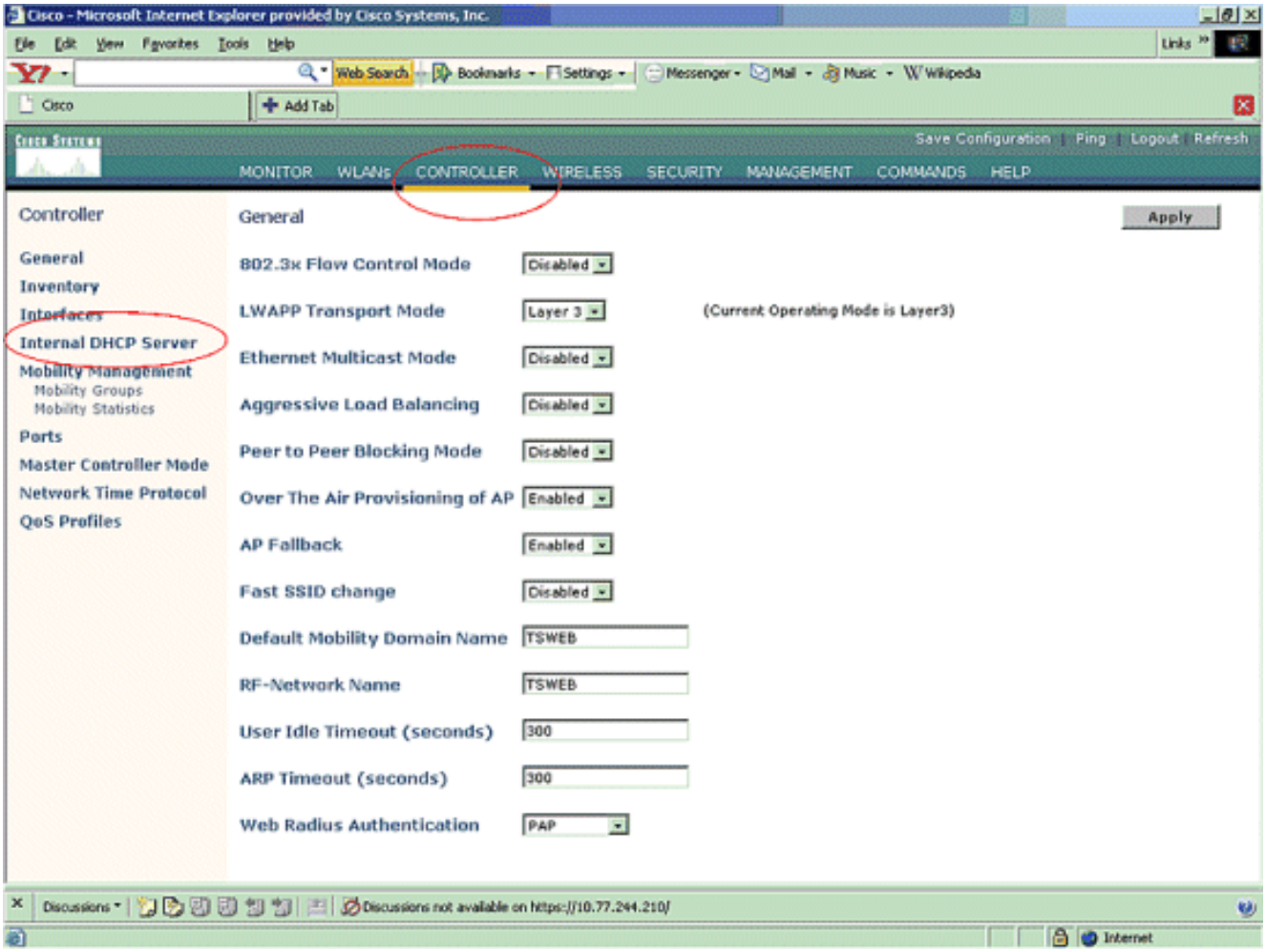
1. Attribuer une adresse IP aux points d'accès
2. Ajouter l'adresse MAC des points d'accès à la liste de filtrage MAC du WLC
3. Enregistrer les AP avec le WLC
4. Configurer le rôle AP et les autres paramètres de pontage
5. Activer le pontage Ethernet sur les points d'accès
6. Activer la configuration automatique sur le WLC

Attribuer une adresse IP aux points d'accès

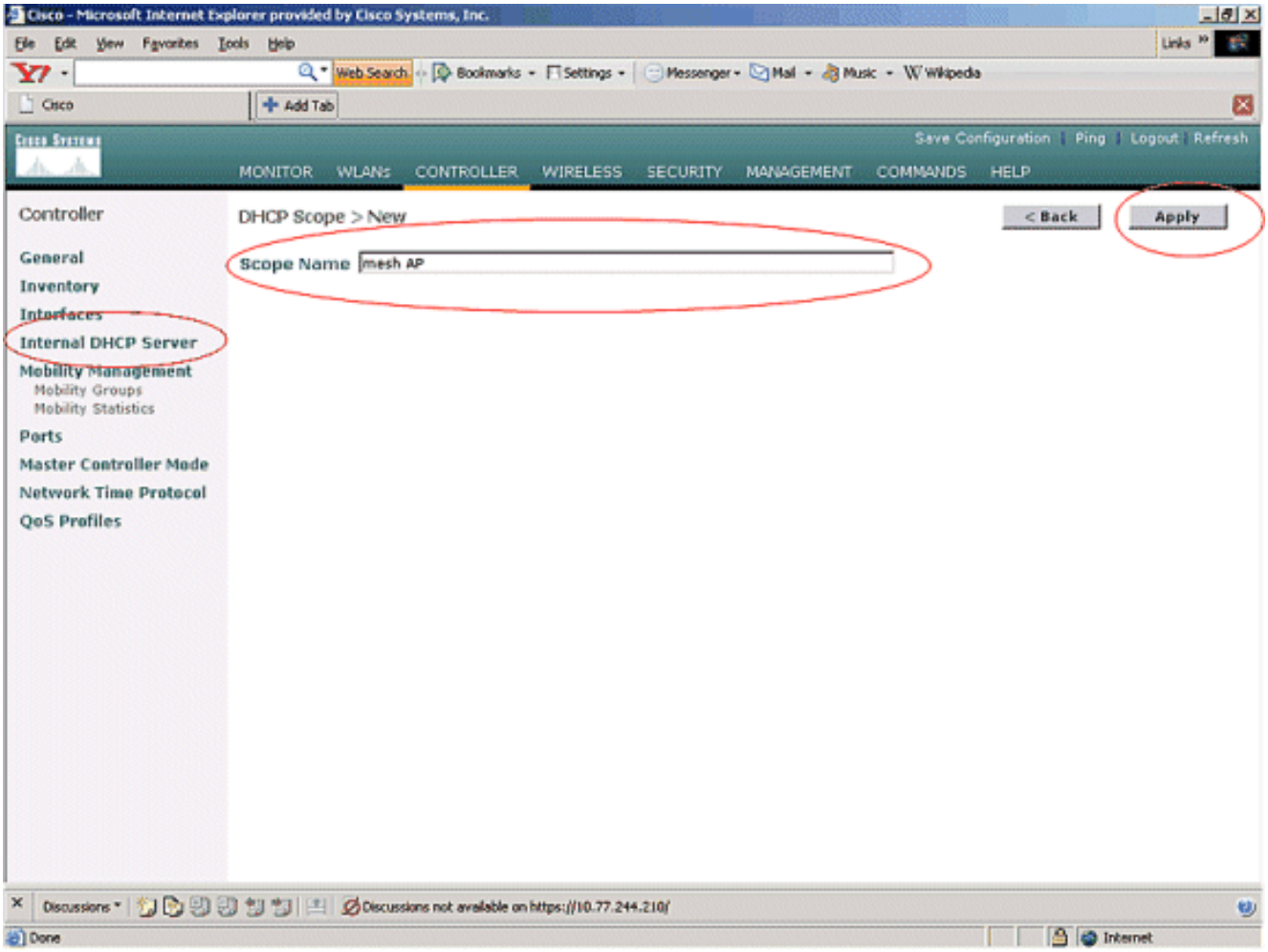
Lorsqu'un point d'accès démarre, il recherche d'abord une adresse IP. Cette adresse IP peut être attribuée dynamiquement avec un serveur DHCP interne externe tel que le serveur DHCP Microsoft Windows®. La dernière version du WLC (4.0 et versions ultérieures) peut attribuer l'adresse IP aux AP avec le serveur DHCP interne sur le contrôleur lui-même. Cet exemple utilise le serveur DHCP interne sur le contrôleur pour attribuer une adresse IP aux AP.

Complétez ces étapes afin d'attribuer une adresse IP aux points d'accès via le serveur DHCP interne sur le WLC.

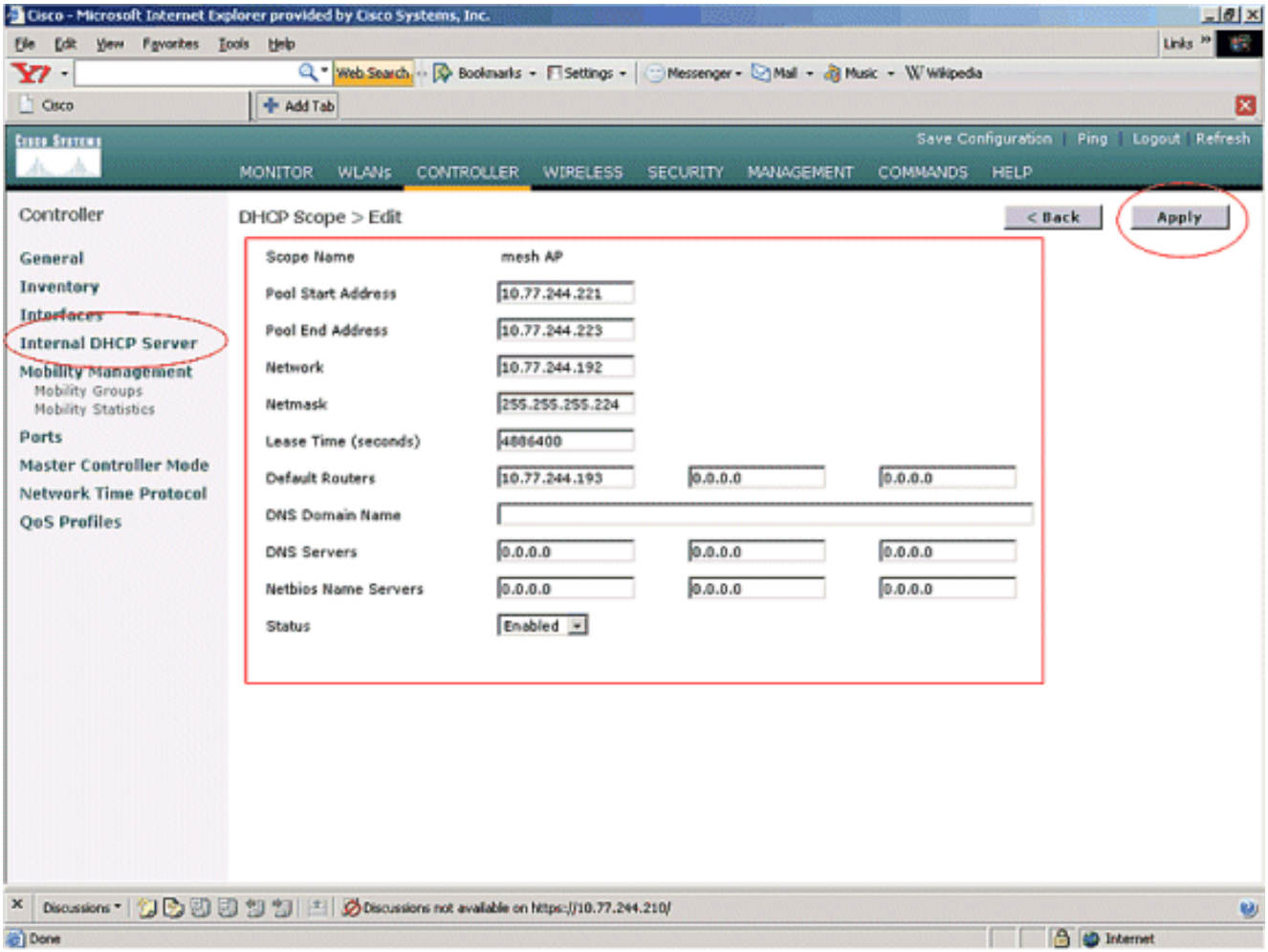
1. Cliquez sur **CONTROLLER** dans le menu principal de l'interface graphique du WLC. Choisissez **Internal DHCP Server** dans le coin gauche de la page principale du contrôleur.



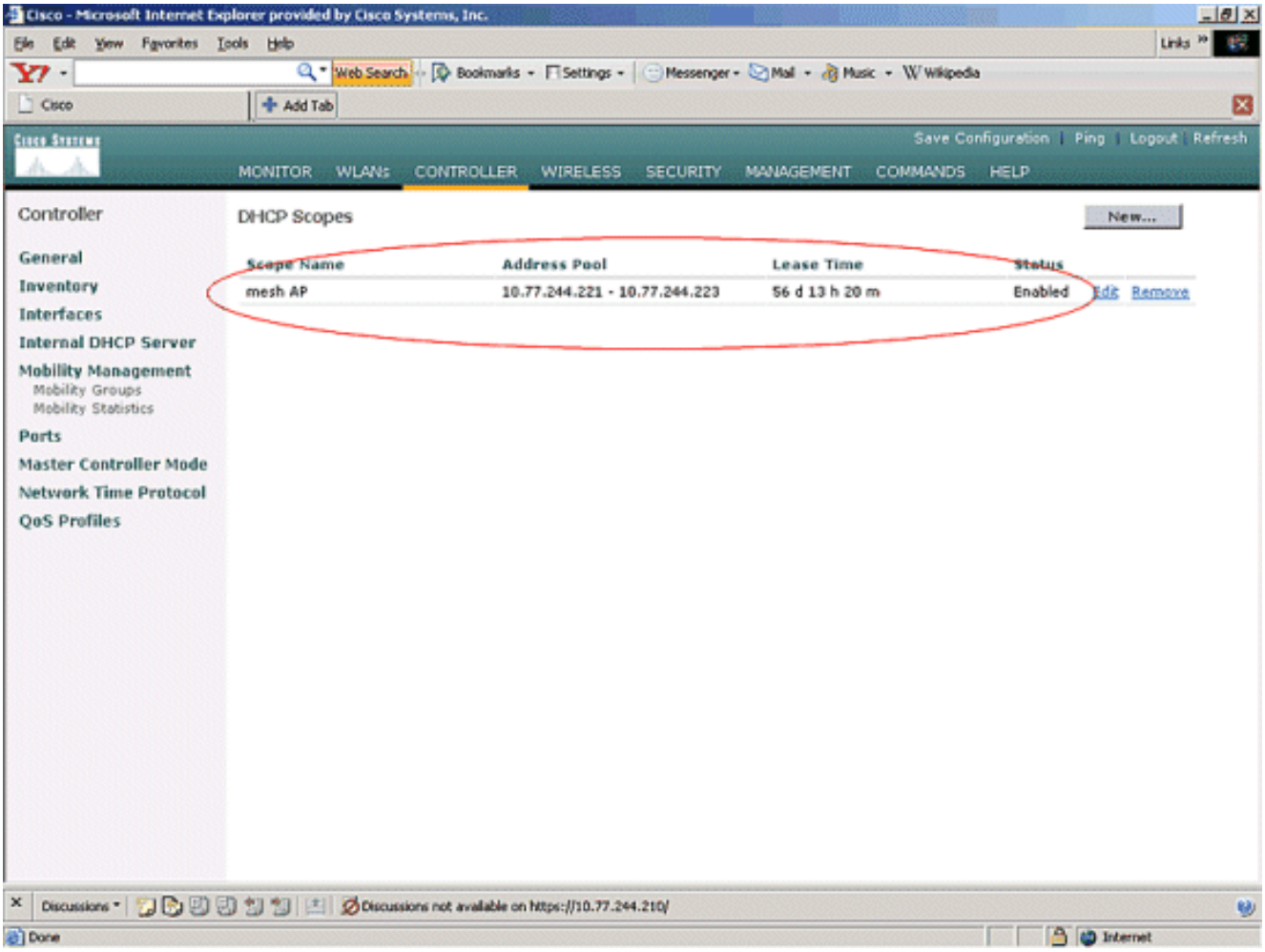
2. Dans la page **Internal DHCP Server**, **cliquez surNew** afin de créer une nouvelle étendue DHCP. Cet exemple attribue le nom de la portée comme **point d'accès maillé**. Cliquez sur Apply. Ceci vous amène à la page de modification de l'étendue DHCP du point d'accès maillé.



3. Dans la page **Étendue DHCP > Modifier**, configurez l'adresse de début du pool, l'adresse de fin du pool, le réseau et le masque de réseau, les routeurs par défaut et tous les autres paramètres nécessaires comme indiqué dans cet exemple. Sélectionnez l'état du serveur DHCP **Enabled** dans la liste déroulante **Status**. Cliquez sur Apply.



4. Maintenant, le serveur DHCP interne est configuré pour attribuer des adresses IP aux points d'accès
maillés.



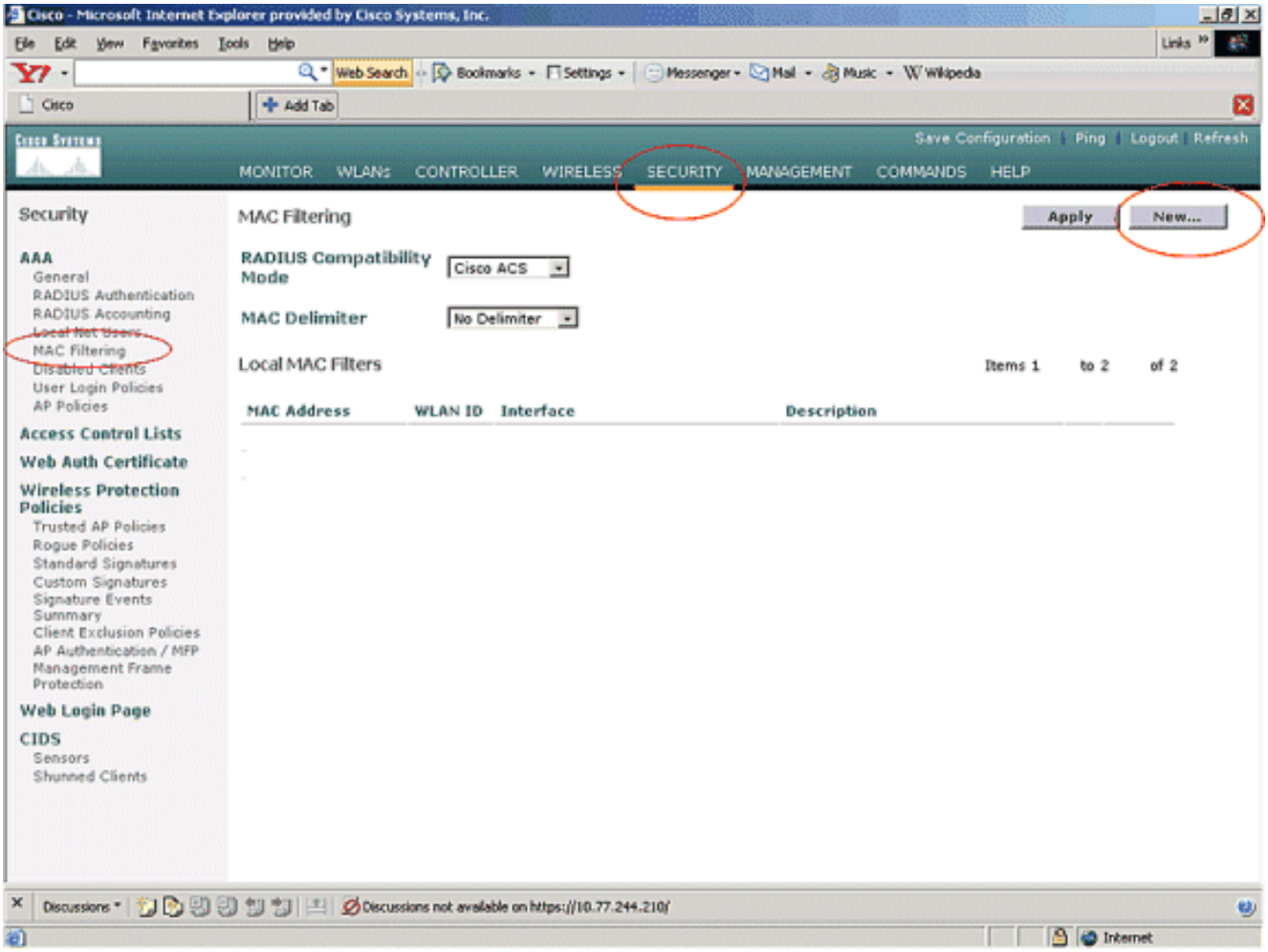
5. Une fois que les points d'accès sont enregistrés avec le contrôleur, attribuez l'adresse IP statique aux points d'accès via l'interface graphique du contrôleur. Si vous attribuez des adresses IP statiques aux points d'accès maillés, cela fournit une convergence plus rapide des points d'accès la prochaine fois qu'ils s'enregistrent auprès du contrôleur.

Ajouter l'adresse MAC des points d'accès à la liste de filtrage MAC du WLC

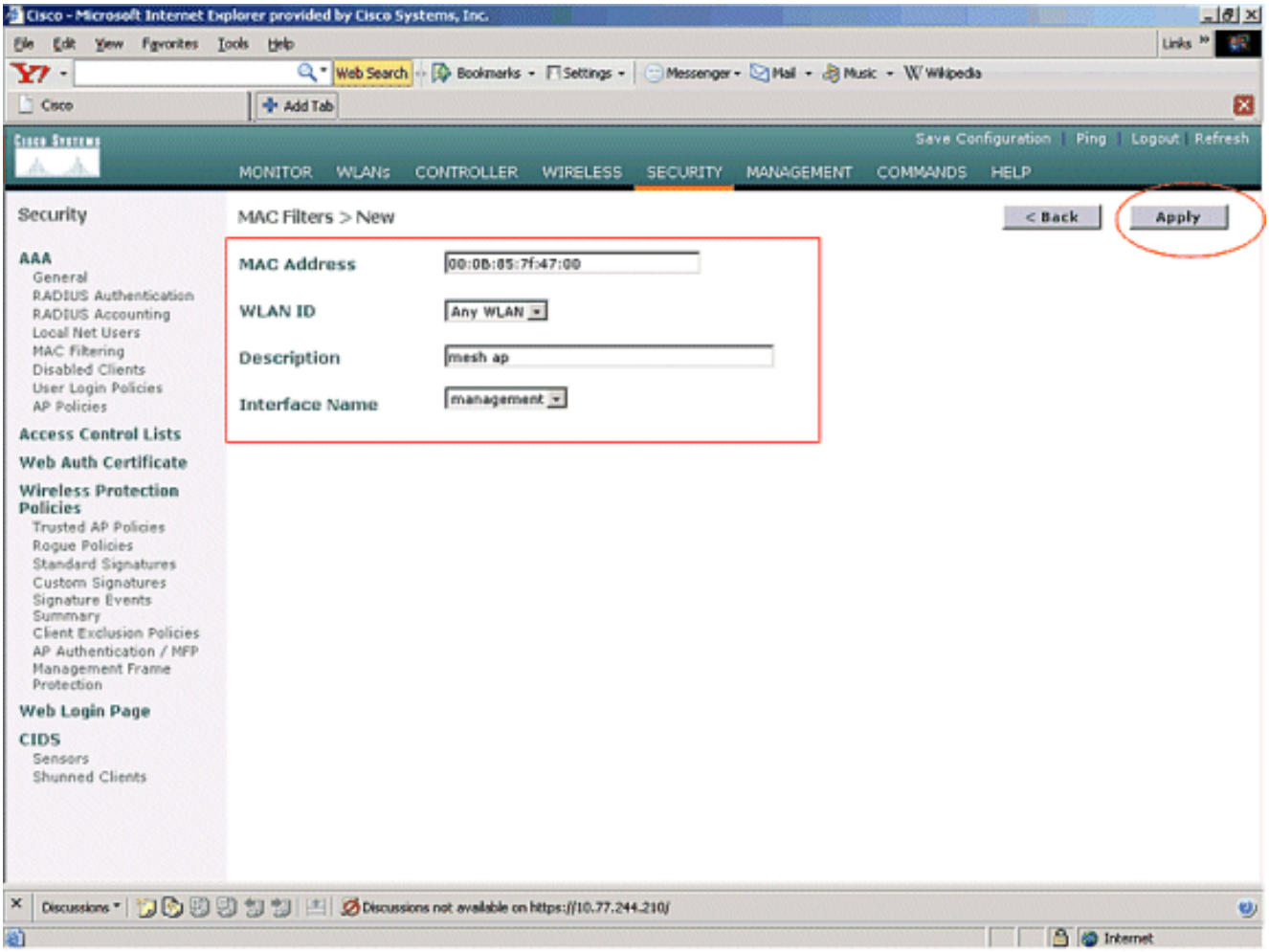
Afin d'enregistrer les AP maillés avec le WLC, vous devez d'abord ajouter l'adresse MAC des AP à la liste de filtrage MAC du WLC. Vous pouvez trouver l'adresse MAC étiquetée sur le côté supérieur du point d'accès maillé.

Complétez ces étapes afin d'ajouter l'AP à la liste de filtrage MAC du WLC.

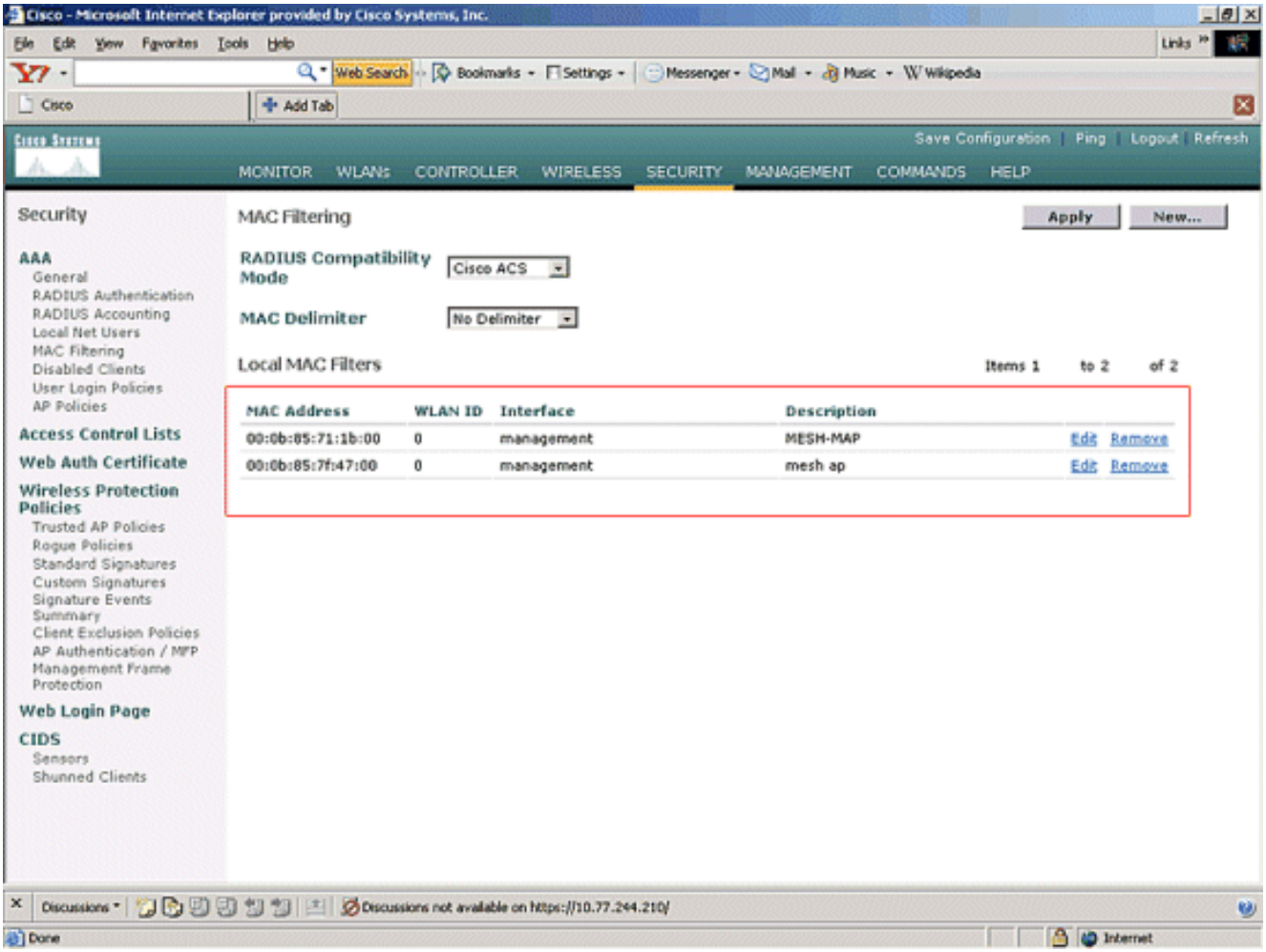
1. Cliquez sur **SÉCURITÉ** dans le menu principal du contrôleur.Sur la page Sécurité, sélectionnez **Filtrage MAC** sous la section **AAA**. Vous accédez ainsi à la page MAC Filtering. Cliquez sur **New** afin de créer des filtres MAC pour les AP maillés.



2. Entrez l'**adresse MAC** du point d'accès et sa **description** dans les zones de texte appropriées comme indiqué dans cet exemple. Choisissez également une **interface WLAN** et **dynamique** dans les menus déroulants WLAN ID et Interface Name, respectivement. Cliquez sur Apply.



3. Répétez les étapes 1 et 2 pour tous les AP impliqués dans ce réseau maillé, de sorte que le filtrage MAC est configuré pour permettre aux AP maillés de s'enregistrer auprès du contrôleur.



Enregistrer l'AP avec le WLC

L'étape suivante consiste à enregistrer les AP maillés avec le WLC. Il existe plusieurs méthodes qu'un point d'accès peut enregistrer auprès du WLC. Référez-vous à Enregistrement léger AP avec WLC pour plus de détails sur la façon dont un AP s'enregistre avec le WLC.

La première fois que vous utilisez les points d'accès maillés, enregistrez tous les points d'accès directement connectés au WLC.

Si vous n'avez pas pu ajouter l'AP à la liste de filtrage MAC du contrôleur, les AP ne peuvent pas rejoindre le WLC au moment de l'enregistrement avec le WLC. La raison est l'échec de l'autorisation à partir de la sortie de la commande **debug lwapp events enable** sur le contrôleur. Voici l'exemple de sortie qui indique un échec d'autorisation.

```
(Cisco Controller) >debug lwapp events enable

.Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to 00:0b:85:33:52:80 on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to ff:ff:ff:ff:ff:ff on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 Received LWAPP JOIN REQUEST from AP
00:0b:85:71:1b:00 to 00:0b:85:33:52:81 on port '2'
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 AP ap:71:1b:00: txNonce  00:0B:85:33
```

```
:52:80 rxNonce  00:0B:85:71:1B:00
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 LWAPP Join-Request MTU path from AP
00:0b:85:71:1b:00 is 1500, remote debug mode is 0
Fri Oct 26 15:52:40 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:71:1b:00
```

Dans cette sortie, vous pouvez voir que la demande de jointure du point d'accès n'est pas acceptée par le contrôleur en raison de l'échec de l'autorisation du point d'accès.

Remarque : Dans les déploiements de réseau maillé normaux qui utilisent principalement des points d'accès maillés de la gamme 1500, il est recommandé de désactiver le paramètre **Autoriser les anciens points d'accès de pontage à authentifier** sur le contrôleur. Ceci peut être fait à partir du mode CLI du contrôleur avec la commande

Remarque : (contrôleur Cisco) **> config network allow-old-bridge-aps disable**

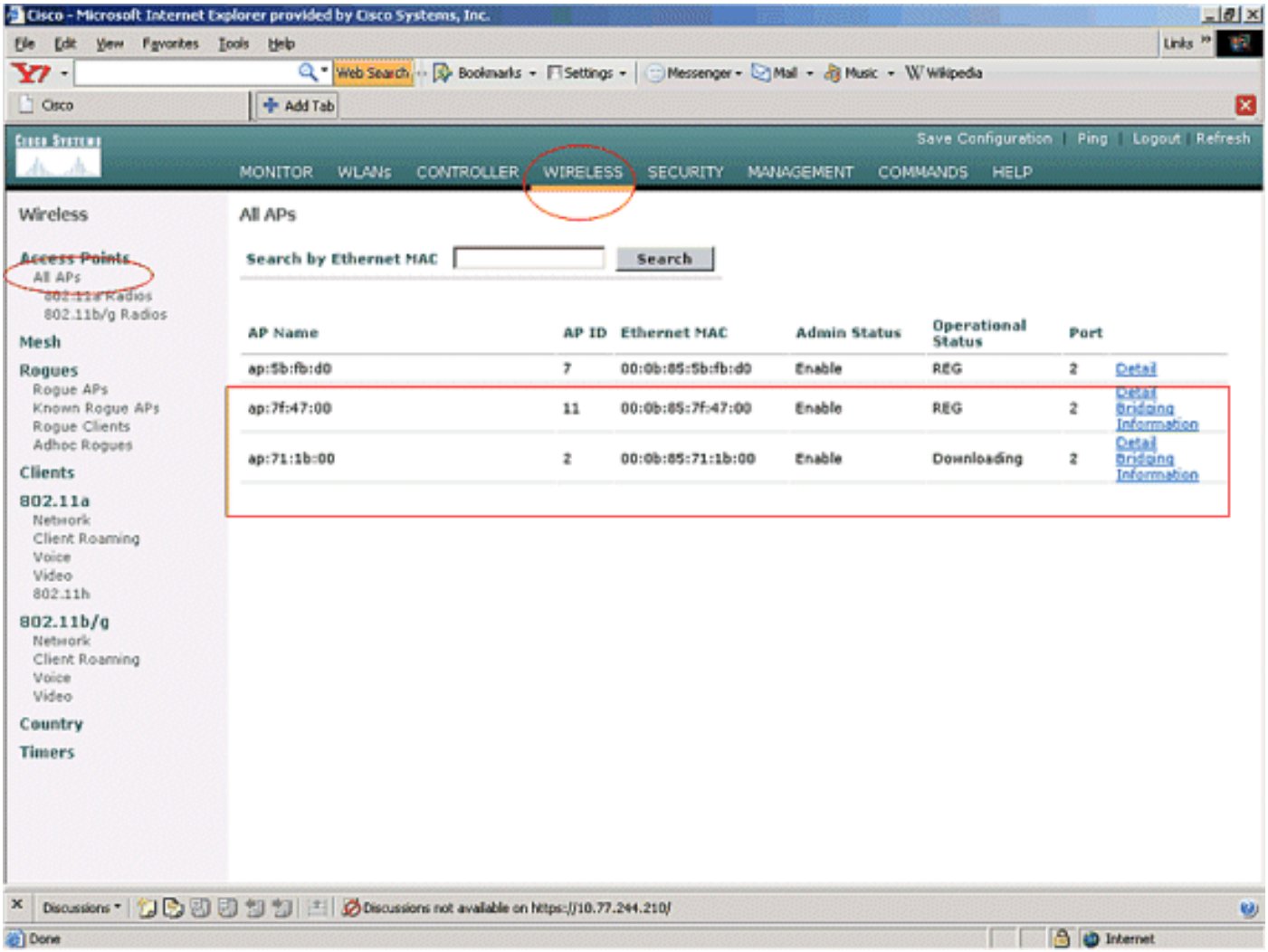
Remarque : La commande a été supprimée dans la version 4.1 et les versions ultérieures, donc ce n'est pas un problème avec WLC 4.1 et les versions ultérieures.

Sur la CLI, vous pouvez utiliser la commande **show ap summary** afin de vérifier que les AP sont enregistrés avec le WLC :

(Contrôleur Cisco) **>show ap summary**

```
AP Name             Slots  AP Model             Ethernet MAC       Location
     Port
------------------  -----  -------------------  -----------------  -------------
---
ap:5b:fb:d0          2     AP1010               00:0b:85:5b:fb:d0  default_locat
ion  2
ap:7f:47:00          2     LAP1510              00:0b:85:7f:47:00  default_locat
ion  2
ap:71:1b:00          2     LAP1510              00:0b:85:71:1b:00  default_locat
ion  2
```

Vous pouvez le vérifier à partir de l'interface utilisateur graphique sous la page **Tous les points d'accès** sans fil.

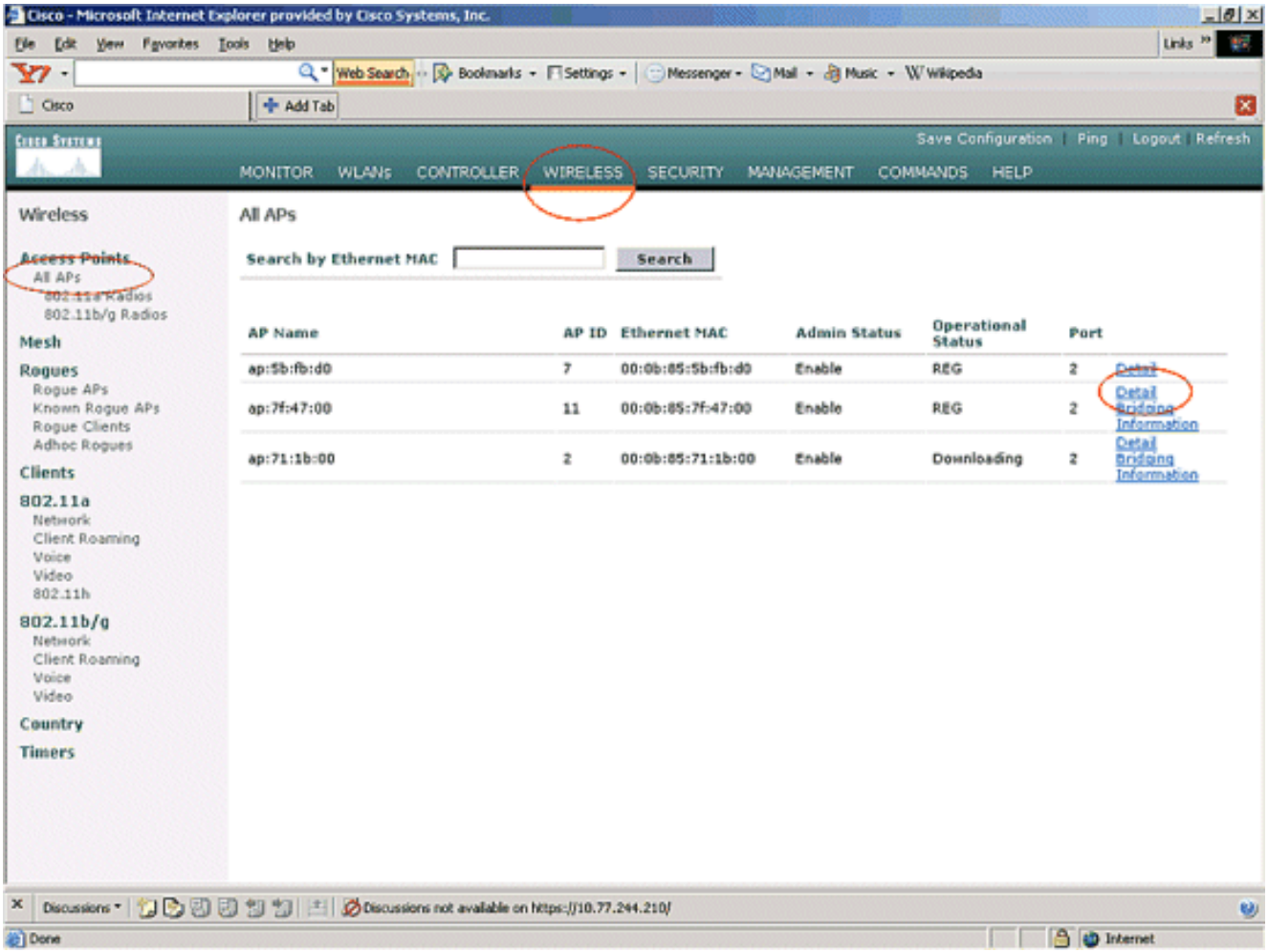


Configurer le rôle AP et les autres paramètres de pontage

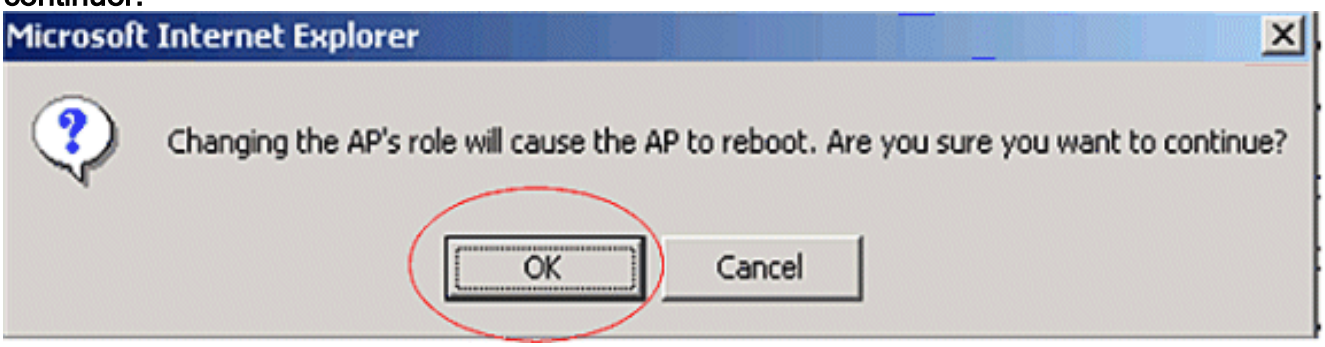
Une fois les AP enregistrés au WLC, vous devez configurer le rôle AP et d'autres paramètres de pontage. Vous devez configurer les AP en tant que RAP et MAP, si nécessaire.

Complétez ces étapes afin de configurer ces paramètres AP :

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



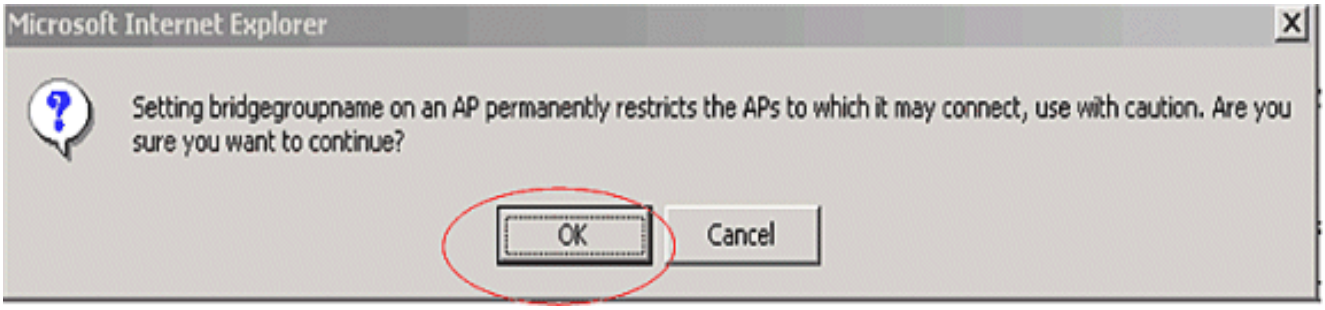
3. Dans la page **Détails** de votre AP 1510, le **mode AP** sous **Général** est automatiquement défini sur **Bridge** pour les AP qui ont une fonctionnalité de pont, comme AP1510. Cette page affiche également ces informations sous Bridging Information.Sous **Informations de pontage**, choisissez l'une de ces options afin de spécifier le rôle de ce point d'accès dans le réseau maillé :MeshAP (MAP)Point d'accès racine (RAP)Les points d'accès configurés en tant que points d'accès racine doivent avoir une connexion câblée au WLC au moment de la mise en oeuvre de la configuration dans votre environnement de production. L'AP configuré comme un AP maillé est connecté sans fil au WLC via son AP parent (RAP). Par défaut, les points d'accès 1510 assument le rôle des MAP lorsqu'ils apparaissent et s'enregistrent auprès du WLC.Lorsque vous configurez le rôle de pont, une zone d'alerte affiche ce message : **AP redémarre**. Cliquez sur **OK pour continuer.**



Vous pouvez configurer le rôle AP avec l'interface de ligne de commande du contrôleur avec la commande **config ap role** *role* .

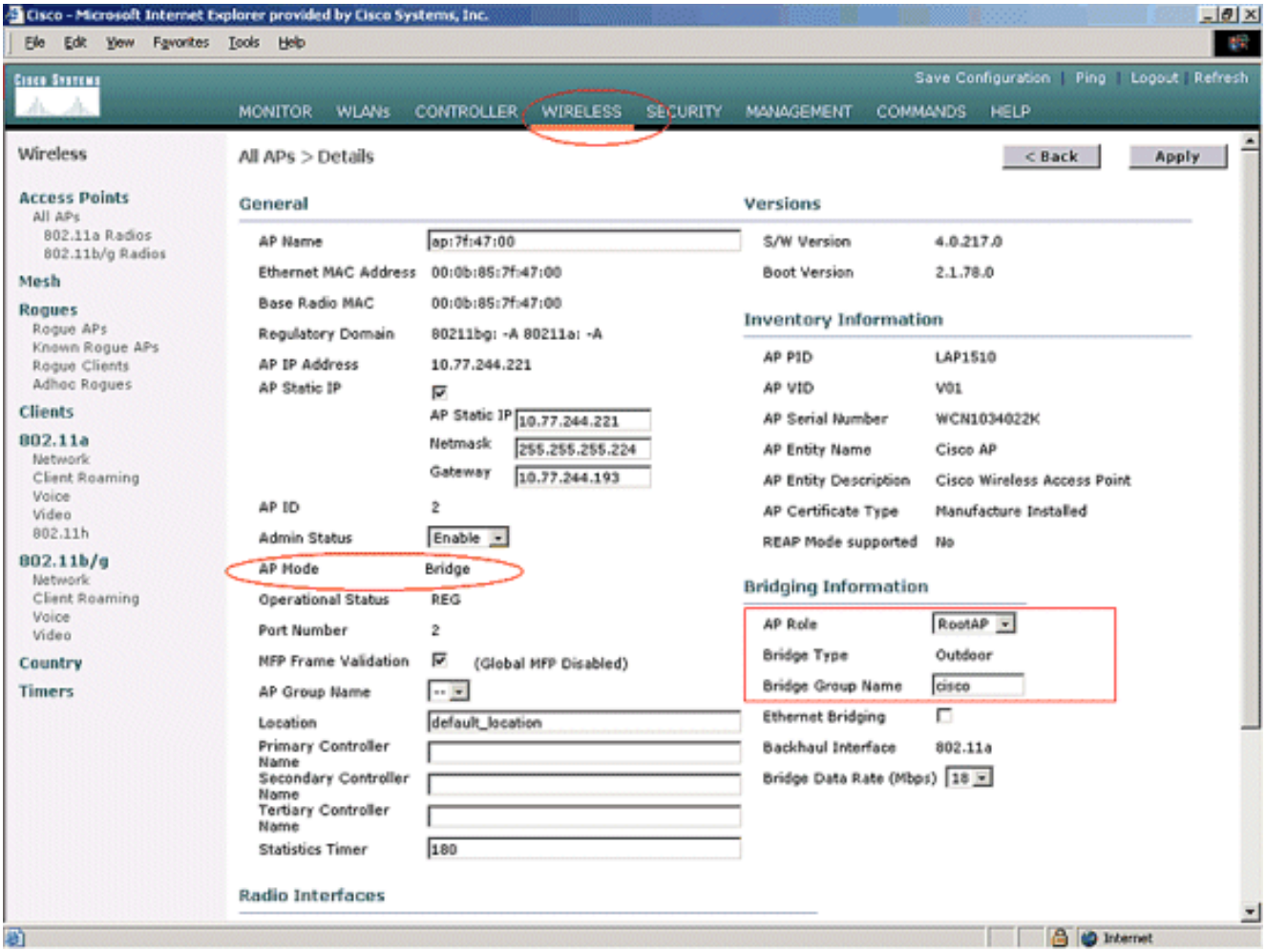
4. Configurez le paramètre **Bridge Group Name**. Il s'agit d'une chaîne de 10 caractères maximum. Utilisez les noms de groupes de ponts pour regrouper logiquement les points d'accès maillés afin d'éviter que deux réseaux du même canal ne communiquent entre eux.

Pour que les points d'accès maillés puissent communiquer, ils doivent avoir le même nom de groupe de ponts. Un nom de groupe de ponts de point d'accès maillé par défaut est attribué au stade de fabrication. Il n'est pas visible pour vous. Le champ Bridge Group Name (Nom du groupe de ponts) apparaît vide dans l'interface utilisateur graphique jusqu'à ce que vous le modifiiez. L'AP s'enregistre pour la première fois auprès du WLC avec ce nom de groupe de ponts par défaut.Cet exemple utilise le nom de groupe de ponts **cisco** sur tous les points d'accès impliqués dans ce réseau maillé.Lorsque vous configurez le nom du groupe de ponts, une zone d'alerte affiche ceci : **La définition du nom du groupe de ponts limite de façon permanente le point d'accès auquel il peut se connecter. »** Cliquez sur **OK pour continuer.**



Vous pouvez configurer le nom du groupe de ponts avec l'interface de ligne de commande du contrôleur à l'aide de la commande **config ap bridgegroupname set *cisco*** .**Remarque :** si vous voulez modifier le nom du groupe de ponts des AP après le déploiement du RAP sur son site distant, configurez d'abord le paramètre Bridge Group Name sur le MAP, puis sur le RAP. Si le RAP est configuré en premier, cela entraîne de graves problèmes de connectivité puisque le MAP passe en mode par défaut, car son parent (RAP) est configuré avec un nom de groupe de ponts différent.**Remarque :** pour les configurations avec plusieurs RAP, assurez-vous que tous les RAP ont le même nom de groupe de ponts pour permettre le basculement d'un RAP à un autre. Inversement, pour les configurations où des secteurs distincts sont nécessaires, assurez-vous que chaque RAP et les PAP associés ont des noms de groupes de ponts distincts.

5. Le **débit de données du pont** est le débit auquel les données sont partagées entre les points d'accès maillés. Ceci est corrigé pour un réseau entier. **Le débit de données par défaut est de 18 Mbits/s, que vous devez utiliser pour la liaison**. Les débits de données valides pour la norme 802.11a sont les suivants : 6, 9, 12, 18, 24, 36, 48 et 54.
6. Si vous configurez le point d'accès en tant que RAP, le paramètre **Interface de liaison** affiche un menu déroulant, mais si vous cliquez sur le bouton déroulant, vous ne voyez que l'option 802.11a. **Sur le MAP, aucun menu déroulant de ce type n'est disponible**. Cliquez sur Apply. Voici la capture d'écran qui explique les étapes 3 à 6.



La configuration de RootAP (RAP) est présentée ici.

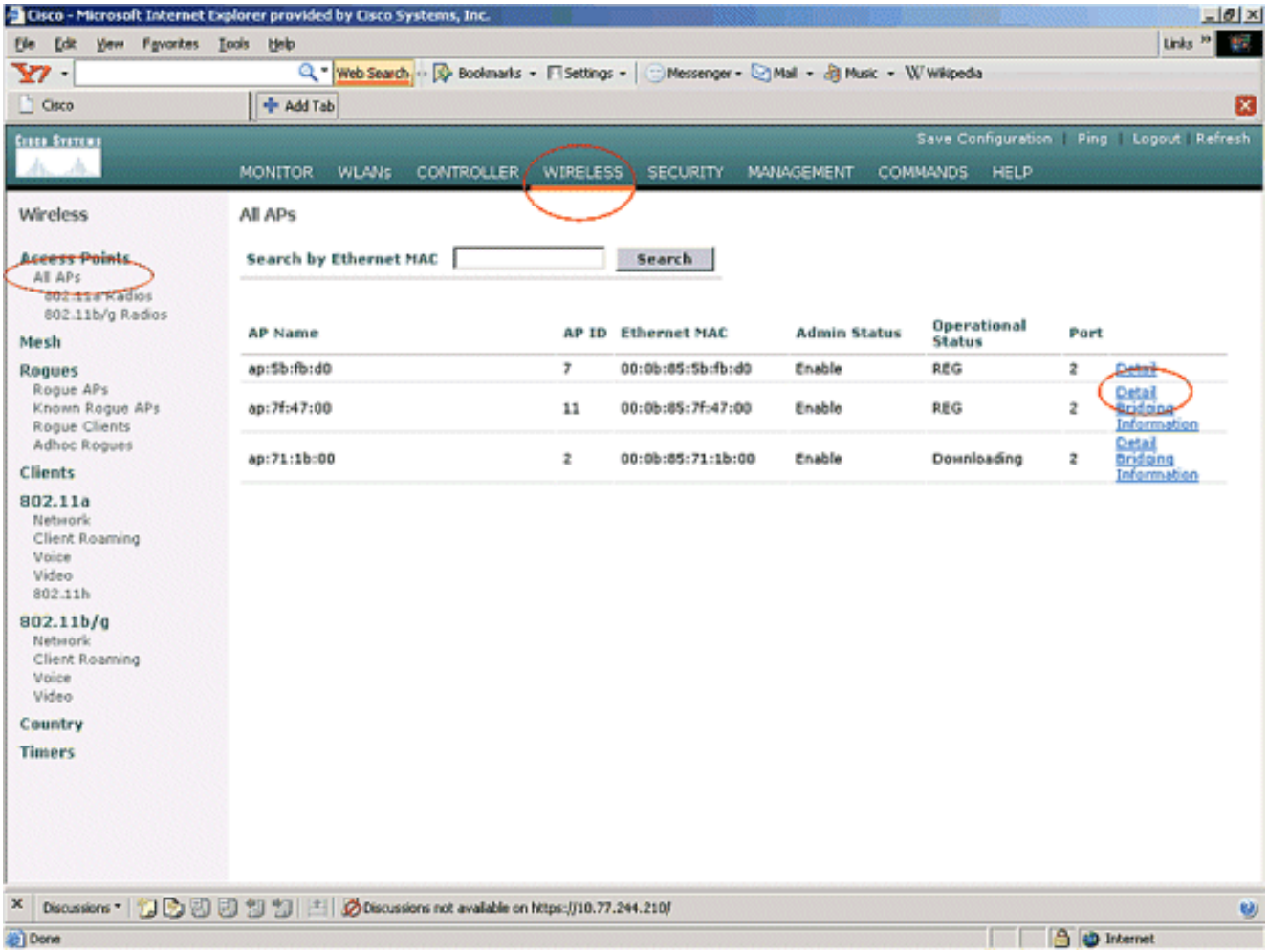
Activer le pontage Ethernet sur les points d'accès

L'étape suivante consiste à activer le pontage Ethernet sur le RAP et tous les MAP dont le port Ethernet est connecté à un périphérique Ethernet. L'une des principales caractéristiques des points d'accès maillés est l'utilisation d'un port Ethernet sur le MAP pour connecter des périphériques externes et fournir un pontage Ethernet entre tous les ports Ethernet des points d'accès impliqués dans le réseau maillé.

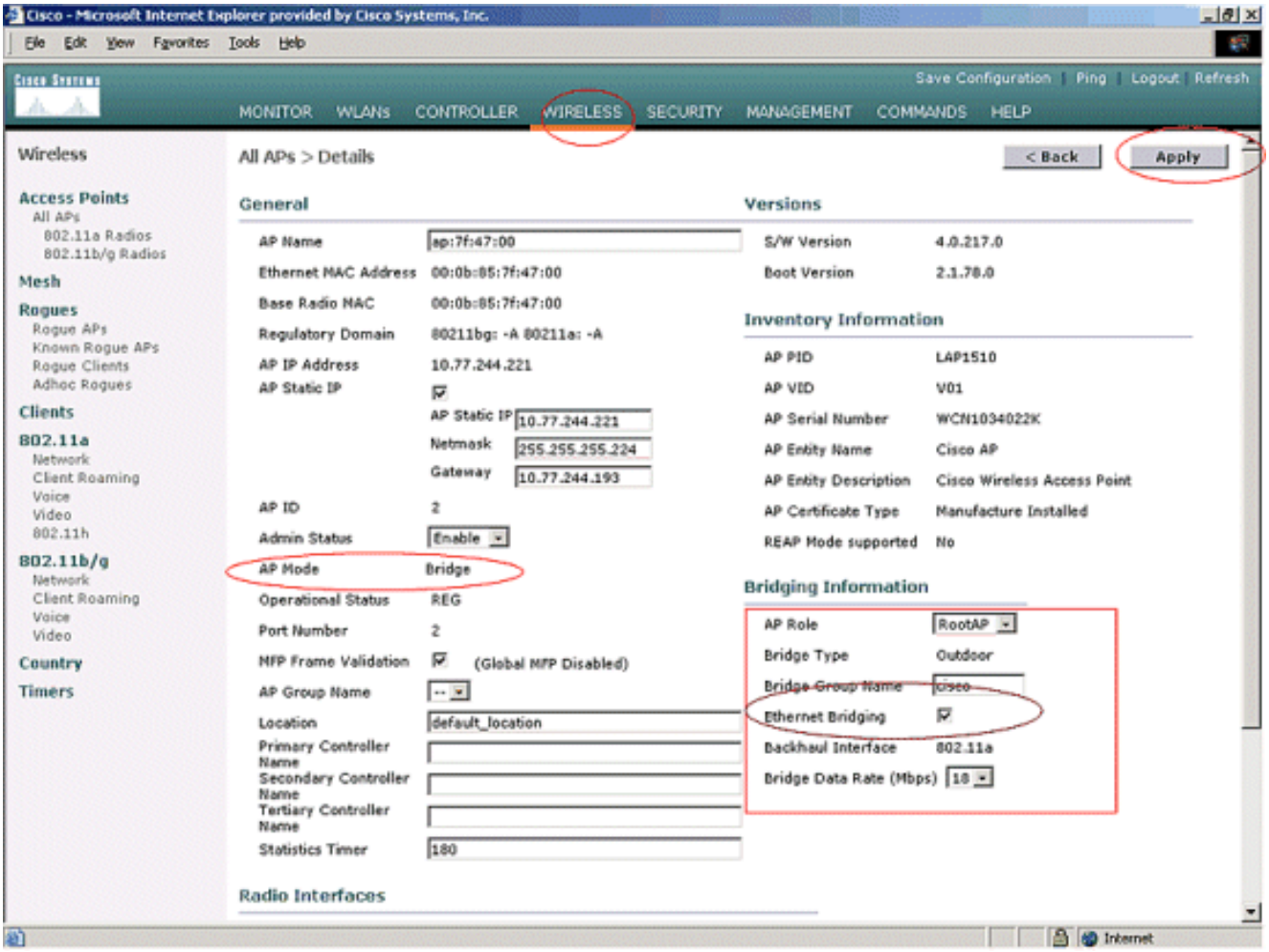
Le maillage WLAN peut transporter simultanément deux types de trafic différents, le trafic client WLAN et le trafic de pont MAP. Le trafic client WLAN se termine sur le contrôleur WLAN et le trafic de pont se termine sur les ports Ethernet des points d'accès maillés 1500. Le trafic Bridge n'atteint pas le WLC. Si un noeud de maillage fonctionne en tant que MAP, le port Ethernet de la MAP est verrouillé. Cela a été fait pour des raisons de sécurité. Si quelqu'un veut utiliser un port Ethernet pour déployer des réseaux point à point (P2P) à pontage multipoint (P2MP) ou pour connecter des périphériques externes, il doit l'activer sur le contrôleur pour chaque MAP.

Complétez ces étapes afin de configurer le pontage Ethernet sur les points d'accès RAP et maillés :

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

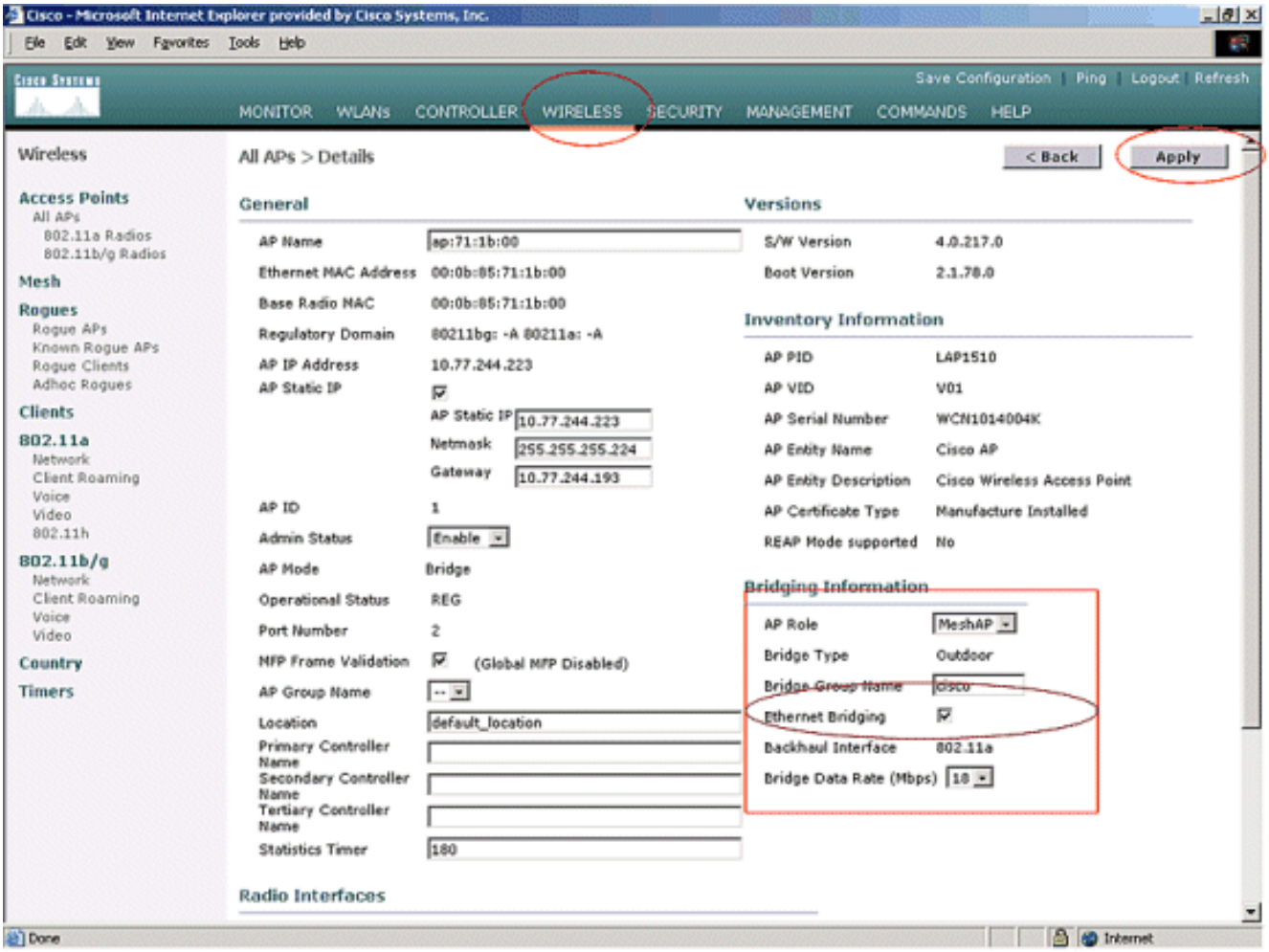


3. Sous **Informations de pontage**, cochez la case en regard de **pontage Ethernet**. Cela active le pontage Ethernet sur le point d'accès.



Si vous utilisez un réseau maillé point à multipoint, activez le pontage Ethernet sur les RAP et uniquement sur les MAP auxquelles les périphériques Ethernet sont connectés. Il n'est pas nécessaire d'activer le pontage Ethernet sur tous les MAP d'un réseau maillé.Si vous avez activé le pontage Ethernet pour utiliser le réseau pour le pontage (P2P ou P2MP), vous devez activer le pontage Ethernet sur tous les noeuds (MAP et RAP). Dans le scénario de pontage, un RAP qui agit en tant que pont racine connecte plusieurs MAP en tant que ponts non racine avec leurs LAN câblés associés.Vous pouvez activer le pontage Ethernet sur les points d'accès à partir de l'interface de ligne de commande du contrôleur à l'aide de la commande suivante : **config ap bridging Enable**.**Remarque :** Tous les commutateurs connectés aux ports Ethernet de vos MAP ne doivent PAS FAIRE le protocole VTP (VLAN Trunking Protocol). VTP peut reconfigurer le VLAN agrégé sur votre maillage et peut provoquer une perte de connexion pour votre RAP à son WLC principal. S'il est mal configuré, il peut arrêter votre déploiement de maillage.

4. Activez également le pontage Ethernet et tous les paramètres de pontage expliqués dans la section précédente du
MAP.



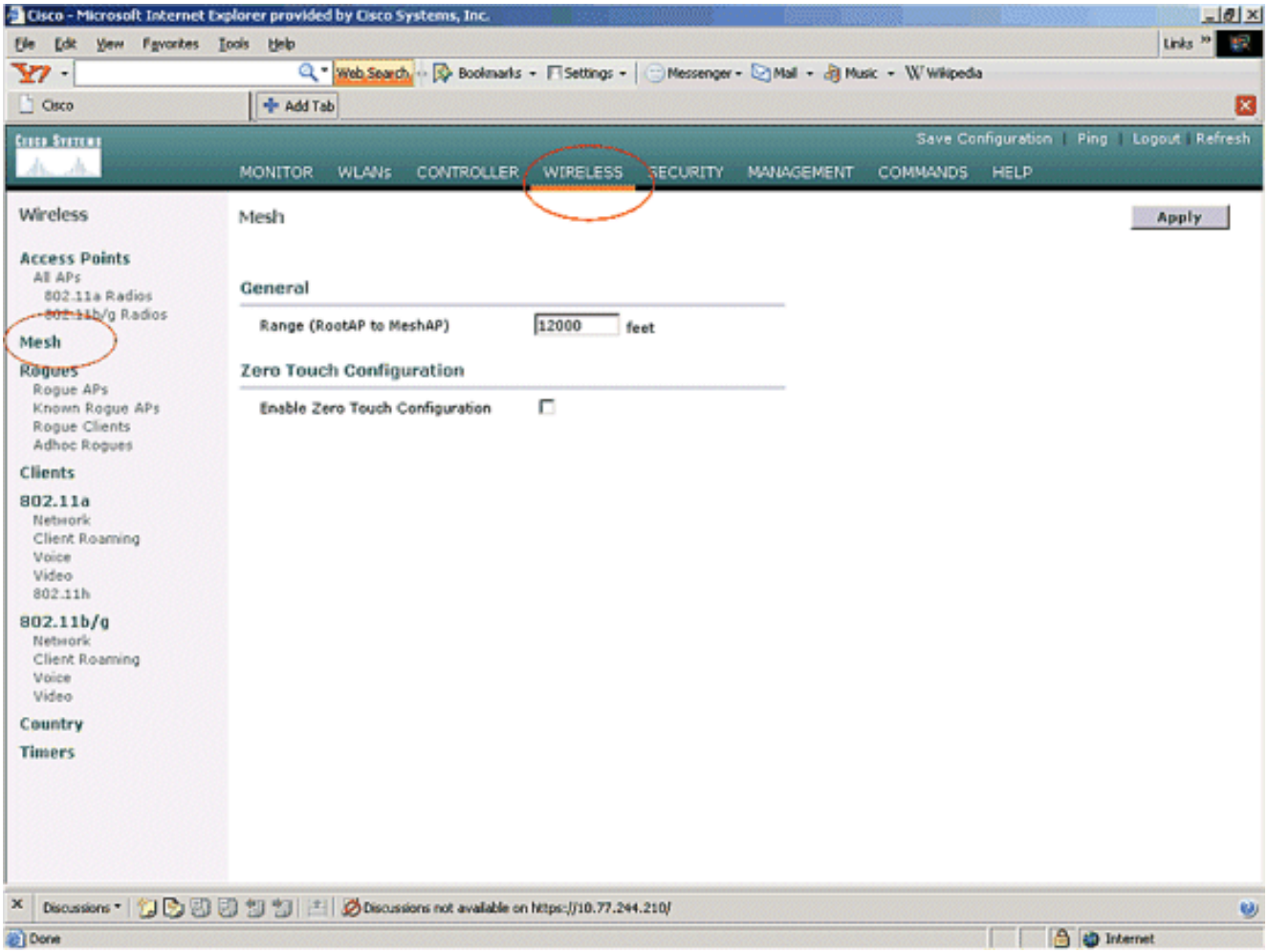
Une fois que vous avez terminé les configurations des paramètres de pontage et de pontage Ethernet sur chaque point d'accès, cliquez sur **Apply** afin d'enregistrer les paramètres. Cela entraîne la désinscription de l'AP du WLC, le redémarrage et l'enregistrement avec le WLC.

Activer la configuration automatique sur le WLC

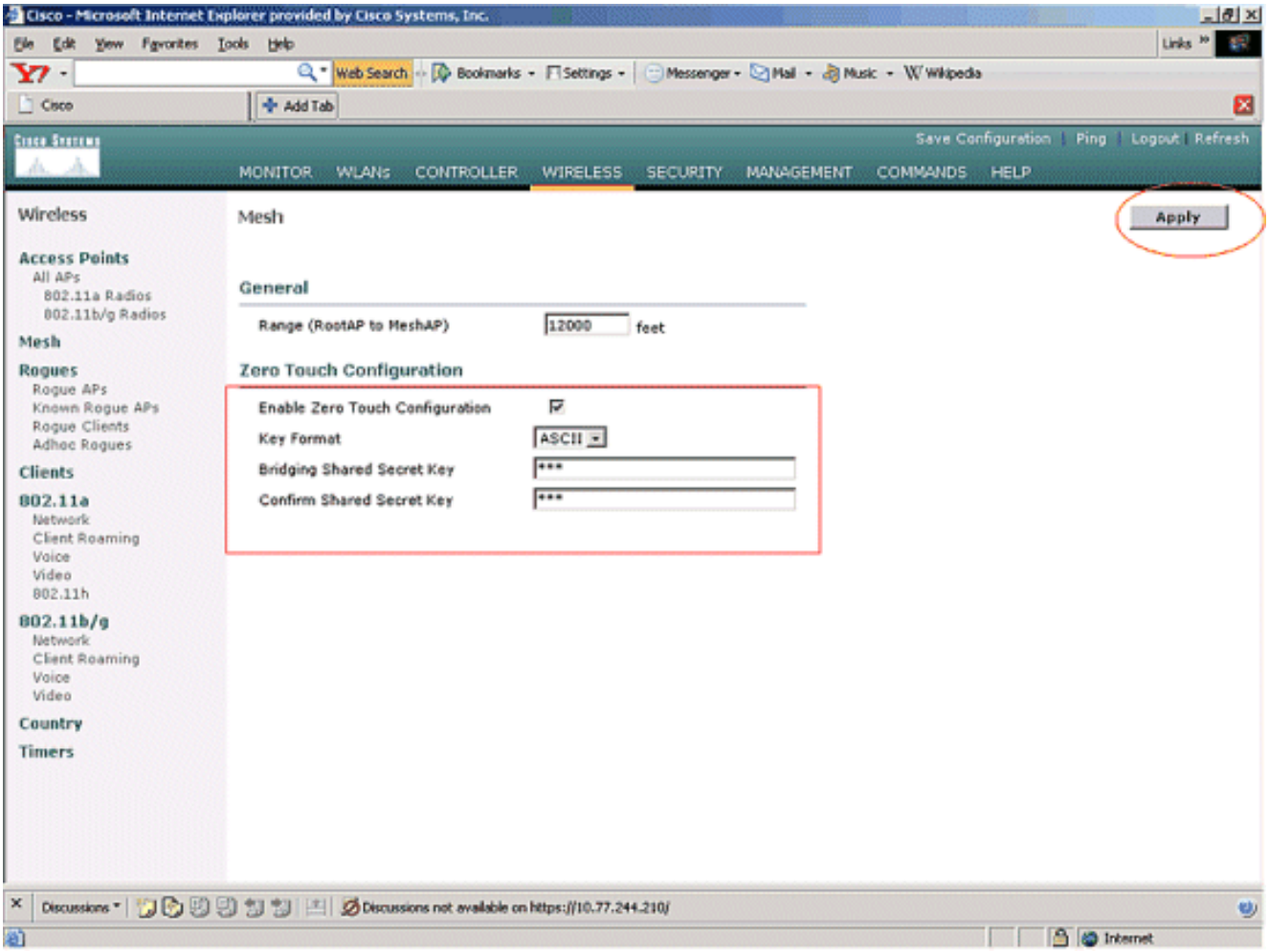
Vous avez maintenant configuré vos points d'accès en tant que RAP et MAP, selon les besoins, ainsi que leurs paramètres de pontage. Activez **la configuration Zero-Touch sur le WLC** de sorte que, une fois que le MAP est retiré de sa connexion câblée avec le WLC et amené au réseau de production (à l'autre extrémité du réseau maillé point à point), le MAP soit en mesure d'établir une connexion LWAPP sécurisée avec le WLC sans aucune connexion câblée au WLC. La valeur par défaut pour la configuration automatique sur le WLC est activée (ou cochée).

Complétez ces étapes afin de configurer la configuration sans intervention sur le WLC.

1. Dans l'interface graphique du contrôleur, sélectionnez **Wireless > Mesh** et cliquez sur **Enable Zero Touch Configuration**.



2. Sélectionnez le format de clé (ASCII ou Hex).
3. Saisissez la clé secrète partagée de pontage.Ce champ n'est activé que si l'option de configuration automatique est activée. Il s'agit de la clé fournie aux points d'accès maillés (MAP) pour qu'ils établissent une connexion LWAPP sécurisée avec le contrôleur LAN sans fil Cisco, tandis que le MAP se connecte sans fil depuis l'autre extrémité du réseau maillé. La clé doit comporter au moins 32 caractères au format hexadécimal ou ASCII. Une clé secrète partagée par défaut est attribuée au stade de fabrication. Il n'est pas visible pour vous.Cet exemple utilise la clé secrète partagée de pontage **cisco**.Lorsque vous modifiez la clé secrète partagée, le contrôleur LAN sans fil Cisco envoie automatiquement la modification à tous les RAP, ce qui entraîne la perte de connectivité des PAP jusqu'à ce qu'ils soient en mesure d'obtenir la nouvelle clé secrète partagée auprès du contrôleur LAN sans fil Cisco.
4. Saisissez à nouveau la clé secrète partagée de pontage dans le champ **Confirmer la clé secrète partagée**.
5. Cliquez sur Apply. Cette capture d'écran explique les étapes 3 à 5.



Si la configuration sans intervention est activée sur le contrôleur LAN sans fil Cisco et que le MAP est déplacé vers l'autre extrémité du réseau maillé, les RAP et les MAP effectuent cette opération pour effectuer une configuration sans intervention sécurisée :

1. S'il s'agit d'un RAP, il dispose déjà d'une connexion LWAPP sécurisée au contrôleur LAN sans fil Cisco et utilise l'interface de liaison RAP configurée (par défaut : 802.11a).
2. S'il s'agit d'un MAP, il analyse les interfaces de liaison et les canaux pour les points d'accès maillés voisins. Lorsqu'il trouve un point d'accès maillé voisin avec le même **nom de groupe de pontage** (configuré dans le cadre des paramètres de pontage) et un chemin vers le contrôleur LAN sans fil Cisco, il fait de ce point d'accès maillé son parent. Si le MAP détecte plusieurs points d'accès maillés voisins, il utilise un algorithme de moindre coût pour déterminer quel parent a le meilleur chemin vers le contrôleur LAN sans fil Cisco.Afin de configurer une connexion LWAPP sécurisée avec le contrôleur LAN sans fil Cisco, le MAP envoie sa clé secrète partagée par défaut, qui est déjà disponible au stade de fabrication du point d'accès, et son adresse MAC pour configurer une connexion sécurisée temporaire. Le contrôleur de réseau local sans fil Cisco valide l'adresse MAC par rapport à la liste de filtrage MAC et, s'il est trouvé, envoie la clé secrète partagée, qui est configurée dans le cadre du paramètre de configuration automatique au MAP et se déconnecte. Le MAP stocke la clé secrète partagée et l'utilise pour configurer une connexion LWAPP sécurisée.Si un MAP perd la connexion au contrôleur LAN sans fil Cisco, il recherche des voisins valides qui utilisent le nom du groupe de ponts de point d'accès maillé et analyse les interfaces et les canaux de liaison. Lorsqu'il trouve un point d'accès maillé voisin, il fait de ce point d'accès maillé son parent. S'il possède déjà une clé secrète partagée, il l'utilise et tente de configurer une connexion LWAPP sécurisée au contrôleur LAN sans fil Cisco. Si la clé secrète partagée ne fonctionne pas, elle utilise la clé secrète par défaut partagée et tente d'obtenir une

nouvelle clé secrète partagée.

Vérification

- Après toutes les configurations, déconnectez le MAP du réseau câblé connecté au WLC et déplacez-le vers l'autre extrémité du maillage. Mettez le maillage sous tension. Avec toutes les configurations appropriées, le MAP peut localiser le RAP comme parent et s'enregistrer sans fil auprès du contrôleur.
- Sur la CLI du WLC, 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 :La commande **show mesh path** *AP name* est utilisée pour vérifier le chemin du contrôleur pour atteindre l'AP spécifié. Voici un exemple :

```
(Cisco Controller) >show mesh path ap:71:1b:00

00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON
(86B), snrUp 10, snrDown 9, linkSnr 8
00:0B:85:7F:47:00 is RAP
```

Cette sortie indique que pour atteindre le AP **ap:71:1b:00(MAP)**, le contrôleur a l'AP avec l'adresse MAC **00:0B:85:7F:47:00** dans son chemin, et ce AP est un **RAP**.

```
(Cisco Controller) >show mesh path ap:7f:47:00

00:0B:85:7F:47:00 is RAP
```

Cette sortie indique que le point d'accès **ap:7f:47:00** est directement connecté au contrôleur puisque ce point d'accès est un **RAP**.La commande **show mesh neigh** *AP name* affiche les informations de voisinage de l'AP spécifié. Voici un exemple :

```
(Cisco Controller) >show mesh neigh ap:7f:47:00

AP MAC : 00:0B:85:71:1B:00

FLAGS : 160 CHILD
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
Numroutes 0, snr 0, snrUp 0, snrDown 10, linkSnr 0
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr  0
lastUpdate   1193504822 (Sat Oct 27 17:07:02 2007)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:0B:85:71:1B:00
```

Cette sortie indique que le voisin de l'AP **ap:7f:47:00** est **MAP 00:0B:85:71:1B:00**, et la MAP est un **ENFANT** à cet AP puisque ce AP est un RAP.

```
(Cisco Controller) >show mesh neigh ap:71:1b:00


AP MAC : 00:0B:85:7F:47:00

FLAGS : 86A NEIGH PARENT BEACON
worstDv 0, Ant 0, channel 161, biters 0, ppiters 10
Numroutes 1, snr 0, snrUp 10, snrDown 10, linkSnr 8
adjustedEase 213, unadjustedEase 256
txParent 106, rxParent 5
poorSnr  5
lastUpdate   1193504822 (Sat Oct 27 17:07:02 2007)
```

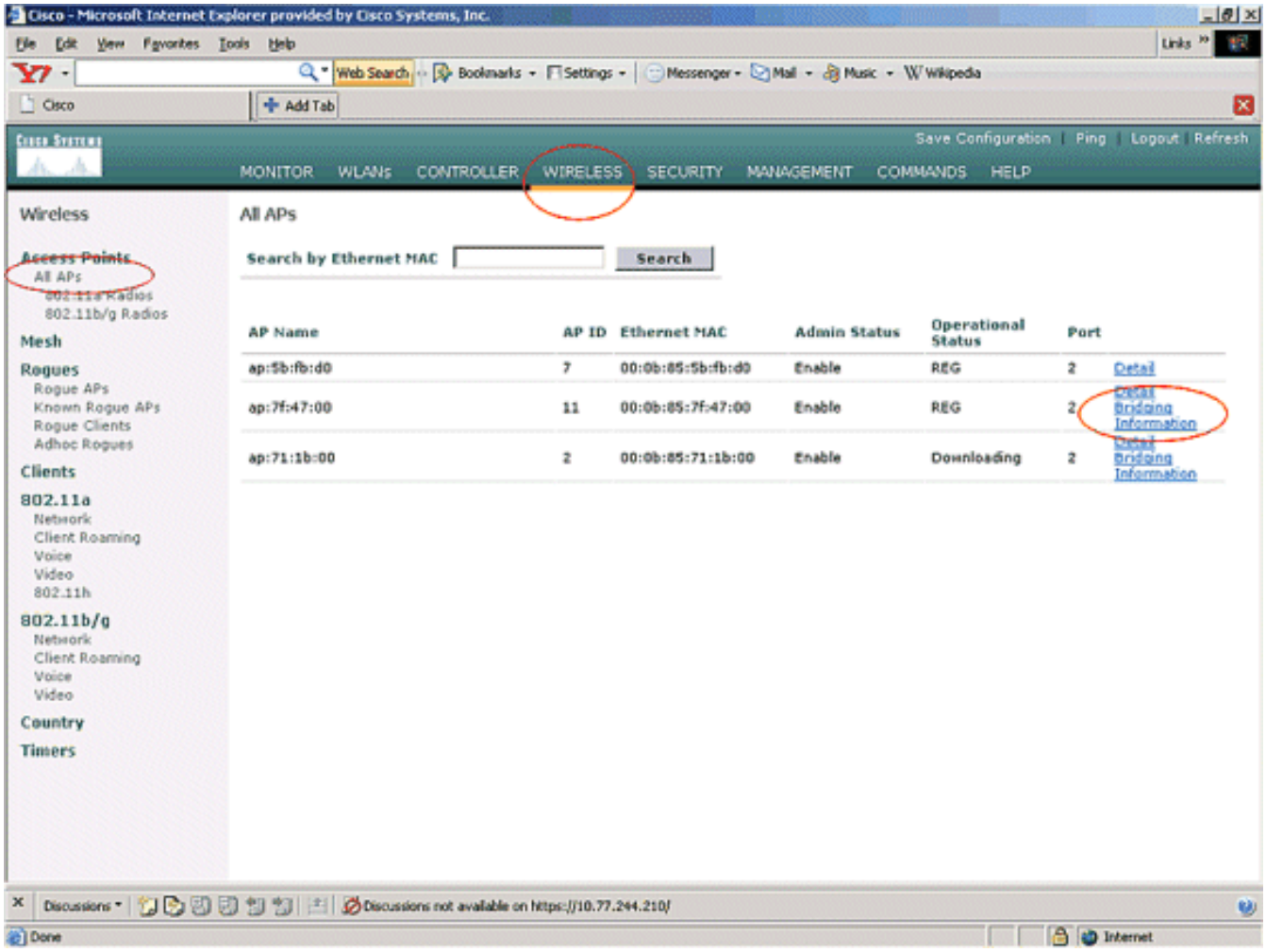
```
parentChange 1009152029 (Mon Dec 24 00:00:29 2001)
Per antenna smoothed snr values: 8 0 0 0
Vector through 00:0B:85:7F:47:00
Vector ease 1 -1,  FWD:  00:0B:85:7F:47:00
```

Cette sortie indique que le voisin de l'AP **ap:71:1b:00** est **RAP 00:0B:85:7F:47:00**, et le RAP est un **PARENT** à cet AP.

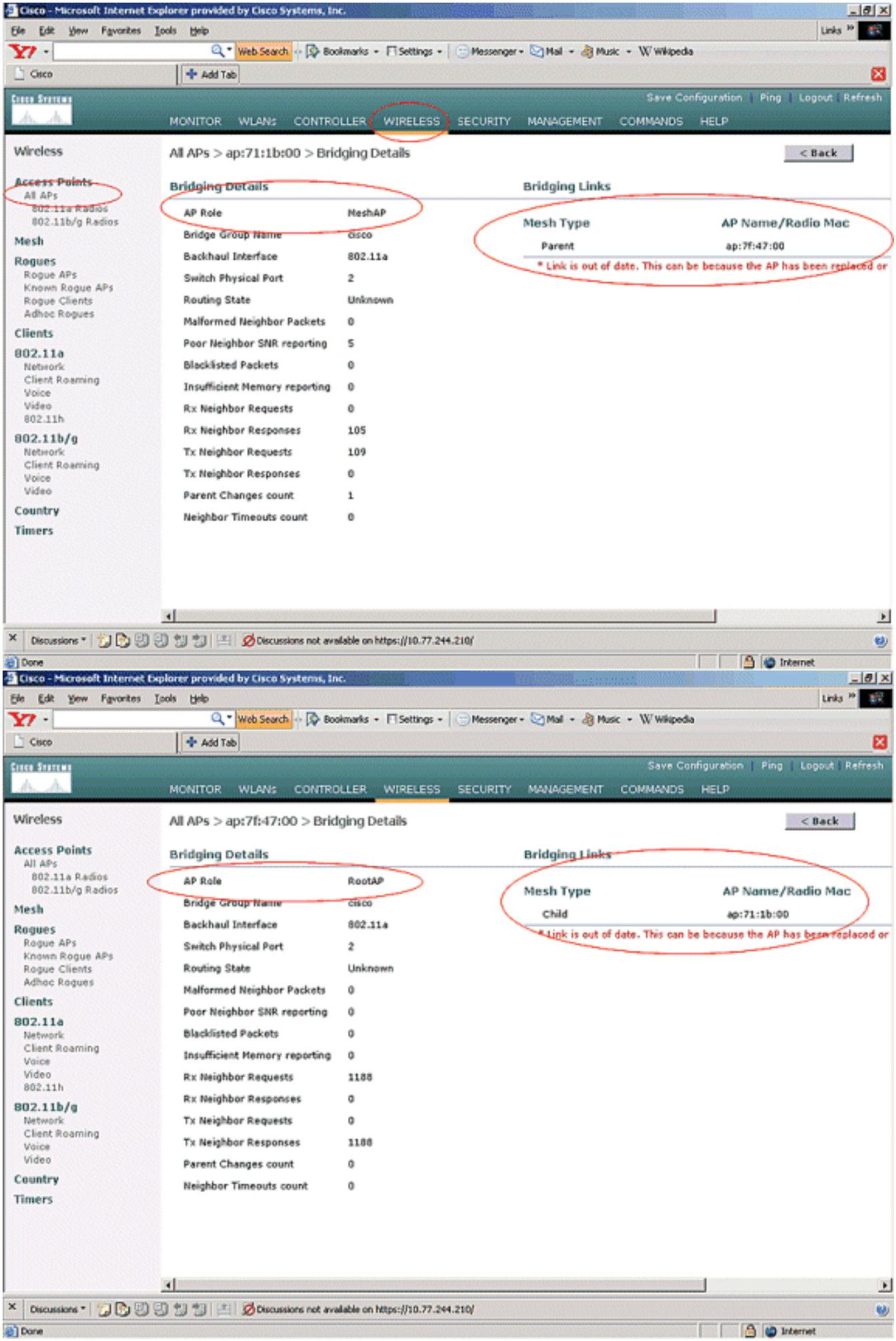
- La commande **show mesh summary** *Ap name* affiche les détails de maillage du point d'accès spécifié. Voici un exemple :

```
(Cisco Controller) >show mesh summary ap:71:1b:00

00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON (86B),
 snrUp 10, snrDown 10, linkSnr 8


(Cisco Controller) >show mesh summary ap:7f:47:00

00:0B:85:71:1B:00 state CHILD (160), snrUp 0, snrDown 10, linkSnr 0
```

- Il est possible de vérifier la même chose à partir de l'interface graphique du contrôleur en procédant comme suit :Dans l'interface graphique du WLC, cliquez sur **Wireless > All APs**.Cliquez sur le lien **Bridging Information** pour votre AP1510 afin d'accéder à la page **Bridging Information** de l'AP.



La page **Détails du pontage** AP répertorie tous les détails du pontage de ce point d'accès, tels que le rôle AP et les informations de type de maillage.



Sur la CLI du WLC, vous pouvez utiliser les commandes **show mesh path** *Cisco AP* et **show mesh**

neigh ***Cisco AP*** afin de vérifier que les AP sont enregistrés auprès du WLC :

Afin de vérifier si votre pontage Ethernet fonctionne correctement, procédez comme suit :

1. Connectez un réseau Ethernet (réseau local Ethernet B, comme indiqué dans le schéma de réseau) au port Ethernet du MAP via un commutateur. Assurez-vous que le commutateur est correctement configuré selon les besoins.
2. Vérifiez la connectivité entre le LAN Ethernet B sur la carte et le réseau câblé (LAN Ethernet A tel qu'indiqué dans le schéma de réseau) connecté au RAP derrière le WLC à l'aide de la commande **ping**. Si **ping** réussit, cela indique que le pontage Ethernet fonctionne correctement.

Dépannage

Ces commandes de dépannage peuvent être utiles :

Dépannage des commandes

- **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 commande indique clairement si un point d'accès ne peut pas rejoindre le WLC en raison d'une non-correspondance de période de validité de certification.C'est la sortie de la commande **debug pm pki enable sur le contrôleur :**

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc()
   for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco
   Systems.
.........................
.........................
.........................
.........................
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
                          validity interval: make sure the controller
                          time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

Dans cette sortie, notez l'information mise en valeur. Ces informations indiquent clairement que le temps du contrôleur est en dehors de l'intervalle de validité du certificat de l'AP, de sorte que l'AP ne peut pas s'enregistrer auprès du contrôleur. Les certificats installés dans AP ont un intervalle de validité prédéfini. Le temps du contrôleur doit être défini de telle manière

qu'il se trouve dans l'intervalle de validité du certificat de l'AP.Référez-vous au document Outils de mise à niveau LWAPP - Conseils de dépannage pour plus d'informations sur les problèmes possibles dans un LAP qui s'enregistre auprès du contrôleur.Référez-vous à Dépannage d'un réseau maillé pour plus d'informations sur le dépannage d'un réseau maillé.

- Voici des commandes de débogage supplémentaires qui peuvent être utiles :**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.

Informations connexes

- Guide de déploiement de la solution de réseau maillé Cisco
- Installation et configuration du point d'accès maillé
- Exemple de configuration de réseau à maillage de contrôleurs de réseau local sans fil
- Guide de démarrage rapide : Points d'accès extérieur légers pour réseau maillé de la gamme Cisco Aironet 1500
- Guide d'installation matérielle du point d'accès extérieur pour réseau maillé de la gamme Cisco Aironet 1500
- Instructions d'installation de l'injecteur de puissance du point d'accès Cisco Aironet 1500
- Points d'accès Q et A de la gamme Cisco Aironet 1500
- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Support et documentation techniques - Cisco Systems