Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)

Contenu

Introduction

Ce document explique les différentes méthodes que le Point d'accès léger (recouvrements) emploie afin de découvrir WLCs. Dans une architecture de réseau sans fil unifié Cisco, les points d'accès (AP) sont légers. Cela signifie qu'ils ne peuvent pas agir indépendamment d'un contrôleur de LAN sans fil (WLC). Les recouvrements doivent d'abord découvrir le WLCs et s'inscrire à eux avant les clients sans fil de service de recouvrements. Il explique également le processus d'enregistrement qui se produit entre le LAP et le WLC après la phase de détection.

> Remarque: Dans la version 5.2 de logiciel contrôleur ou plus tard, des recouvrements de Cisco emploient le contrôle de norme IETF et l'approvisionnement du protocole Sans fil des Points d'accès (CAPWAP) afin de communiquer entre le contrôleur et d'autres recouvrements sur le réseau. Versions de logiciel de logiciel contrôleur plus tôt que l'utilisation de version 5.2 le point d'accès léger Protocol (LWAPP) pour ces transmissions, qui est couvert dans ce document. Voyez pour dépanner un point d'accès léger ne joignant pas un contrôleur LAN Sans fil pour l'enregistrement AP et comment dépanner avec le protocole CAPWAP.

Conditions préalables

Conditions requises

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

- Connaissance du protocole Lightweight Access Point Protocol (LWAPP).
- Connaissance de la façon de configurer des paramètres de base sur le WLC.Si vous êtes un nouvel utilisateur et n'avez pas configuré le WLC pour le fonctionnement de base, référez-vous à utiliser la section de magicien de configuration du *guide de configuration Sans fil de contrôleur LAN de Cisco, version 6.0*.
- Connaissance de la façon de configurer le serveur DHCP Microsoft Windows 2000 et le serveur du Système de noms de domaine (DNS).

Composants utilisés

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

- WLC de la gamme Cisco 4400 qui exécute le microprogramme 4.0.217.0
- LAP de la gamme Cisco 1000
- Serveur DHCP de Windows 2000
- Serveur DNS Windows 2000

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

Les WLC et LAP Cisco font partie de l'architecture de réseau sans fil unifié Cisco. L'architecture de réseau sans fil unifié Cisco centralise la configuration et le contrôle des WLAN sur le WLC. Les LAP ne peuvent pas agir indépendamment du WLC. Le WLC gère les configurations et le microprogramme des LAP. Les LAP ont un déploiement « mains libres », et aucune configuration individuelle des LAP n'est nécessaire.

Afin que les WLC puissent gérer le LAP, le LAP doit détecter le contrôleur et s'enregistrer auprès du WLC. Une fois le LAP enregistré auprès du WLC, des messages LWAPP sont échangés et l'AP lance un téléchargement du microprogramme à partir du WLC (s'il y a une non-correspondance de versions entre l'AP et le WLC). Si le microprogramme à bord de l'AP n'est pas le même que celui du WLC, l'AP télécharge le microprogramme pour rester synchronisé avec le WLC. Le mécanisme de téléchargement du microprogramme utilise LWAPP. Ensuite, le WLC fournit au LAP les configurations qui sont spécifiques aux WLAN de sorte que le LAP puisse accepter des associations de clients. Ces configurations spécifiques aux WLAN incluent ceci :

- Service Set Identifier (SSID)
- Paramètres de sécurité
- Paramètres IEEE 802.11, tels que :Débit de donnéesCanaux radiosNiveaux de puissance

Il y a des différentes méthodes qu'un RECOUVREMENT emploie afin de découvrir le WLC. Ce document décrites différentes méthodes que le LAP peut utiliser pour s'enregistrer auprès du

WLC. Mais d'abord, le document explique la séquence d'opérations qui se produisent quand un RECOUVREMENT s'inscrit au WLC.

> Remarque: L'interface de gestion est l'interface par défaut pour la gestion intrabande du WLC et de la connectivité à des services d'entreprise tels que des serveurs AAA. L'interface de gestion est également utilisée pour des communications de couche 2 entre le WLC et des points d'accès. L'interface de gestion est la seule adresse IP d'interface intrabande qui peut constamment faire l'objet d'un ping sur le WLC.

> Remarque: Un WLC a une ou plusieurs interfaces de gestionnaire AP qui sont utilisées pour toutes les communications de couche 3 entre le WLC et les points d'accès légers après que le point d'accès détecte le contrôleur. L'adresse IP du gestionnaire AP est utilisée comme source du tunnel pour les paquets LWAPP en provenance du WLC vers le point d'accès, et comme destination des paquets LWAPP en provenance du point d'accès vers le WLC. Le gestionnaire AP doit avoir une adresse IP unique. Habituellement, cela est configuré sur le même sous-réseau que l'interface de gestion, mais ce n'est pas nécessairement une condition requise. L'adresse IP d'un gestionnaire AP ne peut pas faire l'objet d'un ping à partir de l'extérieur du WLC. Référez-vous à la section Configuration des ports et des interfaces du Guide de configuration du contrôleur de LAN sans fil Cisco pour plus d'informations.

Enregistrer le LAP auprès du WLC

Cette séquence d'opérations doit se produire pour qu'un RECOUVREMENT s'enregistre à un WLC :

1. Les LAP émettent une demande de détection DHCP pour obtenir une adresse IP, à moins qu'une adresse IP statique ait été précédemment configurée.
2. Le LAP envoie des messages de demande de détection LWAPP aux WLC.
3. Tout WLC qui reçoit la demande de détection LWAPP répond avec un message de réponse de détection LWAPP.
4. Àpartir des réponses de détection LWAPP qu'il reçoit, le LAP sélectionne un WLC à joindre.
5. Le LAP envoie alors une demande de jonction LWAPP au WLC et attend une réponse de jonction LWAPP.
6. Le WLC valide le LAP, puis lui envoie une réponse de jonction LWAPP.
7. Le LAP valide le WLC, ce qui termine le processus de détection et de jonction. Le processus de jonction LWAPP inclut l'authentification réciproque et la dérivation des clés de chiffrement, ce qui est utilisé pour sécuriser le processus de jonction et les futurs messages de contrôle LWAPP.
8. Le LAP s'enregistre auprès du contrôleur.

Le premier problème auquel le LAP est confronté est la façon de déterminer où envoyer les demandes de détection LWAPP (étape 2). Le LAP emploie une procédure de recherche et un algorithme de détection afin de déterminer la liste des WLC auxquels le LAP peut envoyer les messages de demande de détection.

Cette procédure décrit le processus de recherche :

1. Le LAP émet une requête DHCP à un serveur DHCP pour obtenir une adresse IP, à moins

qu'une affectation ait été faite précédemment avec des adresses IP statiques.

2. Si le mode LWAPP de couche 2 est pris en charge sur le LAP, le LAP diffuse un message de détection LWAPP dans une trame LWAPP de couche 2. Tout WLC qui est connecté au réseau et qui est configuré pour le mode LWAPP de couche 2 répond avec une réponse de détection de couche 2. Si le LAP ne prend pas en charge le mode de couche 2, ou si le WLC ou le LAP ne reçoit pas une réponse de détection LWAPP à la diffusion des messages de détection LWAPP de couche 2, le LAP passe à l'étape 3.
3. Si l'étape 1 échoue, ou si le LAP ou le WLC ne prend pas en charge le mode LWAPP de couche 2, le LAP essaie une détection des WLC LWAPP de couche 3.Consultez la section Algorithme de détection des WLC LWAPP de couche 3 de ce document.
4. Si l'étape 3 échoue, le LAP se réinitialise et revient à l'étape 1.

Remarque: Si vous voulez spécifier une adresse IP pour un point d'accès au lieu qu'il y en ait une attribuée automatiquement par un serveur DHCP, vous pouvez utiliser la GUI ou l'interface de ligne de commande du contrôleur pour configurer une adresse IP statique pour le point d'accès. Référez-vous à la section Configuration d'une adresse IP statique sur un point d'accès léger du guide de configuration des WLC pour plus d'informations. Si une adresse IP statique est attribuée au LAP et que ce dernier ne peut pas atteindre le WLC, il revient à DHCP.

Algorithme de détection des WLC LWAPP de couche 2

La communication LWAPP entre l'AP et le WLC peut être dans des trames Ethernet de couche 2 natives. Cela est connu sous le nom de « mode LWAPP de couche 2 ». Bien que défini dans l'ébauche de RFC, le mode LWAPP de couche 2 est considéré comme désapprouvé dans l'implémentation de Cisco. Seuls les LAP de la gamme Cisco 1000 prennent en charge le mode LWAPP de couche 2. En outre, le mode LWAPP de couche 2 n'est pas pris en charge sur les WLC de la gamme Cisco 2000. Ces WLC prennent en charge le mode LWAPP de couche 3.

Voici la première méthode qu'un LAP utilise pour détecter un WLC. Les LAP qui prennent en charge le mode LWAPP de couche 2 diffusent un message de demande de détection LWAPP dans une trame LWAPP de couche 2. S'il y a un WLC du réseau configuré pour le mode LWAPP de couche 2, le contrôleur réagit avec une réponse de détection. Le LAP passe alors à la phase de jonction (voir l'étape 5 de la section Enregistrer le LAP auprès du WLC).

Cette sortie de la commande **debug lwapp events enable** montre la séquence d'événements qui se produisent quand un LAP utilisant le mode LWAPP de couche 2 s'enregistre auprès du WLC :

Remarque: Les lignes de cette sortie ont été déplacées sur deux lignes en raison de contraintes d'espace.

```
Thu Sep 27 00:24:25 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 '2' Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 2 Thu Sep 27
00:24:40 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:48:53:c0 on port '2' Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:48:53:C0 rxNonce 00:0B:85:51:5A:E0 Thu Sep 27 00:24:40 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 27
00:24:40 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index
48)Switch IP: 0.0.0.0, Switch Port: 0, intIfNum 2, vlanId 0AP IP: 0.0.0.0, AP Port: 0, next hop
MAC: 00:0b:85:51:5a:e0 Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully transmission of
LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register
```

```
LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register
LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

Algorithme de détection des WLC LWAPP de couche 3

Les LAP utilisent l'algorithme de détection de couche 3 si la méthode de détection de couche 2 n'est pas prise en charge ou échoue. L'algorithme de détection de couche 3 utilise des options différentes afin d'essayer de détecter des WLC. L'algorithme de détection des WLC LWAPP de couche 3 est utilisé pour générer une liste de contrôleurs. Une fois la liste de contrôleurs générée, l'AP sélectionne un WLC et essaie de joindre le WLC.

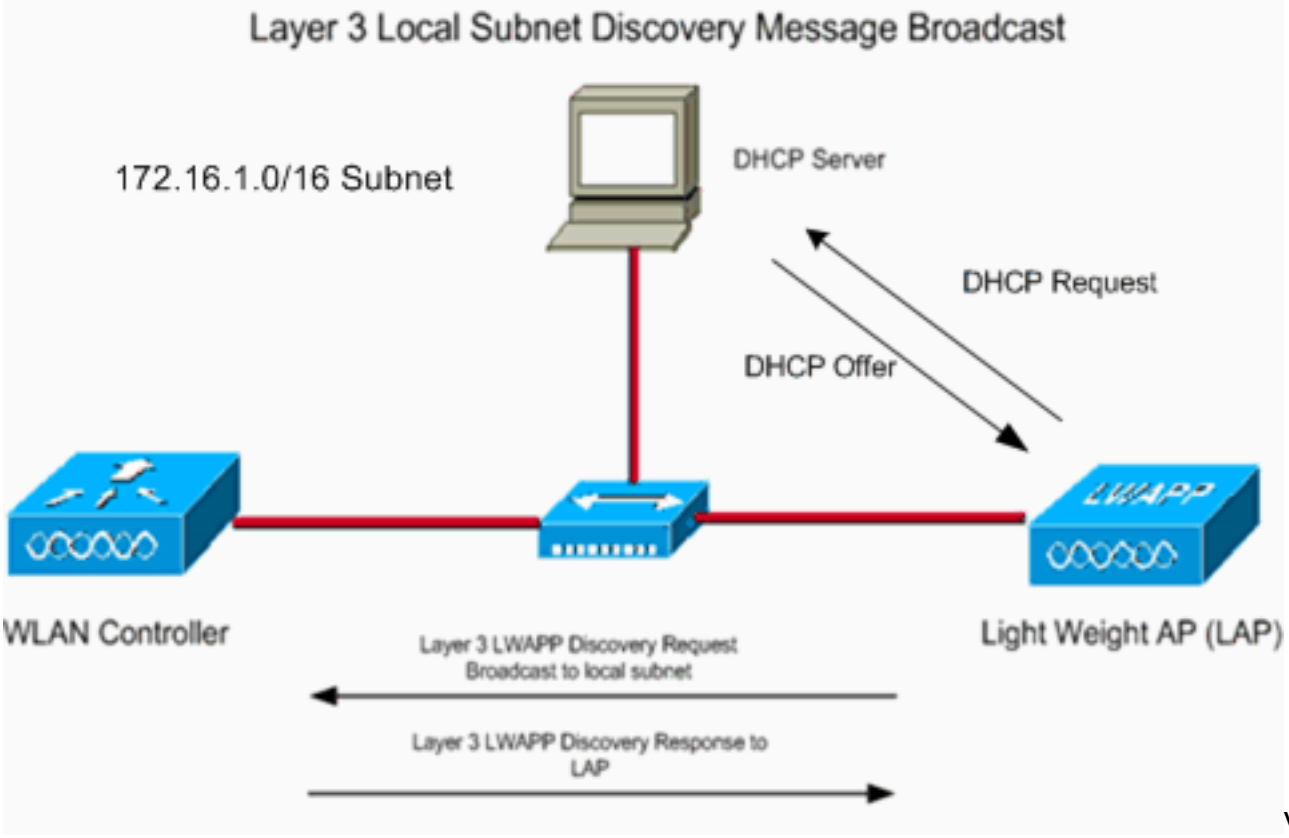
L'algorithme de détection des WLC LWAPP de couche 3 se répète jusqu'à ce qu'au moins un WLC soit trouvé et joint.

> Remarque: Pendant la détection des WLC LWAPP de couche 3, l'AP effectue toujours toutes les étapes 1 à 5 de cette section afin de générer une liste de WLC candidats. Une fois que l'AP a terminé les étapes de détection des WLC LWAPP, il sélectionne un WLC dans la liste des WLC candidats sur la base de certains critères, puis envoie à ce WLC une demande de jonction LWAPP.

Chaque exemple de scénario expliqué dans cette section est indépendant des autres et est fourni seulement pour vous permettre de comprendre la façon dont chaque étape du processus de détection fonctionne. Le LAP emploie toutes les étapes de détection afin de rechercher une liste de WLC candidats avant de sélectionner un WLC à joindre.

Cette procédure décrit les étapes que l'algorithme de détection de couche 3 suit dans la tentative de détecter des WLC :

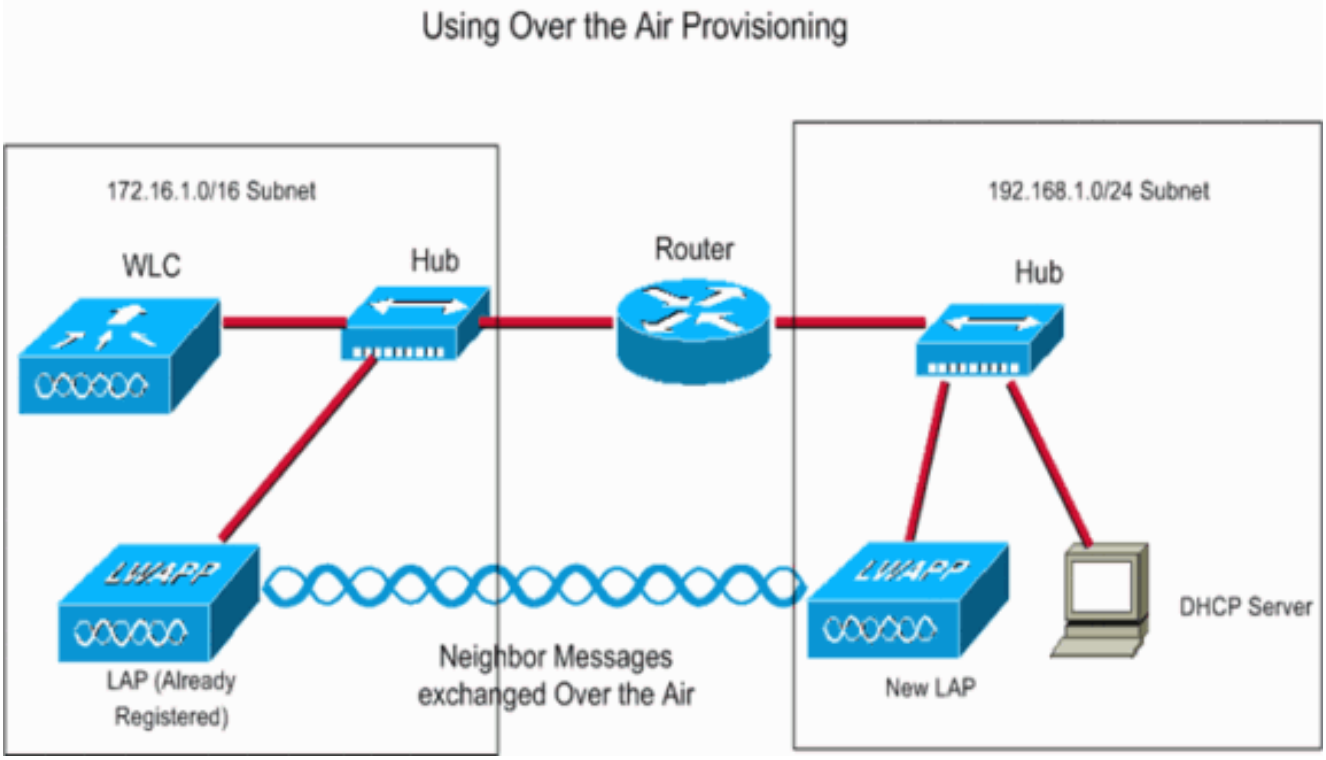
1. Une fois que le LAP obtient une adresse IP du serveur DHCP, le LAP commence le processus de détection suivant :Le LAP diffuse un message de détection LWAPP de couche 3 sur le sous-réseau IP local. Tout WLC qui est configuré pour le mode LWAPP de couche 3 et qui est connecté au même sous-réseau local reçoit le message de détection LWAPP de couche 3.Chacun des WLC qui reçoit le message de détection LWAPP répond avec un message de réponse de détection LWAPP monodiffusion au LAP.



Voici un exemple. Supposez que vous avez un WLC et un RECOUVREMENT dans le même sous-réseau (172.16.1.0/16). Vous avez également un sous-réseau du serveur DHCP. Quand le LAP est activé, il envoie une requête DHCP, avec l'espoir qu'un serveur DHCP fournira une adresse IP. Une fois que le LAP obtient une adresse IP du serveur DHCP, le LAP diffuse un message de détection LWAPP de couche 3 à son sous-réseau local. Puisque le WLC est également sur le même sous-réseau, il reçoit la demande de détection LWAPP du LAP et réagit avec une réponse de détection LWAPP de couche 3. L'exemple de sortie suivant de la commande **debug lwapp events enable** montre ce processus de détection :`(Cisco Controller) >`**`debug lwapp events enable`** `Mon May 22 12:00:21 2006:` **`Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '1'`** `Mon May 22 12:00:21 2006:` **`Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 1`** La sortie de la commande **debug lwapp packet enable** pour la détection de diffusion de sous-réseau local ressemble à cet exemple :`(Cisco Controller) >`**`debug lwapp packet enable`** `Tue May 23 12:37:50 2006: Start of Packet Tue May 23 12:37:50 2006: Ethernet Source MAC (LRAD): 00:0B:85:51:5A:E0 Tue May 23 12:37:50 2006: Msg Type : Tue May 23 12:37:50 2006: DISCOVERY_REQUEST Tue May 23 12:37:50 2006: Msg Length : 31 Tue May 23 12:37:50 2006: Msg SeqNum : 0 Tue May 23 12:37:50 2006:` **`IE : UNKNOWN IE 58`** `Tue May 23 12:37:50 2006: IE Length : 1 Tue May 23 12:37:50 2006: Decode routine not available, Printing Hex Dump Tue May 23 12:37:50 2006: 00000000:` **`00`** Notez les lignes qui sont marquées en gras. La valeur du paramètre **IE 58** indique le type de détection :**`0 - broadcast 1 - configured 2 - OTAP 3 - dhcp server 4 - dns`** Étant donné que c'est une diffusion de sous-réseau local, la valeur du paramètre **IE 58** est **0** dans cette sortie de la commande **debug lwapp packet enable**.

2. Les LAP utilisent également la fonctionnalité Over-the-Air Provisioning (OTAP) pour détecter le WLC. La fonctionnalité OTAP est *désactivée par défaut* dans les versions 4.2.39.13, 5.0.68.0 et ultérieures des WLC. OTAP est *activée par défaut* dans les versions des WLC antérieures à 4.2.39.13. Voici le processus de détection quand OTAP est activée :Les LAP qui sont déjà enregistrés auprès du WLC peuvent annoncer l'adresse IP du WLC aux LAP (afin d'essayer de trouver le WLC) à l'aide de messages de voisins qui sont envoyés sans fil.Les nouveaux LAP qui essayent de détecter des WLC entendent ces messages puis

les messages de demande de détection LWAPP monodiffusion envoyés aux WLC.Les WLC qui reçoivent le message de détection LWAPP répondent par un message de détection LWAPP monodiffusion au LAP.Vous devez avoir OTAP activée seulement pendant les intervalles de configuration des AP. Une fois les AP déployés, désactivez OTAP, ce qui constitue une meilleure pratique en matière de développement. En outre, les AP Cisco Aironet (gamme 1130 AG, 1200 et 1240 AG) sont livrés avec une version complètement démontée du logiciel Cisco IOS® allégé qui s'appelle « image de récupération LWAPP de Cisco IOS ». OTAP n'est pas prise en charge sur ces AP prêts à l'emploi qui exécutent le logiciel Cisco IOS LWAPP. Quand vous mettez à niveau des AP Cisco Aironet du logiciel Cisco IOS autonome vers le mode léger, l'image de récupération LWAPP de Cisco IOS est le logiciel qui est chargé. L'image de récupération LWAPP de Cisco IOS ne prend pas en charge OTAP. Pour prendre en charge OTAP, les LAP Aironet doivent d'abord joindre un WLC afin de télécharger une image LWAPP
Cisco IOS.



Voici un exemple. Supposez que, dans le sous-réseau 172.16.1.0/16, vous avez un RECOUVREMENT qui est déjà inscrit au WLC, et l'OTAP est activé sur le WLC. Quand le nouveau LAP dans le sous-réseau 192.168.1.0/24 est activé, le LAP recherche un serveur DHCP et obtient une adresse IP (si aucune affectation n'a été faite précédemment avec une adresse IP statique). Le LAP envoie alors une demande de détection au sous-réseau local. Comme dans ce scénario, il n'y a aucun WLC dans le sous-réseau local, le LAP essaie d'utiliser OTAP pour détecter des WLC. Le LAP écoute les messages de voisins qui sont envoyés sans fil par les LAP (du sous-réseau 172.16.1.0/16) qui sont déjà enregistrés et recherche des adresses IP de WLC. À partir de la liste des adresses IP de WLC que les nouveaux LAP apprennent des messages des voisins, les nouveaux LAP envoient une demande de détection LWAPP de couche 3 aux WLC. Les WLC qui reçoivent cette demande de détection réagissent avec une réponse de détection LWAPP de couche 3. La sortie de la commande **debug lwapp event enable** suivante illustre la séquence de messages que les WLC envoient :`Tue May 23 14:37:10 2006:` **`Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'`** `Tue May 23 14:37:10 2006:` **`Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 1`** Remarque:

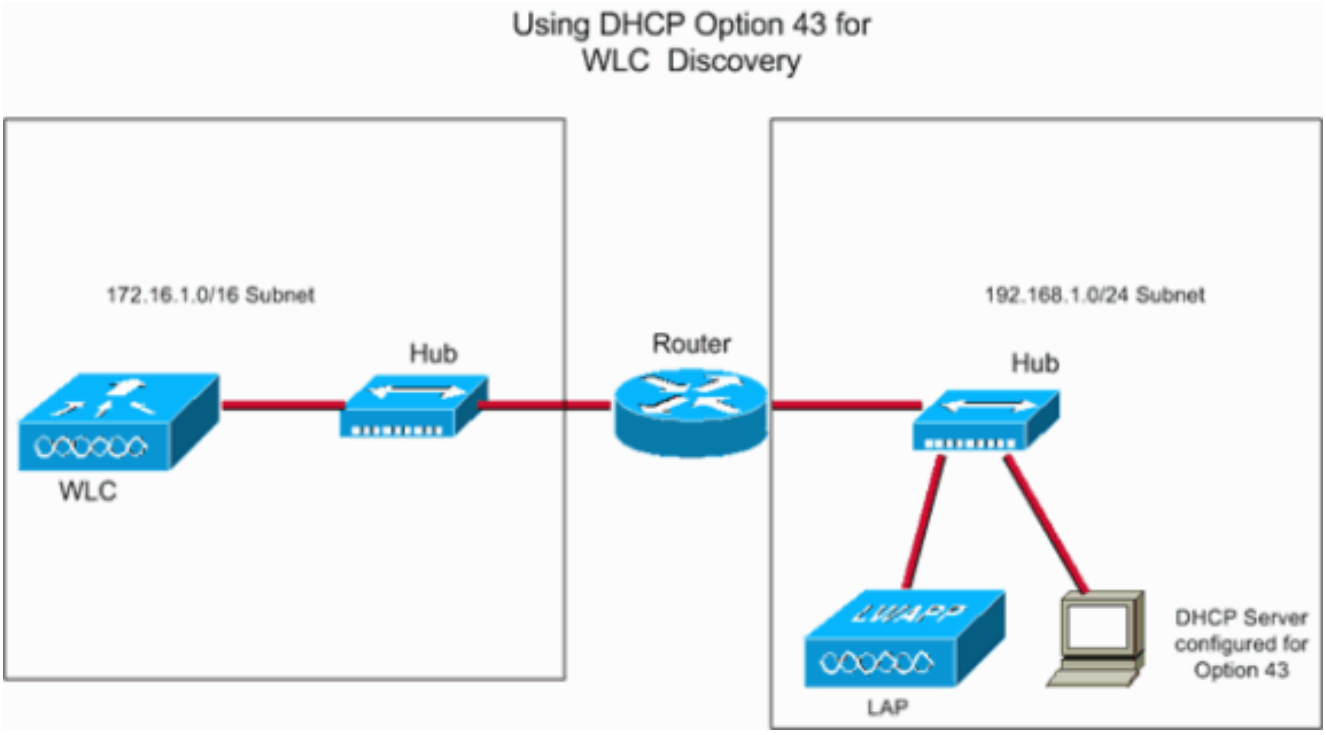
Comme le LAP connaît l'adresse IP du WLC via les messages des voisins, il envoie une demande de détection monodiffusion au WLC. De cette façon, cette étape est différente de la méthode de l'étape 1 de cette procédure, dans laquelle le sous-réseau envoie une diffusion de sous-réseau local.Remarque: La valeur du paramètre **IE 58** dans la sortie de la commande **debug lwapp packet enable** vous montre que le LAP a utilisé OTAP comme méthode de détection.

```
Tue May 23 14:21:55 2006: Start of Packet
Tue May 23 14:21:55 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 14:21:55 2006: Msg Type       :
Tue May 23 14:21:55 2006:    DISCOVERY_REQUEST
Tue May 23 14:21:55 2006: Msg Length     :   31
Tue May 23 14:21:55 2006: Msg SeqNum     :   0
Tue May 23 14:21:55 2006:
IE : UNKNOWN IE 58 Tue May 23 14:21:55 2006: IE Length : 1 Tue May 23 14:21:55 2006: Decode
routine not available, Printing Hex Dump Tue May 23 14:21:55 2006: 00000000: 02 . Tue May
23 14:21:55 2006:
```

3. Si le LAP était enregistré dans un WLC lors d'un déploiement précédent, le LAP tient à jour la liste des adresses IP WLC localement dans NVRAM. Les adresses IP enregistrées des WLC incluent tous les WLC qui sont dans les « groupes de mobilité » WLC joints précédemment. Voici le processus de détection :Les LAP envoient une demande de détection LWAPP de la couche 3 unicast à chaque adresse IP WLC que le LAP possède dans son NVRAM.Les WLC qui reçoivent le message de détection LWAPP répondent par un message de détection LWAPP monodiffusion au LAP.Voici un exemple de sortie de la commande **debug lwapp events enable** et de la commande **debug lwapp packet enable** pour cette méthode de détection WLC : Remarque: Si vous employez la commande **clear ap-config ap_name** afin de réinitialiser les valeurs par défaut du LAP, toutes les configurations de LAP sont réinitialisées. Les configurations qui sont réinitialisées incluent les adresses IP WLC qui sont enregistrées dans NVRAM. Dans ce cas, le LAP doit utiliser une autre méthode de détection du WLC.

```
(Cisco Controller) >debug lwapp events enable Tue May 23
14:37:10 2006: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b:fb:d0 to
00:0b:85:33:84:a0 on port '1' Tue May 23 14:37:10 2006: Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 1 (Cisco Controller) >debug lwapp packet
enable Tue May 23 14:45:36 2006: Start of Packet Tue May 23 14:45:36 2006: Ethernet Source
MAC (LRAD): 00:D0:58:AD:AE:CB Tue May 23 14:45:36 2006: Msg Type : Tue May 23 14:45:36
2006: DISCOVERY_REQUEST Tue May 23 14:45:36 2006: Msg Length : 31 Tue May 23 14:45:36 2006:
Msg SeqNum : 0 Tue May 23 14:45:36 2006: IE : UNKNOWN IE 58 Tue May 23 14:45:36 2006: IE
Length : 1 Tue May 23 14:45:36 2006: Decode routine not available, Printing Hex Dump Tue
May 23 14:45:36 2006: 00000000: 01 . Tue May 23 14:45:36 2006:
```

4. Vous pouvez également programmer les serveurs DHCP pour retourner les adresses IP WLC dans l'« option 43 » spécifique au constructeur dans l'offre DHCP aux LAP. Voici le processus de détection :Quand un RECOUVREMENT obtient une adresse IP du serveur DHCP, le RECOUVREMENT recherche des adresses IP WLC dans le domaine de l'option 43 de l'offre DHCP.Le LAP envoie une demande de détection LWAPP de couche 3 à chacun des WLC mentionnés dans l'option DHCP 43.Les WLC qui reçoivent le message de détection LWAPP répondent par un message de détection LWAPP monodiffusion au LAP.Remarque: Vous pouvez utiliser l'option DHCP 43 quand les LAP et les WLC sont dans différents sous-
réseaux.

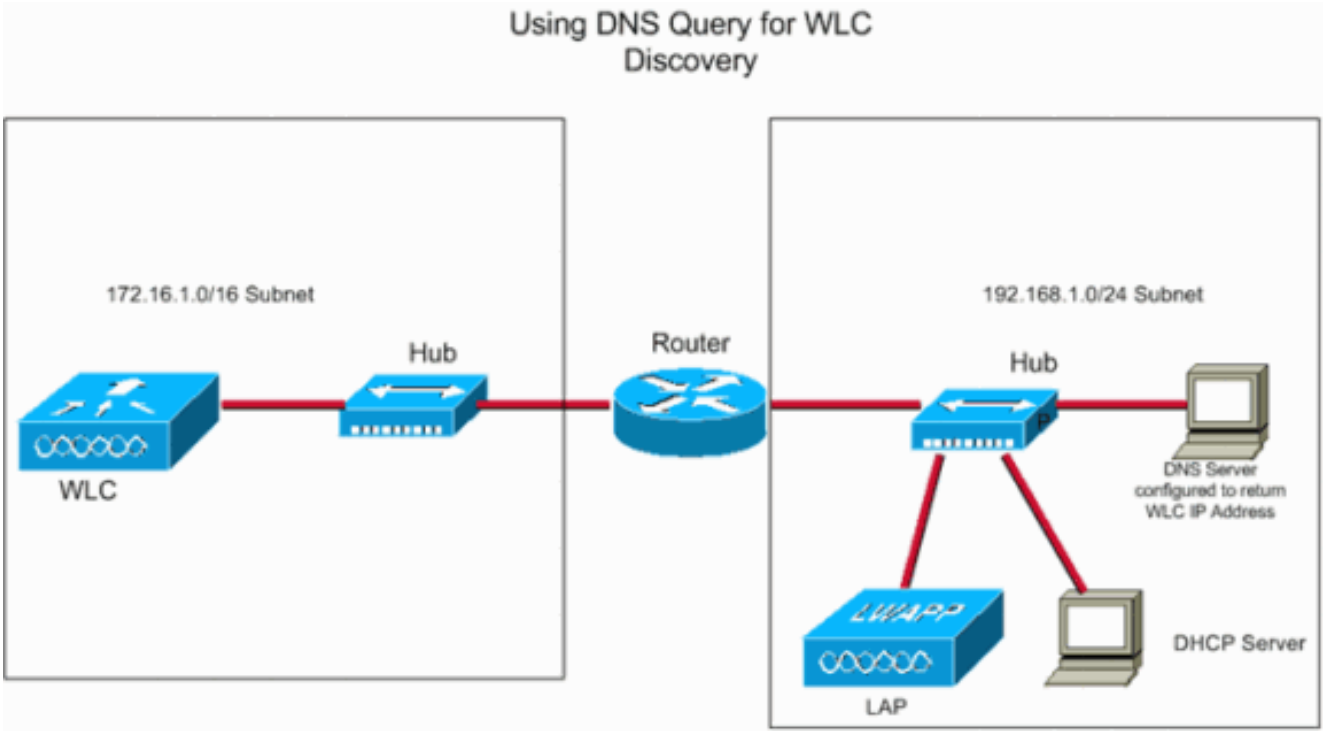


Voici un exemple de scénario. Supposez que vous avez un WLC dans un sous-réseau (par exemple, 172.16.1.0/16) et que les LAP et le serveur DHCP sont dans un sous-réseau différent (par exemple, 192.168.1.0/24). Le routage est activé entre les deux sous-réseaux. Vous pouvez configurer le serveur DHCP pour renvoyer les adresses IP WLC au LAP dans le message d'offre DHCP. Vous pouvez utiliser tout serveur DHCP qui prend en charge l'option 43.Remarque: Référez-vous à l'OPTION DHCP 43 pour un exemple de configuration des points d'accès légers Cisco Aironet pour obtenir des informations sur la façon dont configurer le serveur DHCP de Windows 2000 pour l'option 43.Ainsi, quand le LAP est mis sous tension, il recherche un serveur DHCP afin d'obtenir une adresse IP. Le serveur DHCP alloue une adresse IP au LAP et fournit également la liste des adresses IP WLC en utilisant l'option DHCP 43. Le LAP envoie une demande de détection monodiffusion à chacun des WLC. Les WLC qui écoutent ces messages réagissent avec une réponse de détection, qui lance la procédure d'enregistrement. Cette sortie de la commande **debug lwapp events enable** montre la séquence de messages LWAPP :**Tue May 23 14:43:42 2006: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'** Tue May 23 14:43:42 2006: **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 1** Voici la sortie de la commande **debug lwapp packet enable** qui indique que l'option DHCP 43 a été utilisée comme méthode de détection afin de détecter des adresses IP WLC

```
:Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type       :
Tue May 23 16:14:32 2006:    DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length     :   31
Tue May 23 16:14:32 2006: Msg SeqNum     :   0
Tue May 23 16:14:32 2006:
IE : UNKNOWN IE 58 Tue May 23 16:14:32 2006: IE Length : 1 Tue May 23 16:14:32 2006: Decode
routine not available, Printing Hex Dump Tue May 23 16:14:32 2006: 00000000: 03 . Tue May
23 16:14:32 2006:
```

5. En conclusion, vous pouvez également utiliser le serveur DNS afin de renvoyer des adresses IP WLC au LAP. Voici le processus de détection :Les tentatives de RECOUVREMENT de résoudre le nom DNS « CISCO-CAPWAP-CONTROLLER.local-domain » ou « CISCO-LWAPP-CONTROLLER.local-domain ». Remarque: Dans cette syntaxe de nom DNS, localdomain se rapporte au nom de domaine qui doit être résolu. Par exemple, si le domaine

est cisco.com, alors ce nom DNS est CISCO-LWAPP-CONTROLLER.cisco.com. L'AP doit être informé sur le nom de domaine qui doit être résolu afin qu'AP puisse envoyer la demande au serveur DNS qui a fait cette demande pour résoudre ce nom de domaine particulier. L'AP est au courant de ce nom de domaine via l'option DHCP 15. L'option DHCP 15 spécifie le nom de domaine que l'AP devrait utiliser pour la résolution DNS. Par conséquent, il est nécessaire que l'option DHCP 15 soit configurée avec l'information du nom de domaine. Cela permet au serveur DHCP qui envoie l'adresse IP du serveur DNS d'envoyer également cette information de l'option DHCP 15 (nom de domaine à résoudre) à l'AP.Quand le LAP est en mesure de résoudre ce nom vers une ou plusieurs adresses IP WLC, le LAP envoie une demande de détection de la couche 3 monodiffusion LWAPP à chacun des WLCs.Les WLC qui reçoivent le message de détection LWAPP répondent par un message de détection monodiffusion LWAPP au LAP.Cet exemple utilise la même configuration qui a été utilisée pour l'option DHCP 43 (étape 3). Cependant, dans cet exemple, le serveur DHCP n'utilise pas l'option 43. Au lieu de cela, le serveur DHCP fournit au LAP une adresse IP et donne également l'adresse IP du serveur DNS dans l'offre DHCP. Après que le RECOUVREMENT obtienne l'adresse IP de serveur DNS, le RECOUVREMENT envoie une requête DNS pour le nom DNS « CISCO-CAPWAP-CONTROLLER.local-domain » ou « CISCO-LWAPP-CONTROLLER.local-domain ». Le serveur DNS devrait être configuré afin qu'il renvoie l'adresse IP WLC pour cette requête. Quand le LAP obtient l'adresse IP WLC, le LAP commence la procédure d'enregistrement avec le
WLC.



Cette sortie de la commande **debug lwapp packet enable** montre le type de détection en tant que DNS :

```
Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type       :
Tue May 23 16:14:32 2006:    DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length     :   31
Tue May 23 16:14:32 2006: Msg SeqNum     :   0
Tue May 23 16:14:32 2006:
IE : UNKNOWN IE 58 Tue May 23 16:14:32 2006: IE Length : 1 Tue May 23 16:14:32 2006: Decode
routine not available, Printing Hex Dump Tue May 23 16:14:32 2006: 00000000: 04 . Tue May
```

`23 16:14:32 2006:` Remarque: Si, après la fin des étapes 1 à 5, le LAP ne reçoit pas une réponse de détection LWAPP, il réinitialise et relance l'algorithme de recherche.

6. **Utilisation de l'adresse ip-helper sur le routeur**Bien que ce ne soit pas une partie de l'algorithme de détection de la couche 3, c'est une méthode plus simple qui peut être utilisée quand WLC et les LAP sont dans différents sous-réseaux. Une fois que le LAP obtient une adresse IP du serveur DHCP, le LAP diffuse un message de détection LWAPP de couche 3 à son sous-réseau local. L'adresse IP du WLC est configurée comme l'adresse *ip-helper* sur le routeur. Le routeur transfère ces diffusions aux adresses IP configurées avec la commande *IP-helper* sur l'*interface* sur laquelle la diffusion est entendue. Quand vous utilisez la commande *ip helper-address*, des DIFFUSIONS DIRIGÉES, aussi bien que les unidiffusions, huit ports UDP différents sont transférés automatiquement. Ces ports sont Trivial File Transfer (TFTP) (Port 69), Système de noms de domaine (Port 53), Service horaire (Port 37), Serveur de noms de NetBIOS (Port 137), Serveur de datagramme de NetBIOS (Port 138), Protocole de démarrage (BOOTP) client et serveur (Port 67 et port 68), Service TACACS (Port 49). Puisque la diffusion LWAPP utilise le port UDP *12223*, il doit être explicitement transféré sur le routeur. Voici un exemple de scénario. Supposons que vous avez un WLC dans un sous-réseau, tel que 172.16.0.0/16, et les LAP et le serveur DHCP dans un sous-réseau différent, tel que 192.168.1.0/24. Le routage est activé entre les deux sous-réseaux. Cet exemple affiche la configuration sur le routeur :`Router(config)#interface Fastethernet 0/1 Router(config-if)#ip helper-address 172.16.0.1 !--- IP address of the WLC Router(config-if)#exit Router(config)ip forward-protocol udp 12223` Remarque: Si vous exécutez la version 5.2 ou ultérieures WLC, utilisez le numéro de port UDP 5246 parce que l'émission CAPWAP utilise le port UDP 5246.`Router(config)ip forward-protocol udp 5246`

Processus de sélection du WLC

Après que le LAP effectue les étapes 1 à 5 de l'algorithme de détection WLC LWAP de la couche 3, le LAP sélectionne un WLC de la liste des WLC candidats et envoie à ce WLC une demande de jonction LWAPP.

Les WLC incluent ces informations importantes dans la réponse de détection LWAPP :

- Le sysName du contrôleur
- Le type de contrôleur
- La capacité AP du contrôleur et son chargement AP actuel
- La balise de contrôleur principal
- Une adresse IP AP-manager

Le LAP emploie cette information pour faire une sélection de contrôleur, avec l'utilisation de ces règles de priorité :

1. Si le RECOUVREMENT a été précédemment configuré avec un contrôleur primaire, secondaire, et/ou tertiaire, le RECOUVREMENT examine le champ de sysName de contrôleur (des réponses de LWAPP discovery) afin d'essayer de trouver le WLC qui est configuré en tant que « primaire ". Si le LAP trouve un sysName correspondant pour le contrôleur primaire, le LAP envoie une demande de jointure LWAPP à ce WLC. Si le LAP ne peut pas trouver son contrôleur primaire ou si la jointure LWAPP échoue, le LAP essaie de faire correspondre le sysName du contrôleur secondaire aux réponses de détection LWAPP. Si le LAP trouve une correspondance, il envoie alors une demande de jonction LWAPP au

contrôleur secondaire. Si le WLC secondaire est introuvable ou si la demande de jonction LWAPP échoue, le LAP répète la procédure pour son contrôleur tertiaire.

2. Le LAP regarde le champ d'indicateur du contrôleur principal dans les réponses de détection LWAPP des WLC candidats si l'un de ces éléments est vrai :Aucun contrôleur primaire, secondaire et/ou tertiaire n'a été configuré pour un AP.Ces contrôleurs sont introuvables dans la liste des candidats.Les jonctions LWAPP à ces contrôleurs ont échoué.Si un WLC est configuré comme contrôleur principal, le RECOUVREMENT sélectionne ce WLC et lui envoie une demande de jonction LWAPP.
3. Si le LAP ne peut pas joindre un WLC avec succès sur la base des critères dans l'étape 1 et l'étape 2, le LAP essaie de joindre le WLC qui a la plus grande surcapacité.

Après que le LAP sélectionne un WLC, le LAP envoie une demande de jonction LWAPP au WLC. Dans la demande de jonction LWAPP, le LAP intègre un certificat X.509 signé numériquement. Quand le certificat est validé, le WLC envoie une réponse de jonction LWAPP afin d'indiquer au LAP qu'il est joint avec succès au contrôleur. Le WLC intègre son certificat X.509 signé numériquement dans la réponse de jonction LWAPP que le LAP doit valider. Après que le LAP valide le certificat WLC, le processus de jonction LWAPP est terminé.

Le LAP et le contrôleur de LAN sans fil traitent la fragmentation et le réassemblage pour le tunnel LWAPP. Ils fonctionnent selon l'hypothèse MTU 1500 octets. Ce n'est pas un paramètre configurable. Au niveau de l'AP ou du WLC, si le MTU est supérieur à 1500 octets, il fragmente le paquet et l'envoie. Le système traite jusqu'à quatre fragments depuis la version de 3.2. Les versions antérieures prennent en charge jusqu'à seulement deux fragments.

Voici un lien à un vidéo sur la Communauté de support de Cisco qui explique la procédure d'enregistrement de RECOUVREMENT :

Enregistrement de point d'accès léger avec les contrôleurs LAN Sans fil (WLCs)

Dépannez

La version du microprogramme du contrôleur est 3.2.78.0. Quand vous exécutez la commande **debug lwapp events**, cette sortie apparaît :

```
Sun Sep 3 21:49:51 2006 [ERROR] spam_lrad.c 2544:
 Security processing of Image Data failed from AP 00:17:59:67:76:80
```

Ce message d'erreur signifie que l'image 3.2.78.0 ne prend pas en charge le LAP. En fait, le contrôleur ne peut pas trouver l'image pour le LAP dans sa liste d'images. Par conséquent, le LAP ne peut pas télécharger l'image du WLC. Afin de résoudre ce problème, mettez à niveau le contrôleur vers 3.2.116.0 ou ultérieur. Ceci résout le problème et le LAP joint le contrôleur et télécharge l'image du contrôleur.

Parfois, vous pouvez rencontrer ce message d'erreur au niveau de votre contrôleur :

```
Received a Discovery Request with subnet broadcast with wrong AP IP address (source address).
```

Ce message d'erreur signifie que le contrôleur a reçu une demande de détection via une adresse IP de diffusion qui a une adresse IP source (donnée), qui n'est dans aucun sous-réseau configuré sur le contrôleur. Cela signifie également que le contrôleur a abandonné le paquet. Ceci se produit typiquement quand le client effectue une jonction de tous les VLAN autorisés au lieu de les restreindre aux VLAN sans fil.

Vous pouvez également rencontrer ce message d'erreur :

```
Received a Discovery-Request from <source MAC address>
 for someone else (IP address).
```

Cela signifie que le contrôleur a reçu une demande de détection où l'adresse IP de destination (donnée) n'est pas son adresse IP de gestion. Cela signifie également que le contrôleur a abandonné le paquet.

Il existe beaucoup de raisons pour que la jonction d'un point d'accès léger (LAP) au WLC échoue. Référez-vous à Dépanner un point d'accès léger ne joignant pas un contrôleur de LAN sans fil pour obtenir des informations sur certaines des raisons pour lesquelles un point d'accès léger (LAP) ne peut pas joindre un WLC et comment dépanner les problèmes.

Basculement d'AP entre différents groupes de mobilité

Considérez ce scénario. Le groupe de mobilité **MG1** contient deux contrôleurs, C1 et C2. Ces contrôleurs sont déployés dans un bâtiment, avec des LAP dont la charge est équilibrée entre les deux. La succursale de la société déploie un troisième contrôleur C3, et le configure pour que le groupe de mobilité **MG2.LAPs** de ce contrôleur (C3) n'échoue pas par rapport à l'un des deux autres contrôleurs. Cependant un jour, quand le contrôleur C3 redémarre, les LAP qui ont été initialement enregistrés avec C3 sont à présent enregistrés avec C1 dans le groupe de mobilité **MG1**.

Àprésent, quoique le contrôleur principal soit C3, et qu'il n'existe aucun contrôleur secondaire ou tertiaire, les LAP ont joint C1 ; un redémarrage du LAP ne le ramène pas à C3. Quel est le problème ?

La raison se cache dans le déploiement initial, la société a créé l'un de ces deux scénarios :

- Une entrée DNS pour « CISCO-CAPWAP-CONTROLLER.local-domain » ou « CISCO-

LWAPP-CONTROLLER.local-domain » à indiquer C1 ou C2.
- L'ajout d'une option DHCP 43 pour pointer vers C1 ou C2 afin de soulager l'installation initiale. Une fois l'installation du premier bâtiment terminée, ces entrées n'ont jamais été retirées.

  Remarque: L'AP peut également apprendre des contrôleurs C1 ou C2 par n'importe quelle autre méthode de détection, telle que la diffusion L3 et OTAP ; par conséquent, assurez-vous que les précautions appropriées sont prises pour qu'AP puisse seulement apprendre de ces contrôleurs d'un groupe de mobilité via l'une de ses méthodes.

Quand le contrôleur C3 s'arrête, les LAP qui sont connectés sur lui redémarrent. Ils mènent leur processus de détection comme indiqué. Ils envoient non seulement des demandes de détection à ces contrôleurs dans la configuration NVRAM, mais également aux adresses IP apprises via DNS et DHCP, qui, en conséquence, incluent C1 ou C2.

Puisque C3 est arrêté au moment de la détection, les LAP ne reçoivent pas de RÉPONSE DE DÉTECTION, ainsi ils ne peuvent pas continuer à joindre son contrôleur principal configuré et doivent joindre le contrôleur qu'ils ont connu via DHCP ou DNS.

Une fois que ces LAP ont joint C1 ou C2, ils téléchargent la nouvelle liste du groupe de mobilité, qui inclut des adresses IP pour C1 et C2 uniquement ; ainsi, s'ils sont redémarrés, ils n'ont aucun moyen d'apprendre l'adresse IP de C3 auquel envoyer des demandes de détection ; ils ne peuvent pas joindre ce contrôleur. La seule façon de ramener les LAP vers C3 est d'ajouter C3 à la liste du groupe de mobilité de C1 et C2 ou de changer l'option 43 ou l'entrée DNS.

Il y a plusieurs façons d'empêcher de tels problèmes :

- Il est suggéré que les options DNS et DHCP soient utilisées uniquement lors du déploiement initial et soient supprimées une fois le réseau configuré. De cette façon, l'AP sur le réseau n'a aucun moyen de se renseigner sur d'autres groupes de mobilité.
- Séparez les portées DHCP ou les domaines DNS. Ayez une portée pour le bâtiment 1 et une portée différente pour le bâtiment 2 dans le serveur DHCP d'entreprise ; l'administrateur peut configurer différentes adresses IP de l'option 43 pour chaque portée. Il en est de même pour les domaines DNS ; avec le nom d'hôte building1.companyname.com pour un bâtiment, et building2.companyname.com pour l'autre, vous pouvez avoir différentes options pour CISCO-LWAPP-CONTROLLER pour chaque sous-domaine.
- Vous pouvez également employer des fonctions dans le WLC pour contrôler certains comportements :Dans le cas des AP avec des certificats auto-signés (SSC), ajoutez seulement les SSC aux contrôleurs auxquels vous souhaitez joindre les AP.Dans le cas des AP avec certificats MIC (Manufacturer-Installed Certificates), employez **Authorize APs against AAA function** sur le WLC (avec la commande **config auth-list ap-policy authorize-ap enable**) pour indiquer au contrôleur de vérifier s'il devrait accepter l'AP.Afin de permettre à des AP de se joindre, utilisez une de ces options :Ajoutez-les à la liste d'autorisations du WLC : utilisez la commande **config auth-list add mic <MAC-Address>**.Ajoutez-les comme clients au serveur RADIUS. Called-Station-ID est l'adresse MAC du contrôleur. Si vous séparez les AP en groupes, vous pouvez créer des stratégies pour définir quels AP peuvent être authentifiés par rapport à quels Appeler-Station-Id.

Afin d'obtenir un RECOUVREMENT pour joindre un contrôleur qui n'est pas une partie du groupe de mobilité du contrôleur actuellement joint, vous devez s'assurer que le nom primaire de contrôleur est celui du contrôleur auquel vous souhaitez envoyer le RECOUVREMENT.

Ceci fait, il ne vous reste plus qu'à donner au LAP un moyen de détecter ce contrôleur. Cela peut être fait via l'une des méthodes décrites dans l'algorithme de détection WLC comme expliqué dans ce document.

Informations connexes

- Contrôle des points d'accès légers
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- LWAPP (mode léger) à la conversion autonome et vice versa
- Étude du trafic LWAPP
- Guide de configuration du contrôleur de LAN sans fil Cisco, version 6.0
- Support et documentation techniques - Cisco Systems