Registro de AP Ligero (LAP) a un Controlador de LAN Inalámbrica (WLC)

Contenido

Introducción

Este documento explica los métodos distintos que los Puntos de acceso ligeros (revestimientos) utilizan para descubrir el WLCs. En la arquitectura de Red Inalámbrica Unificada de Cisco , los puntos de acceso (AP) son ligeros. Esto significa que no pueden actuar independientemente de un controlador inalámbrico LAN (WLC). Los revestimientos tienen que primero descubrir que el WLCs y registrarse con ellos antes de los revestimientos mantiene a los clientes de red inalámbrica. El documento también explica el proceso de inscripción que sucede entre LAP y WLC después de la fase de la detección.

> Nota: En el Software Release 5.2 o Posterior del regulador, los revestimientos de Cisco utilizan el control de la norma de IETF y el aprovisionamiento del protocolo de los untos de acceso de red inalámbrica (CAPWAP) para comunicar entre el regulador y otros revestimientos en la red. Versiones de software del regulador anterior que el uso de la versión 5.2 el protocolo del Lightweight Access Point (LWAPP) para estas comunicaciones, que se cubre en este documento. Vea el Troubleshooting al Lightweight Access Point el no unirse a de un regulador del Wireless LAN para el registro AP y cómo resolver problemas con el protocolo CAPWAP.

Prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de Lightweight Access Point Protocol (LWAPP).
- Conocimiento de cómo configurar los parámetros básicos en el WLC.Si usted es usuario nuevo y no ha configurado el WLC para la operación básica, refiera a usar la sección del asistente de configuración de la *guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 6.0*.
- Conocimiento de cómo configurar el servidor DHCP del Microsoft Windows 2000 y el servidor del sistema de nombres del dominio (DN).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de las Cisco 4400 Series que ejecuta firmware 4.0.217.0
- Cisco 1000 Series LAP
- Windows 2000 DHCP Server
- Windows 2000 DNS Server

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Los WLC y LAP de Cisco son parte de la arquitectura de Red Inalámbrica Unificada de Cisco. La arquitectura de Red Inalámbrica Unificada de Cisco centraliza la configuración WLAN y el control en el WLC. Los LAP no pueden actuar independientemente del WLC. El WLC maneja las configuraciones LAP y firmware. Los LAP se implementan "zero touch", y no se requiere una configuración individual de LAP.

Para que el WLC puedan manejar el LAP, el LAP debe detectar el controlador y el registro con el WLC. Después de que el LAP se haya registrado al WLC, se intercambian los mensajes de LWAPP y el AP inicia una descarga de firmware del WLC (si hay una discordancia de la versión entre el AP y el WLC). Si el firmware integrado de AP no es igual que los WLC, el AP descargará el firmware para permanecer en sincronización con el WLC. El mecanismo de descarga de firmware utiliza el LWAPP. Entonces, el WLC proporciona el LAP con las configuraciones que son específicas a los WLAN de modo que el LAP pueda validar a las asociaciones del cliente. Estas configuraciones específicas de WLAN incluyen:

- Identificador de conjunto de servicios (SSID)
- Parámetros de seguridad
- Parámetros IEEE 802.11, como:Velocidad de datosCanales de radioNiveles de potencia

Hay los métodos distintos que un REVESTIMIENTO utiliza para descubrir el WLC. Este documento analiza los diferentes métodos que el LAP puede utilizar para registrar el WLC. Pero

primero, el documento explica la Secuencia de eventos que ocurre cuando un REVESTIMIENTO se registra con el WLC.

> Nota: La interfaz de administración es la interfaz predeterminada para la administración en la banda del WLC y de la Conectividad a los Enterprise Service tales como servidores de AAA. La interfaz de administración también se utiliza para las comunicaciones de la capa dos entre el WLC y los Puntos de acceso. La interfaz de administración es la única constantemente dirección IP de la interfaz de la en-banda del “pingable” en el WLC.

> Nota: UN WLC tiene una o más interfaces del administrador AP que se utilicen para todas las comunicaciones de la capa 3 entre el WLC y los Puntos de acceso ligeros después de que el Punto de acceso descubra el regulador. La dirección IP del administrador AP se utiliza como el origen de túnel para los paquetes lwapp del WLC al Punto de acceso, y como el destino para los paquetes lwapp del Punto de acceso al WLC. El administrador AP debe tener un IP Address único. Esto se configura generalmente en la misma subred como la interfaz de administración, pero esto no es necesariamente un requisito. Una dirección IP del administrador AP no es pingable desde fuera del WLC. Refiera a la sección de los puertos que configura y de las interfaces de la guía de configuración de controlador del Wireless LAN para más información.

Registre el LAP con el WLC

Esta Secuencia de eventos debe ocurrir para que un REVESTIMIENTO se registre a un WLC:

1. Los LAP emiten una solicitud de detección del DHCP para obtener una dirección IP, a menos que haya configurado previamente un dirección IP estático configurar.
2. El LAP envía los mensajes de solicitud de la detección de LWAPP a los WLC.
3. Cualquier WLC que recibe la solicitud de detección de LWAPP responde con un mensaje de respuesta de detección de LWAPP.
4. De las respuestas de detección de LWAPP que el LAP recibe, el LAP selecciona un WLC para unirse.
5. El LAP envía al WLC una solicitud de unión al LWAPP y espera una respuesta de unión al LWAPP.
6. El WLC valida el LAP y después envía una respuesta de unión de LWAPP al LAP.
7. El LAP valida el WLC, que completa la detección y se une a el proceso. El proceso de unión de LWAPP incluye la derivación de la autenticación recíproca y de la clave de cifrado, que se utiliza para asegurar los mensajes de proceso de unión y control del LWAPP futuros.
8. Los registros del LAP con el controlador.

El primer problema que enfrenta el LAP es cómo determinar dónde enviar las solicitudes de detección de LWAPP (paso 2). El LAP utiliza un procedimiento de búsqueda y un algoritmo de detección para determinar la lista de WLC a la cual el LAP puede enviar los mensajes de solicitud de detección.

Este procedimiento describe el proceso de búsqueda:

1. El LAP emite una solicitud de DHCP a un servidor DHCP para obtener una dirección IP, a menos que una asignación se haya realizado previamente con una dirección IP estática.
2. Si se soporta el modo LWAPP de la capa 2 en el LAP, el LAP transmite un mensaje de

detección de LWAPP en una trama del LWAPP de la capa 2. Cualquier WLC que está conectado con la red y que se configura para el modo LWAPP de la capa 2 responde con una respuesta de detección de la capa 2. Si el LAP no soporta el modo de la capa 2, o si el WLC o el LAP no pueden recibir una respuesta de detección de LWAPP al broadcast del mensaje de detección de LWAPP de la capa 2, el LAP continúa con el paso 3.

3. Si el paso 1 falla, o si el LAP o el WLC no soportan al modo LWAPP de la capa 2, el LAP intenta una detección de WLC del LWAPP de la capa 3.Consulte la sección del algoritmo de la detección de WLC del LWAPP de la capa 3 de este documento.
4. Si el paso 3 falla, los reajustes restauraciones y las respuestas del LAP al paso 1.

Nota: Si usted quiere especificar una dirección IP para un Punto de acceso en vez del hacer que uno asigne automáticamente por un servidor DHCP, usted puede utilizar el regulador GUI o CLI para configurar un IP Address estático para el Punto de acceso. Refiera a configurar un IP Address estático en una sección del Lightweight Access Point de la guía de configuración del WLC para más información. Si el REVESTIMIENTO se asigna un IP Address estático y no puede alcanzar el WLC, recurre al DHCP.

Algoritmo de Detección de LWAPP WLC de la Capa 2

La comunicación LWAPP entre el AP y el WLC puede estar en las tramas Ethernet de capa 2 nativas. Esto se conoce como modo LWAPP de la capa 2. Aunque esté definido en el borrador RFC, el modo LWAPP de la capa 2 se considera desaprobado en la implementación de Cisco. Solamente los LAP de las Cisco 1000 Series soportan al modo LWAPP de la capa 2. También, acoda 2 que no soportan al modo LWAPP en el WLCs de las Cisco 2000 Series. Estos WLC soportan el modo LWAPP de la capa 3 solamente.

Éste es el primer método que un LAP utiliza para descubrir un WLC. Los LAP que soportan el modo LWAPP de la capa 2 transmiten un mensaje de solicitud de la detección de LWAPP en una trama de LWAPP de la capa 2. Si hay un WLC en la red configurada para el modo LWAPP de la capa 2, el controlador responde con una respuesta de la detección. El LAP entonces se mueve a la fase de unión (consulte el paso 5 del registro el LAP con la sección del WLC).

Esta salida del comando **debug lwapp events enable** muestra la secuencia de eventos que se produce cuando un LAP que usa el modo LWAPP se registra con WLC:

Nota: Las líneas de esta salida se movieron a las segundas líneas debido a limitaciones de espacio.

```
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
```

Algoritmo de la detección de WLC del LWAPP de la capa 3

Los LAP utilizan el algoritmo de la detección de la capa 3 si el método de detección de la capa 2 no se soporta o si el método de detección de la capa 2 falla. Opciones de las aplicaciones del algoritmo de la detección de la capa 3 las diversas para intentar detectar WLC. El algoritmo de la detección de WLC del LWAPP de la capa 3 se utiliza para construir una lista del controlador. Después de que se construye una lista del controlador, el AP selecciona un WLC e intenta unirse a el WLC.

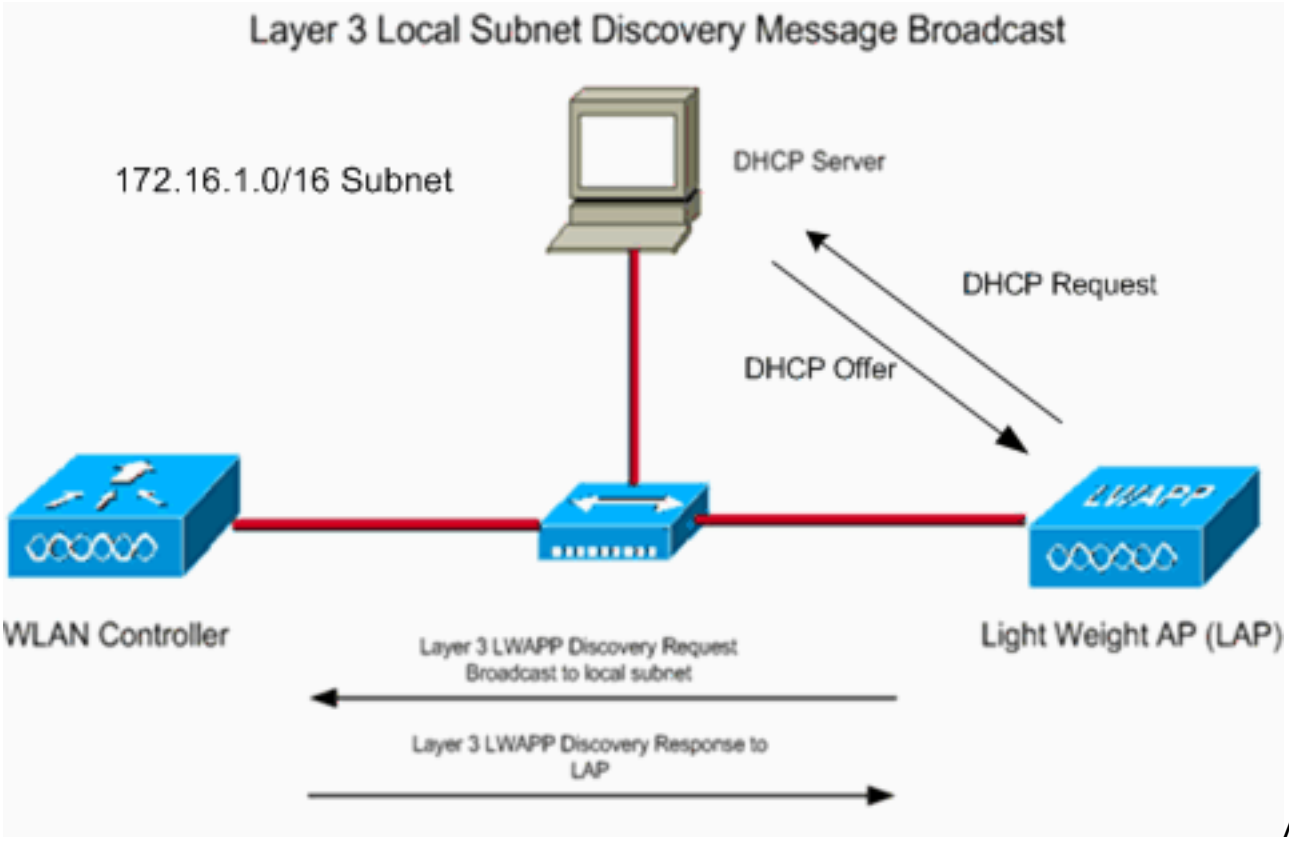
El algoritmo de la detección de WLC de la capa 3 del LWAPP se repite hasta que por lo menos un WLC se encuentra y se une.

> Nota: Durante la detección de WLC de la capa 3 del LWAPP, el AP termina siempre todos los pasos 1 a 5 en esta sección para construir una lista de WLCs del candidato. Después de que el AP ha terminado los pasos de detección de WLC del LWAPP, el AP selecciona un WLC de la lista del WLC del candidato en base de ciertos criterios, y después envía al WLC una solicitud de unión LWAPP.

Cada ejemplo que esta sección explica es independiente de los otras y se proporciona para dar solamente una comprensión de cómo cada paso funciona en el proceso de detección. El LAP utiliza todos los pasos de detección para encontrar una lista de WLC del candidato antes de que seleccione un WLC para efectuar la unión.

Este procedimiento describe los pasos que el algoritmo de la detección de la capa 3 atraviesa cuando intenta detectar WLC:

1. Después de que el LAP obtiene una dirección IP del servidor DHCP, comienza este proceso de detección:El LAP transmite un mensaje de la detección de LWAPP de la capa 3 en la subred del IP local. Cualquier WLC que se configura para el modo LWAPP de la capa 3 y que está conectada con la misma subred local recibe el mensaje de la detección de LWAPP de la capa 3.Cada uno del WLC que recibe el mensaje de la detección de LWAPP contesta con un mensaje de respuesta de detección de LWAPP de unidifusión al LAP.



Aquí está un ejemplo. Asuma que usted tiene un WLC y un REVESTIMIENTO en la misma subred (172.16.1.0/16). También tiene una subred del servidor de DHCP. Cuando el LAP se enciende, envía una solicitud de DHCP, y espera que un servidor DHCP proporcione una dirección IP. Después de que el LAP obtiene una dirección IP del servidor DHCP, el LAP transmite un mensaje de detección de LWAPP de la capa 3 a su subred local. Debido a que el WLC también está la misma subred, el WLC recibe la solictud de detección de LWAPP del LAP y responde con una respuesta de detección de LWAPP de la capa 3. Este ejemplo de salida del comando **debug lwapp events enable** muestra este proceso de detección:

```
(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 salida del comando **debug lwapp packet enable** para la detección de broadcast de subred local se muestra como este ejemplo:

```
(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
```

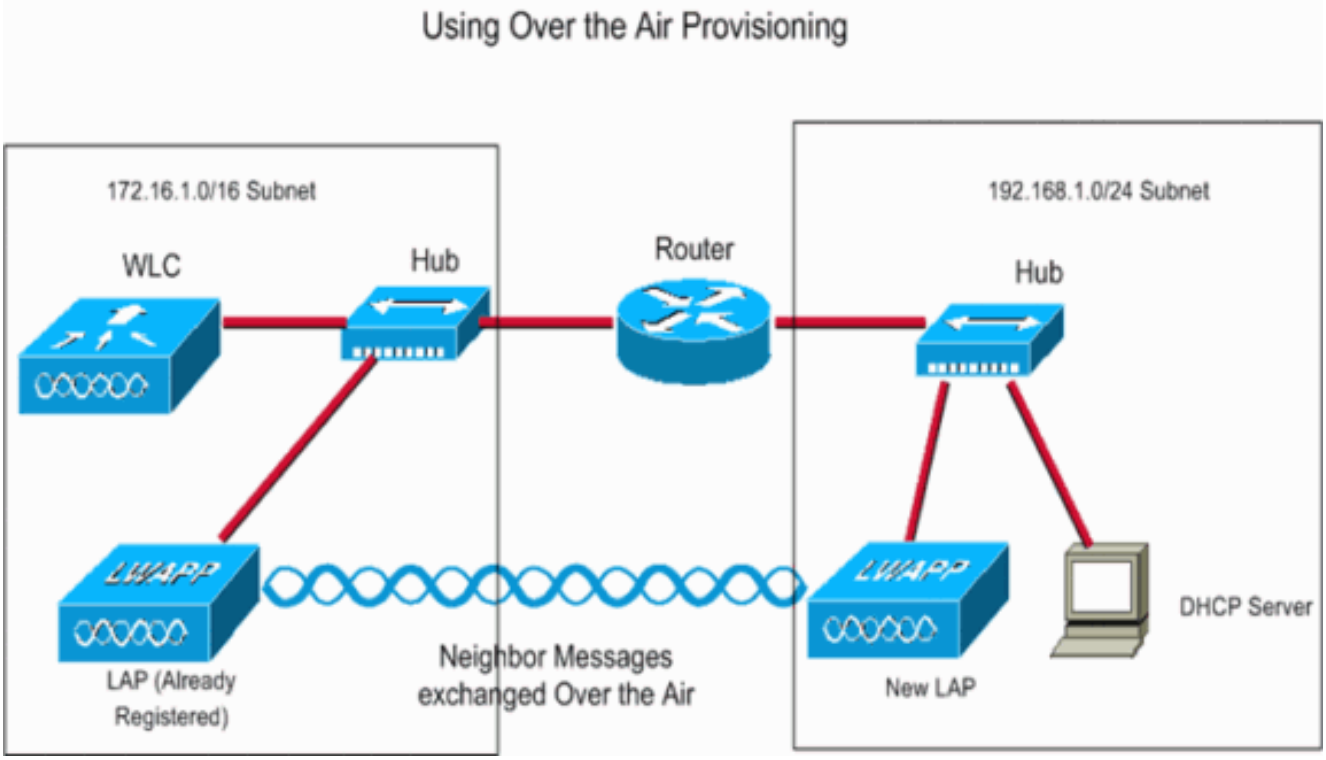
Observe las líneas marcadas en negrita. El valor del parámetro **IE 58** indica el tipo de detección:

```
0 - broadcast
1 - configured
2 - OTAP
3 - dhcp server
4 - dns
```

Debido a que es un broadcast de subred local, el valor de parámetro **IE 58** es **0** en esta

salida del **comando debug lwapp packet enable**.

2. Los LAP también utilizan la función de Provisión en el Aire OTAP) para detectar el WLC. La característica del OTAP *se inhabilita por abandono* en 4.2.39.13, las versiones del WLC de 5.0.68.0 y posterior. El OTAP *se habilita por abandono* en las versiones del WLC anterior de 4.2.39.13. Éste es el proceso de detección cuando se habilita el OTAP:Los LAP que se registran en WLC pueden anunciar la dirección IP del WLC a los LAP (para encontrar WLC) con el uso de los mensajes vecinos que se envían en el aire.Los nuevos LAP que intentan detectar WLC oyen estos mensajes y, por lo tanto, los mensajes de solicitud de LWAPPLos WLC que reciben el mensaje de la detección de LWAPP responden con un mensaje de respuesta de detección de LWAPP de unidifusión al LAP.Debe tener OTAP habilitado solamente durante los intervalos de provisión AP. Después de implementar AP, inhabilite el OTAP como mejor práctica del implementación. Además, los LAP del Cisco Aironet (1130 1200, y 1240 AG series AG,) vienen de fábrica con una versión básica del software ligero de Cisco IOS® que se llama LWAPP RecoveryCisco IOS image . El OTAP no es soportado por los AP que ejecutan LWAPP Cisco IOS Software. Cuando actualiza el Cisco Aironet AP del Cisco IOS Software autónomo a modo ligero, se descarga el software LWAPP Recovery Cisco IOS image. The LWAPP Recovery Cisco IOS image no soporta OTAP. Para soportar el OTAP, los LAP de Aironet deben primero unirse a un WLC para descargar una imagen del Cisco IOS completa del
LWAPP.



Aquí está un ejemplo. Asuma que, en la subred 172.16.1.0/16, usted tiene un REVESTIMIENTO que se registre ya con el WLC, y el OTAP se habilita en el WLC. Cuando sube el nuevo LAP en la subred 192.168.1.0/24, el LAP busca un servidor DHCP y obtiene una dirección IP (si no se hizo ninguna asignación previa con una dirección IP estática). El LAP entonces envía una solicitud de detección a la subred local. Debido a que en este escenario no hay WLC en la subred local, el LAP intenta utilizar el OTAP para detectar WLC. El LAP escucha los mensajes vecinos que son enviados en el aire por los LAP (en la subred 172.16.1.0/16) que se registra ya y buscan las direcciones IP del WLC. De la lista de direcciones IP del WLC que los nuevos LAP aprenden de los mensajes vecinos, los nuevos LAP envían una solicitud de la detección de LWAPP de la capa 3 al WLC. Los WLC que

recibe esta solicitud de detección responde con una respuesta de detección de LWAPP de la capa 3. Esta salida del comando **debug lwapp event enable** muestra la secuencia de mensajes que envían losWLC:

```
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
```

Nota: Como el LAP conoce la dirección IP del WLC a través de los mensajes vecinos, el LAP envía una solicitud de la detección del unicast al WLC. De esta manera, este paso es diferente al método en el paso de progresión 1 de este procedimiento, en el cual el LAP envía un broadcast de la subred local.Nota: El valor del parámetro **IE 58** en la salida del comando **debug lwapp packet enable** muestra que el LAP usó OTAP como método de detección.

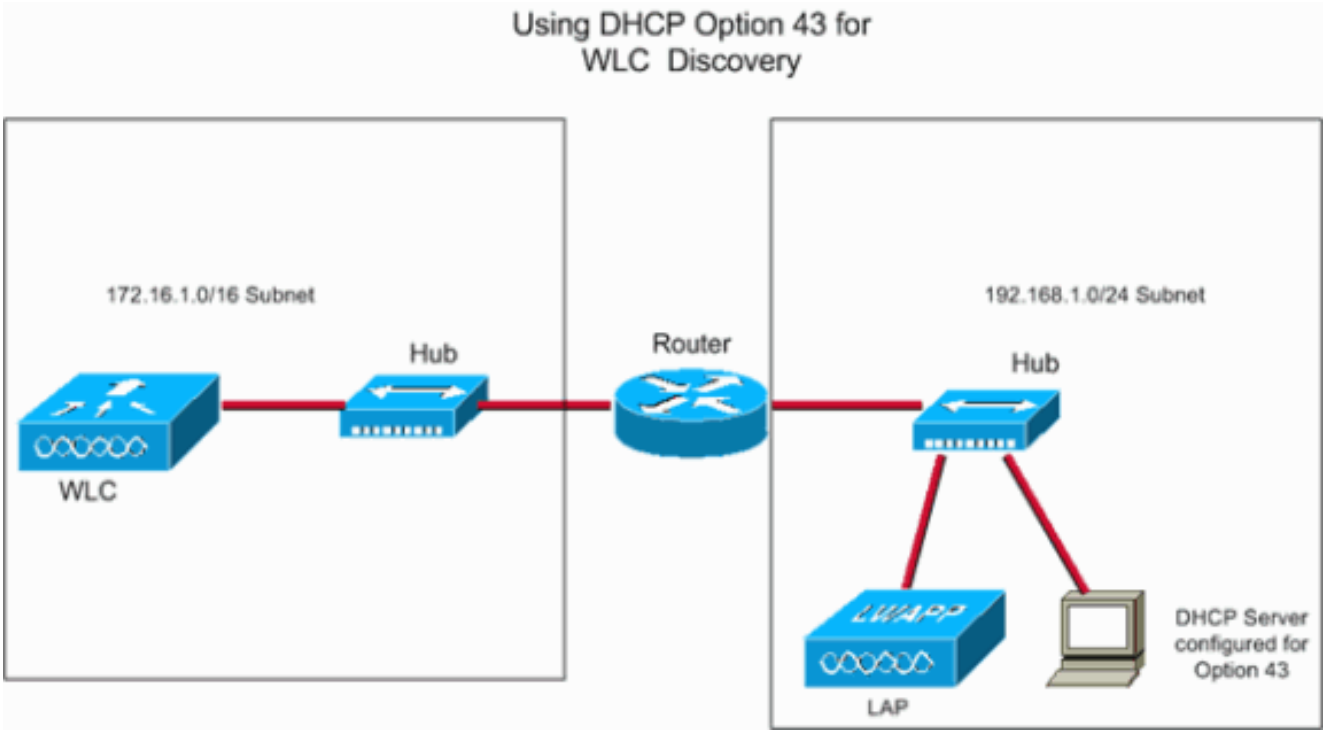
```
Tue May 23 14:21:55 2006: Start of Packet
Tue May 23 14:21:55 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 14:21:55 2006: Msg Type       :
Tue May 23 14:21:55 2006:    DISCOVERY_REQUEST
Tue May 23 14:21:55 2006: Msg Length     :   31
Tue May 23 14:21:55 2006: Msg SeqNum     :   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 el LAP fue registrado a un WLC en una implementación anterior, el LAP mantiene la lista de direcciones IP del WLC localmente en el NVRAM. Los direcciones IP almacenadas del WLC incluyen todo el WLCs que está en "grupos de movilidad" WLC previamente unidos. Éste es el proceso de detección:Los LAP envían una solicitud de la detección de LWAPP de la capa 3 del unicast a cada uno de los direcciones IP del WLC que el LAP tiene en su NVRAM.Los WLC que reciben el mensaje de la detección de LWAPP responden con un mensaje de respuesta de detección de LWAPP de unidifusión al LAP.LA siguiente es la salida de ejemplo del comando **debug lwapp events enable** y el comando **debug lwapp packet enable** para este método de detección WLC: Nota: Si usa el comando **clear ap-config ap_name** para reiniciar el LAP a los valores predeterminados de fábrica, se reajustan todas las configuraciones de LAP. Las configuraciones que se reajustan que incluyen los direcciones IP del WLC que se salva en el NVRAM. En este caso, el LAP debe utilizar un cierto otro método para detectar el 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. Puede también programar los servidores DHCP para volver los direcciones IP del WLC en la “opción específica del vendedor el 43" en la oferta de DHCP a los LAP. Éste es el proceso

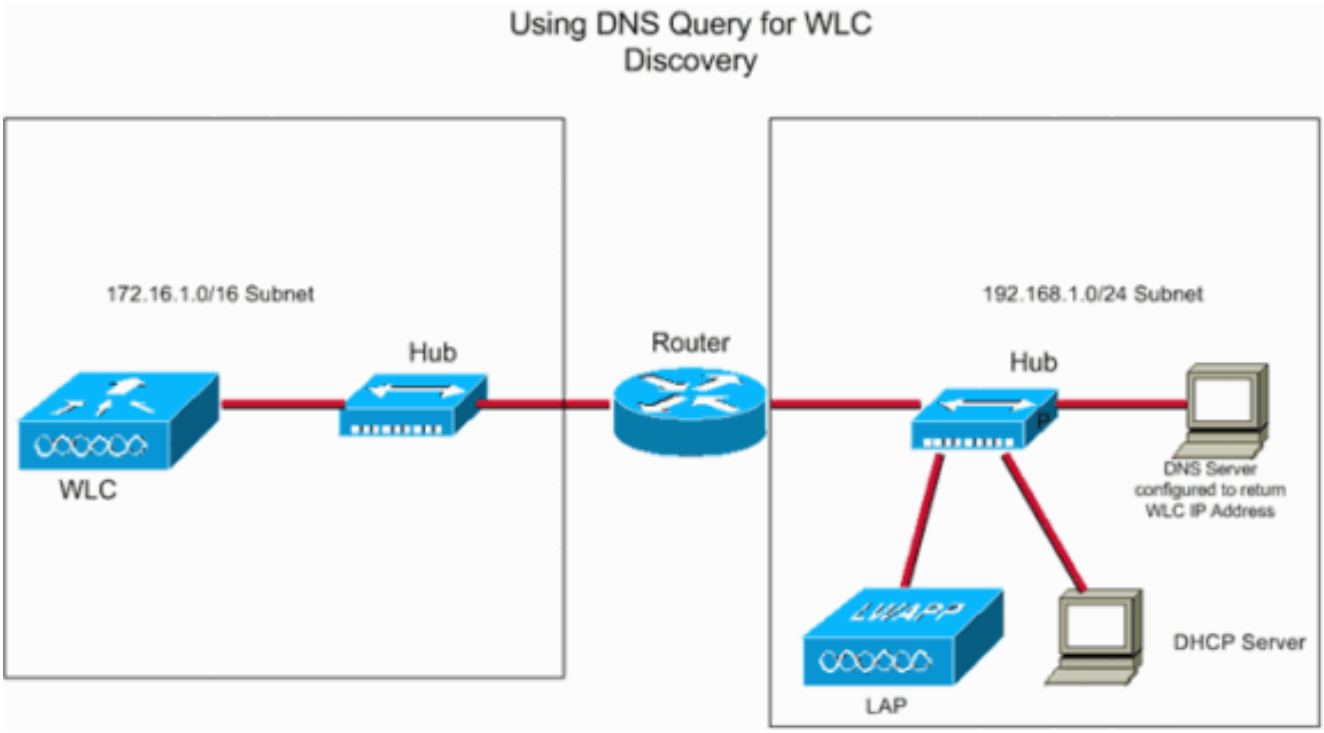
de detección:Cuando un REVESTIMIENTO consigue una dirección IP del servidor DHCP, el REVESTIMIENTO busca los IP Addresses del WLC en el campo de la opción 43 de la oferta de DHCP.El LAP envía una solicitud de la detección de LWAPP de la capa 3 a cada uno de los WLC que se enumera en la opción DHCP 43.Los WLC que reciben el mensaje de la detección de LWAPP responden con un mensaje de respuesta de detección de LWAPP de unidifusión al LAP.Nota: Puede utilizar la opción DHCP 43 cuando los LAP y el WLC están en diversas
subredes.



Aquí está un ejemplo de escenario. Suponga que tiene un WLC en una subred (por ejemplo, 172.16.1.0/16) y los LAP y el servidor DHCP en una diversa subred (por ejemplo, 192.168.1.0/24). La encaminamiento se habilita entre las dos subredes. Puede configurar el servidor DHCP para volver los direcciones IP del WLC al LAP en el mensaje de la oferta de DHCP. Puede utilizar cualquier servidor DHCP que soporte la opción 43.Nota: Refiera a la OPCIÓN DHCP 43 para el ejemplo de configuración ligero de los Puntos de acceso del Cisco Aironet para la información sobre cómo configurar al servidor DHCP del Windows 2000 para la opción 43.De esta manera, cuando el LAP se enciende, busca un servidor DHCP para obtener una dirección IP. El servidor DHCP asigna una dirección IP al LAP y también proporciona la lista de direcciones IP del WLC con el uso de la opción DHCP 43. El LAP envía una solicitud de la detección del unicast a cada WLC. Los WLC que oye estos mensajes contestan con una respuesta de la detección, que inicia el proceso de inscripción. Esta salida del comando **debug lwapp events enable** muestra la secuencia de mensajes del 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**
La siguiente es al salida del comando **debug lwapp packet enable** que indica que la opción DHCP 43 se usó como método de detección para detectar direcciones 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. Finalmente, puede también utilizar el servidor DNS para volver las direcciones IP del WLC al LAP. Éste es el proceso de detección:El REVESTIMIENTO intenta resolver el nombre DNS “CISCO-CAPWAP-CONTROLLER.local-domain” o “CISCO-LWAPP-CONTROLLER.local-domain”. Nota: En este sintaxis del nombre DNS, el localdomain se refiere al nombre de dominio que necesita ser resuelto. Por ejemplo, si el dominio es cisco.com, después este nombre DNS es CISCO-LWAPP-CONTROLLER.cisco.com. El AP necesita ser informado sobre el nombre de dominio que necesita ser resuelto de modo que el AP pueda enviar la solicitud al servidor DNS que hizo la solicitud de resolver este nombre de dominio determinado. El AP es informado de este nombre de dominio con la opción DHCP 15. La opción DHCP 15 especifica el nombre de dominio que el AP debe utilizar para la resolución de DNS. Por lo tanto, es necesario que la opción DHCP 15 esté configurada con la Información sobre el nombre del dominio. Esto permite el servidor DHCP que envía el dirección IP del servidor DNS también para enviar esta información de la opción DHCP 15 (el nombre de dominio que debe ser resuelto) al AP.Cuando el LAP puede resolver este nombre a uno o más direcciones IP del WLC, el LAP envía una solicitud de la detección de LWAPP de la capa 3 del unicast a cada uno del WLCs.Los WLC que recibe la contestación del mensaje de la detección de LWAPP con un mensaje de respuesta de detección de LWAPP de unidifusión al AP.Este ejemplo utiliza la misma disposición que fue utilizada para la opción DHCP 43 (paso de progresión 3). Sin embargo, en este ejemplo, el servidor DHCP no utiliza la opción 43. En vez, el servidor DHCP le proporciona al LAP una dirección IP, y también da la dirección IP del servidor DNS en la oferta de DHCP. Después de que el REVESTIMIENTO consiga la dirección IP del servidor DNS, el REVESTIMIENTO envía una interrogación DNS para el nombre DNS “CISCO-CAPWAP-CONTROLLER.local-domain” o “CISCO-LWAPP-CONTROLLER.local-domain”. El servidor DNS debe ser configurado de forma tal que devuelva la dirección IP del WLC para esta pregunta. Cuando el LAP consigue la dirección IP del WLC, el LAP comienza el proceso de registro con el WLC.



Esta salida del comando **debug lwapp packet enable** muestra el tipo de detección como 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:
```

Nota: Si, después de la realización de los pasos de progresión 1 a 5, el LAP no recibe una respuesta de detección de LWAPP, el LAP reajusta y reinicia el algoritmo de búsqueda.

6. **Use la dirección IP Helper Address en el router**Aunque esto no sea una parte de el algoritmo de la detección de la capa 3, éste es un método más simple que puede ser utilizado cuando el WLC y los LAPs están en diversas subredes. Después de que el LAP obtiene una dirección IP del servidor DHCP, el LAP transmite un mensaje de detección de LWAPP de la capa 3 a su subred local. El dirección IP del WLC se configura como la dirección *ip-auxiliar* en el router. El router reenvía estos broadcasts a la dirección IP configurada con el comando *ip-helper* en la interfaz *interface* en la que se oye el broadcast. Cuando utilizas el comando, los BROADCASTES DIRIGIDOS, así como el unicasts del *ip helper-address*, ocho diversos puertos UDP se remiten automáticamente. Esos puertos son la transferencia de archivo trivial (TFTP) (puerto 69), sistema de nombres del dominio (puerto 53), servicio de tiempo (puerto 37), servidor de nombre de NetBIOS (puerto 137), servidor del datagrama de NetBIOS (puerto 138), cliente y servidor del protocolo de arranque (BOOTP) (puerto 67 y puerto 68), servicio TACACS (puerto 49). Puesto que el puerto *12223 de las* aplicaciones UDP del broadcast del LWAPP él se debe remitir explícitamente en el router. Aquí está un ejemplo de escenario. Asume que tienes un WLC en una subred, tal como 172.16.0.0/16, y los LAPs y el servidor DHCP en una diversa subred, tal como 192.168.1.0/24. La encaminamiento se habilita entre las dos subredes. Este ejemplo muestra la configuración en el router:`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
```

Nota: Si usted funciona con la versión 5.2 o posterior del WLC, utilice el número del puerto 5246 UDP porque el broadcast CAPWAP utiliza el puerto 5246 UDP.

```
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
```

Proceso de selección del WLC

Después de que el LAP termine los pasos de progresión 1 a 5 del algoritmo de la detección de WLC del LWAPP de la capa 3, el LAP selecciona un WLC de la lista del WLC del candidato y lo envía que el WLC un LWAPP se une a la solicitud.

El WLCs embute esta información importante en la respuesta de detección de LWAPP:

- El sysName del controlador
- El tipo de controlador
- La capacidad del controlador AP y su carga actual AP
- El indicador del controlador principal
- Un dirección IP del AP manager

El LAP utiliza esta información para hacer una selección del controlador, con el uso de estas reglas de prioridad:

1. Si el REVESTIMIENTO se ha configurado previamente con un primario, secundario, y/o el controlador terciario, el REVESTIMIENTO examina el campo del sysName del regulador (de las respuestas de detección de LWAPP) en un intento por encontrar el WLC que se configura como “primario ". Si el LAP encuentra un sysName que corresponde con para el controlador primario, el LAP envía un LWAPP se une a la solicitud a ese WLC. Si el LAP no puede encontrar que su controlador primario o si el LWAPP se une a falla, el LAP intenta corresponder con el sysName del controlador secundario a las respuestas de detección de LWAPP. Si el LAP encuentra un emparejamiento, entonces envía un LWAPP se une a al controlador secundario. Si el WLC secundario no puede ser encontrado o el LWAPP se une a falla, el LAP relanza el proceso para su controlador terciario.
2. El LAP mira el campo del indicador del controlador principal en las respuestas de detección de LWAPP del WLCs del candidato si uno de estos elementos es verdad:No primario, secundario, y/o los controladores terciarios se han configurado para un AP.Estos controladores no se pueden encontrar en la lista del candidato.El LWAPP se une a a esos controladores ha fallado.Si un WLC se configura como regulador principal, el REVESTIMIENTO selecciona ese WLC y lo envía que un LWAPP se une a la petición.
3. Si el LAP no puede unirse a con éxito un WLC en base de los criterios en el paso de progresión 1 y el paso de progresión 2, el LAP intenta unirse a el WLC que tiene el exceso de capacidad más grande.

Después de que el LAP seleccione un WLC, el LAP envía un LWAPP se une a la solicitud al WLC. En el LWAPP únete a la solicitud, el LAP embute un certificado digital firmado X.509. Cuando se valida el certificado, el WLC envía un LWAPP se une a la respuesta para indicar al LAP que está unido a con éxito al controlador. El WLC embute sus los propios el certificado digital firmado X.509 en el LWAPP se une a la respuesta que el LAP debe validar. Después de que el

LAP valide el certificado del WLC, el LWAPP se une a el proceso es completo.

El LAP y el controlador del Wireless LAN manejan la fragmentación y el nuevo ensamble para el túnel del LWAPP. Actúan bajo suposición de 1500 bytes MTU. No es un parámetro configurable. En el AP o el WLC, si el MTU es más grande de 1500 bytes, hace fragmentos del paquete y envía el paquete a través. El sistema maneja hasta cuatro fragmentos a partir de la versión 3.2. Las versiones anteriores soportan hasta solamente dos fragmentos.

Aquí está un link a un vídeo en la comunidad del soporte de Cisco que explica el proceso de inscripción del REVESTIMIENTO:

Registro del Lightweight Access Point con los reguladores del Wireless LAN (WLCs)

Troubleshooting

El controlador tiene versión de firmware 3.2.78.0. Cuando ejecuta el comando **lwapp event del debug**, aparece esta salida:

```
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
```

Este mensaje de error significa que la imagen 3.2.78.0 no soporta el LAP. Esencialmente, el controlador no puede encontrar la imagen para el LAP en su lista de imágenes. Por lo tanto, el LAP no puede descargar la imagen del WLC. Para resolver este problema, actualize el controlador a 3.2.116.0 o posterior. Esto resuelve el problema, el LAP se une al controlador y descarga la imagen desde el controlador.

A veces, puede encontrar este mensaje de error en tu controlador:

```
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
```

Este mensaje de error significa que el controlador recibió una solicitud de detección a través de una dirección IP del broadcast que tiene una dirección IP de origen (dada), que no está en ninguna subred configurada en el controlador. También significa que el controlador perdió el paquete. Esto sucede típicamente cuando los troncales todos del cliente no lo prohibieron a VLAN en vez de restricto a la red inalámbirca VLAN.

Usted puede también encontrar este mensaje de error:

```
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
```

Significa que el controlador recibió una solicitud de detección donde la dirección IP de destino (dada), no es la dirección IP de su administrador. También significa que el controlador perdió el paquete.

Hay muchas razones que un Lightweight Access Point (REVESTIMIENTO) puede no poder para unirse al WLC. Refiera al Troubleshooting al Lightweight Access Point que no se une a un regulador del Wireless LAN para la información sobre algunas de las razones que un REVESTIMIENTO no puede unirse a un WLC y cómo resolver problemas los problemas.

Fail-overAP entre diversos grupos de movilidad

Considere este escenario. El grupo de movilidad **MG1** contiene dos controladores, c1 y C2. Estos controladores se despliegan en un edificio, con la carga balanceada de los LAP entre los dos. La sucursal de la compañía implementa un tercer controlador C3, y lo configura para el grupo de movilidad **MG2. LAPs** de ese controlador (c3) no fallan en uno de los otros dos controladores, pero un día, cuando las reinicializaciones del c3 del controlador, los LAPs que ahora fueron registrados originalmente con el c3 se registran al c1 en el grupo **MG1 de** movilidad.

Ahora, aunque el primario de los LAPs es c3, y hay no secundario o terciario, los LAPs se han unido a el c1; un reboot del LAP no lo trae de nuevo al c3. ¿Cuál es el problema?

La razón detrás de esto es ésa dentro de la implementación inicial, la compañía creó uno de dos escenarios:

- Una entrada DNS para “CISCO-CAPWAP-CONTROLLER.local-domain” o “CISCO-LWAPP-CONTROLLER.local-domain” a señalar al c1 o al C2.
- La adición de una opción DHCP 43 de señalar al c1 o al C2 para facilitar las instalaciones iniciales. La instalación del primer edificio fue hecha una vez, estas entradas nunca fue quitada.

  Nota: El AP puede también aprender del c1 o de los controladores C2 por cualquier otro método de detección, tal como broadcast L3 y OTAP, así que asegúrese de que las precauciones apropiadas están tomadas que el AP puede aprender solamente sobre los controladores a partir de un grupo de la movilidad con cualquiera de los métodos.

Cuando va el c3 del controlador abajo, los LAPs que fueron conectados con él reinicialización. Atraviesan el proceso de detección según lo descrito. No sólo envían las solicitudes de la

detección a esos controladores en la configuración de NVRAM, pero también a las direcciones IP aprendidas con los DN y el DHCP, que como consecuencia, incluyen el c1 o el C2.

Puesto que el c3 está abajo a la hora de detección, los LAPs no consiguen una RESPUESTA de DETECCIÓN, así que no pueden proceder a unirse a su controlador primario configurado y deben unirse al controlador que aprendieron con el DHCP o los DN.

Una vez que estos LAPs se unen al c1 o al C2, descargan la nueva lista del grupo de movilidad, que incluye las direcciones IP para solamente el c1 y el C2, así pues, si se reanudan, ellos no tienen ninguna manera de aprender la dirección IP del c3 a la cual enviar las solicituded de detección; no pueden unirse a ese controlador. La única manera de traer los LAP de nuevo al c3 es agregar el c3 a la lista del grupo de la movilidad de c1 y de C2 o cambiar la opción 43 o la entrada DNS.

Hay varias maneras de prevenir tales problemas:

- Se sugiere que los DN y la opción DHCP están utilizados solamente dentro de la implementación inicial y quitados una vez la red está configurados. Esta manera, los AP en la red no tiene ninguna manera de aprender sobre otros grupos de la movilidad.
- Separe los alcances de DHCP o los dominios DNS. Ten un alcance para construir 1 y otro alcance para construir 2 en el servidor DHCP corporativo; el administrador puede configurar diversos direcciones IP de la opción 43 para cada alcance. Igual solicita los dominios DNS; con un nombre de la computadora principal de building1.companyname.com para uno que construye, y building2.companyname.com para otro, puede tener diversas opciones para CISCO-LWAPP-CONTROLLER para cada subdominio.
- Usted puede también utilizar las funciones en el WLC para controlar algunos comportamientos:En el caso de los AP con los certificados de firma automática (SSC), agrega solamente el SSCs a los controladores que deseas los AP para unirse a.En el caso de los AP con los certificados instalados por el fabricante (MIC), utiliza el **autorizar AP contra la función AAA** en el WLC (con el **comando config auth-list ap-policy authorize-apenable**) para que el controlador verifique si debe validar el AP.Para permitir que los AP se unan a, utiliza una de estas opciones:Agréguelos a la lista de la autorización del WLC: use el comando **config auth-list add mic <MAC-Address>** .Agréguelos como clientes al servidor RADIUS. El Called-Station-ID es la dirección MAC del controlador. Si separas los AP en los grupos, puede crear las políticas para definir que los AP pueden autenticar contra qué Llamar-Estación-ID.

Para conseguir un REVESTIMIENTO para unirse a un regulador que no sea parte del grupo de la movilidad del regulador actualmente unido, usted necesita aseegurarse que el nombre del controlador primario sea el del regulador al cual usted desea enviar el REVESTIMIENTO.

Una vez que se hace eso, todo lo que necesitas hacer es dar al LAP una manera de descubrir ese controlador. Esto se puede hacer con los métodos descritos en el algoritmo de la detección de WLC como se explica en este documento.

Información Relacionada

- Control de Puntos de Acceso Ligeros
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- LWAPP (modo ligero) a la conversión autónoma y vice versa

- Estudio del Tráfico de LWAPP
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 6.0
- Soporte Técnico y Documentación - Cisco Systems