Troubleshooting de Punto de Acceso Ligero que no se Une a un Controlador de LAN Inalámbrica

Contenido

AA: BB: XX: DD: DD - APs máximos unidos 6/6
Información Relacionada

Introducción

Este documento ofrece una descripción general del proceso de detección y unión al controlador de LAN inalámbrica (WLC). Este documento también proporciona información sobre algunos de los problemas por los que un punto de acceso ligero (LAP) no puede unirse a un WLC y cómo resolver los problemas.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de la configuración de LAPs y WLCs de Cisco
- Conocimientos básicos de Lightweight Access Point Protocol (LWAPP)

Convenciones

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

Descripción General del Proceso de Detección y Unión de Controladores de LAN Inalámbrica (WLC)

En una red inalámbrica unificada Cisco, en primer lugar los LAPs deben detectarse y unirse a un WLC para que puedan dar servicio a los clientes de red inalámbrica.

Originalmente, los controladores funcionaban solamente en el modo de capa 2. En el modo de capa 2, los LAPs deben estar en la misma subred que la interfaz de administración y la interfaz de administrador de APs del modo de capa 3 no está presente en el controlador. Los LAPs se comunican con el controlador utilizando encapsulación de capa 2 solamente (encapsulación Ethernet) y no asignan una dirección IP mediante Dynamic Host Configuration Protocol (DHCP).

Cuando se desarrolló el modo de capa 3 en el controlador, se introdujo una nueva interfaz de capa 3 denominada administrador de APs. En el modo de capa 3, los LAPs asignaban una dirección IP mediante DHCP primero y después enviaban su solicitud de detección a la interfaz de administración usando las direcciones IP (capa 3). Esto permitió que los LAPs estuvieran en una subred distinta de la interfaz de administración del controlador. El modo de capa 3 es el modo predominante hoy. Algunos controladores y LAPs pueden realizar solamente el modo de capa 3.

Sin embargo, esto presentó un nuevo problema: ¿cómo encontraban los LAPs la dirección IP de administración del controlador cuando estaba en una subred distinta?

En el modo de capa 2, tenían que estar en la misma subred. En el modo de capa 3, el controlador y el LAP esencialmente están jugando al escondite en la red. Si no le dice al LAP dónde está el

controlador a través de la opción DHCP 43 o la resolución DNS de "Cisco-lwapp-controller@local_domain", o lo configura estáticamente, el LAP no sabe en qué parte de la red buscar la interfaz de administración del controlador.

Además de estos métodos, el LAP busca automáticamente en la subred local los controladores con un broadcast local 255.255.255.255. También, el LAP recuerda la dirección IP de administración de cualquier controlador al que se una a través de los reboots. Por lo tanto, si primero pone el LAP en la subred local de la interfaz de administración, éste encontrará la interfaz de administración del controlador y recordará la dirección. Esto se llama impresión. Esto no ayuda a encontrar el controlador si sustituye un LAP posteriormente. Por lo tanto, Cisco recomienda utilizar los métodos de opción DHCP 43 o DNS.

Cuando los LAPs detectan el controlador, no saben si está en el modo de capa 2 o en el modo de capa 3. Por lo tanto, los LAPs conectan siempre con la dirección de interfaz de administración del controlador primero con una solicitud de detección. El controlador entonces dice al LAP en qué modo está en la respuesta de detección. Si el controlador está en el modo de capa 3, la respuesta de detección contiene la dirección IP del administrador de APs de capa 3, de modo que el LAP puede enviar una solicitud de unión a la interfaz del administrador de APs a continuación.

Nota: De forma predeterminada, las interfaces de administración y del administrador del APs se dejan sin etiqueta en su VLAN durante la configuración. En caso de que se etiqueten, asegúrese de que se etiquetan con la misma VLAN para recibir correctamente la respuesta de detección y unión desde el WLC.

El AP LWAPP pasa por este proceso al iniciarse para el modo de capa 3:

1. El LAP se inicia y asigna una dirección IP mediante DHCP, si no tenía asignada previamente una dirección IP estática.
2. El LAP envía solicitudes de detección a los controladores a través de los diversos algoritmos de detección y crea una lista de controladores. Esencialmente, el LAP aprende tantas direcciones de interfaz de administración para la lista de controladores como sea posible mediante:Opción DHCP 43 (adecuada para las compañías globales donde las oficinas y los controladores están en distintos continentes)Entrada DNS para cisco-capwap-controller (adecuada para los negocios locales; puede utilizarse también para encontrar dónde se unen los APs completamente nuevos)**Nota:** Si utiliza CAPWAP, asegúrese de que hay una entrada DNS para cisco-capwap-controllerDirecciones IP de administración de controladores que el LAP recuerda previamenteUn broadcast de capa 3 en la subredProvisión por el aireInformación configurada estáticamenteDe esta lista, el método más fácil a utilizar para el despliegue es tener los revestimientos en la misma subred como la interfaz de administración del regulador y permitir la capa 3 del s del de LAPâ transmitida para encontrar el regulador. Este método se debe utilizar para las compañías que tienen una red pequeña y no poseen un servidor DNS local.El siguiente método de implementación más fácil es utilizar una entrada DNS con DHCP. Puede tener múltiples entradas del mismo nombre DNS. Esto permite al LAP detectar varios controladores. Este método debe ser utilizado por las compañías que tienen todos sus controladores en una sola ubicación y poseen un servidor DNS local. También si la compañía tiene múltiples sufijos DNS y los controladores están segregados por sufijo.La opción DHCP 43 es utilizada por las compañías grandes para localizar la información a través de DHCP. Este método es utilizado por las empresas grandes que tienen un solo sufijo DNS. Por ejemplo, Cisco posee edificios en Europa, Australia y los Estados Unidos. Para asegurar que los LAPs se unan

solamente a controladores localmente, Cisco no puede utilizar una entrada DNS y debe utilizar información de la opción DHCP 43 para decir a los LAPs cuál es la dirección IP de administración de su controlador local.Finalmente, la configuración estática se utiliza para una red que no tenga un servidor DHCP. Usted puede configurar estáticamente la información necesaria unirse a un regulador vía el puerto de la consola y el s CLI del de APâ. Para obtener información sobre cómo configurar estáticamente la información del controlador usando la CLI del AP, refiérase a Configuración Manual de Información del Controlador Usando la CLI del Punto de Acceso.Para ver una explicación detallada sobre los distintos algoritmos de detección que los LAPs utilizan para buscar los controladores, refiérase a Registro del LAP con el WLC.Para obtener información sobre la configuración de la opción DHCP 43 en un servidor DHCP, refiérase a Ejemplo de Configuración de la OPCIÓN DHCP 43 para Puntos de Acceso Ligeros de Cisco Aironet.

3. Envíe una solicitud de detección a cada controlador de la lista y espere la respuesta de detección del controlador que contiene el nombre del sistema, las direcciones IP de administrador de APs, el número de APs ya conectados a cada interfaz de administrador de APs y la capacidad excedente total del controlador.
4. Consulte la lista de controladores y envíe una solicitud de unión a un controlador en este orden (solamente si el AP recibió una respuesta de detección de él):Nombre del sistema de controlador primario (configurado previamente en el LAP).Nombre del sistema de controlador secundario (configurado previamente en el LAP).Nombre del sistema de controlador terciario (configurado previamente en el LAP).Controlador principal (si el LAP no se ha configurado previamente con nombres de controlador primario, secundario o terciario. Utilizado para saber siempre qué LAPs completamente nuevos del controlador se unen).Si no se ve ninguno de los anteriores, haga un balanceo de carga entre los controladores utilizando el valor de capacidad excedente en la respuesta de detección.Si dos controladores tienen la misma capacidad excedente, envíe la solicitud de unión al primer controlador que respondió a la solicitud de detección con una respuesta de detección. Si un solo controlador tiene varios administradores de APs en varias interfaces, elija la interfaz de administrador de APs con el menor número de APs.El controlador responderá a todas las solicitudes de detección sin comprobar los certificados o las credenciales de AP. Sin embargo, las solicitudes de unión deben tener un certificado válido para obtener una respuesta de unión del controlador. Si el LAP no recibe la respuesta de unión elegida, intentará el siguiente controlador de la lista, a menos que sea un controlador configurado (primario/secundario/terciario).
5. Cuando recibe la respuesta de unión, el AP comprueba que tenga la misma imagen que el controlador. Si no, el AP descarga la imagen del controlador, reinicia para cargar la nueva imagen y comienza el proceso de nuevo desde el paso 1.
6. Si tiene la misma imagen de software, pide la configuración del controlador y pasa al estado registrado en el controlador.Después de que descargue la configuración, el AP podría recargarse para aplicar la nueva configuración. Por lo tanto, una recarga adicional puede ocurrir y es un comportamiento normal.

Debug desde el Controlador

Hay algunos comandos **debug** en el controlador que puede utilizar para ver todo este proceso en la CLI.

- **haga el debug de los** paquetes de detección de las demostraciones del del del **enableâ de los lwapp eventes** y únase a los paquetes.
- **haga el debug de la** información del nivel del paquete de las demostraciones del del del **enableâ del paquete lwapp de la** detección y únase a los paquetes.
- **haga el debug del** proceso de validación de certificado de las demostraciones del del del **enableâ del pki P.M**.
- **haga el debug del** del de la **neutralización-allâ** apaga los debugs.

Con una aplicación de terminal que pueda capturar la salida a un archivo del registro, consola o Secure Shell (SSH)/Telnet a su controlador, ingrese estos comandos:

```
config session timeout 120 config serial timeout 120 show run-config (and spacebar thru to collect all) debug mac addr <ap-mac-address> (in xx:xx:xx:xx:xx format) debug client <ap-mac-address> debug lwapp events enable debug lwapp errors enable debug pm pki enable
```

Después de capturar los debugs, utilice el comando **debug disable-all** para desactivar todos los debugs.

Las siguientes secciones muestran la salida de estos comandos **debug** cuando el LAP se registra con el controlador.

debug lwapp events enable

Este comando proporciona información sobre los eventos LWAPP y los errores que ocurren durante el proceso de detección y unión LWAPP.

Ésta es la salida del comando **debug lwapp events enable** para un LAP que tenga la misma imagen que el WLC:

Nota: Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
debug lwapp events enable Wed Oct 24 16:59:35 2007: 00:0b:85:5b: fb:d0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b: fb:d0 to 00:0b:85:33:52:80 on port '2' !--- LWAPP discovery request sent to the WLC by the LAP. Wed Oct 24 16:59:35 2007: 00:0b:85:5b:fb:d0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2 !--- WLC responds to the discovery request from the LAP. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2' !--- LAP sends a join request to the WLC. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 AP ap:5b:fb:d0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:5B:FB:D0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 LWAPP Join-Request MTU path from AP 00:0b:85:5b:fb:d0 is 1500, remote debug mode is 0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully added NPU Entry for AP 00:0b:85:5b:fb:d0 (index 55) Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0 AP IP: 10.77.244.219, AP Port: 49085, next hop MAC: 00:0b:85:5b:fb:d0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:5b:fb:d0 !--- WLC responds with a join reply to the LAP. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Register LWAPP event for AP 00:0b:85:5b:fb:d0 slot 0 -- LAP registers with the WLC Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 !--- LAP requests for the configuration information from the WLC. Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Updating IP info for AP 00:0b:85:5b:fb:d0 -- static 1, 10.77.244.219/255.255.255.224, gtw 10.77.244.220 Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: Send AP Timesync of 1193245188 source MANUAL Wed Oct 24 16:59:48 2007: spamEncodeDomainSecretPayload:Send domain secret TSWEBRET<0d,59,aa,b3,7a,fb,dd,b4,e2,bd,b5,e7,d0,b2,52,4d,ad,21,1a,12> to AP 00:0b:85:5b:fb:d0
```

```
Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:5b:fb:d0 !--- WLC responds by providing all the necessary configuration information
to the LAP. Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'eap fast' Wed
Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48
2007: Running spamEncodeCreateVapPayload for SSID 'webauth' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'eap fast' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'webauth' . . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0
Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5b:fb:d0 . . Wed
Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP Up event for AP 00:0b:85:5b:fb:d0 slot 0!
!--- LAP is up and ready to service wireless clients. Wed Oct 24 16:59:48 2007:
00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5b:fb:d0 . . . Wed Oct
24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP RRM_CONTROL_RES from AP 00:0b:85:5b:fb:d0 !--
- WLC sends all the RRM and other configuration parameters to the LAP.
```

Como se ha mencionado en la sección anterior, una vez que un LAP se registra con el WLC, éste comprueba si tiene la misma imagen que el controlador. Si las imágenes del LAP y el WLC son diferentes, los LAPs descargan la nueva imagen del WLC primero. Si el LAP tiene la misma imagen, continúa descargando la configuración y otros parámetros del WLC.

Verá estos mensajes en la salida del comando **debug lwapp events enable** si el LAP descarga una imagen del controlador como parte del proceso de registro:

```
Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from AP
00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from
AP 00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES
from AP 00:0b:85:5b:fb:d0
```

Una vez que la descarga de imagen esté completa, el LAP reiniciará y ejecutará el algoritmo de detección y unión otra vez.

debug pm pki enable

Como parte del proceso de unión, el WLC autentica cada LAP verificando que su certificado es válido.

Cuando el AP envía la solicitud de unión LWAPP al WLC, éste incorpora su certificado X.509 en el mensaje LWAPP. El AP también genera un ID de sesión aleatorio que se incluye también en la solicitud de unión LWAPP. Cuando el WLC recibe la solicitud de unión LWAPP, valida la firma del certificado X.509 usando la llave pública del AP y comprueba que el certificado haya sido emitido por una autoridad certificadora de confianza.

También mira la fecha de inicio y la época para el intervalo de la validez del certificado AP y compara la esa fecha y el tiempo a su propia fecha y hora (por lo tanto el reloj del del del controllerâ s necesita ser fijado cerca de la fecha y hora actual). Si se valida el certificado X.509, el WLC genera un llave de encripción AES aleatoria. El WLC sondea el llave AEA en su motor de criptografía de modo que pueda encriptar y desencriptar los futuros mensajes de control del LWAPP intercambiados con el AP. Observe que los paquetes de datos se envían sin encriptar en el túnel LWAPP entre el LAP y el controlador.

El comando **debug pm pki enable** muestra el proceso de validación de la certificación que ocurre durante la fase de unión en el controlador. El comando **debug pm pki enable** también visualizará la llave hash del AP durante el proceso de unión si el AP tiene un certificado autofirmado (SSC) creado por el programa de conversión LWAPP. Si el AP tiene un certificado instalado manufacturado (MIC), no verá una llave hash.

Nota: Todos los AP fabricados después de junio de 2006 tienen un MIC.

Ésta es la salida del comando **debug pm pki enable** cuando el LAP con un MIC se une al controlador:

Nota: Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: locking ca cert table
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b8591c3c0, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <issuer>  C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:91:c3:c0
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 2d812f0c
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 20f00bf3
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: user cert verfied using >bsnOldDefaultCaCert< Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: ValidityString (current): 2007/10/25/13:52:59 Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: AP version is 0x400d900, sending Cisco ID cert...
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <cscoDefaultIdCert> Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59
2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 2, ID cert >bsnSslWebadminCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 3, ID cert >bsnSslWebauthCert< Thu Oct 25 13:52:59 2007:
sshpmGetIssuerHandles: Airespace ID cert ok; sending it... Thu Oct 25 13:52:59 2007:
sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing
to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row
4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 5,
CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCID: comparing to row 0, ID
cert >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromHandle: calling
sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: called
to get cert for CID 156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 0,
certname >bsnOldDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
```

```
1, certname >bsnDefaultRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 2, certname >bsnDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 3, certname >bsnDefaultBuildCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing
to row 4, certname >cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID:
comparing to row 5, certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007:
sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03
2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: called to get cert for CID 156af135 Thu Oct 25 13:53:03
2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 3, certname >bsnDefaultBuildCert< Thu
Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 4, certname
>cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 5,
certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: called to
encrypt 16 bytes Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: successfully encrypted, out is
192 bytes Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for CID 156af135 Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: match in row 0
Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 172 bytes Thu
Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 24 bytes Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25 13:53:03
2007: sshpmPrivateKeyEncrypt: encrypted bytes: 384 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: called with 0xae0c358 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: freeing public key
```

Para un LAP con un SSC, la salida del comando **debug pm pki enable** será parecida a la siguiente. Observe que el hash SSC también se ve en esta salida.

Nota: Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
(Cisco Controller) > debug pm pki enable Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate
<bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
cscoDefaultMfgCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert< Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on
Public Key Data Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122
300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003
82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd
7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0
39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3
9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce
cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e
c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e
c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db
251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc
1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490
881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b
d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693
f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f
76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3
b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f
de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8
```

```
eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301
0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This is the actual SSC key-hash value. Mon May 22
06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode
is 0
```

Debug desde el LAP

Si los debugs del controlador no indican una solicitud de unión, puede hacer un debug del proceso desde el LAP, siempre que el LAP tenga un puerto de consola. Puede ver el proceso de inicio del LAP con estos comandos, pero primero debe entrar en el modo enable (la contraseña predeterminada es Cisco):

- el del del **detailâ DHCP del debug** muestra la información de la opción DHCP 43.
- el del del **udpâ del IP del debug** muestra el unir a/los paquetes de detección al regulador así como a las interrogaciones del DHCP y DNS (todos los éstos son paquetes UDP. El puerto 12223 es el puerto de origen del s del del controllerâ).
- el del del **eventâ del cliente del lwapp del debug** muestra los lwapp eventes para el AP.
- el del del **allâ del undebug** inhabilita los debugs en el AP.

Éste es un ejemplo de la salida del comando **debug ip udp**. Esta salida parcial da una idea de los paquetes que son enviados por el LAP durante el proceso de inicio para detectar un controlador y unirse a él.

```
UDP: sent src=10.77.244.199(20679), dst=10.77.244.208(12223)
!--- LWAPP Discovery Request sent to a controller to which !--- the AP was previously registered
to. UDP: sent src=10.77.244.199(20679), dst=172.16.1.50(12223) !--- LWAPP Discovery Request
using the statically configured controller information. UDP: sent src=10.77.244.199(20679),
dst=255.255.255.255(12223) !--- LWAPP Discovery Request sent using subnet broadcast. UDP: sent
src=10.77.244.199(20679), dst=172.16.1.51(12223) !--- LWAPP Join Request sent to AP-Manager
interface on statically configured controller.
```

Cómo Evitar Problemas Relacionados con DHCP

Los LAPs que utilizan DHCP para buscar una dirección IP antes de iniciar el proceso de detección del WLC podrían tener problemas al recibir una dirección DHCP debido a la configuración incorrecta de los parámetros relacionados con DHCP. Esta sección explica cómo funciona DHCP con los WLCs y proporciona algunas de las prácticas recomendadas para evitar problemas relacionados con DHCP.

Para DHCP, el controlador se comporta como un router con una dirección de ayudante IP. Es decir, completa la dirección IP del gateway y reenvía la solicitud a través de un paquete unicast directamente al servidor DHCP.

Cuando la oferta de DHCP vuelve al controlador, éste cambia la dirección IP del servidor DHCP a su dirección IP virtual. La razón por la que hace esto es que cuando Windows se traslada entre los APs, lo primero que hace es intentar entrar en contacto con el servidor DHCP y renovar la dirección.

Siendo 1.1.1.1 la dirección del servidor DHCP (dirección IP virtual típica en un controlador), el controlador puede interceptar ese paquete y responder rápidamente a Windows.

Éste es también el motivo de que la dirección IP virtual sea la misma en todos los controladores. Si un equipo portátil de Windows se traslada a un AP en otro controlador, intentará entrar en contacto con la interfaz virtual en el controlador. Debido al evento de movilidad y a la

transferencia de contexto, el nuevo controlador al que se ha trasladado el cliente Windows ya tiene toda la información para responder a Windows otra vez.

Si quiere utilizar el servidor DHCP interno en el controlador, lo único que tiene que hacer es poner la dirección IP de administración como servidor DHCP en la interfaz dinámica que cree para la subred. Después asigne esa interfaz a la WLAN.

La razón de que el controlador necesite una dirección IP en cada subred es para que pueda completar la dirección del gateway DHCP en la solicitud DHCP.

Éstos son algunos de los puntos que debe recordar cuando configure los servidores DHCP para la WLAN:

1. La dirección IP del servidor DHCP no debe quedar dentro de ninguna subred dinámica que esté en el controlador. Estará bloqueada, pero puede anularse con este comando: **config network mgmt-via-dynamic-interface** on version 4.0 only (command not available in version 3.2)
2. El controlador remitirá el DHCP a través de unicast desde su interfaz dinámica (en el código posterior) usando su dirección IP en esa interfaz. Asegúrese de que cualquier firewall permita que esta dirección llegue al servidor DHCP.
3. Asegúrese de que la respuesta del servidor DHCP pueda llegar a la dirección dinámica del controlador en esa VLAN a través de cualquier firewall. Haga ping en la dirección de interfaz dinámica desde el servidor DHCP. Haga ping en el servidor DHCP con una dirección IP de origen de la dirección de gateway de la interfaz dinámica.
4. Asegúrese de que la VLAN del AP se permite en los switches y routers, y que sus puertos están configurados como trunks para que los paquetes (incluido DHCP) etiquetados con la VLAN se permitan a través de la red alámbrica.
5. Asegúrese de que el servidor DHCP esté configurado para asignar una dirección IP en la VLAN del AP. Puede configurar también el WLC como servidor DHCP. Para obtener más información sobre cómo configurar el servidor DHCP en el WLC, refiérase a la sección Utilización de la GUI para Configurar DHCP de la Guía de Configuración del Controlador de LAN Inalámbrica Cisco, Versión 5.0.
6. Verifique que la dirección IP del controlador en su interfaz dinámica quede dentro de uno de los alcances DHCP en el servidor DHCP.
7. Finalmente, verifique que no esté utilizando un servidor DHCP que no responda a solicitudes DHCP unicast como PIX.

Si no puede resolver su problema de DHCP, hay 2 soluciones:

- Pruebe un servidor DHCP interno. Configure la dirección del servidor DHCP en la interfaz dinámica para que sea la dirección IP de administración y después el conjunto interno DHCP. Si el alcance DHCP está habilitado, debería funcionar.
- Verifique que no hay respuesta a la solicitud DHCP enviando la salida en la CLI (consola o SSH) de estos debugs:0. debug mac addr <mac address>
  1. debug dhcp message enable
  2. debug dhcp packet enable Esto debe indicar que el paquete DHCP se reenvió, pero el controlador no recibió una respuesta.

Finalmente, debido a la seguridad en el controlador, no es recomendable poner una VLAN o subred en el controlador que también contiene los LAPs, a menos que esté en la subred de la interfaz de administración.

Nota: El servidor RADIUS o el servidor DHCP no debe estar en ninguna de las subredes de la interfaz dinámica del controlador. La seguridad bloqueará los paquetes de devolución que intentan comunicar con el controlador.

Utilización de Servidores Syslog para Resolver Problemas del Proceso de Unión de LAP

El software del controlador versión 5.2 le permite configurar los APs para enviar todos los errores relacionados con CAPWAP a un servidor Syslog. No necesita habilitar ningún comando debug en el controlador porque todos los mensajes de error CAPWAP se pueden ver desde el propio servidor Syslog. Para obtener más información sobre esta función y los comandos usados para habilitarla, lea la sección Troubleshooting del Proceso de Unión de Puntos de Acceso de la Guía de Configuración del Controlador de LAN Inalámbrica Cisco, versión 5.2 .

El LAP no se Une al Controlador, ¿Por Qué?

Comprobación Previa de los Elementos Básicos

- ¿Pueden comunicarse el AP y el WLC?
- Aseegurese el AP está consiguiendo un direccionamiento del DHCP (marque los arriendos del servidor DHCP para la dirección MAC del s del de APâ).
- Intente hacer un ping del AP desde el controlador.
- Compruebe si la configuración STP en el switch es correcta para que no se bloqueen los paquetes a las VLANs.
- Si los pings han sido exitosos, asegúrese que el AP tenga por lo menos un método por el cual se detecte al menos una consola o telnet/ssh del WLC en el controlador para ejecutar los debugs.
- Cada vez que el AP reinicia, inicia la secuencia de la detección de WLC e intenta localizar el AP. Reinicie el AP y marque si se une al WLC.

Aquí se indican algunos de los problemas más frecuentes por los cuales los LAPs no se unen al WLC.

Problema 1: La hora del controlador está fuera del intervalo de validez del certificado

Complete estos pasos para resolver este problema:

1. Ejecute los comandos **debug lwapp errors enable** y debug pm pki enable.La salida del comando **debug lwapp event enable** muestra el debug de mensajes del certificado que se transmiten entre el AP y el WLC. La salida muestra claramente un mensaje de que se rechaza el certificado.**Nota:** Asegúrese de tener en cuenta la diferencia de Tiempo Universal Coordinado (UTC).Ésta es la salida del comando **debug lwapp events enable** en el controlador:**Nota:** Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.
```
Thu Jan  1 00:09:46 1970: 00:0b:85:5b:fb:d0 Received LWAPP DISCOVERY
REQUEST
from AP 00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Jan 1 00:09:46 1970: 00:0b:85:5b:fb:d0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2
```

```
Thu Jan  1 00:09:57 1970: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2'
Thu Jan  1 00:09:57 1970: 00:0b:85:5b:fb:d0 LWAPP Join-Request does not include valid
certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:5b:fb:d0. Thu Jan 1 00:09:57 1970:
00:0b:85:5b:fb:d0 Unable to free public key for AP 00:0B:85:5B:FB:D0 Thu Jan 1 00:09:57
1970: spamProcessJoinRequest : spamDecodeJoinReq failed
```

Ésta es la salida del comando **debug pm pki enable** en el controlador. Esta salida sigue el proceso para la validación del certificado.**Nota:** Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
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)
```

Esta información muestra claramente que la hora del controlador está fuera del intervalo de validez del certificado del LAP. Por lo tanto, el LAP no puede registrarse con el controlador. Los certificados instalados en el LAP tienen un intervalo de validez predefinido. El tiempo del regulador debe ser fijado de una manera tal que esté dentro del intervalo de la validez del certificado del certificado del s del de LAPâ.

2. Ejecute el comando **show time** desde la CLI del controlador para verificar que la fecha y la hora ajustadas en su controlador estén dentro de este intervalo de validez. Si la hora del controlador es anterior o posterior al intervalo de validez de este certificado, cambie la hora del controlador para que esté dentro de este intervalo.**Nota:** Si la hora no está fijada correctamente en el controlador, elija **Commands > Set Time** en el modo de GUI del controlador o ejecute el comando config time en la CLI del controlador para ajustar su hora.
3. En los LAPs con acceso a CLI, verifique los certificados con el comando **show crypto ca certificates** desde la CLI del AP.Este comando permite verificar el intervalo de validez del certificado fijado en el AP. Aquí tiene un ejemplo:

```
AP0015.63e5.0c7e#show crypto ca
certificates .....................................
..................................... .....................................
..................................... Certificate Status: Available Certificate
Serial Number: 4BC6DAB80000000517AF Certificate Usage: General Purpose Issuer: cn=Cisco
Manufacturing CA o=Cisco Systems Subject: Name: C1200-001563e50c7e ea=support@cisco.com
cn=C1200-001563e50c7e o=Cisco Systems l=San Jose st=California c=US CRL Distribution Point:
http://www.cisco.com/security/pki/crl/cmca.crl Validity Date: start date: 17:22:04 UTC Nov
30 2005 end date: 17:32:04 UTC Nov 30 2015 renew date: 00:00:00 UTC Jan 1 1970 Associated
Trustpoints: Cisco_IOS_MIC_cert .............................
..................................... .....................................
```

No se muestra la salida entera porque puede haber muchos intervalos de validez asociados a la salida de este comando. Necesita considerar solamente el intervalo de validez especificado por el

punto de confianza asociado: Cisco_IOS_MIC_cert con el nombre de AP relevante en el campo de nombre. En esta salida de ejemplo, es Name: `C1200-001563e50c7e`. Éste es el intervalo de validez del certificado real que se considerará.

Problema 2: Discordancia en el dominio regulador

Ve este mensaje en la salida del comando **debug lwapp events enable**:

Nota: Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
Wed Oct 24 17:13:20 2007: 00:0b:85:91:c3:c0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:80 on port '2'
Wed Oct 24 17:13:20 2007: 00:0e:83:4e:67:00 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:91:c3:c0 on Port 2
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:81 on  port '2'
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 AP ap:91:c3:c0:
txNonce  00:0B:85:33:52:80 rxNonce  00:0B:85:91:C3:C0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 LWAPP Join-Request MTU path
from AP 00:0b:85:91:c3:c0 is 1500, remote debug mode is 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully added NPU Entry
for AP 00:0b:85:91:c3:c0 (index 48)
Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0
AP IP: 10.77.246.18, AP Port: 7228, next hop MAC: 00:17:94:06:62:88
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully transmission
of LWAPP Join-Reply to AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:91:c3:c0 to  00:0b:85:33:52:81
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP info for AP 00:0b:85:91:c3:c0 --
static 0, 10.77.246.18/255.255.255.224, gtw 10.77.246.1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP 10.77.246.18 ===> 10.77.246.18
for AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 0 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211a Regulatory Domain
(-N) does not match with country (US )  reg. domain -AB for the slot 0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 1 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211bg Regulatory Domain (-N)
does not match with country (US ) reg. domain -AB for the slot 1 Wed Oct 24 17:13:47 2007:
spamVerifyRegDomain AP RegDomain check for the country US failed Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: Regulatory Domain check Completely FAILED The AP will
not be allowed to join Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 apfSpamProcessStateChangeInSpamContext: Deregister
LWAPP event for AP 00:0b:85:91:c3:c0 slot 1 Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0 Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 1
```

El mensaje indica claramente que hay una discordancia en el dominio regulador del LAP y del WLC. El WLC soporta múltiples dominios reguladores, pero cada uno de ellos debe estar seleccionado para que un LAP pueda unirse desde ese dominio. Por ejemplo, el WLC que utiliza el dominio regulador - A se puede utilizar solamente con los APs que utilizan el dominio regulador - A (y así sucesivamente). Cuando compras los AP y el WLCs, asegúrese de que compartan el mismo dominio controlador. Solo entonces se pueden registrar los LAPs con el WLC.

Nota: Las radios 802.1b/g y 802.11a deben estar en el mismo dominio regulador para un solo LAP.

Problema 3: Mensaje de error El AP no puede unirse porque se ha llegado al número máximo de APs en la interfaz 2

Puede que vea este mensaje de error cuando el AP intente unirse al controlador:

```
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 4498: AP cannot join because the maximum number of
APs on interface 2 is reached.
```

De forma predeterminada, los controladores de la serie 4400 pueden soportar hasta 48 APs por puerto. Cuando intenta conectar más de 48 APs en el controlador, recibe este mensaje de error. Sin embargo, puede configurar su controlador de la serie 4400 para soportar más APs en una sola interfaz (por puerto) usando uno de estos métodos:

- Agregación de links (para los controladores en modo de capa 3)
- Múltiples interfaces de administrador de APs (para los controladores en modo de capa 3)
- Conexión de puertos adicionales (para los controladores en modo de capa 2)

Para obtener más información, refiérase a Configuración de un Controlador de la Serie 4400 para Soportar Más de 48 Puntos de Acceso.

Nota: Cisco ha introducido WLCs de la serie 5500 para usuarios corporativos con capacidades adicionales. No tiene restricciones respecto al número de APs por puerto. Refiérase a la sección Elección entre Agregación de Links y Múltiples Interfaces de Administrador de APs de la Guía de Configuración del Controlador de LAN Inalámbrica Versión 6.0 para obtener más información.

Problema 4: Con los APs SSC, se inhabilita la política de AP SSC

Si la política SSC se inhabilita en el controlador, se ve este mensaje de error en el controlador desde la salida de los comandos **debug lwapp events enable** y debug pm pki enable:

```
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Wed Aug 9 17:20:21 2006 [ERROR] spam_crypto.c 1509: Unable to free public key for
AP 00:12:44:B3:E5:60
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include valid
certificate in CERTIFICATE_PAYLOAD from AP 00:12:44:b3:e5:60. Wed Aug 9 17:20:21 2006 [CRITICAL]
sshpmPkiApi.c 1493: Not configured to accept Self-signed AP cert
```

Complete estos pasos para resolver este problema:

Realice una de estas dos acciones:

- Ejecute el comando **show auth-list** en la CLI del controlador para comprobar si éste está configurado para aceptar APs con SSCs.Éste es un ejemplo de salida:`#show auth-list`
  `Authorize APs against AAA ..... disabled Allow APs with Self-signed Certificate (SSC) .... enabled Mac Addr Cert Type Key Hash ---------- --------- ---------- 00:09:12:2a:2b:2c SSC 12345678901234567890123456789012345678901`
- Elija **Security > AP Policies** en la GUI.Compruebe si la casilla de verificación **Accept Self Signed Certificate** está marcada. Si no, márquela.Elija **SSC** como tipo de certificado.Añada el AP a la lista de autorización con la dirección MAC y la llave hash.Esta llave hash se puede

obtener de la salida del comando **debug pm pki enable**. Vea en el Problema 6 información sobre la obtención del valor de llave hash.

Problema 5: Lista de autorización de AP habilitada en el WLC; LAP no incluido en la lista de autorización

En estos casos, verá este mensaje en el controlador en la salida del comando **debug lwapp events enable**:

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:51:5a:e0
```

Si está utilizando un LAP que tiene un puerto de consola, verá este mensaje cuando ejecute el comando **debug lwapp client error**:

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: No more AP manager IP addresses remain.
```

De nuevo, esto es una indicación clara de que el LAP no es parte de la lista de autorización de AP en el controlador.

Puede ver el estado de la lista de autorización de AP usando este comando:

```
(Cisco Controller) >show auth-list Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Para añadir un LAP a la lista de autorización de AP, utilice el comando **config auth-list add mic <AP MAC Address>**. Para obtener más información sobre cómo configurar la autorización de LAP, refiérase a Ejemplo de Configuración de la Autorización del Punto de Acceso Ligero (LAP) en una Red Inalámbrica Unificada de Cisco.

Problema 6: La llave hash pública SSC es incorrecta o falta

Complete estos pasos para resolver este problema:

1. Ejecute el comando **debug lwapp events enable**.Éste verifica que el AP intenta unirse.
2. Ejecute el comando **show auth-list**.Este comando muestra la llave hash pública que el controlador tiene en almacenamiento.
3. Ejecute el comando **debug pm pki enable**.Este comando muestra la llave hash pública real. La llave hash pública real debe coincidir con la llave hash pública que el controlador tiene en almacenamiento. Una discrepancia causa el problema. Éste es un ejemplo de salida de este

mensaje de debug:**Nota:** Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
(Cisco Controller) > debug pm pki enable Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle... Mon May 22
06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Mon May 22 06:34:10
2006: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon May 22 06:34:10
2006: sshpmGetCID: comparing to row 1, CA cert bsnDefaultRootCaCert< Mon May 22 06:34:10
2006: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon May 22 06:34:10 2006:
sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon May 22 06:34:10 2006:
sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Mon May 22 06:34:10
2006: sshpmGetCID: comparing to row 5, CA cert cscoDefaultMfgCaCert< Mon May 22 06:34:10
2006: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon May 22 06:34:10
2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data Mon May 22 06:34:10
2006: sshpmGetIssuerHandles: Key Data 30820122 300d06092a864886 f70d0101 Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f003082010a 02820101 Mon May
22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0cad8df69 b366fd4c Mon
May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b87625143b95a34
49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data
f81fa6ce cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key
Data dde0648e c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
Key Data 0f463f9e c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006:
sshpmGetIssuerHandles: Key Data 7dd485db 251e2e079cd31041 b0734a55 Mon May 22 06:34:14
2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502dc54e75f2 6d28fc6b Mon May 22
06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e3102d37140 7c9c865a Mon May
22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f7a9bac00 d13ff85f Mon
May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bcbc1acc13
0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3
b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data
fe64641f de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key
Data 1bfae1a8 eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles:
Key Data f7020301 0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This is the actual SSC key-hash value. Mon
May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote
debug mode is 0 Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization
failure for 00:0e:84:32:04:f0
```

Complete estos pasos para resolver el problema:

1. Copie la llave hash pública de la salida del comando **debug pm pki enable** y utilícela para sustituir la llave hash pública de la lista de autenticación.
2. Ejecute el comando **config auth-list add ssc AP_MAC AP_key** para añadir la dirección MAC del AP y la llave hash a la lista de autorización.Éste es un ejemplo de este comando:**Nota:** Este comando se ha movido a la segunda línea debido a limitaciones de espacio.

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
```

Problema 7: Se han producido daños en el certificado o la llave pública en el AP

El LAP no se une a un controlador debido a un problema del certificado.

Ejecute los comandos **debug lwapp errors enable** y debug pm pki enable. Ve mensajes que indican los certificados o llaves dañados.

Nota: Algunas líneas de la salida se han movido a la segunda línea debido a limitaciones de espacio.

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
```

LWAPP Join Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0f:24:a9:52:e0. Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP

Utilice una de estas dos opciones para resolver el problema:

- Petición del del MIC APâ un Return Materials Authorization (RMA).
- ¿Downgrade del del de SSC APâ al Cisco IOS? Software Release 12.3(7)JA.Si es un AP con un SSC, vuelva a convertirlo a IOS usando el botón MODE. Después utilice la herramienta de upgrade a lwapp para volver a convertirlo a LWAPP. Esto debería crear el certificado otra vez.

Complete estos pasos para volver a la versión anterior:

1. Utilice la opción de botón de restablecimiento.
2. Borre la configuración del controlador.
3. Ejecute de nuevo el upgrade.

Para obtener más información sobre la vuelta a la versión anterior de un LAP, refiérase a Upgrade de Puntos de Acceso Autónomos de Cisco Aironet al Modo Ligero.

Si tiene un WCS, puede enviar los SSCs al nuevo WLC. Para obtener más información sobre cómo configurar los APs usando el WCS, refiérase a la sección Configuración de Puntos de Acceso de la *Guía de Configuración de Cisco Wireless Control System, Versión 5.1*.

Problema 8: El controlador podría estar funcionando en modo de capa 2

Complete este paso para resolver este problema:

Compruebe el modo de funcionamiento del controlador. Los AP convertidos soportan solamente la detección de capa 3. Los AP convertidos no soportan la detección de capa 2.

Complete estos pasos para resolver el problema:

1. Ajuste el WLC para estar en el modo de capa 3.
2. Reinicie y configure la interfaz de administrador de APs.Si tiene un puerto de servicio, como el puerto de servicio en 4402 o 4404, debe tenerlo en una superred distinta que la de las interfaces de administrador de APs y de administración.

Problema 9: Recibe este mensaje de error en el AP después de la conversión a LWAPP

Ve este mensaje de error:

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs
no certs in the  SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

El AP se recarga después de 30 segundos y el proceso se inicia de nuevo.

Complete estos pasos para resolver este problema:

1. Tiene un AP SSC. Conviértalo de nuevo a una imagen IOS autónoma.
2. Borre la configuración ejecutando el comando **write erase** y recárguela. No guarde la configuración durante la recarga.

Problema 10: El controlador recibe el mensaje de detección de AP en la VLAN incorrecta (ve el debug del mensaje de detección, pero no la respuesta)

Ve este mensaje en la salida del comando **debug lwapp events enable**:

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Este mensaje significa que el controlador recibió una solicitud de detección a través de una dirección IP de broadcast que tiene una dirección IP de origen que no está en ninguna subred configurada en el controlador. Esto también significa que el controlador está descartando el paquete.

El problema es que el AP no está enviando la solicitud de detección a la dirección IP de administración. El controlador está informando de una solicitud de detección de broadcast desde una VLAN que no está configurada en el controlador. Esto ocurre normalmente cuando los trunks del cliente permitieron las VLANs en vez de restringirlas a VLANs inalámbricas.

Complete estos pasos para resolver este problema:

1. Si el controlador está en otra subred, los APs se deben **imprimir** para la dirección IP del controlador o deben recibir la dirección IP del controlador usando uno de los métodos de detección.
2. El switch se configura para permitir algunas VLANs que no están en el controlador. Restrinja las VLANs permitidas en los trunks.

Problema 11: 1250 LAP incapaz de unirse al WLC

La configuración consiste en un WLC 2106 que ejecuta la versión 4.1.185.0. Un AP 1250 de Cisco no puede unirse al controlador.

El log en el WLC muestra esto:

```
Mon Jun 2 21:19:37 2008AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2
21:19:37 2008 AP Associated. Base Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:26 2008 AP
Disassociated. Base Radio MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:20 2008 AP with MAC
f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2 21:19:20 2008 AP Associated. Base
Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:09 2008 AP Disassociated. Base Radio
MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:03 2008 AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x)
is unknown.
```

Solución: Esto es porque el LAP de la serie 1250 de Cisco no se soporta en la versión 4.1. El AP Cisco Aironet 1250 Series se soporta desde la versión del controlador 4.2.61 y posterior. Para solucionar este problema, haga un upgrade del software de controlador a 4.2.61.0 o posterior.

Problema 12: AP incapaz de unirse al WLC, firewall bloqueando los puertos necesarios

Si se utiliza un firewall en la red de la empresa, asegúrese de que los puertos siguientes estén habilitados en el firewall para que el LAP pueda unirse al controlador y comunicarse con él.

Debe habilitar estos puertos:

- Habilite estos puertos UDP para el tráfico LWAPP:Datos - 12222Control - 12223
- Habilite estos puertos UDP para el tráfico de movilidad:16666 - 1666616667 - 16667
- Habilite los puertos UDP 5246 y 5247 para el tráfico CAPWAP.
- TCP 161 y 162 para SNMP (para el sistema de control inalámbrico [WCS])

Estos puertos son opcionales (dependiendo de sus requisitos):

- UDP 69 para TFTP
- TCP 80 y/o 443 para HTTP o HTTPS para acceso a GUI
- TCP 23 y/o 22 para Telnet o SSH para acceso a CLI

Problema 13: Dirección IP duplicada en la red

Éste es otro problema frecuente que se ve cuando el AP intenta unirse al WLC. Puede que vea este mensaje de error cuando el AP intente unirse al controlador.

```
No more AP manager IP addresses remain
```

Una de las razones de este mensaje de error es que hay una dirección IP duplicada en la red que coincide con la dirección IP del administrador de APs. En tal caso, el LAP permanece en un ciclo de activación y no puede unirse al controlador.

Los debugs mostrarán que el WLC recibe las solicitudes de detección LWAPP de los APs y transmite una respuesta de detección LWAPP a los APs. Sin embargo, los WLCs no reciben la solicitud de unión LWAPP de los APs.

Para resolver este problema, haga un ping del administrador de APs desde un host cableado en la misma subred IP que el administrador de APs. Después compruebe la memoria caché de ARP. Si se encuentra una dirección IP duplicada, remueva el dispositivo con la dirección IP duplicada o cambie la dirección IP en el dispositivo de modo que tenga una dirección IP única en la red.

El AP puede entonces unirse al WLC.

Problema 14: Los APs LWAPP no se unen al WLC si la MTU de la red es inferior a 1500 bytes

Esto es debido al ID de bug Cisco **CSCsd94967**. Los APs LWAPP podrían no unirse a un WLC. Si la solicitud de unión LWAPP es superior a 1500 bytes, LWAPP debe fragmentarla. La lógica para todos los APs LWAPP es que el tamaño del primer fragmento es 1500 bytes (incluyendo el encabezado IP y UDP) y del segundo fragmento es 54 bytes (incluyendo el encabezado IP y UDP). Si la red entre los APs LWAPP y el WLC tiene un tamaño de MTU inferior a 1500 (como podría encontrarse cuando se utiliza un protocolo de tunelización como IPSec VPN, GRE, MPLS, etc.), el WLC no puede gestionar la solicitud de unión LWAPP.

Encontrará este problema en estas condiciones:

- WLC que ejecuta el software versión 3.2 o anterior

- La MTU de trayectoria de red entre el AP y el WLC es inferior a 1500 bytes

Para resolver este problema, utilice cualquiera de estas opciones:

- Hacer un upgrade al software del WLC 4.0, si la plataforma lo soporta. En la versión 4.0 del WLC, este problema se corrige permitiendo que el túnel LWAPP reensamble hasta 4 fragmentos.
- Aumentar la MTU de trayectoria de red a 1500 bytes.
- Utilizar REAPs 1030 para las ubicaciones accesibles a través de trayectorias de MTU baja. Las conexiones LWAPP REAP a los APs 1030 se han modificado para gestionar esta situación reduciendo la MTU usada para el modo REAP.

Problema 15: El AP de la serie 1142 no se une al WLC, mensaje de error en el WLC: lwapp_image_proc: unable to open tar file

Los APs de la serie 1142 se soportan solamente con la versión del WLC 5.2 y posterior. Si ejecuta versiones del WLC anteriores a la 5.2, no puede registrar el LAP en el controlador y verá un mensaje de error similar a éste:

```
*Mar 27 15:04:38.596: %LWAPP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.597: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.606: %LWAPP-3-CLIENTERRORLOG: not receive read response(3)
*Mar 27 15:04:38.609: lwapp_image_proc: unable to open tar fileMar 12 15:47:27.237
spam_lrad.c:8317 LWAPP-3-IMAGE_DOWNLOAD_ERR3:
Refusing image download request from AP 0X:2X:D0:FG:a7:XX - unable to open
image file /bsn/ap//c1140
```

Para registrar los LAPs 1140 en el WLC, haga un upgrade del firmware en el WLC a la versión 5.2 o posterior.

Problema 16: Los LAPs de la serie 1000 no pueden unirse al controlador de LAN inalámbrica, el WLC ejecuta la versión 5.0

Esto es porque la versión de software del WLC 5.0.148.0 o posterior no es compatible con los APs Cisco Aironet 1000 Series. Si usted tiene las Cisco 1000 Series TRASLAPA en una red, que funciona con las versiones 5.0.48.0 del WLC, el REVESTIMIENTO de las 1000 Series no se une al regulador y usted ve este mensaje trampa en el WLC.

```
"AP with MAC xx:xx:xx:xx:xx:xx is unkown"
```

Problema 17: Revestimientos con la imagen de la malla no capaz de unirse al WLC

El Lightweight Access Point no se registra con el WLC. El registro visualiza esto el mensaje de error

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
 Type: WLAN USER
```

Esto puede suceder si el Lightweight Access Point fue enviado con una imagen de la malla y está en el modo Bridge. Si el REVESTIMIENTO fue pedido con el software de la malla en él, usted necesita agregar el REVESTIMIENTO a la lista de la autorización AP. Elija la **Seguridad > las directivas AP** y agregue el **AP a la** lista de la autorización. El AP debe después unirse a, descargar la imagen del regulador, después del registro con el WLC en el modo Bridge. Entonces usted necesita cambiar el AP al modo local. El REVESTIMIENTO descarga la imagen, reinicia y se registra de nuevo al regulador en el modo local.

Problema 18: Mensaje de error - Descarte de la solicitud de detección primaria desde el AP XX: AA: BB: XX: DD: DD - APs máximos unidos 6/6

Hay un límite respecto al número de LAPs que un WLC puede soportar. Cada WLC soporta un número de LAPs determinado, que depende del modelo y de la plataforma. Este mensaje de error se ve en el WLC cuando éste recibe una solicitud de detección después de haber alcanzado su capacidad de APs máxima.

A continuación se indica el número de LAPs soportados en las distintas plataformas y modelos de WLC:

- El controlador de la serie 2100 soporta hasta 6, 12 o 25 LAPs. Esto depende del modelo de WLC.
- El 4402 soporta hasta 50 LAPs, mientras que el 4404 soporta hasta 100. Esto hace que sea ideal para las empresas de gran tamaño y las aplicaciones de alta densidad.
- Catalyst 6500 Series Wireless Services Module (WiSM) es un Catalyst 6500 Switch integrado y dos Cisco 4404 Controllers que soportan hasta 300 LAPs.
- Cisco 7600 Series Router WiSM es un Cisco 7600 Router integrado y dos Cisco 4404 Controllers que soporta hasta 300 LAPs.
- Cisco 28/37/38xx Series Integrated Services Router es el módulo de red de router 28/37/38xx integrado y controlador Cisco que soporta hasta 6, 8, 12 o 25 LAPs, dependiendo de la versión del módulo de red. Las versiones que soportan 8, 12 o 25 APs y la versión de 6 puntos de acceso NME-AIR-WLC6-K9 ofrecen un procesador de alta velocidad y más memoria integrada de tarjeta que la versión de 6 puntos de acceso NM-AIR-WLC6-K9.
- Catalyst 3750G Integrated WLC Switch es un Catalyst 3750 Switch integrado y un Cisco 4400 Series Controller que soporta hasta 25 o 50 LAPs.

Información Relacionada

- Ejemplo de Configuración de Autorización de Punto de Acceso Ligero (LAP) en una Red Inalámbrica Unificada de Cisco
- Registro de AP Ligero (LAP) a un Controlador de LAN Inalámbrica (WLC)
- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, versión 4.1
- Soporte Técnico y Documentación - Cisco Systems