Solucione problemas de un AP ligero que no puede unirse a un WLC

Contenido

Introducción

Este documento describe el proceso de detección y unión del controlador LAN inalámbrico (WLC) de AireOS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de Lightweight Access Points (LAP) y Cisco AireOS WLC
- Conocimientos básicos sobre el protocolo de punto de acceso ligero (CAPWAP)

Componentes Utilizados

Este documento se centra en los WLC de AireOS y no cubre Catalyst 9800 aunque el proceso de unión es en su mayoría similar.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Descripción General del Proceso de Detección y Unión de 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.

Sin embargo, esto plantea una pregunta: ¿cómo encontraron los LAP la dirección IP de administración del controlador cuando está en una subred diferente?

Si no le indica al LAP dónde está el controlador a través de la opción DHCP 43, la resolución del sistema de nombres de dominio (DNS) de Cisco-capwap-controller.local_domain, o lo configura estáticamente, el LAP no sabe dónde en la red encontrar 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. Además, el LAP recuerda la dirección IP de administración de su controlador y los controladores presentes como peers de movilidad incluso a través de reinicios. Sin embargo, tan pronto como el AP se une a otro WLC, solamente recuerda la IP de ese nuevo WLC y sus pares de la movilidad y no los anteriores. Por lo tanto, si coloca el LAP primero en la subred local de la interfaz de administración, encuentra la interfaz de administración del controlador y recuerda la dirección. Esto se llama impresión. Esto no ayuda a encontrar el controlador si sustituye un LAP posteriormente. Por lo tanto, Cisco recomienda el uso de la opción DHCP 43 o los métodos DNS.

Los LAPs siempre se conectan a la dirección de la interfaz de administración del controlador primero con una solicitud de detección. El controlador entonces le dice al LAP la dirección IP de la interfaz del administrador AP de la capa 3 (que también puede ser la administración predeterminada) para que el LAP pueda enviar una solicitud de unión a la interfaz del administrador AP siguiente.

El AP pasa por este proceso al inicio:

- **El LAP se inicia y asigna una dirección IP mediante DHCP, si no tenía asignada previamente una dirección IP estática.**

- **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:**

a. **Opción DHCP 43 (buena para las empresas globales en las que las oficinas y los controladores se encuentran en diferentes continentes).**

b. **Entrada DNS para** cisco-capwap-controller (buena para empresas locales - también se puede utilizar para encontrar dónde se unen los nuevos AP) Si utiliza CAPWAP, asegúrese de que haya una entrada DNS para cisco-capwap-controller.

- **Direcciones IP de administración de controladores que el LAP recuerda previamente.**
- **Un broadcast de capa 3 en la subred.**
- **Información configurada estáticamente .**
- **Los controladores presentes en el grupo de la movilidad del WLC el AP se unieron por última vez.**

De esta lista, el método más fácil de usar para la implementación es tener los LAPs en la misma subred que la interfaz de administración del controlador y permitir que el broadcast de la capa 3 de los LAPs encuentre el controlador. Este método se debe utilizar para empresas 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 empresas que tienen todos sus controladores en una única 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 por el 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. Puede configurar estáticamente la información necesaria para unirse a un controlador mediante el puerto de la consola y la CLI de los AP. Para obtener información sobre cómo configurar estáticamente la información del controlador mediante la CLI del AP, utilice este comando:

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Para obtener información sobre cómo configurar la opción DHCP 43 en un servidor DHCP, consulte el ejemplo de configuración de la opción DHCP 43

- 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 del administrador de AP, el número de AP ya conectados a cada interfaz del administrador de AP y la capacidad excedente general para el controlador.

- 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):

a. Nombre del sistema del controlador principal (configurado previamente en LAP).

b. Nombre del sistema del controlador secundario (configurado previamente en LAP).

c. Nombre del sistema del controlador terciario (configurado previamente en LAP).

d. Controlador primario (si el LAP no se ha configurado previamente con ningún nombre de controlador primario, secundario o terciario). Se utiliza para saber siempre qué controlador es un nuevo LAP se une).

e. Si no se observa ninguna de las condiciones anteriores, balancee la carga entre los controladores mediante el uso del 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 responde a todas las solicitudes de detección sin una verificación de certificado o 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 una respuesta de unión de su elección, el LAP intenta el controlador siguiente en la lista, a menos que el controlador sea un controlador configurado (primario/secundario/terciario).

- 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.

- Si tiene la misma imagen de software, pide la configuración del controlador y pasa al estado registrado en el controlador.

Después de descargar la configuración, el AP puede volver a cargarse para aplicar la nueva configuración. Por lo tanto, una recarga adicional puede ocurrir y es un comportamiento normal.

Debug desde el Controlador

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

- **debug capwap events enable**: muestra los paquetes de detección y los paquetes de unión.

- **debug capwap packet enable**: muestra la información de nivel de paquete de los paquetes de detección y de unión.

- **debug pm pki enable**: muestra el proceso de validación de certificados.

- **debug disable-all**: desactiva las depuraciones.

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:

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

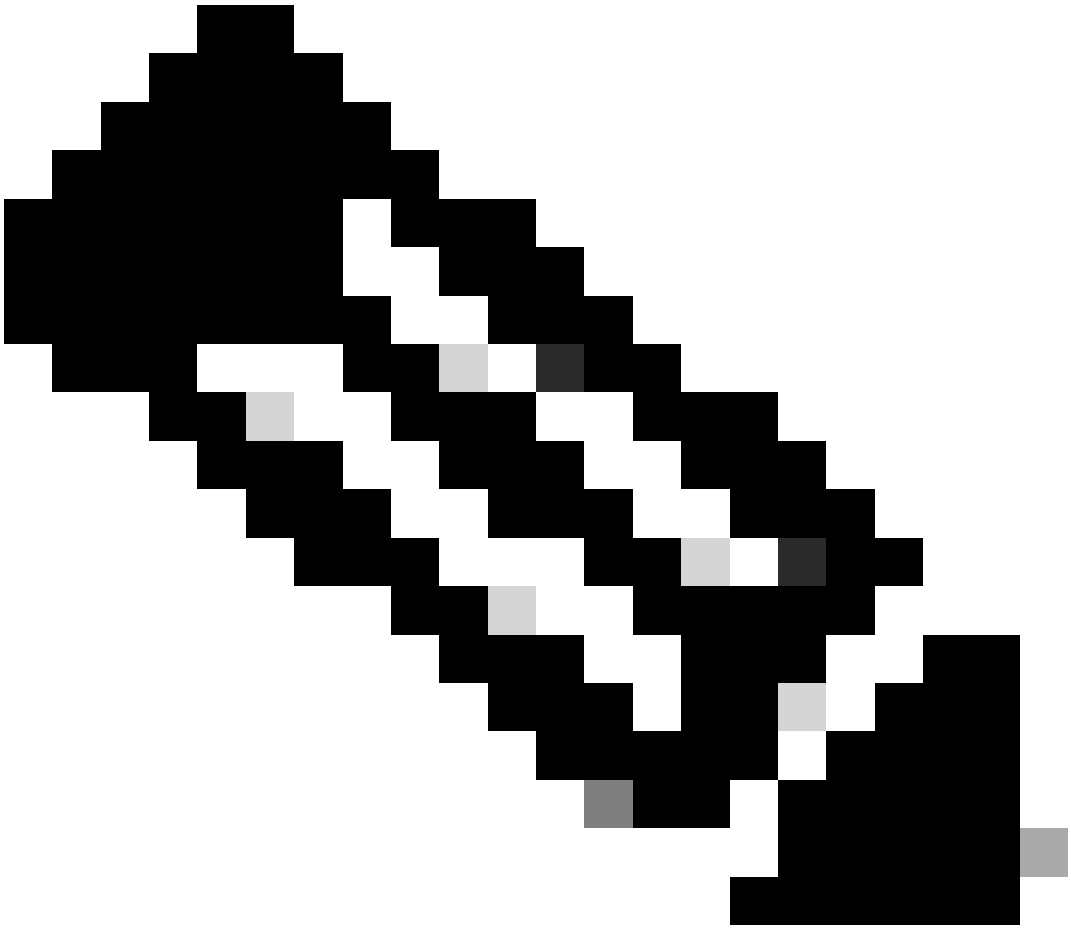
Una vez capturados los debugs, utilice el debug disable-all comando para inhabilitar todos los debugs.

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

debug capwap events enable

Este comando proporciona información sobre los eventos y errores CAPWAP que se producen en el proceso de detección y unión CAPWAP.

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



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

<#root>

debug capwap events enable

```
*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317
```

!--- CAPWAP discovery request sent to the WLC by the LAP.

```
*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317
```

!--- WLC responds to the discovery request from the LAP.

```
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317
```

!--- LAP sends a join request to the WLC.

```
*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join
```

!--- WLC responds with a join reply to the LAP.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure

!--- LAP requests for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99

!--- WLC responds by providing all the necessary configuration information to the LAP.

*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.

!--- LAP is up and ready to service wireless clients.

*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- 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.

Puede ver estos mensajes en el resultado del **debug capwap events enable** comando si el LAP descarga una imagen del controlador como parte del proceso de registro:

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Una vez que se completa la descarga de la imagen, el LAP se reinicia y ejecuta la detección y se une al algoritmo nuevamente.

debug pm pki enable

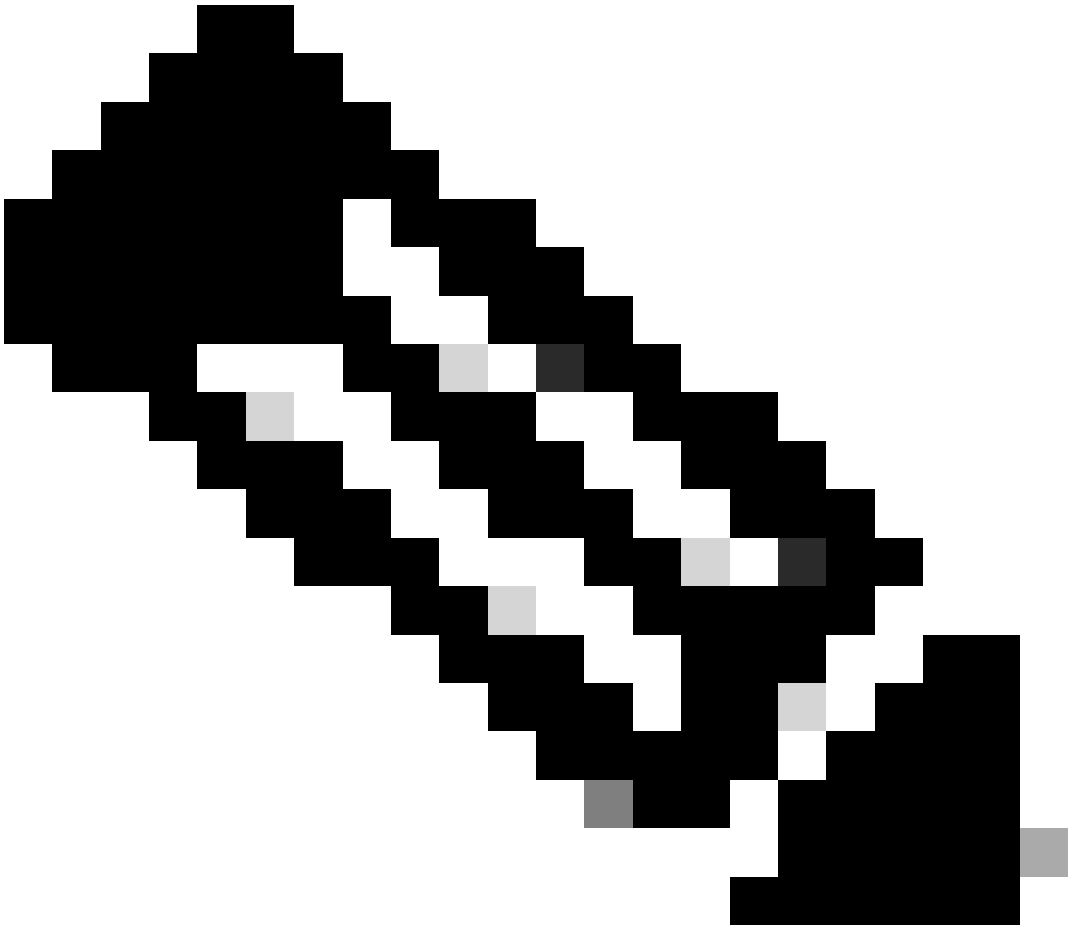
Como parte del proceso de unión, el WLC autentica cada LAP mediante la confirmación de que su certificado es válido.

Cuando el AP envía la solicitud de unión CAPWAP al WLC, incrusta su certificado X.509 en el mensaje CAPWAP. El AP también genera un ID de sesión aleatorio que también se incluye en la solicitud de unión CAPWAP. Cuando el WLC recibe la solicitud de unión CAPWAP, valida la firma del certificado X.509 con la clave pública AP y verifica que el certificado fue emitido por una autoridad de certificación de confianza.

También observa la fecha y hora de inicio del intervalo de validez del certificado AP y compara esa fecha y hora con su propia fecha y hora (por lo tanto, el reloj del controlador debe configurarse cerca de la fecha y hora actuales). Si se valida el certificado X.509, el WLC genera un llave de encripción AES aleatoria. El WLC conecta las claves AES en su motor crypto para que pueda cifrar y descifrar futuros mensajes de control CAPWAP intercambiados con el AP. Observe que los paquetes de datos se envían en el claro en el túnel CAPWAP entre el LAP y el

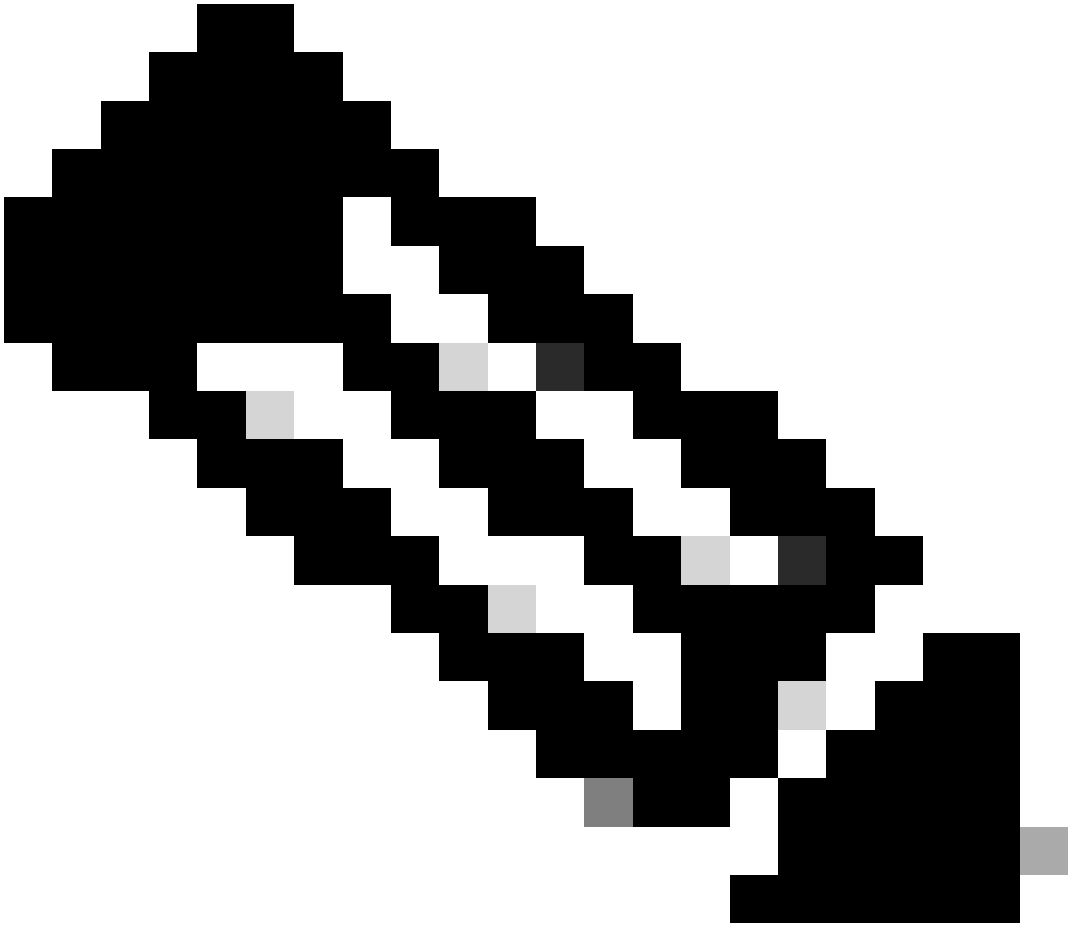
controlador.

El **debug pm pki enable** comando muestra el proceso de validación de la certificación que ocurre en la fase de unión en el controlador. El **debug pm pki enable** comando también muestra la llave hash AP en 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 fabricado (MIC), usted no ve una llave hash.



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

Este es el resultado del **debug pm pki enable** comando 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 restricciones de espacio.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject


*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Depuración desde el AP

Si los debugs del controlador no indican una solicitud de unión, puede depurar el proceso desde el AP si el AP tiene un puerto de consola. Puede ver el proceso de inicio del AP con estos comandos, pero primero debe entrar en el modo de habilitación (la contraseña predeterminada es Cisco).

- **debug dhcp detail** : muestra información de la opción DHCP 43.
- **debug ip udp**: muestra todos los paquetes UDP recibidos y transmitidos por el AP.
- debug capwap client event : muestra los eventos capwap para el AP.
- **debug capwap client error**: muestra errores capwap para AP.

- **debug dtls client event**: muestra los eventos DTLS para el AP.
- **debug dtls error enable**: muestra errores DTLS para el AP.
- **undebug all**: inhabilita los debugs en el AP.

Aquí hay un ejemplo de la salida de los debug capwapcomandos. Esta salida parcial da una idea de los paquetes enviados por el AP en el proceso de arranque para descubrir y unirse a un controlador.

<#root>

```
AP can discover the WLC via one of these options :

!--- AP discovers the WLC via option 43

*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set

!--- capwap Discovery Request using the statically configured controller information.

*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set

!--- Capwap Discovery Request sent using subnet broadcast.
```

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

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

Comprobación Previa de los Elementos Básicos

- ¿Pueden comunicarse el AP y el WLC?
- Asegúrese de que el AP obtenga una dirección de DHCP (verifique las concesiones del servidor DHCP para la dirección MAC del AP).
- Haga ping en el AP desde el controlador.
- Verifique si la configuración STP en el switch es correcta, por lo que los paquetes a las VLAN no se bloquean.
- 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 se reinicia, inicia la secuencia de detección del WLC e intenta localizar el AP. Reinicie el AP y compruebe si se une al WLC.

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

Aviso práctico: Vencimientos del certificado - FN63942

Los certificados integrados en el hardware son válidos durante un período de 10 años después de la fabricación. Si sus AP o WLC tienen más de 10 años, los certificados caducados pueden causar problemas de unión de AP. Encontrará más información sobre este problema en este aviso práctico: Aviso práctico: FN63942.

Posibles problemas que buscar: Ejemplos

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

Complete estos pasos para resolver este problema:

- Ejecute debug dtls client error + debug dtls client event comandos en el AP:

<#root>

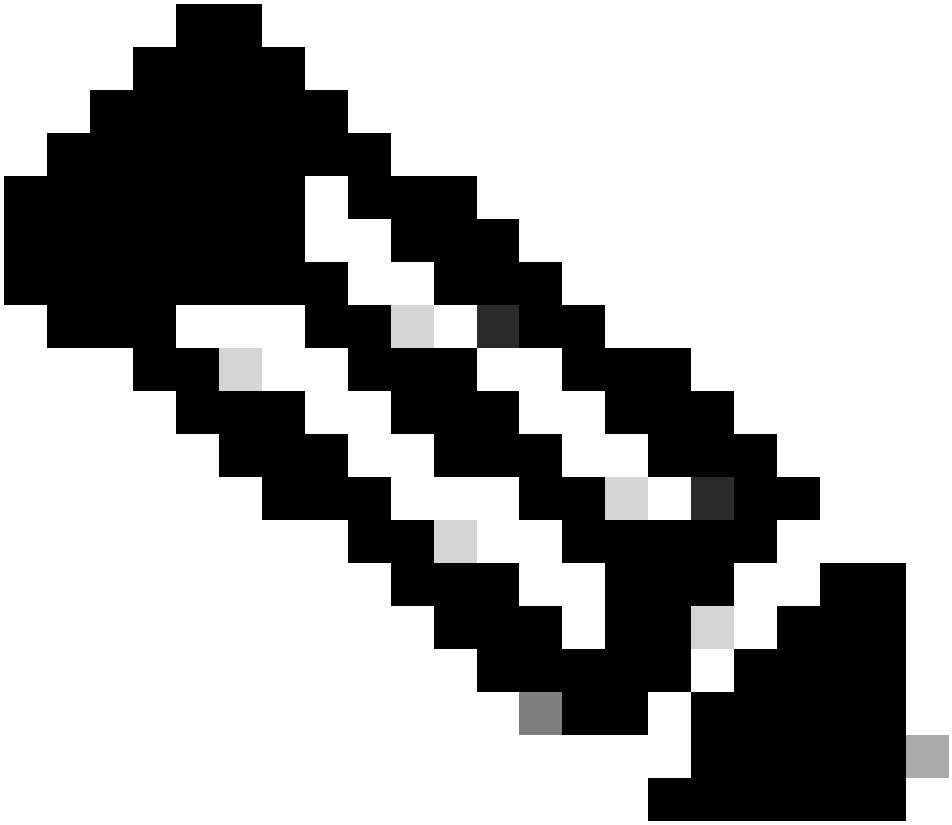
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Esta información muestra claramente que el tiempo del controlador está fuera del intervalo de validez del certificado del AP. Por lo tanto, el AP no puede registrarse con el controlador. Los certificados instalados en el AP tienen un intervalo de validez predefinido. La hora del controlador debe configurarse de modo que esté dentro del intervalo de validez del certificado AP.

- Ejecute el **show time** comando de la CLI del controlador para verificar que la fecha y la hora establecidas en el controlador se encuentren 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 configurada correctamente en el controlador, elija Commands > Set Time en el modo GUI del controlador, o ejecute el comando config time en la CLI del controlador para establecer la hora del controlador.

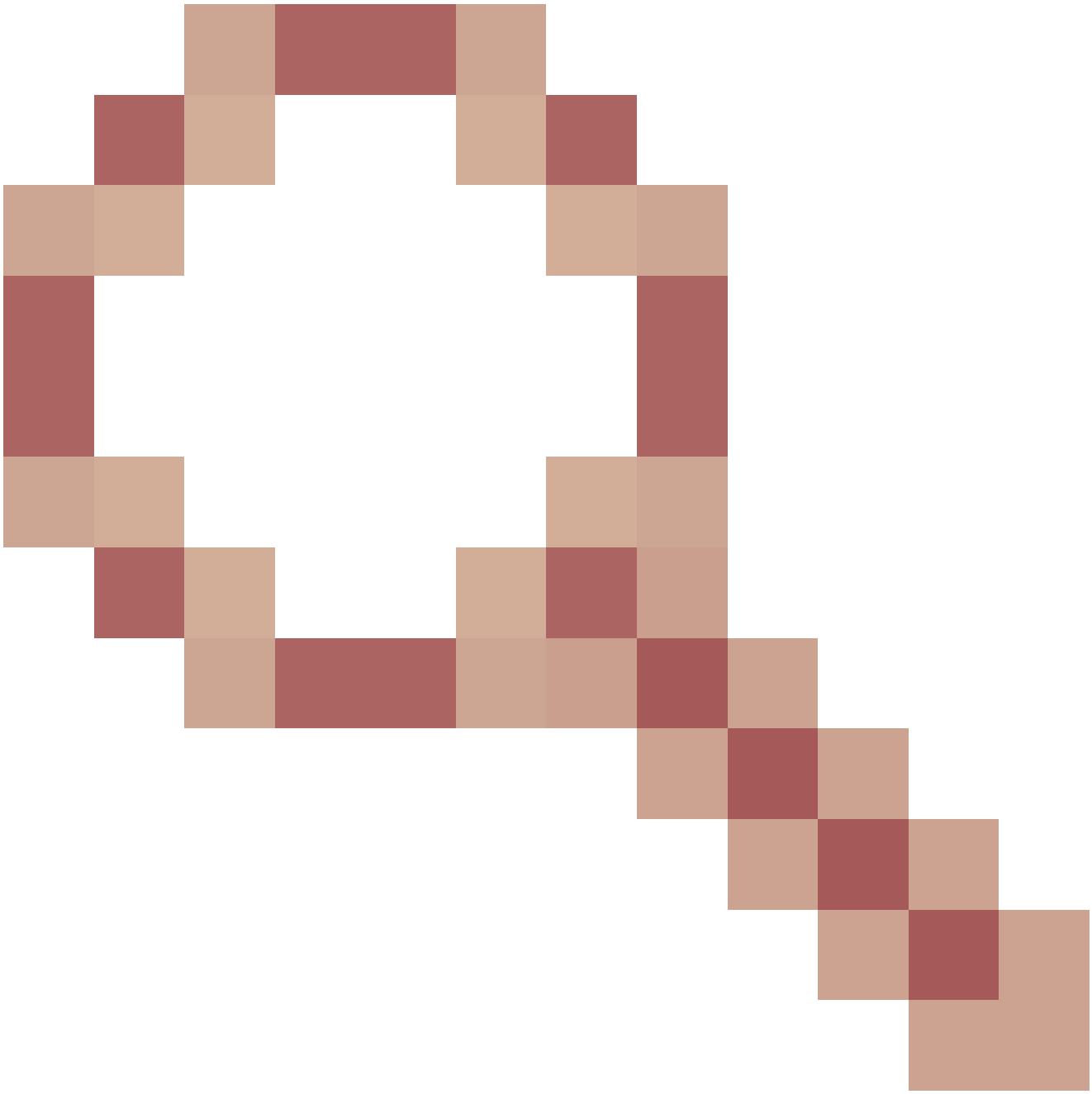
- En los AP con acceso CLI, verifique los certificados con el **show crypto ca certificates** comando de la CLI AP.

Este comando permite verificar el intervalo de validez del certificado fijado en el AP. Aquí tiene un ejemplo:

```
AP00c1.649a.be5c#show crypto ca cert
.........................................
.........................................
.........................................
.............................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
.................................
.................................
.................................
```

No se muestra el resultado completo porque puede haber muchos intervalos de validez asociados con el resultado de este comando. Considere 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.

- Consulte el ID de bug de Cisco CSCuq19142



LAP/WLC MIC o la caducidad de la vida de SSC causa la falla de DTLS: ID de bug de Cisco CSCuq19142.

Problema 2: Discordancia en el dominio de regulación

Verá este mensaje en el resultado del **debug capwap events enable** comando:

<#root>

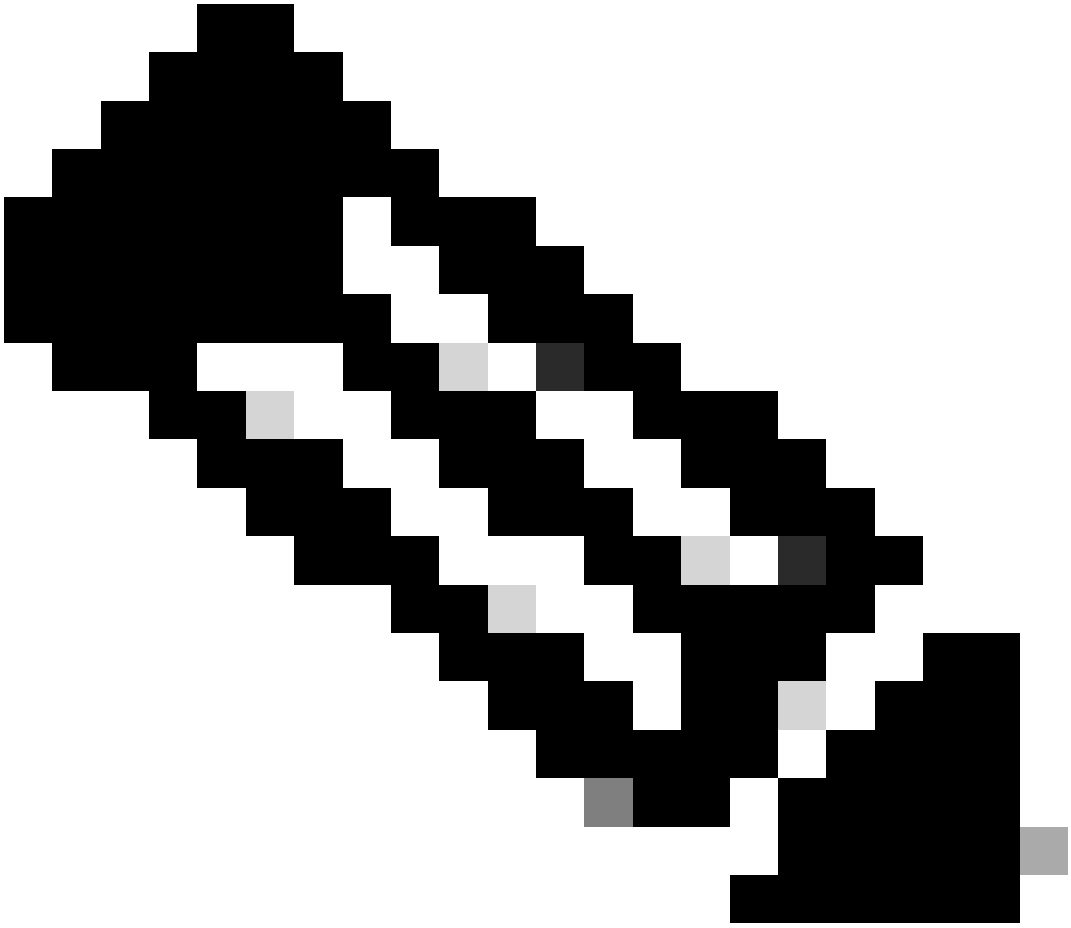
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

El mensaje indica claramente que hay una discordancia en el dominio regulador del LAP y del WLC. El WLC soporta múltiples dominios de regulación, pero cada dominio de regulación debe ser seleccionado antes de que un AP 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). Al adquirir puntos de acceso, asegúrese de que comparten el mismo dominio de regulación. Solamente entonces los AP podrán registrarse con el WLC.



Nota: tanto las radios 802.1b/g como 802.11a deben estar en el mismo dominio de regulación para un solo AP.

Problema 3: Lista de autorización de AP habilitada en el WLC; el LAP no está en la lista de autorización

En estos casos, verá este mensaje en el controlador en el resultado del debug capwap events enable comando:

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP 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
CAPWAP 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
CAPWAP 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 CAPWAP 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 CAPWAP 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 utiliza un LAP que tiene un puerto de consola, verá este mensaje cuando ejecute el debug capwap client error comando:

```
<#root>

APO01d.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 forma parte de la lista de autorización de AP en el controlador.

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

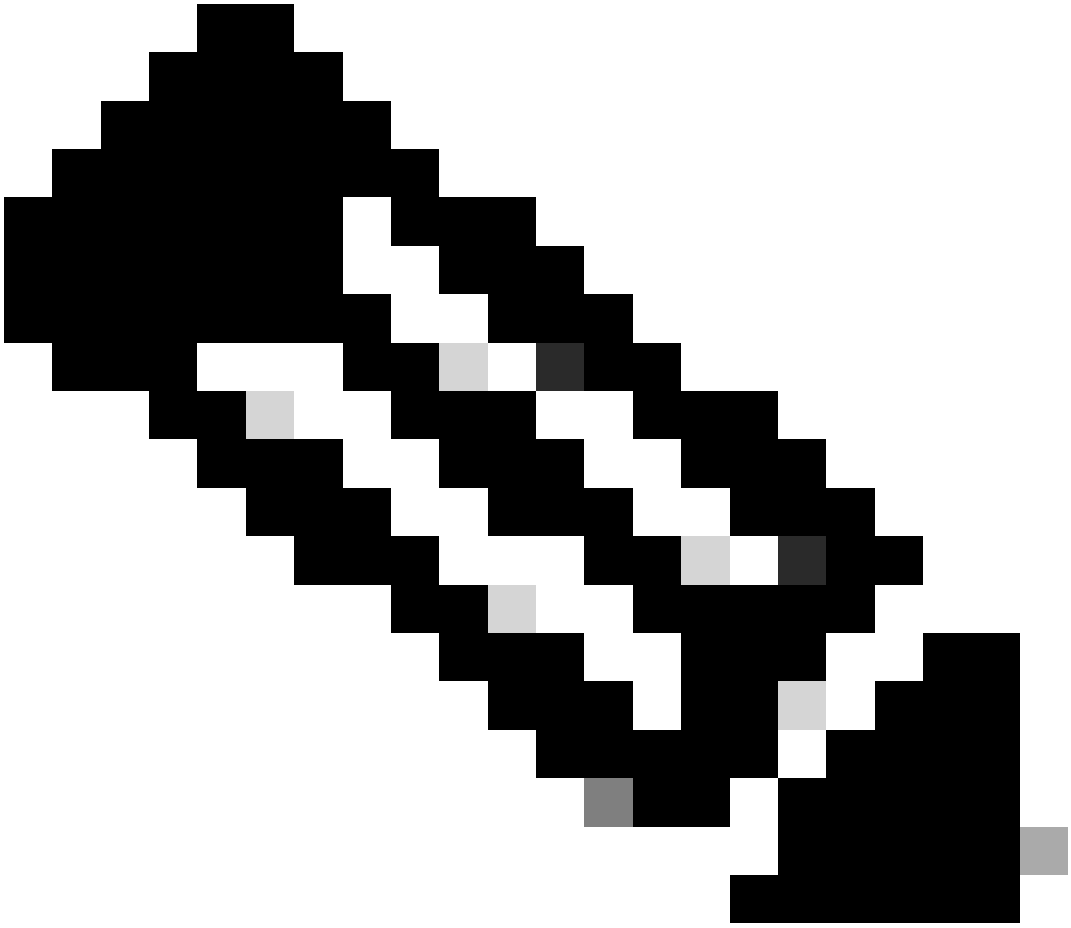
```
<#root>

(Cisco Controller) >

show auth-list

Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Para agregar un LAP a la lista de autorización AP, utilice el config auth-list add mic <AP MAC Address> comando. 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 4: Hay un certificado o corrupción de clave pública en el AP

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

Ejecute los debug capwap errors enablecomandos y **debug pm pki enable** command. Ve mensajes que indican los certificados o llaves dañados.



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

<#root>

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

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:

- MIC AP: Solicite una autorización de devolución de mercancía (RMA).
- LSC AP - Vuelva a proveer su certificado LSC.

Problema 5: El controlador recibe un mensaje de detección de AP en una VLAN incorrecta (verá el mensaje de detección debug, pero no response)

Puede ver este mensaje en el resultado deldebug capwap events enable comando:

<#root>

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 por una dirección IP de difusión con una dirección IP de origen que no está en ninguna subred configurada en el controlador. Esto también significa que el controlador es el que descarta el paquete.

El problema es que el AP no es lo que envió la solicitud de detección a la dirección IP de administración. El controlador informa de una solicitud de detección de broadcast desde una VLAN que no está configurada en el controlador. Esto ocurre generalmente cuando los trunks permitieron las VLAN y no las restringieron a las VLAN inalámbricas.

Complete estos pasos para resolver este problema:

- Si el controlador está en otra subred, los AP deben estar **preparados** para la dirección IP del controlador, o los AP deben recibir la

dirección IP del controlador con el uso de uno de los métodos de detección.

- El switch está configurado para permitir algunas VLAN que no están en el controlador. Restrinja las VLANs permitidas en los trunks.

Problema 6: AP no puede unirse al WLC, firewall que bloquea los puertos necesarios

Si se utiliza un firewall en la red de la empresa, asegúrese de que estos puertos estén habilitados en el firewall para que el LAP se una y se comunique con el controlador.

Debe habilitar estos puertos:

- Habilite estos puertos UDP para el tráfico CAPWAP:
  - Datos - 5247
  - Control - 5246
- Habilite estos puertos UDP para el tráfico de movilidad:
  - 16666 - 16666
  - 16667 - 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 (según 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 7: Dirección IP duplicada en la red

Este es otro problema común visto cuando el AP intenta unirse al WLC. Puede ver este mensaje de error cuando el AP intenta unirse al controlador.

<#root>

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 mantiene las iniciaciones del ciclo de la energía y no puede unirse al controlador.

Los debugs muestran que el WLC recibe las solicitudes de detección de LWAPP de los AP y transmite una respuesta de detección de LWAPP a los AP.

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, quite el dispositivo con la dirección IP duplicada o cambie la dirección IP en el dispositivo para que tenga una dirección IP única en la red.

El AP puede entonces unirse al WLC.

Problema 8: Los LAP con la imagen de la malla no pueden unirse al WLC

El Lightweight Access Point no se registra con el WLC. El registro muestra el siguiente mensaje de error:

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

Esto puede suceder si el Lightweight Access Point se envió con una imagen de malla y está en el modo Bridge. Si el LAP fue pedido con el software de la malla en él, usted necesita agregar el LAP a la lista de autorización AP. Elija **Security > AP Policies** y agregue **AP** a la lista de autorización. El AP debe entonces unirse, descargar la imagen del controlador, después registrarse con el WLC en el modo del puente. Luego debe cambiar el AP al modo local. El LAP descarga la imagen, se reinicia y se vuelve a registrar en el controlador en el modo local.

Problema 9: Dirección incorrecta de Microsoft DHCP

Los puntos de acceso pueden renovar sus direcciones IP rápidamente cuando se hace un intento de unirse a un WLC, lo que puede hacer que los servidores DHCP de Windows marquen estas IP como BAD_ADDRESS que podría agotar rápidamente el conjunto DHCP. Consulte para obtener más información en el capítulo Client Roaming de la Guía de Configuración de Cisco Wireless Controller, Release 8.2.

Información Relacionada

- **Soporte técnico y descargas de Cisco**

- **Proceso de unión de PA con Catalyst 9800**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).