Preguntas Más Frecuentes sobre Mensajes de Error y de Sistema del Controlador de la LAN inalámbrica (WLC)

Contenido

Introducción

Este documento proporciona información sobre las preguntas más frecuentes (FAQ) sobre los mensajes de error y los mensajes del sistema para los Cisco Wireless LAN (WLAN) Controllers (WLC).

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

FAQ de los mensajes de error

Q. Hemos iniciado la conversión de más de 200 puntos de acceso (AP) de Cisco IOS® Software to Lightweight AP Protocol (LWAPP) con Cisco 4404 WLC. Hemos terminado la conversión de 48 AP y recibimos un mensaje en el WLC que indica: **[ERROR] spam_lrad.c 4212: El AP no puede conectarse a porque se alcanzó el número máximo de AP en la interfaz 1.** ¿Por qué se produce el error?

A. Debe crear interfaces adicionales de administrador AP para soportar más de 48 AP. De lo contrario, recibe el siguiente el error:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Configure las interfaces múltiples del administrador AP y configure puertos de respaldo o primarios que otras interfaces del administrador AP no utilicen. *Debe* crear una segunda interfaz del administrador AP para activar AP adicionales. Pero, asegúrese de que sus configuraciones del puerto del puerto primario y de la salvaguardia para cada encargado no solapen. Es decir si el administrador AP 1 utiliza el puerto 1 como el primario y el puerto 2 como el de respaldo, el administrador AP 2 debe utilizar el puerto 3 como el primario y el puerto 4 como el de respaldo.

Q. Tengo un controlador del Wireless LAN (WLC) 4402 y utilizo 1240 Lightweight Access Point (LAP). Estoy intentando habilitar la cifrado del 128-bit en el WLC.

Cuando selecciono la cifrado WEP de 128 bits en el WLC, recibo un error que dicen ese 128-bit no se soporta en el 1240s: `[ERROR] spam_lrad.c 12839: No crear el mde SSID en CISCO AP xx: xx: xx: xx: xx: xx porque el dígito binario WEP128 no se soporta.` ¿Por qué recibo este error?

A. Las longitudes de clave mostradas en el WLCs son realmente el número de bits que estén en el secreto compartido y no incluyan el 24-bits del vector de inicialización (iv). Muchos productos, que incluye los productos Aironet, lo llaman una clave WEP del 128-bit. En la realidad es un clave del 104-bit con 24-bit IV. Los tamaños de clave del 104-bit son lo que debe habilitar en el WLC para el cifrado WEP del 128-bit.

Si usted elige el tamaño de clave del 128-bit en el WLC, es realmente un 152-bit (128 + 24 IV) cifrados de la clave WEP. Solamente los revestimientos de las Cisco 1000 Series (AP1010, AP1020, AP1030) utilizan el uso de la configuración de la clave WEP del bit WLC 128.

Q. Porqué consigo los tamaños de la clave WEP de los bits 128 no se soportan en 11xx, 12xx y 13xx AP modelo. `Wlan no será avanzado a estos puntos de acceso.` ¿mensaje de error cuando intento configurar el WEP en un WLC?

A. En un controlador del Wireless LAN, cuando elige el WEP estático como el método de seguridad de la capa 2, tienes estas opciones o los tamaños de la clave WEP.

- no establecido
- 40 bits
- 104 bits
- bits 128

Estos valores de los tamaños de clave no incluyen 24-bit el vector de inicialización (iv), que se concatena con la clave WEP. Así pues, para un WEP 64-bit, necesitas elegir **40 bits** como los tamaños de la clave WEP. El controlador agrega el 24-bit IV a esto para hacer una clave WEP 64-bit. Semejantemente, para una clave WEP del dígito binario 128, elige **104 bits**.

Los controladores también soportan 152 claves WEP del dígito binario (dígito binario 128 + 24 dígitos binarios IV). Esta configuración no se soporta en el 11xx, el 12xx y el 13xx AP modelo. Tan cuando intentas configurar el WEP con 144 bits, el controlador da un mensaje que esta configuración WEP no está avanzada a 11xx, a 12xx y a 13xx AP modelo.

Q. Los clientes no pueden autenticar a un WLAN que se configure para el WPA2 y el controlador visualiza el apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: : `No podía procesar el RSN y DEFORMAR los IE. coloca no usando RSN (WPA2) en el WLAN que requiere RSN.MobileStation:00:0c:f1:0c:51:22, SSID:` mensaje de error del <>. ¿Por qué recibo este error?

A. Esto ocurre sobre todo debido a la incompatibilidad en el lado del cliente. Intenta estos pasos de progresión para fijar este problema:

- Marca si el cliente es Wi-fi certificado para el WPA2 y marca la configuración del cliente para el WPA2.
- Marca la hoja de datos para ver si la utilidad de cliente soporta el WPA2. Instala cualquier corrección liberada por el vendedor para soportar el WPA2. Si utilizas la utilidad de Windows,

aseegurare que has instalado la corrección del WPA2 de Microsoft para soportar el WPA2.
- Actualiza el driver y el firmware del cliente.
- Apaga las extensiones Aironet en el WLAN.

Q. Una vez que reinicio el WLC, consigo `lunes el 17 de julio 15:23:28 la anomalía 2006 MFP detectada - 3023 eventos inválidos MIC encontrados según lo violados por la radio 00:XX:XX:XX y detectados por el interfaz dot11 en el slot0 de AP 00:XX:XX:XX en 300 segundos al observar las respuestas de la punta de prueba,` mensaje de error de las `tramas de recuperación de problemas.` ¿Por qué este error ocurre y cómo me libro de él?

A. Se considera este mensaje de error cuando los marcos con los valores incorrectos MIC son detectados por los revestimientos activados MFP. Refiera a la protección del capítulo de la Administración de la infraestructura (MFP) con WLC y TRASLAPE el ejemplo de la configuración para más información sobre MFP. Complete uno de estos cuatro pasos:

1. Controle y quite a cualquier granuja o APs inválidos o cliente en su red, que generen los marcos inválidos.
2. Inhabilite la infraestructura MFP, si MFP no se activa en otros miembros del grupo de la movilidad como los revestimientos pueden oír los marcos de la Administración de los revestimientos del otro WLCs en el grupo que no tienen MFP activado. Refiera al FAQ inalámbrico de los Grupos de movilidad del regulador LAN (WLC) para más información sobre el grupo de la movilidad.
3. El arreglo para este mensaje de error está disponible en las versiones 4.2.112.0 y 5.0.148.2 WLC. Actualice el WLCs a cualquiera de estas versiones.
4. Como última opción, intente recargar el REVESTIMIENTO que genera este mensaje de error.

Q. El cliente AIR-PI21AG-E-K9 se asocia con éxito a un Access Point (AP) usando la autenticación de Protocol Flexible de la autenticación ampliable vía la tunelización seguro (EAP-FAST).). Sin embargo, cuando el AP asociado se conmuta apagado, el cliente no vaga por a otro AP. Este mensaje aparece continuamente en el registro de mensajes del controlador: `"Fri 2 de junio 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: ¿Incapaz de permitir al usuario en el sistema - quizás registran al usuario ya sobre el sistema? Fri 2 de junio 14:48:49 2006 [SECURITY] apf_ms.c 2557: Incapaz de borrar el nombre de usuario para el móvil el 00:40:96:ad:75:f4". ¿Por qué?`

A. Cuando la placa cliente necesita hacer la itinerancia, envía un pedido de autenticación, pero no maneja correctamente los claves (no informa a AP/controller, no contesta a los reauthentications).

Esto se documenta en el Id. de bug Cisco CSCsd02837 (clientes registrados solamente). Este bug ha sido fijo con los adaptadores del cliente del Cisco Aironet 802.11a/b/g instala al Asistente 3.5.

Generalmente el incapaz de borrar el nombre de usuario para el mensaje móvil también ocurre debido a ninguno de estos razones:

- El nombre de usuario determinado se utiliza en más de un dispositivo del cliente.
- El método de autenticación usado para ese WLAN tiene una identidad anónima externa. Por ejemplo, en el PEAP-GTC o en el EAP-FAST, es posible definir un nombre de usuario

genérico como identidad (visible) externa, y el nombre de usuario real se oculta dentro del túnel TLS entre el cliente y el servidor de radio, así que el controlador no puede verlo y utilizarlo. En estos casos, este mensaje puede aparecer. Este problema se considera generalmente con un cierto otro vendedor y algún cliente del firmware antiguo.

Q. Cuando instalo la nueva cuchilla del módulo de servicios de red inalámbrica (WiSM) en el 6509 Switch y implemento el protocolo de autenticación ampliable protegido (PEAP) con el servidor del Microsoft IAS, recibo este error: *** 1 de marzo 00:00:23.526: %LWAPP-5-CHANGED: Estado cambiado LWAPP al DISCOVERY * 1 de marzo 00:00:23.700: %SYS-5-RELOAD: Recarga pedida por la razón del LWAPP CLIENT.Reload: INIT CRYPTO FALLADO. * 1 de marzo 00:00:23.700: %LWAPP-5-CHANGED: Estado cambiado LWAPP a ABAJO * 1 de marzo 00:00:23.528: %LWAPP-5-CHANGED: Estado cambiado LWAPP al DISCOVERY * 1 de marzo 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs ningunos certs en el archivo privado de SSC * 1 de marzo 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: * 1 de marzo 00:00:23.557: lwapp_crypto_init: PKI_StartSession falló * 1 de marzo 00:00:23.706: %SYS-5-RELOAD:** Recarga pedida por el CLIENTE del LWAPP. ¿Por qué?

A. Los debugs de RADIUS y dot1x muestran que el WLC envía una solicitud de acceso, pero no existe ninguna respuesta del servidor IAS. Termina estos pasos de progresión para resolver problemas el problema:

1. Verifique la configuración de servidor IAS.
2. Verifique el archivo de registro.
3. Instale el software, tal como Ethereal, que puede darle los detalles de la autenticación.
4. Detenga y comience el servicio IAS.

Q. Los Lightweight Access Point (LAPs) no se registran con el controlador. ¿Cual podría ser el problema? Veo estos mensajes de error en el controlador: **Thu 3 de febrero 03:20:47 2028: La solicitud de unión al LWAPP no incluye el certificado válido en CERTIFICATE_PAYLOAD de AP 00:0b:85:68:f4:f0. Thu 3 de febrero 03:20:47 2028:** Incapaz de liberar la clave pública para AP 00:0B:85:68:F4:F0.

A. Cuando el Access Point (AP) envía la solicitud al WLC para unirse al Lightweight Access Point Protocol (LWAPP), incluye el certificado X.509 en el mensaje del LWAPP También genera un ID de sesión al azar que se incluye en la solicitud de unión al LWAPP. Cuando el WLC recibe la solicitud de unión al LWAPP, valida la firma del certificado X.509 usando la clave pública y los controles AP que el certificado fue publicado por un Certificate Authority de confianza. También mira la fecha de inicio y el intervalo de la validez del certificado AP, y compara la esa fecha y el tiempo a su propia fecha y hora.

Este problema puede ocurrir debido a un ajuste de reloj incorrecto en el WLC. Para fijar el reloj en el WLC, emita los comandos **show time** y **config time**.

Q. El AP del Lightweight Access Point Protocol (LWAPP) no puede unirse a su controlador. El registro del controlador del Wireless LAN (WLC) visualiza un mensaje similar a este: La solicitud de unión al LWAPP no incluye el certificado válido en CERTIFICATE_PAYLOAD de AP 00:0b:85:68:ab:01. ¿Por qué?

A. Usted puede recibir este mensaje de error si el túnel del LWAPP entre el AP y el WLC atraviesa un trayecto de red con un MTU bajo 1500 bytes. Esto causa la fragmentación de los

paquetes LWAPP. Esto es un bug conocido en el controlador. Consulte el ID de bug Cisco CSCsd39911 (clientes registrados solamente).

La solución es actualizar el firmware del controlador a 4.0(155).

Q. Estoy intentando establecer la tunelización del invitado entre mi controlador interno y el controlador virtual del ancla en el De-Militarized Zone (DMZ). Sin embargo, cuando un usuario intenta asociarse a un invitadoSSID, el usuario no puede recibir la dirección IP del DMZ, según lo esperado. Por lo tanto, el tráfico de usuarios no hace túnel en el controlador en el DMZ. La salida del comando móvil del handoff del debug visualiza un mensaje similar a esto: `Discordancia de la política de seguridad para el WLAN <Wlan ID>. Petición de la exportación del ancla del IP del conmutador: IP address del <controller > ignorado.` ¿Cuál es el problema?

A. La tunelización del invitado proporciona la seguridad complementaria para el acceso del invitado-usuario a la red inalámbrica corporativa. Esto ayuda a asegurarse de que los Usuarios invitados no pueden acceder la red corporativa sin primero el paso a través del firewall corporativo. Cuando un usuario se asocia a un WLAN que se señale como el invitado WLAN, el tráfico de usuarios es tunneled al Controlador de WLAN que está situado en el DMZ fuera del firewall corporativo.

Ahora, en consideración a este escenario, puede haber varias razones de este invitado que hace un túnel para no funcionar según lo esperado. Pues el **resultado del comando de debug** implica, el problema pudo estar con la discordancia en las políticas de seguridad unas de los configuradas para ese WLAN determinado en el interno así como en los controladores DMZ. Marca si las políticas de seguridad así como otras configuraciones, tales como del tiempo de la sesión configuraciones hacia fuera, están correspondidas con.

Otras razones comunes para este problema son el controlador DMZ que no es asegurado a sí mismo para ese WLAN determinado. Para un invitado que hace un túnel para trabajar correctamente y para que el DMZ administre la dirección IP del usuario (usuario que pertenece a un invitado WLAN), es esencial que el asegurar apropiado está hecho para ese WLAN determinado.

Q. Veo que muchos “CPU recibir la cola del multicast es llena en mensajes del controlador” en el controlador 2006 del Wireless LAN (WLC), pero no en los 4400 WLCs. ¿Por qué? Tengo multicast inhabilitado en los controladores. ¿Cuál es la diferencia en el límite de cola del multicast entre las 2006 y 4400 plataformas del WLC?

A. Porque el multicast está invalidado en los controladores, los mensajes que causan esta alarma pudieron ser mensajes del (ARP) del Address Resolution Protocol. No hay diferencia con la profundidad de espera en cola (512 paquetes) entre el WLCs 2000 y los 4400 WLCs. La diferencia es que los 4400 paquetes ARP de los filtros NPU mientras que todo se hace en el software en el 2006. Esto explica porqué el WLC 2006 ve los mensajes pero no los 4400 WLC. UN WLC 44xx procesa los paquetes multicast vía el hardware (con el CPU). Paquetes multicast un 2000 de los procesos del WLC vía el software. Procesamiento de la CPU es más eficiente que el software. Por lo tanto, la cola 4400's se borra más rápidamente, mientras que lucha el WLC 2006 un dígito binario cuando ve muchos estos mensajes.

Q. Veo el “[SECURITY] apf_foreignap.c 763: `El STA [00:0A:E4:36:1F:9B] recibió un paquete en el puerto 1 pero ningún AP no nativo configurados para este puerto.”` mensaje de `error` en uno de mis reguladores. ¿Qué este error significa y qué medidas debo tomar para resolverlo?

A. Se considera este mensaje cuando el controlador recibe un pedido de DHCP para un MAC Address para el cual no tenga una máquina de estado. Esto se ve a menudo de un Bridge o de un sistema que haga funcionar una máquina virtual como VMware. El controlador escucha los pedidos de DHCP porque realiza el snooping del DHCP así que sabe qué direccionamientos se asocian a los clientes que se asocian a su (APS) de los puntos de acceso. Todo el tráfico para los clientes de red inalámbrica pasa a través del controlador. Cuando el destino de un paquete es un cliente de red inalámbrica, va al controlador y después pasa a través del túnel del protocolo del Lightweight Access Point (LWAPP) al AP y apagado al cliente. Una cosa que se puede hacer para ayudar a atenuar este mensaje es permitir solamente los VLAN que se utilizan en el controlador sobre el troncal que va al controlador con el **switchport vlan permite el** comando en el switch.

Q. Porqué veo este mensaje de error en la consola: ¿Los Msg “fijaron el gateway predeterminado” del vector del sistema fallado, el valor del error identificación = 0x0050b986 = 0xfffffffc?

A. Esto puede deber CPU elevada cargar. Cuando el controlador CPU se carga pesadamente por ejemplo cuando hace las copias de archivo u otras tareas, no tiene tiempo para procesar todo el Acks que el NPU envíe en respuesta a los mensajes de configuración. Cuando ocurre esto, el CPU genera los mensajes de error. Sin embargo, los mensajes de error no afectan el servicio o las funciones.

Esto se documenta en la sección del controlador pesadamente cargado CPU de los Release Note para los Controladores de LAN y los Lightweight Access Point de la Red Inalámbrica Cisco para la versión 3.2.116.21.

Q. Recibo estos mensajes de error dominantes del Wired Equivalent Privacy (WEP) en mi sistema de control inalámbrico (WCS): `La clave WEP configurada en la estación puede ser incorrecta. El MAC Address de la estación es “xx: xx: xx: xx: xx: xx”, la radio baja MAC AP es “xx: xx: xx: xx: xx: xx”` y la ranura ID es '1'. Sin embargo, no utilizo el WEP como el parámetro de seguridad en mi red. Utilizo solamente el acceso protegido Wi-fi (WPA). ¿Por qué recibo estos mensajes de error WEP?

A. Si todas tus configuraciones relacionadas con la seguridad son perfectas, los mensajes que recibes ahora están debido a los fallos de funcionamiento. Hay algunos bug conocido en el controlador. Consulte bug Cisco ID CSCse17260 (clientes registrados solamente) y CSCse11202 (clientes registrados solamente), que estado “la clave WEP configurada en la estación puede ser incorrecto con los **clientes WPA y TKIP respectivamente**”. En realidad, **CSCse17260** es un duplicado de **CSCse11202**. El parche para **CSCse11202** está ya disponible con la versión 3.2.171.5 del WLC.

Nota: Las últimas versiones del WLC tienen un parche para estos bugs.

Q. Utilizamos un servidor RADIUS externo para autenticar a los clientes de red inalámbrica a través del controlador. El controlador envía este mensaje de error regularmente: ningunos servidores de radio están respondiendo. ¿Por qué vemos

estos mensajes de error?

A. Cuando una solicitud sale del WLC al servidor RADIUS, cada paquete tiene una secuencia numerada de la cual el WLC espera una respuesta. Si no hay respuesta, hay un mensaje que muestra el radio-servidor que no responde.

El tiempo predeterminado para que el WLC oiga detrás del servidor de radio es 2 segundos. Esto se fija del WLC GUI bajo la **seguridad > autenticación-servidor**. El máximo es 30 segundos. Por lo tanto, puede ser que sea útil fijar este vez hacia fuera valora a su máximo para resolver este problema.

A veces, los servidores de radio realizan los **"descartes silenciosos" del** paquete de pedidos que viene del WLC. El servidor de radio puede rechazar este los paquetes debido para certificar la discordancia y varias otras razones. Esto es una acción válida al lado del servidor. También, en estos casos, el controlador marcará el servidor de radio como no respondiendo.

Para superar los descartes silenciosos publican, invalidan la característica **agresiva del failover** en el WLC.

Si la característica **agresiva del failover** se habilita en el WLC, el WLC es demasiado agresivo marcar el servidor de AAA como no respondiendo. Sin embargo, esto no debe ser hecha porque el servidor de AAA no pudo ser responsivo solamente a ese cliente particular (haciendo el descarte silencioso). Puede ser una respuesta a otros clientes válidos (con los certificados válidos). Sin embargo, el WLC pudo todavía marcar el servidor de AAA como no respondiendo y no funcional.

Para superar esto, inhabilite la función **aggressive failover**. Publique el **comando disable de la agresivo-Conmutación por falla del radio de los config del** regulador CLI para realizar esto. Si esto está inhabilitado, entonces el controlador fallará solamente con el servidor de AAA siguiente si hay 3 clientes consecutivos que no pueden recibir una respuesta del servidor de radio.

Q. Varios clientes no pueden asociarse a un LWAPP y el controlador registra el IAPP-3-MSGTAG015: `iappSocketTask:` mensaje de error devuelto iappRecvPkt del error. ¿Por qué esto sucede?

A. Esto sucede sobre todo debido a un problema con los adaptadores de Intel que soportan CCX v4, pero que funcionan con una versión del cliente anterior de 10.5.1.0. Si actualiza el software a 10.5.1.0 o superior, esto resuelve este problema. Consulte ID de bug Cisco CSCsi91347 (clientes registrados solamente) para más información sobre este mensaje de error.

Q. Veo este mensaje de error en el controlador del Wireless LAN (WLC): Se alcanzó la cantidad máxima de intentos para solicitar EAP-Identity (21) para STA 00:05:4e:42:ad:c5. ¿Por qué?

A. Este mensaje de error ocurre cuando el usuario intenta conectar con una red WLAN protegida por EAP y ha fallado el número preconfigurado de tentativas de EAP. Cuando el usuario no puede autenticar, el controlador excluye al cliente y el cliente no puede conectar con la red hasta que el temporizador de la exclusión expire o sea reemplazado manualmente por el administrador.

La exclusión detecta los intentos de autenticación hechos por un único dispositivo. Cuando ese dispositivo excede un número máximo de incidentes, ese MAC Address no se permite asociarse

más de largo.

La exclusión ocurre:

- Después de 5 fallas de autenticación consecutivas para las autenticaciones compartidas (se excluye el 6to intento)
- Después de 5 incidentes consecutivos de la asociación para la autenticación de MAC (se excluye el 6to intento)
- Después de 3 fallas de autenticación consecutivas del EAP/802.1X (se excluye el 4to intento)
- Cualquier incidente externo del servidor de políticas (NAC)
- Cualquier caso de duplicación de la dirección IP
- Después de 3 incidentes consecutivos de la autenticación Web (se excluye el 4to intento)

El temporizador durante cuánto tiempo excluyen a un cliente se puede configurar, y exclusión se puede habilitar o invalidar en el controlador o el nivel WLAN.

Q. Veo este mensaje de error en el controlador del Wireless LAN (WLC): **`Una alerta del switch de la categoría es generada con la severidad 1 por el switch WLCSCH01/10.0.16.5 que el mensaje de la alerta es el controlador '10.0.16.5'.`** Los servidores del RADIO no están respondiendo a los pedidos de autenticación. ¿Cuál es el problema?

A. Esto pudo estar debido a el Id. de bug Cisco CSCsc05495. Debido a este bug, el controlador inyecta periódicamente las Pares AV incorrectas (atributo 24, “estado”) en los mensajes del pedido de autenticación que violan un RADIO RFP y causan los problemas para algunos servidores de autenticación. Este bug es fijo en 3.2.179.6.

Q. Recibo un mensaje de error del perfil del ruido bajo el monitor > las radios 802.11b/g. ¿Quiero entender porqué veo este mensaje fallido?

A. El estatus del perfil FAILED/PASSED del ruido se fija después del resultado de la prueba hecho por el WLC y en comparación con el umbral actual del conjunto. Por abandono, el valor del ruido se fija a -70. El estado fallido indica que el valor de umbral para ese parámetro particular o el Access Point (AP) se ha excedido. Usted puede ajustar los parámetros en el perfil, pero se recomienda para cambiar las configuraciones después de que entiendas claramente el diseño de red y cómo afectará al funcionamiento de la red.

Los umbrales de radio de la administración de recursos (RRM) PASSED/FAILED global se fijan para todos los AP en los **parámetros globales 802.11a > los parámetros globales autos RF** y **802.11b/g > las** paginaciones **autos RF**. RRM los umbrales PASSED/FAILED se fijan individualmente para este AP en las **802.11 interfaces AP >** paginaciones del **perfil del funcionamiento**.

Q. No puedo el set port 2 como el puerto de backup para la interfaz del AP manager. El mensaje de error devuelto es no podría configuración del set port. Puedo al set port 2 como el puerto de backup para la interfaz de administración. El puerto activo actual para ambas interfaces es el puerto 1. ¿Por qué?

A. Un AP manager no tiene un puerto de backup. Era soportado en las versiones anteriores. Desde la versión 4.0 y posterior, el puerto de backup para la interfaz del AP manager no se soporta. En general, un solo AP manager se debe configurar en cada puerto (sin respaldo). Si utilizas la agregación de la conexión (RETRASO), hay solamente un AP manager.

La interfaz estática (o permanente) del AP manager se debe asignar al puerto 1 del sistema de distribución y debe tener una dirección IP único. No puede ser asociada a un puerto de backup. Se configura generalmente en el mismo VLAN o la subred IP que la interfaz de administración, pero esto no es un requisito.

Q. Veo este mensaje de error: **El AP '00:0b:85:67:6b:b0 recibió un error WPA MIC el el '1' del protocolo de la estación '00:13:02:8d:f6:41.** Se han activado las medidas contrarias y el tráfico se ha suspendido por 60 segundos. ¿Por qué?

A. El Message Integrity Check (MIC) incorporado en el acceso protegido Wi-fi (WPA) incluye un contador de la trama que prevenga un ataque del intermediario. Este error significa que alguien en la red está intentando jugar de nuevo el mensaje que fue enviado por el cliente original, o puede ser que signifique que el cliente es defectuoso.

Si un cliente falla en varias ocasiones el control MIC, el regulador inhabilita la red inalámbrica (WLAN) en el interfaz AP donde los errores se detectan por 60 segundos. Registran al primer error MIC, y un temporizador se inicia para activar la aplicación de las contramedidas. Si un error subsiguiente MIC ocurre en el plazo de 60 segundos del error anterior más reciente, después un STA cuya entidad del 802.1x de IEEE ha actuado como suplicante el deauthenticate sí mismo o deauthenticate todo el STAs con una asociación de seguridad si su entidad del 802.1x de IEEE actuaba como Authenticator.

Además, el dispositivo no recibe ni transmite ninguna marcos de datos TKIP-cifrada, y no recibe ni transmite ninguna marcos de datos unencrypted con excepción de los mensajes del 802.1x de IEEE, a o desde cualquier par por un período de por lo menos 60 segundos después de que detecta la segunda falla. Si el dispositivo es un AP, rechaza las nuevas asociaciones con el TKIP durante este período de 60 segundos; en el final del período de 60 segundos, el AP reanuda los funcionamientos normales y permite STAs (con referencia a) al socio.

Esto previene un ataque posible contra el esquema de cifrado. Estos errores MIC no se pueden apagar en las versiones WLC antes de 4.1. Con la versión 4.1 y posterior inalámbrica del regulador LAN, hay un comando de cambiar la época de la exploración para los errores MIC. El comando es **id> <wlan del seconds> del asentamiento <0-60 del tkip de la Seguridad de WLAN de los config**. Utilice el valor 0 para inhabilitar la detección de error MIC para las contramedidas.

Q. Este mensaje de error se considera en mis registros del controlador: **[ERROR] dhcp_support.c 357: dhcp_bind(): dhcpstate del servPort fallado. ¿Por qué?**

A. Estos mensajes de error se consideran sobre todo cuando el puerto del servicio del controlador tiene DHCP habilitado, pero no reciben una dirección IP de un servidor DHCP.

Por abandono, la interfaz de puerto del servicio físico tiene un DHCP cliente instalado y busca un direccionamiento vía el DHCP. El WLC intenta pedir un DHCP Address para el puerto del servicio. Si no hay servidor DHCP disponible, después un pedido de DHCP para el puerto del servicio falla. Por lo tanto, esto genera los mensajes de error.

La solución alternativa es configurar una dirección IP estático al puerto del servicio (incluso si el puerto del servicio está desconectado) o tener un servidor DHCP disponible asignar un dirección IP al puerto del servicio. Entonces, recarga el controlador, si es necesario.

El puerto del servicio es realmente reservado para la administración fuera de banda del

controlador y de la recuperación del sistema, y el mantenimiento en caso de desperfecto de la red. Es también el único puerto que es activo cuando el controlador está en el modo de arranque. El puerto del servicio no puede llevar los Tags 802.1Q. Por lo tanto, debe ser conectado con un puerto de acceso en el switch de vecino. El uso del puerto del servicio es opcional.

La interfaz de puerto del servicio controla las comunicaciones a través y es asociada estáticamente por el sistema al puerto del servicio. Debe tener una dirección IP en una diversa subred de la gestión, del AP manager, y de cualquier interfaz dinámica. También, no puede ser asociada a un puerto de backup. El puerto del servicio puede utilizar el DHCP para obtener una dirección IP, o él puede ser asignado un dirección IP estático, pero un gateway predeterminado no se puede asignar a la interfaz de puerto del servicio. Las Rutas estáticas se pueden definir a través del controlador para el acceso remoto a redes al puerto del servicio.

Q. Mis clientes de red inalámbrica no pueden conectar con el Wireless LAN (WLAN) la red. El WiSM que el Access Point (AP) está conectado con señala este mensaje: Ataque grande DOS de NAV del AP con la radio baja MAC 00:0g:23:05:7d:d0, la ranura ID 0 y el MAC de origen 00:00:00:00:00:00. ¿Qué significa?

A. Como condición para acceder al medio, la capa MAC marca el valor de su vector de la asignación de la red (NAV). NAV es un residente contrario en cada estación que represente la cantidad de tiempo que las necesidades anteriores de la trama de enviar su trama. NAV debe ser cero antes de que una estación pueda intentar enviar una trama. Antes de que la transmisión de un bastidor, una estación calcule la cantidad de tiempo necesaria enviar la trama basada en la longitud y la velocidad de datos de la trama. La estación pone un valor que represente este vez en el campo de la duración en la cabecera del bastidor. Cuando las estaciones reciben la trama, examinan este valor de campo de la duración y lo utilizan como la base para fijar su NAVs correspondiente. Este proceso reserva el media para la estación remitente.

Un alto NAV indica la presencia de un valor inflado de NAV (mecanismo virtual de la detección de portadora para 802.11). Si el MAC Address señalado es 00:00:00:00:00:00, está siendo probablemente spoofed (potencialmente un ataque real) y necesitas confirmar esto con una captura de paquetes.

Q. Después de configurar y reinicializar el controlador, no podemos acceder al controlador en el modo Secure Web (https). Se recibe este mensaje de error mientras intenta acceder al modo Secure Web del controlador: **Secure Web:** Web Authentication Certificate not found (error). ¿Cuál es la razón de este problema?

A. Puede haber varias razones asociadas a este problema. Una razón comun se puede relacionar con la configuración de la interfaz virtual del controlador. Para resolver este problema, quite la interfaz virtual y luego vuelva a generarla con este comando:

```
WLC>config interface address virtual 1.1.1.1
```

Luego, reinicie el controlador. Después de reiniciado el controlador, genere nuevamente el certificado del webauth localmente en el controlador con este comando:

```
WLC>config certificate generate webauth
```

En la salida de este comando, usted debe ver este mensaje: Se ha generado el certificado de Autenticación Web.

Después de la reinicialización, usted debería poder acceder al modo seguro de Web del controlador..

Q. Los controladores señalan a veces este mensaje de alerta del ataque de la firma de la inundación de la anulación de asociación ID contra los clientes válidos en quienes el MAC Address del atacante es el de un Access Point (AP) unido a ese controlador: : **Alerta: Ataque de la firma de la inundación de Disassoc ID" detectado contra "protocolo '802.11b/g del name> del <AP el" AP en el controlador "x.x.x.x". La descripción de la firma es "Inundación de anulación de asociación", con la precedencia "x". El MAC Address del atacante es "hh: hh: hh: hh: hh: el hh", número de canal es "x", y el número de detecciones es "x".** ¿Por qué esto ocurre?

A. Esto está debido a el Id. de bug Cisco CSCsg81953 (clientes registrados solamente).

Los ataques de inundación de la anulación de asociación ID contra los clientes válidos están señalados a veces donde está el el MAC Address del atacante de un AP unido a ese controlador.

Cuando asocian al AP pero para a un cliente el comunicar debido a "cómo retirar la placa", vagando por fuera del rango, del etc. al AP, el AP esperará hasta el tiempo de espera inactivo. Una vez que se alcanza el idle timeout, el AP envía que cliente una trama de la anulación de asociación. Cuando el cliente no reconoce la trama de la anulación de asociación, el AP retransmite los tiempos numerosos de la trama (alrededor 60 tramas). El subsistema ID del controlador oye que éstos retransmiten y las alertas con este mensaje.

Este bug es resuelto en la versión 4.0.217.0. Actualiza tu versión del controlador a esta versión para superar este mensaje de alerta contra los clientes válidos y los AP.

Q. Recibo este mensaje de error en el syslog del controlador: **[WARNING] apf_80211.c 2408: Recibió un mensaje con una velocidad soportada inválida del <xx de la estación: xx: xx: xx: xx: xx: xx> [error] apf_utils.c 198: Velocidad soportada que falta. ¿Por qué?**

A. Realmente, los mensajes perdidos de la velocidad soportada indican que el WLC está configurado para ciertas tarifas de datos requeridos bajo configuraciones sin hilos, pero la tarjeta NIC está faltando la tarifa requerida.

Si tienes velocidades de datos, tales como 1 y 2M, conjunto para requerido en el controlador pero la tarjeta NIC no comunica en estas velocidades de datos, puede recibir a este tipo de mensaje. Lo siguiente es un mal comportamiento de la tarjeta NIC . Por otra parte, si es tu controlador se habilita 802.11g y el cliente es 802.11b(only) una tarjeta, esto es un mensaje legítimo. Si estos mensajes no causan problemas y las tarjetas pueden todavía conectar, estos mensajes pueden ser ignorados. Si los mensajes son específico de la tarjeta, asegúrese de que el driver para esta tarjeta esté actualizado.

Q. Este Syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decodifique los Msg: no podía hacer juego el** mensaje de error del **<id> identificación de la red inalámbrica (WLAN)** es la difusión en nuestra red. ¿Por qué esto ocurre y cómo lo paro?

WLC>config certificate generate webauth

A. Este mensaje es difusión al lado de los revestimientos. Se ve esto cuando usted ha configurado la característica de la invalidación de la red inalámbrica (WLAN) para una red inalámbrica (WLAN) y esa red inalámbrica (WLAN) determinada no se hace publicidad.

Configure el `host 0.0.0.0 global del Syslog ap de los config` para pararlo o usted puede poner una dirección IP específica si usted tiene un servidor de Syslog de modo que el mensaje sea difusión al servidor solamente.

Q. Recibo este mensaje de error en mi controlador del Wireless LAN (WLC): **[ERROR] fichero: apf_mm.c: Línea: 581: Anuncia la colisión para 00:90:7a:05:56:8a móvil, borrando. ¿Por qué?**

A. Generalmente, este mensaje de error indica que el controlador había anunciado las colisiones para un cliente de red inalámbrica (es decir los AP separados anuncian que tienen el cliente), y el controlador no recibió las manos a partir de un AP al siguiente. No hay estado de la red a mantener. Borra al cliente de red inalámbrica y ten el intento del cliente otra vez. Si ocurre este problema con frecuencia, puede haber un problema con la configuración de la movilidad. Si no, puede ser que sea una anomalía que se relaciona con un cliente o una condición específica.

Q. Mi controlador aumenta este mensaje de alarma: Umbral de la cobertura de '12' violado. ¿Cuál es este error y cómo pueden él ser resueltos?

A. Se aumenta este mensaje de alarma cuando una relación señal-ruido del cliente (SNR) cae debajo del valor de umbral del SNR para la radio determinada. 12 es el valor de umbral predeterminado del SNR para la detección del agujero de la cobertura.

El algoritmo de la detección y corrección del agujero de la cobertura determina si existe un agujero de la cobertura cuando niveles del SNR de los clientes los' pasan debajo de un umbral dado del SNR. Este umbral del SNR varía basado en dos valores: La potencia de transmisión AP y la cobertura del controlador perfilan el valor.

Detalladamente, el umbral del SNR del cliente es definido por la potencia de transmisión cada AP (representada en el dBm), menos el valor constante de 17dBm, menos el valor configurable del perfil de la cobertura del usuario (este valor se omite DB 12).

- **Valor del atajo del SNR del cliente (|DB|) = [AP Transmit Power (dBm) – Constant (17 dBm) – Coverage Profile (dB)]**

Este valor configurable del perfil de la cobertura del usuario se puede acceder de esta manera:

1. En el WLC GUI, diríjase al título principal de la red inalámbrica y selecciona la **opción de red** para el estándar de WLAN de la opción en el lado izquierdo (802.11a o 802.11b/g). Entonces, **auto** selecto **RF** en la derecha de la parte superior de la ventana.
2. En los parámetros globales autos RF pagina, encuentra la sección de los umbrales del perfil. En esta sección, puede encontrar el valor de la cobertura (3 a el dbm 50). Este valor es el valor configurable del perfil de la cobertura del usuario.
3. Este valor se puede editar para influenciar el valor de umbral del SNR del cliente. La otra manera de influenciar este umbral del SNR es aumentar la potencia de transmisión y compensar la detección del agujero de la cobertura.

Q. Estoy utilizando ACS v 4.1 y un controlador del Wireless LAN 4402 (WLC). Cuando el WLC intenta a la MAC-autenticidad a un cliente de red inalámbrica a ACS 4.1, el ACS no puede responder con el ACS y señala este mensaje de error: El "*error interno ha ocurrido*". Tengo todas mis configuraciones correctas. ¿Por qué este error interno ocurre?

A. Hay un Id. de bug Cisco relacionado autenticación CSCsh62641 (clientes registrados solamente) en el ACS 4.1, donde el ACS da el error interno tiene mensaje de error ocurrido.

Este bug pudo ser el problema. Hay una corrección disponible para este bug en la paginación de las descargas ACS 4.1 (clientes registrados solamente) que debe fijar el problema.

Q. El controlador del Wireless LAN de las Cisco 4400 Series (WLC) no iniciará. Este mensaje de error se recibe en el controlador: **** Incapaz de utilizar ide 0:4 para el fatload ** negro 0 revelador 0 del error (ningún IRQ): registro del error del estatus 0x51:** 10 ** No puede leer en el dispositivo 0. ¿Por qué?

A. La razón de este error pudo ser problemas del hardware. Abre un caso TAC para resolver problemas más lejos este problema. Para abrir un caso TAC, necesitas tener un contrato válido con Cisco. Consulte el soporte técnico para entrar en contacto el TAC de Cisco.

Q. El controlador del Wireless LAN (WLC) se ejecuta en los problemas de la memoria intermedia. Una vez que las memorias intermedias están repletas, el controlador causa un crash y necesita ser reanudado para traerlo detrás en línea. Estos mensajes de error se consideran en el registro de mensajes: **Lunes 9 de abril 10:41:03 2007 [error] dtl_net.c 506: Fuera buffer del sistema lunes del 9 de abril 10:41:03 2007 [error] sysapi_if_net.c 537: No puede afectar un aparato nuevo Mbuf. Lunes 9 de abril 10:41:03 2007 [error] sysapi_if_net.c 219: MbufGet: ningún mbufs libre. ¿Por qué?**

A. Esto es debido al Id. de bug Cisco CSCsh93980 (clientes registrados solamente). Este bug ha sido resuelto en la versión 4.1.185.0 del WLC. Actualice su regulador para superar a esta versión de software o a más adelante este mensaje.

Q. Realizamos la actualización de nuestro controlador del Wireless LAN (WLC) 4400s al código 4.1 y nuestro syslog fue bombardeado por los mensajes, tales como esto: **3 de mayo 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED:** STA [00:17:f2:43:26:93, 0.0.0.0] ARP (1) de Op. Sys. recibido con SPA inválido 192.168.1.233/TPA 192.168.1.233. ¿Qué estos mensajes indican?

A. Esto puede ocurrir cuando el WLAN es marcado como el DHCP requirió. En estos casos, solamente las estaciones que reciben una dirección IP con el DHCP se permiten asociarse. No se permite a los clientes estáticos asociarse a esta red inalámbrica (WLAN). El WLC actúa como agente de relé DHCP y registra la dirección IP de todas las estaciones. Se genera este mensaje de error cuando el WLC recibe el pedido ARP de una estación antes de que el WLC haya recibido los paquetes DHCP de la estación y haya registrado su dirección IP.

Q. Cuando utilizas el poder sobre los Ethernet (PoE) en el controlador del Wireless LAN de Cisco 2106, las radios AP no se habilitan. El AP no puede verificar el suficiente In-line Power. **Número de slot de radio invalidado.** el mensaje de error

aparece. ¿Cómo puedo solucionarlo?

A. Este mensaje de error ocurre cuando el switch, que acciona para arriba el punto de acceso, es un switch PRE-estándar pero el AP no soporta el modo PRE-estándar de alimentación de entrada.

Un switch PRE-estándar de Cisco es uno que no soporta la administración de la energía inteligente (IPM) pero tiene energías suficientes para una punta de acceso estándar.

Debe habilitar el modo PRE-**Estándar de** poder en el AP que se sujeta a este mensaje de error. Esto se puede hacer del controlador CLI con el **poder ap de los config PRE-estándar {habilita | neutralización} {toda |** Comando de **Cisco_AP}**.

Este comando se debe configurar ya, si procede, si actualizas al Software Release 4.1 de una versión anterior. Pero, es posible que necesitas ingresar este comando para las nuevas instalaciones, o si reajustas el AP a los valores predeterminados de fábrica.

Estos 15-watt Switch PRE-estándar de Cisco están disponibles:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

Q. El controlador genera un dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: `Incapaz de agregar una entrada ARP para xx: xx. - xxx.x al procesador de red. la entrada no existe.` mensaje de Syslog similar a esto. ¿Qué hace este mensaje de Syslog significa?

A. Mientras que algún cliente de red inalámbrica envía una respuesta ARP, las necesidades de la unidad del procesador de red (NPU) de saber esa contestación. La respuesta ARP se remite tan a NPU pero al software WLC no debe intentar agregar esta entrada al procesador de red. Si hace así pues, se generan estos mensajes. No hay impacto de las funciones en el WLC debido a esto pero el WLC genera este mensaje de Syslog.

Q. He instalado y he configurado un nuevo WLC de Cisco 2106. El WLC indica que el sensor de temperatura ha fallado. Cuando registras en la interfaz Web conforme al “resumen del controlador,” dice el “sensor fallado” al lado de la temperatura interna. Todo aparece funcionar normalmente.

A. El incidente del sensor de temperatura interna es cosmético y se puede resolver con una actualización a la versión 4.2.61.0 del WLC.

WLC 2106 y WLC 526 **empleado o después de que 07/01/2007** pueda utilizar el chip del sensor de temperatura de otro vendedor. Este nuevo sensor funciona muy bien, pero no es compatible con el software más adelante que la versión 4.2. Por lo tanto, un más viejo software no puede leer

la temperatura y muestra este error. El resto de las funciones del controlador no son afectadas por este defecto.

Hay un Id. de bug Cisco sabido CSCsk97299 (clientes registrados solamente) relacionado con este problema. Este bug se menciona en el Release Note de la versión 4.2 del WLC.

Q. Consigo el radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: No podía encontrar el servidor de radio apropiado para el <WLAN WLAN ID> - incapaz de encontrar mensaje de un servidor predeterminado el" para TODOS LOS SSID. Este mensaje aparece incluso para los SSID que no utilizan los servidores de AAA.

A. Este mensaje de error significa que el controlador no podía entrar en contacto el servidor del RADIUS predeterminado o que uno no fue definido.

Una razón posible de este comportamiento es el Id. de bug Cisco CSCsk08181 (clientes registrados solamente), que ha sido resuelto en la versión 4.2. Actualiza tu controlador a la versión 4.2.

Q. El mensaje: `10 de julio 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: El MAC Address de origen de la interfaz 1 no se encuentra.` el mensaje de error aparece en el controlador del Wireless LAN (WLC). ¿Qué esto indica?

A. Esto significa que el controlador tenía un error mientras que envió un CPU el paquete originado.

Q. Estos mensajes de error aparecen en el controlador del Wireless LAN (WLC):

- `10 de julio 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: No podido leer el archivo de configuración "cliWebInitParms.cfg"`
- `10 de julio 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: No podido leer el archivo de configuración "rfidInitParms.cfg"`
- `10 de julio 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: No podido leer el archivo de configuración "dhcpParms.cfg"`
- `10 de julio 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: No podido leer el archivo de configuración "bcastInitParms.cfg"`
- `18 de marzo 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: No podido suprimir el fichero: retiro del fichero sshpmInitParms.cfg fallado. - Proceso: Nombre: fp_main_task, Id:11ca7618`
- `18 de marzo 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: No podido suprimir el fichero: retiro del fichero bcastInitParms.cfg fallado. - Proceso: Nombre: fp_main_task, Id:11ca7618`

¿Qué este el mensaje de error indica?

A. Estos mensajes son mensajes de información y son parte del procedimiento normal del cargador del programa inicial. Estos mensajes aparecen debido a un error leer o suprimir varios diversos archivos de configuración. Cuando los ficheros de configuración determinada no se encuentran o si el archivo de configuración no puede ser leído, la secuencia de los config para cada proceso envía este mensaje, por ejemplo, ningunos config del servidor del DHCP, ningunos config de las etiquetas (identificación RF), y así sucesivamente. Éstos son los mensajes de la bajo-gravedad que pueden ser ignorados con seguridad. Estos mensajes no interrumpen la operación del controlador.

Q. El HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-

UNABLE_TO_KEEP_ROUGE_CONTAIN: `Incapaz de mantener 00:14:XX:02:XX:XX rogue el estado contenido - ningún AP disponible para contener.` el mensaje de error aparece. ¿Qué esto indica?

A. Esto significa que el AP que realizó la función no fiable de la contención está no más disponible, y el regulador no puede encontrar ningún AP conveniente para realizar la contención no fiable.

Q. `El DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (1) de Op. Sys. recibido con el` mensaje del sistema `inválido del BALNEARIO 192.168.1.152/TPA 192.168.0.206` aparece en el regulador LAN de la Tecnología inalámbrica. ¿Qué este mensaje implica?

A. Es posible que el sistema detectó la falsificación de ARP o el envenenamiento. Pero, este mensaje no implica necesariamente que ha ocurrido cualquier falsificación de ARP malévola. El mensaje aparece cuando estas condiciones son verdades:

- UNA red inalámbrica (WLAN) se configura con el DHCP requerido, y un dispositivo cliente, después de asociar en esa red inalámbrica (WLAN), transmite un mensaje ARP sin el primer DHCP que completa. Éste puede ser comportamiento normal; puede suceder, por ejemplo, cuando el cliente se dirige estáticamente, o cuando el cliente lleva a cabo un arriendo válido del DHCP de una asociación anterior. El mensaje de error puede parecer este ejemplo:
  `WLC>config certificate generate webauth`

  El efecto de esta condición es que el cliente no puede enviar o recibir cualquier tráfico de datos, hasta que él los DHCP con el WLC.Refiera a la sección de los mensajes DTL del guía de mensajes del sistema inalámbrico del regulador LAN de Cisco para más información.

Q. Los revestimientos no utilizan la potencia sobre los Ethernetes (POE) de accionar para arriba. Veo que abre una sesión el regulador LAN de la Tecnología inalámbrica:

```
AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power
```

¿Cuál es el problema?

A. Esto puede suceder si la potencia sobre las configuraciones de los Ethernetes (POE) no se configura correctamente. Cuando un Punto de acceso que se ha convertido al modo ligero, por ejemplo, un AP1131 o un AP1242, o un Punto de acceso de las 1250 Series es accionado por un alimentador de corriente que esté conectado con un conmutador pre-inteligente de la administración de la energía de Cisco (pre-IPM), usted necesita configurar la potencia sobre los Ethernetes (PoE), también conocidos como potencia en línea.

Refiera a configurar la potencia sobre los Ethernetes para más información sobre cómo configurar la potencia sobre los Ethernetes (POE).

Q. Usted ve este mensaje en el regulador LAN de la Tecnología inalámbrica (WLC):

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

¿Qué esto indica?

A. Los Puntos de acceso ligeros siguen cierto algoritmo para encontrar un regulador. El descubrimiento y se une al proceso se explica detalladamente en el registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (WLC)

Este mensaje de error se considera en el WLC, cuando recibe una petición del descubrimiento después de que haya alcanzado su capacidad del máximo AP.

Si el controlador primario para un REVESTIMIENTO no se configura o si su un nuevo fuera del REVESTIMIENTO del cuadro, envía las peticiones del descubrimiento LWAPP a todos los reguladores accesibles. Si el descubrimiento pide los alcances un regulador que se ejecute en su capacidad completa AP, WLC consigue las peticiones y realiza que esté en su capacidad del máximo AP, y no responde a la petición y da este error.

Q. ¿Dónde puedo encontrar más información sobre los mensajes del sistema del LWAPP?

A. Consulte guía de mensajes del sistema del Controlador de LAN de la Red Inalámbrica Cisco, 4.2 para más información sobre los mensajes del sistema del LWAPP.

Q. `El error que extrae el` mensaje de error de los `ficheros del webauth` aparece en el regulador LAN de la Tecnología inalámbrica (WLC). ¿Qué esto indica?

A. WLC no puede cargar un manojo de encargo de la autenticación Web/del paso si de los ficheros liados tiene mayor de 30 caracteres en el nombre de fichero, que incluye la extensión de archivo. El manojo auténtico personalizado de la red tiene un límite de hasta 30 caracteres para los nombres de fichero. Asegúrese de que no hay nombres de fichero dentro del manojo mayores de 30 caracteres.

Q. Los reguladores inalámbricos LAN (WLCs), funcionando con el código 5.2 o 6.0 con un gran número de grupos AP, GUI de la red pueden no visualizar a todos los grupos configurados AP. ¿Cuál es el problema?

A. Los grupos que falta AP pueden ser considerados si usted utiliza la **demostración** CLI que los ap-**grupos wlan** ordenan.

Intente agregar a un grupo adicional AP a la lista. Por ejemplo, 51 grupos AP desplegados, y los 51.os faltan (la página 3). Agregue al 52.o grupo, y la página 3 debe aparecer en el GUI de la red.

Para resolver este problema, mejora a la versión 7.0.220.0 WLC.

Información Relacionada

- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Preguntas frecuentes sobre Troubleshooting de WiSM
- FAQ inalámbrico del Troubleshooting del regulador LAN (WLC)
- Página de Soporte de Red Inalámbrica

- Soporte Técnico y Documentación - Cisco Systems