# Comprensión y solución de problemas de señales de mantenimiento CAPWAP en Catalyst 9800 WLC

## Contenido



## Introducción

Este documento describe los keepalives de control CAPWAP, los keepalives de datos y las retransmisiones,

### Contexto

CAPWAP proporciona el marco de comunicación entre los puntos de acceso de Cisco y el controlador de LAN inalámbrica en las plataformas Cisco Catalyst 9800. Utiliza canales de datos y control independientes, junto con mecanismos de keepalive y retransmisión definidos para mantener la conectividad.

En este artículo se explican las señales de mantenimiento de control CAPWAP, las señales de mantenimiento de datos y las retransmisiones, incluidos los temporizadores asociados, el comportamiento de los errores y los indicadores clave de solución de problemas.

# Dos canales separados, dos mecanismos diferentes

CAPWAP se ejecuta sobre dos canales UDP, y cada uno tiene su propio mecanismo de vida

| Canal | Puerto predeterminado (UDP) | Mecanismo de vida |
|---|---|---|
| Control | 5246 | Solicitud de eco/respuesta de eco |
| Datos | 5247 | Mantenimiento de Data Channel |

keepalive de control CAPWAP (eco/latido)

Propósito

El keepalive de control CAPWAP se utiliza para confirmar que el punto de acceso aún es accesible en el canal de control.

Su propósito es muy simple: verifica que la conexión de control entre el AP y el controlador sigue activa y responde. No se utiliza para transportar actualizaciones de configuración o datos de cliente. En su lugar, sirve como un mecanismo activo para la trayectoria de control CAPWAP sobre el puerto UDP 5246.

Quién envía el Keepalive

El punto de acceso es el dispositivo que inicia activamente el keepalive de control.

Cuando es necesario, el AP envía una solicitud de eco CAPWAP al controlador. El controlador entonces responde con una respuesta de eco correspondiente. Esta respuesta confirma que el controlador recibió la solicitud y que el canal de control está funcionando en ambas direcciones.

La respuesta coincide con la solicitud, lo que permite que el AP confirme que está recibiendo una respuesta válida a la señal de mantenimiento que envió.

Este comportamiento es importante porque muestra que el keepalive de control no es principalmente un mecanismo de sondeo controlado por controlador. En cambio, el AP es responsable de verificar la disponibilidad del canal de control, y el controlador responde en consecuencia.

El intervalo de eco se basa en la inactividad, no en una programación fija

Este es uno de los aspectos más comúnmente malinterpretados de las señales de mantenimiento de control CAPWAP.

Una suposición común es que el AP envía una solicitud de eco cada 30 segundos como un latido periódico fijo. En la práctica, no es así como funciona.

El keepalive de control se basa en la inactividad del canal de control. Esto significa que el AP envía una solicitud de eco independiente solamente cuando el canal de control ha estado inactivo para el intervalo configurado. Si ya se está intercambiando otro tráfico de control entre el AP y el controlador, no hay necesidad de enviar un paquete de eco separado.

Cualquier comunicación de control válida entre el AP y el controlador prueba efectivamente que el canal de control está vivo. Debido a eso, el tráfico de control CAPWAP normal reinicia el temporizador de señal de mantenimiento.

Entre los ejemplos de este tipo de tráfico de control se incluyen:

- intercambios de configuración
- actualizaciones de administración de recursos de radio
- Mensajes de control relacionados con WLAN
- eventos de control relacionados con el cliente
- estadísticas o mensajes de sincronización de estado
- otros paquetes de control CAPWAP intercambiados como parte del funcionamiento normal

Como resultado, las solicitudes de eco independientes se ven solamente durante períodos en los que el canal de control está silenciado.

Ejemplo sencillo

Puede verificar los temporizadores de eco CAPWAP en el AP usando el comando show capwap client timer.

<#root>

```
Training-AP#

show capwap client timer


CAPWAP TIMERS Running Current / Max (seconds)
PATHMTU_TIMER : 23 / 30
```

```
MSG_CLIENT_STAT : 124 / 180
DATA_CHANNEL_KEEP_ALIVE_TIMER : 24 / 30

ECHO_INTERVAL_TIMER : 23 / 30


PERIODIC_ECHO_TIMER : 233 / 300


PRIMARY_DISCOVERY_TIMER : 50 / 120
CAPWAP_WDG_UPDATE_TIMER : 4 / 5
FLASH_WRITE_INTERVAL_TIMER : 21 / 60
```

Cronómetros

El mecanismo de keepalive de control se basa en dos valores de temporización importantes.

| Ítem | Valor Predeterminado | Descripción |
|---|---|---|
| Intervalo de eco | 30 segundos | La cantidad de inactividad del canal de control antes de que el AP envíe una solicitud de eco independiente |
| Temporizador muerto de control del controlador | 90 segundos | La cantidad máxima de tiempo que el controlador permite sin recibir tráfico de control válido antes de declarar la sesión de control inactiva |

Qué ocurre cuando falla el Keepalive del control

Si el canal de control se vuelve silencioso por más tiempo que el tiempo de espera permitido, el controlador finalmente declara que la sesión de control se ha perdido.

En ese momento, el controlador trata al AP como no más accesible en el canal de control y comienza el cierre de la sesión. Esto normalmente incluye cerrar la conexión de control y quitar el estado de sesión de control activo del AP.

El AP puede entonces intentar restablecer la conectividad redescubriendo y volviendo a unirse al controlador, dependiendo del escenario de falla.

Implicaciones de Troubleshooting

Comprender este comportamiento de keepalive es esencial durante la resolución de problemas.

Los paquetes de eco que faltan no siempre significan un problema

Si una captura de paquetes no muestra Solicitudes de eco cada 30 segundos, no indica automáticamente un error. Puede significar simplemente que está fluyendo suficiente tráfico de control CAPWAP, por lo que no se requiere un eco independiente.

El Espaciado De Eco Irregular Suele Ser Normal

Los ecos suelen aparecer a intervalos no uniformes porque se desencadenan por inactividad. Debe ocurrir lo siguiente.

Centrarse en la actividad general del canal de control

Al resolver problemas de desconexión de AP, es más útil preguntar:

- ¿El controlador sigue recibiendo tráfico de control CAPWAP del AP?
- ¿El canal de control está silenciado durante el tiempo suficiente para activar el temporizador de inactividad?
- ¿Hay problemas de red que afectan sólo a la ruta de control?
- ¿La pérdida de paquetes, el comportamiento del firewall, los problemas de NAT o las caídas del plano de control interrumpen el tráfico UDP 5246?

El verdadero problema no es la ausencia de paquetes de eco periódicos por sí mismos. El verdadero problema es la pérdida de la comunicación del canal de control durante el tiempo suficiente para que el controlador declare el AP inalcanzable.

Keepalive de datos CAPWAP

Propósito

El eco del control CAPWAP confirma que el canal de control funciona, pero no prueba que el canal de datos también funcione correctamente. Dado que la trayectoria de control y la trayectoria de datos pueden fallar independientemente, CAPWAP utiliza una señal de mantenimiento de datos independiente en el puerto UDP 5247.

El propósito del keepalive de datos es:

- verifique que el AP aún pueda alcanzar el controlador en el canal de datos
- mantener el estado del túnel de datos del AP
- ayuda a detectar errores que afectan sólo a la ruta de datos

Quién lo envía y cómo responde el controlador

El AP envía el keepalive de datos, y el controlador responde con una respuesta del keepalive de datos.

La respuesta puede cifrarse o descifrarse, en función de si el cifrado del canal de datos está habilitado.

Si el keepalive es válido, el controlador lo utiliza para confirmar que la trayectoria de datos del AP aún es alcanzable. Si el paquete no se puede hacer coincidir con una sesión de AP válida, o si la respuesta no se puede enviar, la señal de mantenimiento se descarta y la trayectoria de datos se puede considerar finalmente como fallida.

Cómo lo valida el controlador

Antes de aceptar el keepalive, el controlador realiza una validación básica para asegurarse de que el paquete pertenece al AP correcto.

El controlador verifica que:

- el keepalive contiene información de CAPWAP válida
- la dirección MAC de radio AP está presente
- el paquete se puede hacer coincidir con una sesión AP

El controlador primero intenta identificar la sesión usando la dirección IP de origen y el puerto UDP de origen. Si eso falla, puede recurrir al uso de la dirección MAC de radio AP.

Esto es importante para los AP detrás de NAT o PAT, donde el canal de datos puede llegar desde un puerto UDP traducido diferente que el canal de control. En tales casos, el controlador puede aprender y actualizar la tupla de canal de datos real del AP.

Si el paquete parece pertenecer a un AP diferente de la sesión ya asociada con esa combinación de puerto IP, el keepalive se rechaza para evitar la asignación incorrecta de la sesión.

Qué ocurre después de la validación

Una vez que se acepta el keepalive, el controlador lo procesa según el estado de sesión actual del AP.

- Si la sesión de datos ya está establecida, el keepalive simplemente actualiza la actividad.
- Si este es el primer keepalive de datos válido, el controlador puede utilizarlo para aprender o actualizar la información del canal de datos del AP y completar el establecimiento del túnel de datos.

Este primer keepalive es especialmente importante porque ayuda al controlador a programar correctamente el túnel de datos, incluidos los casos en los que el AP está detrás de NAT o PAT.

Una vez que la sesión de datos esté completamente establecida, las señales de mantenimiento futuras seguirán la ruta de estado estable normal y se utilizarán únicamente para mantener la actividad.

Comportamiento importante

Un keepalive de datos válido hace más que confirmar el estado de la ruta de datos. También actualiza la actividad general de la sesión del AP en el controlador.

Esto significa que, en el controlador, la actividad del canal de datos contribuye al estado general de la sesión AP. Como resultado, los mecanismos de control y de actividad de los datos están relacionados, aunque tienen diferentes propósitos.

Temporizadores de keepalive de datos del lado AP

El AP controla el intervalo de keepalive de datos y decide cuándo se debe considerar que el túnel de datos está inactivo.

| Ítem | Valor Predeterminado |
|---|---|
| Intervalo de keepalive de datos | 30 segundos |
| Retroceso de retransmisión | 3 s, 6 s, 12 s, luego 15 s |
| Intervalo muerto de datos | 180 segundos |

En condiciones normales, el AP envía un keepalive de datos cada 30 segundos.

Si el AP no recibe una respuesta, lo reintenta usando un patrón de backoff. Si la falla continúa durante 180 segundos, el AP declara el túnel de datos inactivo.

# Retransmisiones CAPWAP

Principio básico: La fiabilidad funciona en ambas direcciones

La mensajería de control CAPWAP utiliza un modelo de solicitud y respuesta, aunque se ejecute sobre UDP. Para proporcionar fiabilidad, el dispositivo que envía una solicitud también es responsable de retransmitirla hasta que se reciba la respuesta esperada.

Esto significa que las retransmisiones son simétricas:

- Para las solicitudes del controlador al AP, como una actualización de la configuración, el controlador administra la retransmisión.
- Para las solicitudes de AP al controlador, tales como Discovery, Join, Configuration Status, los mensajes relacionados con la imagen y Echo Requests, el AP maneja la retransmisión.

Este es un punto importante para la resolución de problemas. Si ve retransmisiones de AP a controlador en una captura de paquetes, generalmente significa que el AP simplemente está reintentando su propia solicitud porque no recibió la respuesta esperada. Esto es normal durante la unión y también puede ocurrir durante la actividad de eco de control.

Comportamiento de retransmisión del lado controlador

En el controlador, la retransmisión es manejada por una máquina de estado de confiabilidad de transmisión dedicada.

En términos sencillos, el controlador:

1. acepta una solicitud que requiere confirmación
2. lo coloca en una cola de transmisión por AP
3. envía la solicitud
4. espera la respuesta coincidente
5. lo quita de la cola cuando llega la respuesta o lo retransmite cuando caduca el temporizador

Esta lógica se sigue por separado para cada sesión AP. El controlador también mantiene una ventana de transmisión y un conteo de mensajes de solicitud pendientes.

Cómo decide el controlador si retransmitir

Cada vez que caduca el temporizador de retransmisión, el controlador revisa las entradas de solicitud en cola y toma una de estas decisiones:

1. Respuesta recibida fuera de servicio

Si la respuesta para esa solicitud ya se ha recibido, incluso si llegó fuera de secuencia, el controlador no vuelve a transmitir el mensaje.

2. Límite de reintentos excedido

Si la solicitud ya ha sido retransmitida más de las veces permitidas, el controlador trata esto como una falla y aborta el proceso de transmisión para esa sesión AP.

En ese momento, la sesión AP se termina.

3. La solicitud aún no es lo suficientemente antigua

El controlador no retransmite inmediatamente cada mensaje en cola en cada evento del temporizador. Una solicitud debe permanecer en la cola durante al menos el intervalo de retransmisión antes de poder enviarse de nuevo.

De forma predeterminada, este intervalo de retransmisión es de 3 segundos.

4. Retransmitir la solicitud

Si la solicitud sigue pendiente, ha envejecido el tiempo suficiente y no ha excedido el límite de reintentos, el controlador la reenvía en el canal de control CAPWAP e incrementa el contador de reintentos.

Caso especial: AP de cadena de margarita cableada

Para las implementaciones de malla que utilizan una trayectoria AP de cadena de margarita cableada, el controlador permite un presupuesto de reintento más grande.

En este caso, el límite de reintentos normal se triplica de forma efectiva.

Con el conteo de reintentos predeterminado de 5, esto significa que el controlador puede

reintentar hasta 15 veces antes de declarar la falla.

Esta excepción existe porque estas topologías pueden requerir una mayor tolerancia para el retraso o la pérdida de mensajes.

Comportamiento de retransmisión del lado AP

El AP también retransmite sus propias solicitudes CAPWAP, pero utiliza un patrón diferente que el controlador.

Mientras que el controlador utiliza un intervalo de retransmisión fijo, el AP utiliza backoff exponencial. Esto significa que el tiempo de espera aumenta después de cada intento fallido.

Con la configuración predeterminada, el tiempo de reintento de AP es aproximadamente:

- 6 segundos
- 12 segundos
- 24 segundos
- 48 segundos
- 96 segundos

Este comportamiento se aplica a las solicitudes CAPWAP originadas en AP tales como:

- Descubrimiento
- Incorporarse
- intercambios relacionados con configuración
- transacciones de control cifradas
- Solicitudes de eco

Estos parámetros de reintento se aprenden del controlador como parte de la configuración de unión de AP.

Huella digital de diagnóstico en capturas de paquetes

El patrón de retransmisión en sí es a menudo una pista útil durante la resolución de problemas.

| Patrón de retransmisión | Fuente probable |
| --- | --- |
| Retransmisiones espaciadas uniformemente, | Retransmisión en el lado del |

| Patrón de retransmisión | Fuente probable |
|---|---|
| aproximadamente cada 3 segundos | controlador |
| Retransmisiones que se extienden más a lo largo del tiempo, como 6s, 12s, 24s, 48s, 96s | Retransmisión del lado AP con retroceso exponencial |

Esta es una manera práctica de determinar qué lado está reintentando, especialmente durante fallas de unión o problemas relacionados con el eco.

Qué Sucede Cuando Se Agotan Los Reintentos

Si las retransmisiones continúan sin recibir la respuesta esperada, ambas partes finalmente se rinden, pero sus acciones de recuperación son diferentes.

Lado del controlador

Si el controlador agota su presupuesto de reintento, anula el proceso de transmisión y termina la sesión AP. Esto hace que se cierren el control CAPWAP y las sesiones de datos.

lado AP

Si el AP agota sus propios intentos de reintento, abandona ese controlador y comienza de nuevo desde el principio, generalmente volviendo a la fase de detección e intentando una reincorporación completa.

Botones y valores predeterminados de configuración

El comportamiento de retransmisión se controla mediante dos configuraciones principales en el perfil de unión de AP.

| Comando | Valor Predeterminado | Función |
|---|---|---|
| conteo de retransmisión capwap | 5 | Número máximo de intentos de retransmisión |
| Capwap retransmit interval | 3 segundos | Intervalo de retransmisión base |

Estos valores influyen tanto en la confiabilidad de la unión como en otros reintentos de control CAPWAP originados en AP, incluidos los reintentos relacionados con el eco.

## Referencia de temporizador consolidado

En esta tabla se resumen los principales temporizadores CAPWAP descritos en este artículo.

| Temporizador | Valor Predeterminado | Plano | OWNER | Descripción |
|---|---|---|---|---|
| Intervalo de eco de control | 30 segundos | Control | AP | Si el AP no transmite el tráfico de control CAPWAP durante 30 segundos, envía una solicitud de eco. |
| Temporizador de control de latido muerto | 90 segundos | Control | Controlador | El controlador espera un tráfico de control válido dentro de esta ventana. Si no se recibe nada, la sesión de control se considera inactiva. |
| Intervalo de retransmisión de control | 3 segundos | Control | Controlador | El controlador retransmite sus propias solicitudes CAPWAP sin respuesta en un intervalo fijo. |
| Controlar conteo de retransmisión | 5 intentos | Control | Controlador | Recuento máximo de reintentos para solicitudes CAPWAP originadas en el controlador. En escenarios de cadena de margarita cableada, esto puede aumentar a 15 intentos. |
| AP control retransmit backoff | 6, 12, 24, 48, 96 segundos | Control | AP | El AP retransmite sus propias solicitudes CAPWAP usando el backoff exponencial. |
| Intervalo de keepalive de datos | 30 segundos | Datos | AP | En condiciones normales, el AP envía un keepalive de datos cada 30 segundos. |
| Data keepalive retry backoff | 3, 6, 12, 15, 15 segundos | Datos | AP | Si se pierde una respuesta de keepalive de datos, el AP reintenta usando |

| Temporizador | Valor Predeterminado | Plano | OWNER | Descripción |
|---|---|---|---|---|
| | | | | backoff, limitado a 15 segundos. |
| Intervalo muerto del canal de datos | 180 segundos | Datos | AP | Si el AP no mantiene exitosamente el intercambio de keepalive de datos dentro de este período, declara que el túnel de datos está inactivo. |

## Diferencias en paralelo:

Keepalive frente a retransmisión

Aunque a veces se confunden, keepalive y la retransmisión tienen diferentes propósitos.

| Aspecto | Keepalive | Retransmisión |
|---|---|---|
| Objetivo principal | Verifica que el peer aún es accesible | Vuelve a intentar una solicitud específica cuando no se recibe ninguna respuesta |
| Alcance | Por sesión o por canal | Por mensaje |
| Activador | Tiempo de espera de inactividad o actividad | Una solicitud permanece sin responder |
| Método de seguimiento | Basado en tiempo | Basado en el recuento de reintentos |
| Significado de falla | Ya no se puede alcanzar el canal o la sesión | Un intercambio CAPWAP específico ha fallado repetidamente |
| Resultado de fallo | La sesión se puede declarar inactiva | El controlador puede terminar la sesión o el AP puede reiniciar la unión |

## Cadenas de registro de seguimiento de RA por mecanismo

Para el seguimiento específico de AP, recopile los registros para el AP y busque estas cadenas exactas.

Recopilación de registros

Uso:

- debug wireless mac <ap-radio-mac>
- show logging profile wireless filter mac <ap-radio-mac> to-file bootflash:<file>

Controlar keepalive/heartbeat

Buscar por:

- Manejo de solicitud de eco
- Generar respuesta de eco
- Respuesta de eco enviada para solicitud con el número de secuencia <N>.
- El temporizador de latidos se reinició con un nuevo valor <ms>
- Pulsación del temporizador de latido invocada
- Vencimiento del temporizador de latidos

keepalive de datos

Buscar por:

- Se recibió keepalive de datos
- sess de datos ya establecidos
- DTLS de datos no establecido
- Actualizando entrada de túnel de datos CAPWAP
- Error al procesar keepalive de datos. Motivo: La sesión CAPWAP no está en estado de ejecución o configuración
- Mensaje de keepalive no válido, sin bloque capwap
- Mensaje de señal de mantenimiento no válido, sin WTP MAC
- Error al procesar keepalive, no se ha encontrado la sesión CAPWAP
- La señal de mantenimiento de datos se recibe en un puerto diferente al puerto de control: <port>
- Se recibe keepalive de datos para diferentes AP <mac>
- No se pudo actualizar la información de tupla de datos en la tabla de sesión WTP para el host remoto: <ip>
- Error al actualizar la entrada de túnel de datos CAPWAP

Gestión de keepalive del plano de datos

Buscar por:

- Los datos recibidos se mantienen activos de <src> a <dst>
- Respuesta de keepalive de datos enviada <enc/plain>
- Descarte de paquetes keepalive de IP: <ip>, sesión desconocida
- Descarte de paquetes keepalive de IP: <ip>, no se pudo obtener el estado de DTLS de datos
- No se pudo enviar la respuesta de activación de mantenimiento de datos
- Error en el mensaje keepalive de datos de equilibrio de carga

Retransmisión

Buscar por:

- retransmit timer callback
- Retransmitiendo seqnum <N> porque está en cola y aún no ha vuelto
- Retransmitiendo mensaje: <msg-name> intento de retransmisión: <M>
- entrada con número de secuencia: <N> está en cola durante <S> segundos. No retransmitiendo
- Finalización de sesión CAPWAP, retransmisiones máximas caducadas para: <msg> ...
- Limpieza del recurso de sesión CAPWAP al salir del AP.

Desconexión de sesión

Buscar por:

- Finalizando sesión CAPWAP de AP.
- Cierre la sesión CAPWAP DTLS.
- capwap-dtls control session close
- capwap-dtls data session close
- Último paquete de control recibido hace <S> segundos.
- Último paquete de mantenimiento de datos activo recibido hace <S> segundos.
- Se cerró la sesión CAPWAP DTLS para AP, causa: <reason>

# Examples:

## Escenario laboral

Verificación de depuración de AP

Este comando de depuración de AP se puede utilizar para monitorear el control CAPWAP y la comunicación de keepalive de datos entre el AP y el WLC.

```
#debug capwap client event
```

Estos registros de depuración muestran una secuencia de comunicación CAPWAP satisfactoria.

A las 13:11:44, el AP transmitió una solicitud de eco CAPWAP al WLC sobre el puerto UDP 5246. Durante el mismo intervalo, el AP también transmitió un paquete CAPWAP Data Keepalive sobre el puerto UDP 5247. Los registros confirman que el WLC respondió con éxito a ambas solicitudes.

Las marcas de tiempo indican un ciclo de comunicación CAPWAP normal:

- 13:11:44.0917 - Solicitud de eco transmitida.
- 13:11:44.0918 - Datos Keepalive transmitidos.
- 13:11:44.0926 - Keepalive de datos recibidos del WLC.
- 13:11:44.0940 - Respuesta de eco recibida del WLC.

Estas marcas de tiempo confirman que tanto el control CAPWAP como los canales de datos funcionan según lo esperado con una latencia de ida y vuelta insignificante.

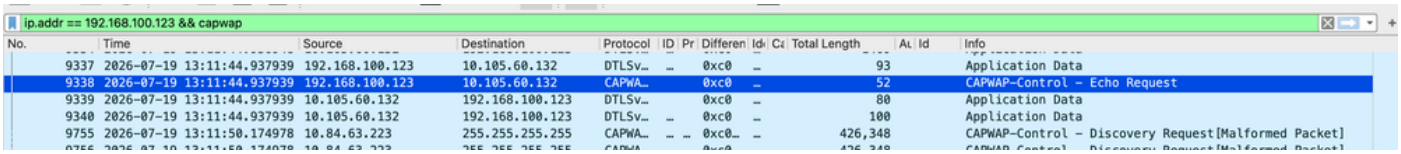
```
[*07/19/2026 13:11:14.0817] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0917] Echo Request: Send count 22
[*07/19/2026 13:11:44.0917] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 13:11:44.0918] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 13:11:44.0926] chatter: [RX]KEEPALIVE: Count 164
[*07/19/2026 13:11:44.0927] Sending KEEPALIVE to WTP SM
[*07/19/2026 13:11:44.0927] Capwap data keep-alive Msg.
[*07/19/2026 13:11:44.0927] [RX]KEEPALIVE: Session ID 3221108139, Next scheduled for TX in 30 sec
[*07/19/2026 13:11:44.0927] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0940] [RX]Echo Response from 10.105.60.132
[*07/19/2026 13:11:44.0004] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 13:12:14.0004] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:12:14.0005] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 13:12:14.0005] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
```

Validación de paquetes de control CAPWAP (puerto UDP 5246)

Análisis de captura de paquetes

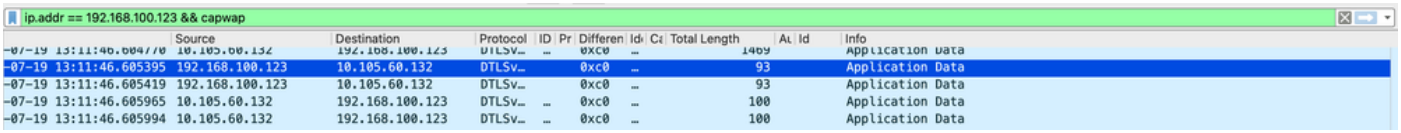
La captura de paquetes confirma que el AP generó una solicitud de eco CAPWAP a las 13:11:44 sobre el puerto UDP 5246.

El WLC recibió con éxito el paquete, procesó la solicitud e inmediatamente generó la respuesta de eco correspondiente. Dado que el canal de control CAPWAP está protegido mediante el cifrado DTLS, la respuesta aparece como datos de aplicación cifrados en la captura de paquetes.




Verificación de paquetes de switch

La captura del paquete del switch confirma que los paquetes de control CAPWAP cifrados fueron recibidos con éxito del WLC y reenviados hacia el AP.

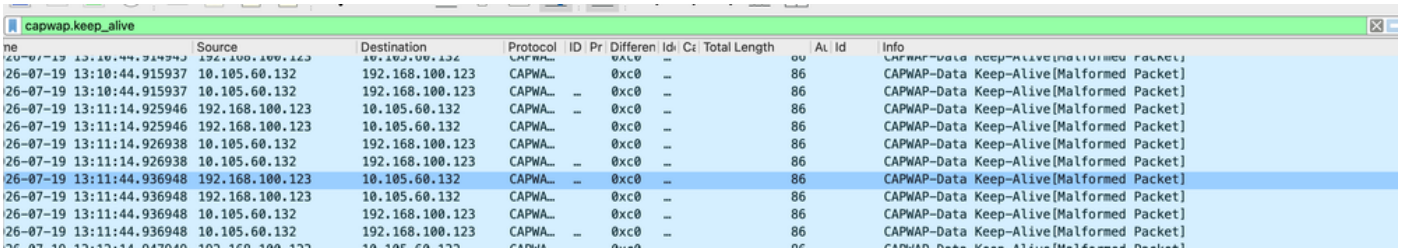



Validación de keepalive de datos CAPWAP (puerto UDP 5247)

El AP transmite periódicamente los paquetes de keepalive de datos CAPWAP sobre el puerto UDP 5247 para verificar el estado del túnel de datos CAPWAP.

A las 13:11:44, el AP transmitió un paquete de Keepalive de datos hacia el WLC. El WLC recibió con éxito el paquete e inmediatamente respondió con la respuesta de keepalive correspondiente.

Este intercambio exitoso confirma que la trayectoria de datos CAPWAP sigue operativa y que la comunicación bidireccional entre el AP y el WLC funciona normalmente

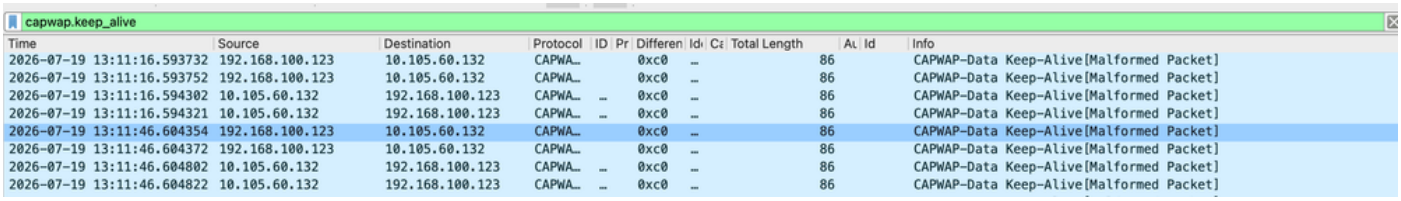


Verificación de paquetes de switch

La captura de paquetes del switch valida además que los paquetes de keepalive de datos CAPWAP fueron reenviados con éxito entre el AP y el WLC sin interrupción.

El flujo de paquetes observado confirma que:

- Los paquetes Keepalive de datos alcanzaron con éxito el WLC.
- El WLC generó la respuesta de keepalive esperada.
- El switch reenvió la respuesta al AP.
- No se produjo ninguna pérdida de paquetes en la ruta de reenvío.



capwap.keep_alive

| Time | Source | Destination | Protocol | ID | Pr | Differen | Id | Ca | Total Length | At | Id | Info |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2026-07-19 13:11:16.593732 | 192.168.100.123 | 10.105.60.132 | CAPWA… | | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:16.593752 | 192.168.100.123 | 10.105.60.132 | CAPWA… | | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:16.594302 | 10.105.60.132 | 192.168.100.123 | CAPWA… | … | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:16.594321 | 10.105.60.132 | 192.168.100.123 | CAPWA… | … | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:46.604354 | 192.168.100.123 | 10.105.60.132 | CAPWA… | | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:46.604372 | 192.168.100.123 | 10.105.60.132 | CAPWA… | | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:46.604802 | 10.105.60.132 | 192.168.100.123 | CAPWA… | … | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |
| 2026-07-19 13:11:46.604822 | 10.105.60.132 | 192.168.100.123 | CAPWA… | … | | 0xc0 | … | | 86 | | | CAPWAP-Data Keep-Alive[Malformed Packet] |

## Paquetes de control (UDP 5246) descartados en el switch de enlace ascendente de punto de acceso

Esta prueba demuestra el comportamiento de un AP cuando el puerto de control CAPWAP (UDP 5246) se descarta en el switch de link ascendente AP.

El objetivo es validar el comportamiento de AP, WLC, y de la red cuando los paquetes de control CAPWAP se impiden de alcanzar el AP, a pesar de que el WLC procesa y responde con éxito a las peticiones.

En esta situación:

- El AP continúa transmitiendo solicitudes de eco CAPWAP hacia el WLC.
- El WLC recibe y procesa con éxito cada solicitud de eco.
- El WLC genera la respuesta de eco correspondiente.
- El switch de link ascendente AP recibe la respuesta pero no la reenvía de vuelta al AP.
- Dado que el AP nunca recibe la respuesta de eco, finalmente excede el conteo máximo de retransmisión y reinicia la máquina de estado CAPWAP.

Análisis de depuración de PA

A las 12:11:55.4568, el AP transmitió una solicitud de eco CAPWAP hacia el WLC sobre el puerto

5246 UDP.

Solicitud de eco: Enviar conteo 0

A diferencia del escenario de trabajo normal, no se recibió ninguna respuesta de eco. Como resultado, el AP inició las retransmisiones según el temporizador CAPWAP predeterminado.

Las retransmisiones se produjeron en los siguientes husos horarios:

| Hora | Evento |
|---|---|
| 12:12:00.2587 | Recuento de retransmisión = 1 |
| 12:12:03.2599 | Recuento de retransmisión = 2 |
| 12:12:06.2610 | Recuento de retransmisión = 3 |
| 12:12:09.2624 | Recuento de retransmisión = 4 |
| 12:12:12.2637 | Recuento de retransmisión = 5 |

Después de la quinta retransmisión fallida, el AP declaró la sesión de control CAPWAP inalcanzable.

A las 12:12:15.2647, AP informó:

Se ha superado el recuento máximo de retransmisión, volviendo al modo DISCOVER.

Inmediatamente después, el AP reinició la máquina de estado CAPWAP para iniciar un nuevo proceso de detección.

```
[*07/17/2026 12:11:54.2577] [RX]KEEPALIVE: Session ID 4068929293, Next scheduled for TX in 30 sec
[*07/17/2026 12:11:54.2577] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/17/2026 12:11:55.4568] Echo Request: Send count 0
[*07/17/2026 12:11:55.4568] [TX]Echo Request: Sent 1 Lost 269
[*07/17/2026 12:12:00.2587] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:03.2599] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:06.2610] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:09.2624] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:12.2637] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
```

```
[*07/17/2026 12:12:15.2647] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/17/2026 12:12:15.2647] Failed to reach capwap down with retransmission 3 times
```

Los seguimientos WLC RA confirman que el controlador no experimentó ningún problema de procesamiento.

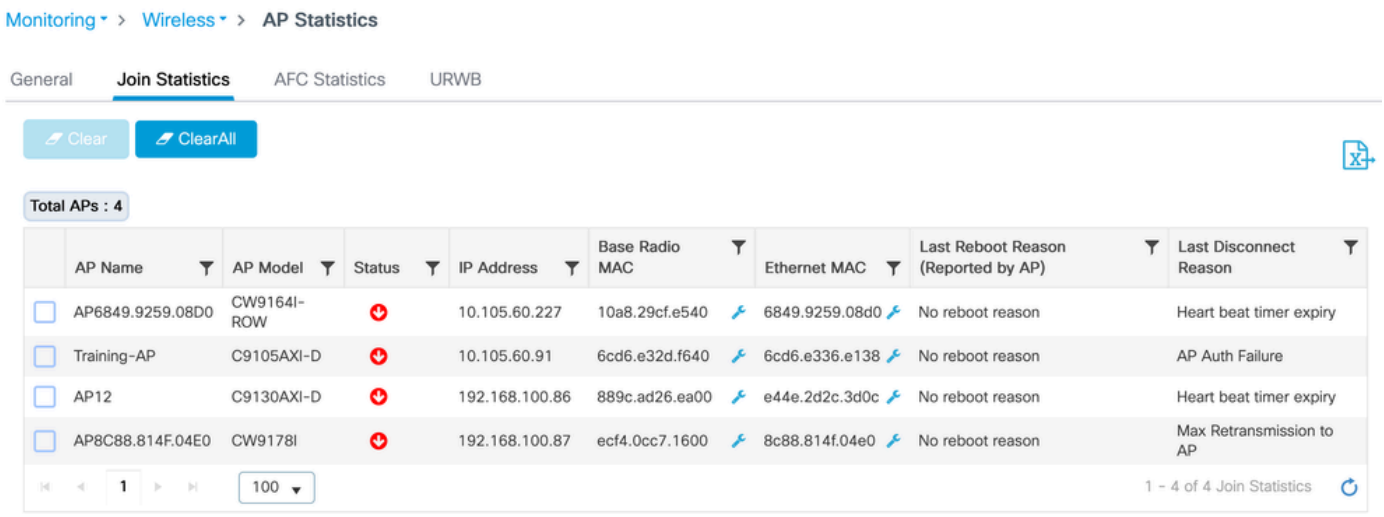
A las 12:11:58.731835712, el WLC recibió con éxito la solicitud de eco CAPWAP transmitida por el AP. Estos registros demuestran que el WLC procesó la solicitud con éxito y generó la respuesta apropiada. Más tarde, a las 12:12:19.802183814, el WLC recibió un DTLS Close Notify del AP. El AP se desconectó porque nunca recibió las respuestas de eco transmitidas por el controlador. En consecuencia, el WLC terminó la sesión DTLS y registró la desasociación del AP.

<#root>

```
2026/07/17 12:12:19.802274790 {wncd_x_R0-1}{2}: [ewlc-dtls-sess] [16522]: (info):

 Remote Host: 192.168.100.120[5256] MAC: 889c.ad26.ea00  dtls session closed


2026/07/17 12:12:19.802279648 {wncd_x_R0-1}{2}: [ewlc-infra-capwap-dgram] [16522]: (debug): dgram handl
2026/07/17 12:12:19.802317470 {wncd_x_R0-1}{2}: [ewlc-capwapmsg-sess] [16522]: (debug): Encrypted DTLS
2026/07/17 12:12:19.802321202 {wncd_x_R0-1}{2}: [capwapac-smgr-srvr] [16522]: (debug): Mac: 889c.ad26.e
2026/07/17 12:12:19.802376588 {wncd_x_R0-1}{2}: [ap-join-info-db] [16522]: (note): MAC: 889c.ad26.ea00

AP disconnect initiated. Name : AP12, Ethernet mac : e44e.2d2c.3d0c, Reason: DTLS close alert from peer,
```

<#root>

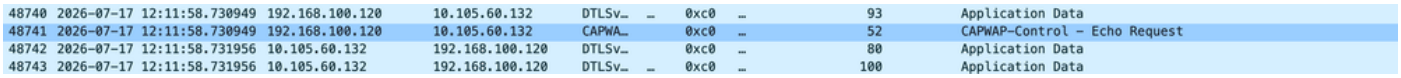
```
VK-WLC#show wireless stats ap history | i AP12


AP12                              889c.ad26.ea00  Joined     07/17/26 12:24:18  NA
AP12                              889c.ad26.ea00  Disjoined  07/17/26 12:12:19  NA
AP12                              889c.ad26.ea00  Joined     07/17/26 12:09:25  NA

AP12                           889c.ad26.ea00  Disjoined  07/17/26 12:08:33  NA                  Heart be
```

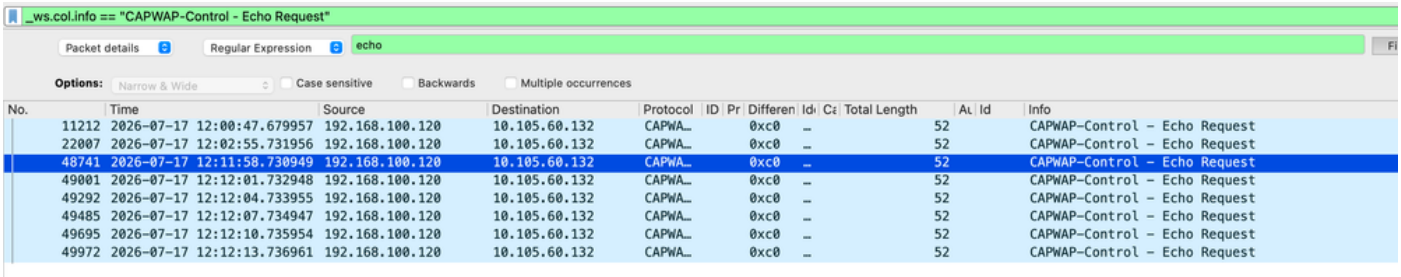



El WLC EPC confirma que:

- Al mismo tiempo, la solicitud de eco CAPWAP alcanzó con éxito el WLC.
- El WLC generó una respuesta de eco CAPWAP cifrada.
- La respuesta aparece como Datos de aplicación, ya que el tráfico de control CAPWAP está protegido por el cifrado DTLS.

Por lo tanto, el EPC confirma que el controlador transmitió la respuesta con éxito. Esto elimina el WLC como el origen del problema.




Las capturas de paquetes recolectadas en el switch de link ascendente AP proporcionan la prueba final.

Las capturas demuestran que:

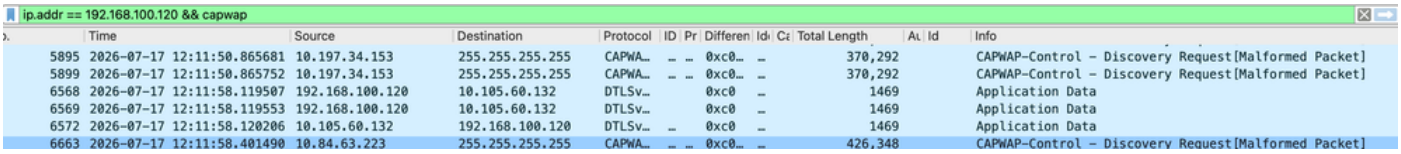
- El switch recibió con éxito la respuesta de eco cifrada transmitida por el WLC.

- La respuesta es visible como Application Data, lo que se espera debido al cifrado DTLS.
- La respuesta no fue reenviada hacia el AP.

Esto explica por qué:

- El AP nunca recibió la respuesta de eco CAPWAP.
- El AP continuó retransmitiendo solicitudes de eco.
- El contador de retransmisión finalmente excedió el umbral configurado.
- El AP reinició la máquina de estado CAPWAP.

Las capturas de paquetes identifican claramente el switch como el punto donde se interrumpió el tráfico de control CAPWAP




## El puerto de datos CAPWAP (UDP 5247) se descarta en el switch de enlace ascendente AP

Esta prueba valida el comportamiento del AP cuando el puerto de datos CAPWAP (UDP 5247) se descarta en el switch de enlace ascendente AP mientras el puerto de control CAPWAP (UDP 5246) permanece operativo.

A diferencia del escenario anterior, el AP continúa manteniendo la conexión de control CAPWAP con el WLC intercambiando con éxito los mensajes CAPWAP Echo sobre el puerto UDP 5246. Sin embargo, dado que los paquetes de keepalive de datos CAPWAP no pueden completar el viaje de ida y vuelta, el AP finalmente declara la trayectoria de datos CAPWAP como inalcanzable e inicia un reinicio CAPWAP.

Los logs de depuración de AP confirman que el canal de control CAPWAP permaneció operativo durante toda la prueba.

Al comienzo de la captura, las solicitudes de eco CAPWAP transmitidas a través del puerto UDP 5246 siguieron recibiendo respuestas de eco válidas del WLC, lo que confirma la comunicación ininterrumpida del plano de control.

Sin embargo, a las 14:30:15, el AP transmitió un paquete CAPWAP Data Keepalive sobre el puerto UDP 5247. Dado que no se recibió ninguna respuesta de Data Keepalive correspondiente, el AP inició el mecanismo de reintento. Las retransmisiones se pueden observar en estas marcas

de tiempo:

| Grupo fecha/hora | Evento |
|---|---|
| 14:30:15 | Datos iniciales transmitidos por Keepalive |
| 14:30:19 | Reintentar 1 |
| 14:30:25 | Reintentar 2 |
| 14:30:37 | Reintentar 3 |
| 14:30:49 | Reintentar 4 |
| 14:31:01 | Reintentar 5 |
| 14:31:13 | Reintento final |

Aunque las respuestas de eco CAPWAP continuaron recibiéndose durante este período, el AP no recibió ninguna respuesta para los paquetes de keepalive de datos. Después de agotar los intentos de reintento, el AP informó de un tiempo de espera de keepalive de datos sin cifrar e inició un reinicio CAPWAP. Aproximadamente a las 14:31:16, el AP finalizó la sesión CAPWAP existente y volvió al proceso de detección.

```
AP12#[*07/19/2026 14:30:15.9995] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:15.9995] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 14:30:15.9996] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:30:19.0002] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:19.0002] [TX]KEEPALIVE: Schedule for Retransmit in 6 sec sec_drop_count=0
[*07/19/2026 14:30:19.0003] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:30:25.0023] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:25.0024] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:25.0024] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:30:37.0066] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:37.0066] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:37.0067] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:30:49.0109] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:49.0109] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:49.0109] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:31:01.0151] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:31:01.0151] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:31:01.0152] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
[*07/19/2026 14:31:13.0195] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:31:13.0195] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:31:13.0196] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
```

```
[*07/19/2026 14:31:16.0207] Warning, unencrypted data keepalive failed
[*07/19/2026 14:31:16.0207] Going to restart CAPWAP (reason : data keepalive not received)...
```

Para el canal de datos CAPWAP, los seguimientos indican que el controlador no recibió los paquetes de keepalive de datos esperados. Eventualmente, después de que el AP declaró la falla de keepalive de datos, el WLC registró la terminación de la sesión de DTLS y el evento de desconexión de AP. La secuencia observada en los seguimientos de RA confirma que el controlador permaneció operativo hasta que el AP se desconectó voluntariamente debido al tiempo de espera de keepalive de datos.

Rastreos RA con MAC Ethernet AP:

<#root>

```
2026/07/19 14:31:16.842212773 {fman_rp_R0-0}{2}: [source] [20448]: (debug): ipc(mqipc/wncd_2/wncd-fmrp)
2026/07/19 14:31:16.842250177 {wncd_x_R0-2}{2}: [errmsg] [16638]: (note): %CAPWAPAC_SMGR_TRACE_MESSAGE-
2026/07/19 14:31:16.842251233 {wncd_x_R0-2}{2}: [capwapac-smgr-sess-fsm] [16638]: (note): Mac: 889c.ad2
```

**Last Data Keep Alive Packet received 90 seconds ago.**

```
2026/07/19 14:31:16.843318439 {wncmgrd_R0-0}{2}: [loadbalance-algo] [16262]: (note): Algo counter decre
2026/07/19 14:31:16.843318599 {wncd_x_R0-2}{2}: [wsa-core] [16638]: (debug): WSA AP EVT Create Populate
2026/07/19 14:31:16.843320409 {wncd_x_R0-2}{2}: [wsa-core] [16638]: (debug): WSA AP EVT Create Populate
```

**DISJOIN - AP Mac:889c.ad26.ea00 , new ap disconnect reason 'DTLS close alert from peer' (26)**

Rastreos de RA con radio mac:

<#root>

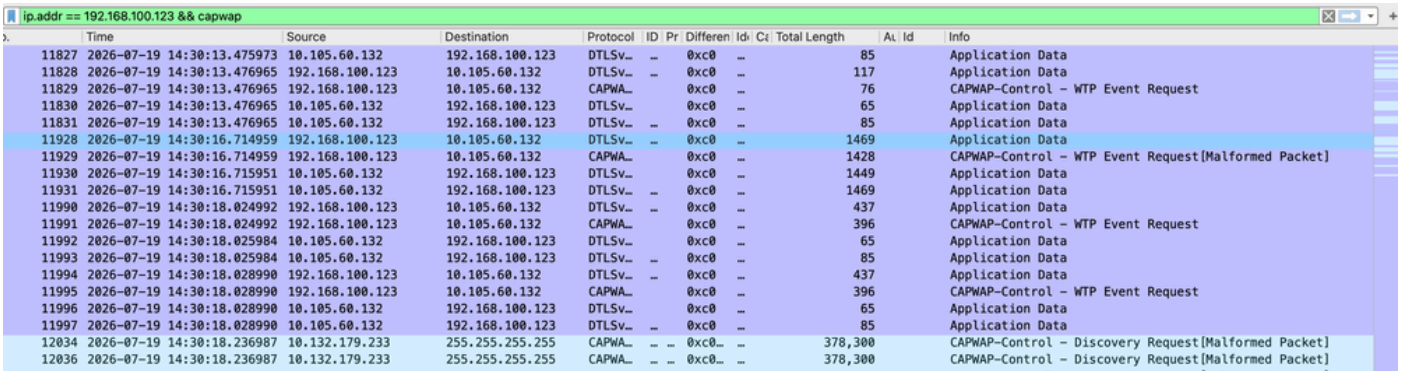
```
2026/07/19 14:31:16.737070835 {wncd_x_R0-2}{2}: [capwapac-smgr-sess] [16638]: (debug): Mac: 889c.ad26.e
2026/07/19 14:31:16.737072831 {wncd_x_R0-2}{2}: [capwapac-smgr-srvr] [16638]: (debug): Mac: 889c.ad26.e
2026/07/19 14:31:16.737076419 {wncd_x_R0-2}{2}: [msc-fsm] [16638]: (debug): @msc_event {"entity":"/capw
2026/07/19 14:31:16.737078137 {wncd_x_R0-2}{2}: [msc-fsm] [16638]: (debug): @msc_event {"entity":"/capw
2026/07/19 14:31:16.841870791 {wncd_x_R0-2}{2}: [ap-join-info-db] [16638]: (note): MAC: 889c.ad26.ea00
```

**AP disconnect initiated. Name : AP12, Ethernet mac : e44e.2d2c.3d0c, Reason: DTLS close alert from peer,**

```
2026/07/19 14:31:16.841890831 {wncd_x_R0-2}{2}: [capwapac-smgr-srvr] [16638]: (debug): MAC: 889c.ad26.e
```

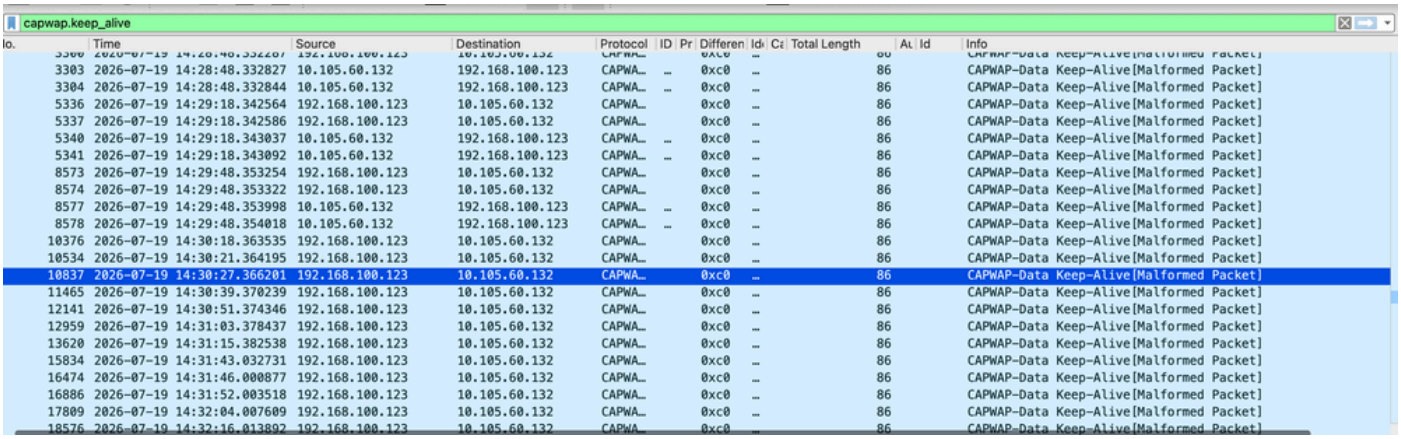
El EPC recolectado en el WLC valida el procesamiento de paquetes del lado del controlador. Las capturas confirman que los paquetes de control CAPWAP se siguieron intercambiando con éxito durante la prueba pero no se recibió ningún paquete de keepalive de datos en el wlc. Esta

observación se alinea con los registros de depuración del AP y demuestra que el mecanismo de keepalive de datos falló a pesar de que el canal de control permaneció activo.




Switch:

Las capturas de paquetes recolectadas en el switch de link ascendente AP muestran que los paquetes estaban presentes en el switch pero que no fueron reenviados al wlc




## Desactivación de keepalive de datos CAPWAP

Esta función fue introducida bajo el ID de bug Cisco CSCvs66015

Esta característica es útil para solucionar problemas en estos escenarios.

1. Solucionar problemas de desconexiones de AP: Después de inhabilitar capwap data keep-alive, podemos ver si AP sigue desconectándose debido a capwap control keep-alive e identificar la causa raíz de las desconexiones de keepalive de AP.
2. Evite las desconexiones debido a capwap data-keepalive como solución alternativa hasta que identifique la razón de las caídas de capwap data keep-alive.
3. Sniffer AP en implementaciones de sucursal flexible conectadas a través de un enlace WAN

con bajo rendimiento. Si queremos recopilar capturas de paquetes OTA configurando uno de los AP para que esté en modo sniffer, todos los paquetes capturados se transmiten al WLC a través del link WAN usando el puerto de datos capwap. Si lo hace, sobrecarga el enlace WAN y afecta a toda la sucursal.

4. Si se inhabilita capwap data keep-alive para AP en modo sniffer y se crea una ACL en la sucursal para descartar paquetes de datos capwap de ese AP concreto, el AP permanece conectado ya que el control capwap está bien y luego puede recopilar OTA del puerto de switch del AP sin sobrecargar el link WAN con capturas de paquetes.

Activación/desactivación de keepalive de datos COS-AP desde el WLC 9800. De forma predeterminada, el keepalive de datos en WLC y AP está habilitado.

Comando WLC:

1) Mostrar el estado con la cadena "Datos sin cifrar mantener activo"

```
show ap config general
```

2) Activar/desactivar keepalive de datos con nombre de AP

```
ap name AP-NAME keepalive
ap name AP-NAME no keepalive
```

Activar/desactivar keepalive de datos COS-AP desde el propio AP. De forma predeterminada, el keepalive de datos en AP está habilitado.

Comando AP:

1) Mostrar el estado con la cadena "Datos sin cifrar Mantener activo"

```
show capwap client config
```

2) Activar/desactivar keepalive de datos en AP

```
capwap ap unencrypted_data_keepalive enable
capwap ap unencrypted_data_keepalive disable
```

Por ejemplo:

Verificación de keepalive deshabilitada en el nivel de AP:

```
AP12#capwap ap unencrypted_data_keepalive disable
```

<#root>

```
AP12#show capwap client configuration
```

```
AdminState                          : ADMIN_ENABLED(1)
Name                                : AP12
Location                            : default location
Primary controller name             : VK-WLC
Primary controller IP               : 10.105.60.132
Secondary controller name           : 9800-demo
Secondary controller IP             : 10.106.39.156
Tertiary controller name            :
ssh status                          : Enabled
ApMode                              : Local
ApSubMode                           : Not Configured
Link-Encryption                     : Disabled

Unencrypted Data Keep Alive         : Disabled

OfficeExtend AP                     : Disabled
Discovery Timer                     : 10
```

Depuraciones de AP:

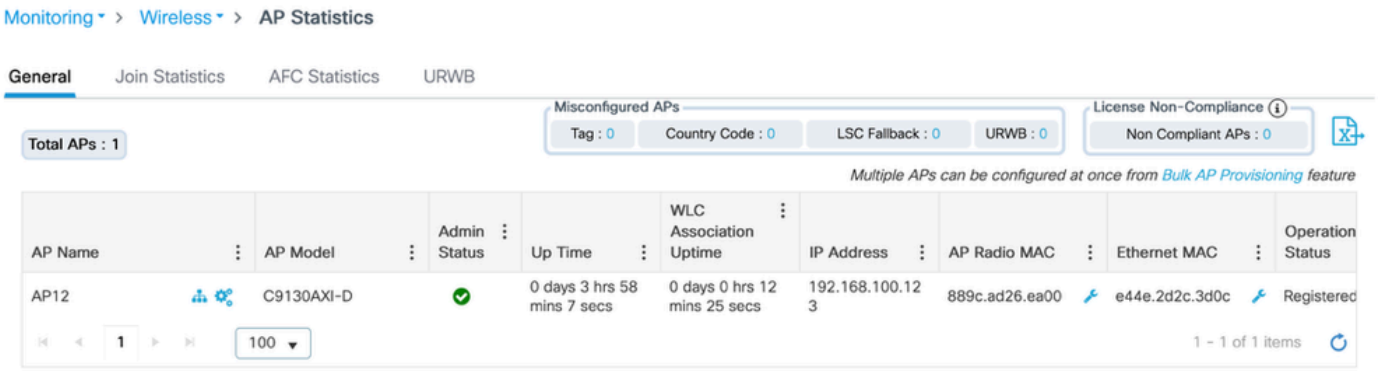
En el debug de AP podemos ver que no hay intercambio de paquetes keepalive de datos entre el AP y el wlc, solo vemos el intercambio de paquetes de control.

AP12#debug capwap client keepalive

```
AP12#[*07/19/2026 15:24:33.4087] Echo Request: Send count 0
[*07/19/2026 15:24:33.4087] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 15:24:33.4112] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:24:34.0006] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:25:34.0032] Echo Request: Send count 1
[*07/19/2026 15:25:34.0032] [TX]Echo Request: Sent 2 Lost 2
[*07/19/2026 15:25:34.0056] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:25:34.0006] [RX]Echo Response from 10.105.60.132 RttCount 2
```

```
[*07/19/2026 15:27:34.0327] Echo Request: Send count 2
[*07/19/2026 15:27:34.0327] [TX]Echo Request: Sent 3 Lost 2
[*07/19/2026 15:27:34.0347] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:27:34.0004] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:28:34.0025] Echo Request: Send count 3
[*07/19/2026 15:28:34.0025] [TX]Echo Request: Sent 4 Lost 2
[*07/19/2026 15:28:34.0050] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:28:34.0022] [RX]Echo Response from 10.105.60.132 RttCount 2
AP12#[*07/19/2026 15:29:43.5772] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.
[*07/19/2026 15:30:04.0140] Echo Request: Send count 4
[*07/19/2026 15:30:04.0140] [TX]Echo Request: Sent 5 Lost 2
[*07/19/2026 15:30:04.0164] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:30:04.0011] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:30:27.7695] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.13
```

A pesar de que los paquetes keepalive de datos se estaban descartando, pero como desactivamos la verificación keepalive de datos, podemos ver que el AP permanece estable en el wlc sin verse afectado por la caída de paquetes keepalive.



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).