

Entender e solucionar problemas de manutenção de atividade do CAPWAP no Catalyst 9800 WLC

Contents

[Introdução](#)

[Contexto](#)

[Dois canais separados, dois mecanismos diferentes](#)

[Retransmissões CAPWAP](#)

[Referência do Temporizador Consolidado](#)

[Diferenças lado a lado](#)

[Cadeias de Caracteres do Log de Rastreamento RA por Mecanismo](#)

[Examples:](#)

[Cenário de trabalho](#)

[Validação de Pacote de Controle CAPWAP \(Porta UDP 5246\)](#)

[Validação da manutenção de atividade de dados CAPWAP \(porta UDP 5247\)](#)

[Pacotes de controle \(UDP 5246\) sendo descartados no Switch de uplink AP](#)

[Porta de dados CAPWAP \(UDP 5247\) sendo descartada no switch de uplink AP](#)

[Desabilitação da Manutenção de Atividade de Dados do CAPWAP](#)

Introdução

Este documento descreve as manutenções de atividades de controle CAPWAP, manutenções de atividades de dados e retransmissões,

Contexto

O CAPWAP fornece a estrutura de comunicação entre os pontos de acesso da Cisco e o controlador de LAN sem fio nas plataformas Cisco Catalyst 9800. Ele usa canais de dados e controle separados, juntamente com mecanismos de keepalive e retransmissão definidos para manter a conectividade.

Este artigo explica as manutenções de atividades de controle do CAPWAP, manutenções de atividades de dados e retransmissões, incluindo os temporizadores associados, o comportamento de falha e os principais indicadores de solução de problemas.

Dois canais separados, dois mecanismos diferentes

O CAPWAP é executado em dois canais UDP e cada um tem seu próprio mecanismo de vida

Canal	Porta padrão (UDP)	Mecanismo de vida
Controle	5246	Solicitação de Eco/Resposta de Eco
Dados	5247	Keep-Alive de canal de dados

Manutenção de atividade do controle CAPWAP (eco / pulsação)

Propósito

O keepalive de controle CAPWAP é usado para confirmar se o access point ainda está acessível no canal de controle.

Seu propósito é muito simples: ele verifica se a conexão de controle entre o AP e a controladora ainda está ativa e responsiva. Ele não é usado para transportar atualizações de configuração ou dados do cliente. Em vez disso, ele serve como um mecanismo de vida para o caminho de controle CAPWAP sobre a porta UDP 5246.

Quem envia o Keepalive

O access point é o dispositivo que inicia ativamente a manutenção de atividade do controle.

Quando necessário, o AP envia uma solicitação de eco CAPWAP para a controladora. O controlador responde com uma Resposta de Eco correspondente. Essa resposta confirma que o controlador recebeu a solicitação e que o canal de controle está funcionando em ambas as direções.

A resposta corresponde à solicitação, o que permite que o AP confirme que está recebendo uma resposta válida para a manutenção de atividade enviada.

Esse comportamento é importante porque mostra que a manutenção de atividade do controle não é principalmente um mecanismo de pesquisa orientado por controlador. Em vez disso, o AP é responsável por verificar a alcançabilidade do canal de controle e a controladora responde de acordo.

O Intervalo de Eco Baseia-se na Inatividade, Não em uma Programação Fixa

Este é um dos aspectos mais comumente mal compreendidos da manutenção de atividade de controle do CAPWAP.

Uma suposição comum é que o AP envia uma Solicitação de Eco a cada 30 segundos como uma pulsação periódica fixa. Na prática, não é assim que funciona.

A manutenção de atividade do controle é baseada na inatividade do canal de controle. Isso significa que o AP envia uma Solicitação de Eco autônoma somente quando o canal de controle estiver ocioso durante o intervalo configurado. Se outro tráfego de controle já estiver sendo trocado entre o AP e o controlador, não há necessidade de enviar um pacote de eco separado.

Qualquer comunicação de controle válida entre o AP e o controlador prova efetivamente que o canal de controle está ativo. Por causa disso, o tráfego de controle CAPWAP normal reinicia o temporizador keepalive.

Exemplos desse tráfego de controle podem incluir:

- trocas de configuração
- atualizações de gerenciamento de recursos de rádio
- Mensagens de controle relacionadas à WLAN
- eventos de controle relacionados ao cliente
- mensagens de sincronização de estatísticas ou de estado
- outros pacotes de controle CAPWAP trocados como parte da operação normal

Como resultado, as Solicitações de Eco autônomas são vistas apenas durante os períodos em que o canal de controle é silencioso.

Exemplo simples

Você pode verificar os temporizadores de eco CAPWAP no AP usando o 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

Cronômetros

O mecanismo de keepalive do controle se baseia em dois valores de temporização importantes.

Item	Valor padrão	Descrição
Intervalo de eco	30 segundos	A quantidade de inatividade do canal de controle antes que o AP envie uma Solicitação de Eco autônoma
Temporizador de inatividade de controle do controlador	90 segundos	O tempo máximo que o controlador permite sem receber tráfego de controle válido antes de declarar a sessão de controle inativa

O que acontece quando a manutenção de atividade do controle falha

Se o canal de controle ficar silencioso por mais tempo do que o tempo limite permitido, o controlador finalmente declara a sessão de controle como perdida.

Nesse ponto, o controlador trata o AP como não mais alcançável no canal de controle e começa a sessão de encerramento. Isso normalmente inclui o fechamento da conexão de controle e a remoção do estado da sessão de controle ativa do AP.

O AP pode então tentar restabelecer a conectividade redescobrimdo e unindo novamente o controlador, dependendo do cenário de falha.

Troubleshooting de Implicações

Entender esse comportamento do keepalive é essencial durante a solução de problemas.

Pacotes de eco ausentes nem sempre significam um problema

Se uma captura de pacote não mostrar solicitações de eco a cada 30 segundos, isso não indicará automaticamente uma falha. Isso pode simplesmente significar que outro tráfego de controle CAPWAP suficiente está fluindo, de modo que nenhum eco autônomo é necessário.

O Espaçamento Irregular De Eco É Normalmente Normal

Os ecos frequentemente aparecem em intervalos não uniformes porque são acionados pela inatividade. Este é um comportamento esperado.

Foco na atividade geral do canal de controle

Ao Troubleshoot desconexões de AP, é mais útil perguntar:

- A controladora ainda está recebendo algum tráfego de controle CAPWAP do AP?
- O canal de controle está silencioso por tempo suficiente para acionar o temporizador de Dead?
- Há problemas de rede que afetam somente o caminho de controle?
- A perda de pacotes, o comportamento do firewall, os problemas de NAT ou as quedas do plano de controle estão interrompendo o tráfego UDP 5246?

O problema real não é a ausência de pacotes de eco periódicos sozinhos. O problema real é a perda de comunicação do canal de controle por tempo suficiente que o controlador declara o AP inalcançável.

Manutenção de atividade de dados CAPWAP

Propósito

O eco de controle CAPWAP confirma que o canal de controle está funcionando, mas não prova que o canal de dados também está íntegro. Como o caminho de controle e o caminho de dados podem falhar independentemente, o CAPWAP usa uma manutenção de atividade de dados separada na porta UDP 5247.

A finalidade da manutenção de atividade de dados é:

- verifique se o AP ainda pode alcançar o controlador no canal de dados
- manter o estado do túnel de dados do AP
- ajudam a detectar falhas que afetam somente o caminho de dados

Quem envia e como o controlador responde

O AP envia a manutenção de atividade de dados, e o controlador responde com uma Resposta de manutenção de atividade de dados.

A resposta pode ser criptografada ou não, dependendo se a criptografia do canal de dados estiver habilitada.

Se o keepalive for válido, o controlador o usará para confirmar se o caminho de dados do AP ainda está acessível. Se o pacote não puder ser correspondido a uma sessão de AP válida, ou se a resposta não puder ser enviada, a manutenção de atividade será descartada e o caminho de dados poderá ser eventualmente considerado com falha.

Como o controlador o valida

Antes de aceitar o keepalive, o controlador executa a validação básica para garantir que o pacote pertença ao AP correto.

O controlador verifica se:

- o keepalive contém informações de CAPWAP válidas
- o endereço MAC do rádio do AP está presente
- o pacote pode corresponder a uma sessão de AP

Primeiro, o controlador tenta identificar a sessão usando o endereço IP de origem e a porta UDP de origem. Se isso falhar, pode recorrer ao uso do endereço MAC do rádio do AP.

Isso é importante para APs atrás de NAT ou PAT, onde o canal de dados pode chegar de uma porta UDP traduzida diferente do canal de controle. Nesses casos, o controlador pode aprender e atualizar a tupla de canais de dados real do AP.

Se o pacote parecer pertencer a um AP diferente da sessão já associada a essa combinação de porta-IP, a manutenção de atividade será rejeitada para evitar mapeamento de sessão incorreto.

O que acontece após a validação

Uma vez que o keepalive é aceito, o controlador o processa com base no estado de sessão atual do AP.

- Se a sessão de dados já estiver estabelecida, o keepalive simplesmente atualiza a atividade.
- Se esta for a primeira manutenção de atividade de dados válida, a controladora pode usá-la para aprender ou atualizar as informações do canal de dados do AP e concluir o estabelecimento do túnel de dados.

Esse primeiro keepalive é especialmente importante porque ajuda o controlador a programar corretamente o túnel de dados, incluindo os casos em que o AP está atrás do NAT ou do PAT.

Depois que a sessão de dados estiver totalmente estabelecida, os keepalives futuros seguem o caminho normal de estado estacionário e são usados apenas para manter a atividade.

Comportamento importante

Um keepalive de dados válido faz mais do que confirmar a integridade do caminho de dados. Ele também atualiza a atividade geral da sessão do AP no controlador.

Isso significa que, no controlador, a vida do canal de dados contribui para a integridade geral da sessão do AP. Como resultado, os mecanismos de controle e vida útil dos dados são relacionados, mesmo que sirvam a propósitos diferentes.

Temporizadores de manutenção de atividade de dados do lado AP

O AP controla o intervalo de keepalive dos dados e decide quando o túnel de dados deve ser considerado inativo.

Item	Valor padrão
Intervalo de keepalive de dados	30 segundos
Backoff de retransmissão	3s, 6s, 12s, depois 15s
Intervalo de inatividade de dados	180 segundos

Sob condições normais, o AP envia um keepalive de dados a cada 30 segundos.

Se o AP não receber uma resposta, ele tentará novamente usando um padrão de backoff. Se a falha continuar por 180 segundos, o AP declara o túnel de dados inativo.

Retransmissões CAPWAP

Princípio do núcleo: A confiabilidade funciona em ambas as direções

O sistema de mensagens de controle CAPWAP usa um modelo de solicitação e resposta, mesmo que seja executado em UDP. Para fornecer confiabilidade, o dispositivo que envia uma solicitação também é responsável por retransmiti-la até que a resposta esperada seja recebida.

Isso significa que as retransmissões são simétricas:

- Para solicitações de controlador para AP, como uma atualização de configuração, o controlador lida com a retransmissão.
- Para solicitações AP para controlador, como Discovery, Join, Configuration Status, mensagens relacionadas à imagem e Echo Requests, o AP manipula a retransmissão.

Este é um importante ponto de solução de problemas. Se você vir retransmissões de AP para controlador em uma captura de pacotes, isso geralmente significa que o AP está simplesmente tentando novamente sua própria solicitação porque não recebeu a resposta esperada. Isso é normal durante a junção e também pode ocorrer durante a atividade de eco de controle.

Comportamento de retransmissão no lado do controlador

No controlador, a retransmissão é tratada por uma máquina de estado de confiabilidade de transmissão dedicada.

Em termos simples, o controlador:

1. aceita uma solicitação que requer confirmação
2. coloca-o em uma fila de transmissão por AP
3. envia a solicitação
4. aguarda a resposta correspondente
5. remove-o da fila quando a resposta chega ou retransmite-o quando o temporizador expira

Essa lógica é rastreada separadamente para cada sessão AP. O controlador também mantém uma janela de transmissão e uma contagem de mensagens de solicitação pendentes.

Como a controladora decide se retransmite

Cada vez que o temporizador de retransmissão expira, a controladora revisa as entradas de requisição na fila e toma uma destas decisões:

1. Resposta já recebida fora de ordem

Se a resposta para essa solicitação já tiver sido recebida, mesmo que ela tenha chegado fora de sequência, a controladora não retransmitirá a mensagem novamente.

2. Limite de repetição excedido

Se a solicitação já foi retransmitida mais do que o número permitido de vezes, a controladora trata isso como uma falha e aborta o processo de transmissão para essa sessão AP.

Nesse ponto, a sessão do AP é encerrada.

3. A solicitação ainda não é antiga o suficiente

O controlador não retransmite imediatamente todas as mensagens em fila em todos os eventos do temporizador. Uma solicitação deve permanecer na fila durante pelo menos o intervalo de retransmissão antes de ser qualificada para ser enviada novamente.

Por padrão, esse intervalo de retransmissão é de 3 segundos.

4. Retransmitir a solicitação

Se a solicitação ainda estiver pendente, tiver envelhecido o suficiente e não tiver excedido o limite de repetição, o controlador a reenviará no canal de controle CAPWAP e incrementará o contador de repetição.

Caso especial: APs conectados em cascata

Para implantações de malha usando um caminho de AP daisy-chain com fio, o controlador permite um orçamento maior para novas tentativas.

Nesse caso, o limite normal de novas tentativas é efetivamente triplicado.

Com a contagem de repetições padrão de 5, isso significa que o controlador pode tentar

novamente até 15 vezes antes de declarar a falha.

Essa exceção existe porque essas topologias podem exigir mais tolerância para atraso ou perda de mensagem.

Comportamento de retransmissão do lado do AP

O AP também retransmite suas próprias solicitações CAPWAP, mas usa um padrão diferente do controlador.

Enquanto o controlador usa um intervalo de retransmissão fixo, o AP usa backoff exponencial. Isso significa que o tempo de espera aumenta após cada tentativa com falha.

Com as configurações padrão, o tempo de repetição do AP é aproximadamente:

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

Esse comportamento se aplica a solicitações CAPWAP originadas pelo AP, como:

- Descoberta
- União
- trocas relacionadas à configuração
- transações de controle criptografadas
- Solicitações de Eco

Esses parâmetros de nova tentativa são aprendidos do controlador como parte da configuração de junção do AP.

Impressão digital de diagnóstico em capturas de pacotes

O próprio padrão de retransmissão é frequentemente uma pista útil durante a solução de problemas.

Padrão de retransmissão	Origem provável
Retransmissões uniformemente espaçadas, aproximadamente a cada 3 segundos	Retransmissão no lado do controlador
Retransmissões que se espalham com o tempo, como 6s, 12s, 24s, 48s, 96s	Retransmissão do lado do AP com backoff exponencial

Essa é uma maneira prática de determinar qual lado está tentando novamente, especialmente durante falhas de ingresso ou problemas relacionados ao eco.

O que acontece quando as tentativas se esgotam

Se as retransmissões continuarem sem receber a resposta esperada, ambos os lados eventualmente desistem, mas suas ações de recuperação são diferentes.

Lado do controlador

Se o controlador esgotar seu orçamento de repetição, ele abortará o processo de transmissão e encerrará a sessão AP. Isso faz com que as sessões de controle e dados do CAPWAP sejam fechadas.

lado AP

Se o AP esgotar suas próprias tentativas de repetição, ele abandona esse controlador e começa novamente desde o início, normalmente retornando à fase de Descoberta e tentando uma junção completa.

Botões e padrões de configuração

O comportamento de retransmissão é controlado por duas configurações principais no perfil de junção AP.

Comando	Valor padrão	Função
contagem de retransmissão de capwap	5	Número máximo de tentativas de retransmissão

Comando	Valor padrão	Função
capwap retransmit interval	3 segundos	Intervalo de retransmissão base

Esses valores influenciam a confiabilidade da junção e outras tentativas de controle CAPWAP originadas pelo AP, incluindo novas tentativas relacionadas ao eco.

Referência do Temporizador Consolidado

Esta tabela resume os principais temporizadores CAPWAP discutidos neste artigo.

Cronômetro	Valor padrão	Plano	PROPRIETÁRIO	Descrição
Controlar intervalo de eco	30 segundos	Controle	AP	Se o AP não transmitir o tráfego de controle CAPWAP por 30 segundos, ele enviará uma Echo Request.
Controlar timer de pulsação morto	90 segundos	Controle	Controlador	O controlador espera um tráfego de controle válido nesta janela. Se nada for recebido, a sessão de controle será considerada inativa.
Controlar intervalo de retransmissão	3 segundos	Controle	Controlador	A controladora retransmite suas próprias solicitações de CAPWAP não respondidas em um intervalo fixo.
Contagem de retransmissão de controle	5 tentativas	Controle	Controlador	Contagem máxima de novas tentativas para solicitações CAPWAP originadas pelo controlador. Em cenários de interconexão em cascata com fio, isso pode aumentar para 15 tentativas.
AP control retransmit backoff (Controle AP	6, 12, 24, 48, 96	Controle	AP	O AP retransmite suas próprias solicitações CAPWAP usando

Cronômetro	Valor padrão	Plano	PROPRIETÁRIO	Descrição
retransmite backoff)	segundos			backoff exponencial.
Intervalo de keepalive de dados	30 segundos	Dados	AP	Sob condições normais, o AP envia um keepalive de dados a cada 30 segundos.
Retorno de nova tentativa de manutenção de atividade de dados	3, 6, 12, 15, 15 segundos	Dados	AP	Se uma resposta de manutenção de atividade de dados for perdida, o AP tentará novamente usando backoff, limitado a 15 segundos.
Intervalo inativo do canal de dados	180 segundos	Dados	AP	Se o AP não mantiver com êxito o intercâmbio de keepalive de dados dentro desse período, ele declara o túnel de dados inoperante.

Diferenças lado a lado

Keepalive vs. Retransmissão

Embora às vezes estejam confusos, keepalive e retransmission servem a propósitos diferentes.

Aspecto	Manutenção de atividade	Retransmissão
Principal objetivo	Verifica se o peer ainda está acessível	Repete uma solicitação específica quando nenhuma resposta é recebida
Escopo	Por sessão ou por canal	Por mensagem
Gatilho	Inatividade ou tempo limite de atividade	Uma solicitação permanece sem resposta
Método de rastreamento	Baseado em tempo	Baseado em contagem de repetição

Aspecto	Manutenção de atividade	Retransmissão
Significado da falha	O canal ou a sessão não pode mais ser alcançado	Uma troca CAPWAP específica falhou repetidamente
Resultado da falha	A sessão pode ser declarada inativa	O controlador pode encerrar a sessão ou o AP pode reiniciar a junção

Cadeias de Caracteres do Log de Rastreamento RA por Mecanismo

Para rastreamento específico de AP, colete logs para o AP e procure essas strings exatas.

Coleção de logs

Uso:

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

Controlar keepalive/heartbeat

Procurar:

- Lidando com solicitações de eco
- Criar resposta de eco
- Resposta de eco enviada para solicitação com o número de sequência <N>.
- Temporizador de Pulsação reiniciado com novo valor <ms>
- Toque do timer de pulsação invocado
- Expiração do temporizador de pulsação

Manutenção de atividade de dados

Procurar:

- Data keepalive recebido
- sessão de dados já estabelecida
- O DTLS de dados não está estabelecido

- Atualizando entrada de túnel de dados CAPWAP
- Falha ao processar a manutenção de atividade de dados. Razão: A sessão CAPWAP não está em execução ou no estado de configuração
- Mensagem de keepalive inválida, sem bloqueio capwap
- Mensagem de keepalive inválida, sem WTP MAC
- Falha ao processar keepalive, sessão CAPWAP não encontrada
- A manutenção de atividade de dados é recebida em uma porta diferente da porta de controle: <porta>
- A manutenção de atividade de dados é recebida para AP <mac> diferente
- Falha ao atualizar informações da tupla de dados na tabela de sessão WTP para o host remoto: <ip>
- Falha ao atualizar entrada de túnel de dados CAPWAP

Manuseio de keepalive do plano de dados

Procurar:

- Dados recebidos mantidos ativos de <src> para <dst>
- Resposta de manutenção de atividade de dados <enc/plain> enviada
- Descartando pacote de manutenção de atividade do IP: <ip>, sessão desconhecida
- Descartando pacote de manutenção de atividade do IP: <ip>, falha ao obter o status DTLS dos dados
- Falha ao enviar resposta de keep-alive de dados
- Falha na mensagem de keep-alive de dados de balanceamento de carga

Retransmissão

Procurar:

- retransmit timer callback
- Retransmitindo o número de sequência <N>, pois ele está na fila e ainda precisa ser retransmitido
- Mensagem de retransmissão: Tentativa de retransmissão de <msg-name>: <M>
- entrada com número seq: <N> está na fila por <S> segundos. Não está retransmitindo
- Término da sessão CAPWAP, máximo de retransmissões expiradas para: <mensagem> ...
- Limpeza de recursos da sessão CAPWAP em licença AP.

Desmontagem da sessão

Procurar:

- Encerrando a sessão AP CAPWAP.

- Feche a sessão CAPWAP DTLS.
- fechamento de sessão de controle capwap-dtls
- fechamento de sessão de dados capwap-dtls
- Último Pacote de Controle recebido há <S> segundos.
- Último Pacote Keep Alive de Dados recebido há <S> segundos.
- Sessão CAPWAP DTLS fechada para AP, causa: <motivo>

Examples:

Cenário de trabalho

Verificação de depuração AP

Esse comando de depuração de AP pode ser usado para monitorar o controle CAPWAP e a comunicação de manutenção de atividade de dados entre o AP e a WLC.

```
#debug capwap client event
```

Esses logs de depuração demonstram uma sequência de comunicação CAPWAP bem-sucedida.

Às 13:11:44, o AP transmitiu uma solicitação de eco CAPWAP à WLC pela porta UDP 5246. Durante o mesmo intervalo, o AP também transmitiu um pacote CAPWAP Data Keepalive pela porta UDP 5247. Os registros confirmam que a WLC respondeu com êxito às duas solicitações.

Os timestamps indicam um ciclo de comunicação CAPWAP normal:

- 13:11:44.0917 - Solicitação de Eco transmitida.
- 13:11:44.0918 - Data Keepalive transmitido.
- 13:11:44.0926 - Data Keepalive recebido do WLC.
- 13:11:44.0940 - Resposta de Eco recebida do WLC.

Esses carimbos de data e hora confirmam que o controle CAPWAP e os canais de dados estão funcionando conforme esperado com latência de ida e volta 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
```

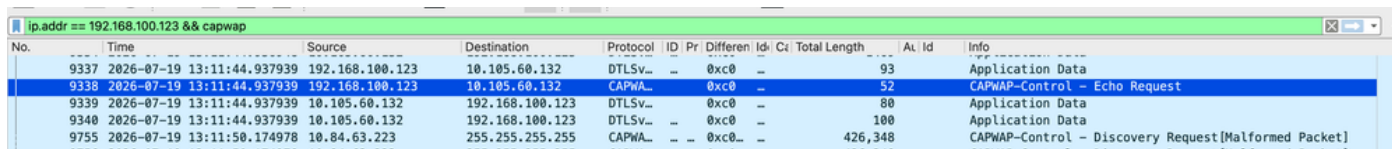
```
[*07/19/2026 13:11:44.0918] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 13:11:44.0926] chatter: [RX]KEEPALIVE: Count 164
[*07/19/2026 13:11:44.0927] Sending KEEPALIVE to WTP SM
[*07/19/2026 13:11:44.0927] Capwap data keep-alive Msg.
[*07/19/2026 13:11:44.0927] [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: 10.105.60.132
```

Validação de Pacote de Controle CAPWAP (Porta UDP 5246)

Análise de captura de pacotes

A captura do pacote confirma que o AP gerou uma solicitação de eco CAPWAP em 13:11:44 sobre a porta UDP 5246.

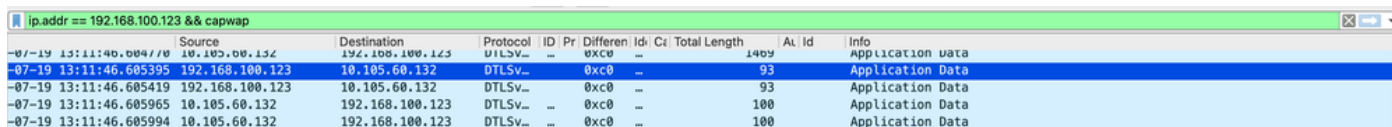
A WLC recebeu com êxito o pacote, processou a solicitação e gerou imediatamente a Resposta de Eco correspondente. Como o canal de controle CAPWAP é protegido usando a criptografia DTLS, a resposta aparece como dados de aplicativo criptografados na captura de pacotes.



No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	Al	Id	Info
9337	2026-07-19 13:11:44.937939	192.168.100.123	10.105.60.132	DTLSv...	...	0xc0	...	93					Application Data
9338	2026-07-19 13:11:44.937939	192.168.100.123	10.105.60.132	CAPWA...	...	0xc0	...	52					CAPWAP-Control - Echo Request
9339	2026-07-19 13:11:44.937939	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	80					Application Data
9340	2026-07-19 13:11:44.937939	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	100					Application Data
9755	2026-07-19 13:11:50.174978	10.84.63.223	255.255.255.255	CAPWA...	...	0xc0	...	426,348					CAPWAP-Control - Discovery Request [Malformed Packet]

Verificação de Pacote de Switch

A captura do pacote do switch confirma que os pacotes de controle CAPWAP criptografados foram recebidos com êxito da WLC e encaminhados para o AP.



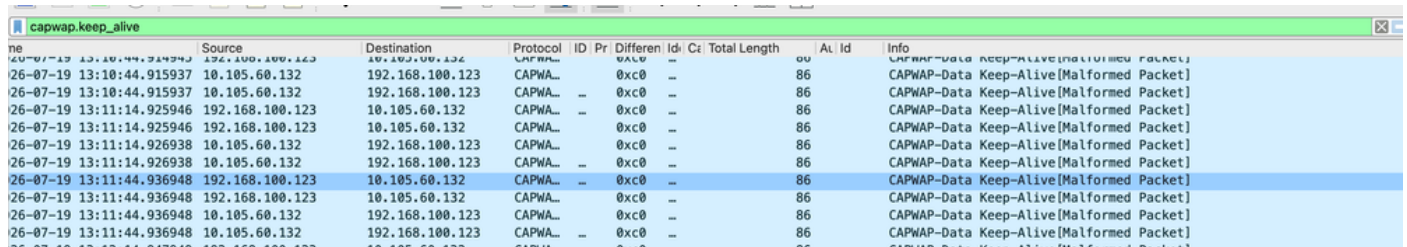
No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	Al	Id	Info
~07-19 13:11:46.605419	192.168.100.123	10.105.60.132	DTLSv...	...	0xc0	...	1409						Application Data
~07-19 13:11:46.605419	192.168.100.123	10.105.60.132	DTLSv...	...	0xc0	...	93						Application Data
~07-19 13:11:46.605965	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	100						Application Data
~07-19 13:11:46.605994	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	100						Application Data

Validação da manutenção de atividade de dados CAPWAP (porta UDP 5247)

O AP transmite periodicamente pacotes CAPWAP Data Keepalive pela porta UDP 5247 para verificar a integridade do túnel de dados CAPWAP.

Às 13:11:44, o AP transmitiu um pacote de Data Keepalive para a WLC. A WLC recebeu com êxito o pacote e respondeu imediatamente com a resposta de keepalive correspondente.

Essa troca bem-sucedida confirma que o caminho de dados CAPWAP permanece operacional e que a comunicação bidirecional entre o AP e a WLC está funcionando normalmente



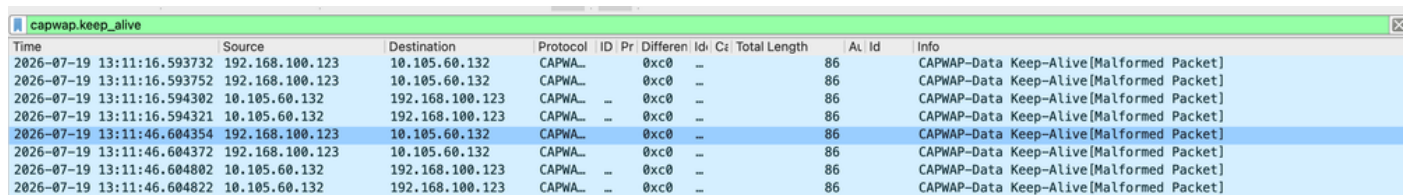
Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	Al	Id	Info
26-07-19 13:10:44.915937	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:10:44.915937	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:44.936948	192.168.100.123	10.105.60.132	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:44.936948	192.168.100.123	10.105.60.132	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]
26-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA...	0xc0	--	--	--	--	86	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]

Verificação de Pacote de Switch

A captura de pacotes do switch valida ainda mais se os pacotes CAPWAP Data Keepalive foram encaminhados com êxito entre o AP e a WLC sem interrupção.

O fluxo de pacotes observado confirma que:

- Os pacotes Data Keepalive chegaram com êxito à WLC.
- A WLC gerou a resposta de keepalive esperada.
- O switch encaminhou a resposta de volta ao AP.
- Nenhuma perda de pacote ocorreu no caminho de encaminhamento.



Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	Al	Id	Info
2026-07-19 13:11:16.593732	192.168.100.123	10.105.60.132	CAPWA...	0xc0	--	--	--	--	86	86	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	86	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	86	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	86	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	86	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	86	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	86	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	86	86	CAPWAP-Data Keep-Alive[Malformed Packet]

Pacotes de controle (UDP 5246) sendo descartados no Switch de uplink AP

Este teste demonstra o comportamento de um AP quando a CAPWAP Control Port (UDP 5246) está sendo descartada no switch de uplink do AP.

O objetivo é validar o AP, a WLC e o comportamento da rede quando os pacotes de controle CAPWAP são impedidos de alcançar o AP, apesar da WLC ter processado e respondido com êxito às solicitações.

Neste cenário:

- O AP continua transmitindo as solicitações de eco CAPWAP para a WLC.
- A WLC recebe e processa com êxito cada Solicitação de Eco.
- A WLC gera a resposta de eco correspondente.
- O switch de uplink do AP recebe a resposta, mas não a encaminha de volta ao AP.
- Como o AP nunca recebe a Resposta de Eco, ele excede a contagem máxima de retransmissão e reinicia a máquina de estado CAPWAP.

Análise de depuração AP

Às 12:11:55.4568, o AP transmitiu uma solicitação de eco CAPWAP para o WLC pela porta UDP 5246.

Solicitação de Eco: Enviar contagem 0

Diferentemente do cenário de trabalho normal, nenhuma Resposta de Eco foi recebida. Como resultado, o AP iniciou retransmissões de acordo com o temporizador CAPWAP padrão.

As retransmissões ocorreram nestes carimbos de data/hora:

Tempo	Evento
12:12:00.2587	Contagem de Retransmissão = 1
12:12:03.2599	Contagem de Retransmissão = 2
12:12:06.2610	Contagem de Retransmissão = 3
12:12:09.2624	Contagem de Retransmissão = 4
12:12:12.2637	Contagem de Retransmissão = 5

Após a quinta retransmissão malsucedida, o AP declarou a sessão de controle CAPWAP inalcançável.

Às 12:12:15.2647, o AP informou:

Contagem máxima de retransmissão excedida, retornando ao modo DISCOVER.

Imediatamente depois, o AP reiniciou a máquina de estado CAPWAP para iniciar um novo processo de descoberta.

```
[*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
```

Os rastreamentos RA da WLC confirmam que a controladora não teve nenhum problema de processamento.

Às 12:11:58.731835712, a WLC recebeu com êxito a Solicitação de Eco CAPWAP transmitida pelo AP. Esses logs demonstram que a WLC processou a solicitação com êxito e gerou a resposta apropriada. Posteriormente, às 12:12:19.802183814, a WLC recebeu uma Notificação de Fechamento DTLS do AP. O AP foi desconectado porque nunca recebeu as Respostas de Eco transmitidas pelo controlador. Consequentemente, a WLC encerrou a sessão DTLS e registrou a desassociação do 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

Monitoring > Wireless > AP Statistics

General Join Statistics AFC Statistics URWB

Clear

ClearAll



Total APs : 4

	AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
☐	AP6849.9259.08D0	CW9164I-ROW	⬇	10.105.60.227	10a8.29cf.e540	6849.9259.08d0	No reboot reason	Heart beat timer expiry
☐	Training-AP	C9105AXI-D	⬇	10.105.60.91	6cd6.e32d.f640	6cd6.e336.e138	No reboot reason	AP Auth Failure
☐	AP12	C9130AXI-D	⬇	192.168.100.86	889c.ad26.ea00	e44e.2d2c.3d0c	No reboot reason	Heart beat timer expiry
☐	AP8C88.814F.04E0	CW9178I	⬇	192.168.100.87	ecf4.0cc7.1600	8c88.814f.04e0	No reboot reason	Max Retransmission to AP

1 - 4 of 4 Join Statistics

O WLC EPC confirma que:

- Ao mesmo carimbo de data/hora, a solicitação de eco CAPWAP atingiu com êxito a WLC.
- A WLC gerou uma Resposta de Eco CAPWAP criptografada.
- A resposta aparece como Application Data, já que o tráfego de controle CAPWAP é protegido pela criptografia DTLS.

O EPC confirma, portanto, que a controladora transmitiu a resposta com êxito. Isso elimina a WLC como a origem do problema.

48740	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	DTLSv...	--	0xc0	--	93	Application Data
48741	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	CAPWA...	--	0xc0	--	52	CAPWAP-Control - Echo Request
48742	2026-07-17 12:11:58.731956	10.105.60.132	192.168.100.120	DTLSv...	--	0xc0	--	80	Application Data
48743	2026-07-17 12:11:58.731956	10.105.60.132	192.168.100.120	DTLSv...	--	0xc0	--	100	Application Data

_ws.col.info == "CAPWAP-Control - Echo Request"										
Packet details Regular Expression echo										
Options: Narrow & Wide Case sensitive Backwards Multiple occurrences										
No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cz	Total Length
11212	2026-07-17 12:00:47.679957	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
22007	2026-07-17 12:02:55.731956	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
48741	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
49001	2026-07-17 12:12:01.732948	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
49292	2026-07-17 12:12:04.733955	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
49485	2026-07-17 12:12:07.734947	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
49695	2026-07-17 12:12:10.735954	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request
49972	2026-07-17 12:12:13.736961	192.168.100.120	10.105.60.132	CAPWA...	0xc0	--	--	52		CAPWAP-Control - Echo Request

As capturas de pacotes coletadas no switch de uplink do AP fornecem a evidência final.

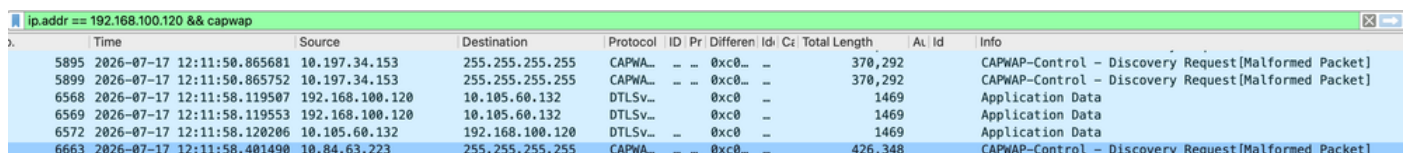
As capturas demonstram que:

- O switch recebeu com êxito a Resposta de Eco criptografada transmitida pela WLC.
- A resposta é visível como Application Data, o que é esperado devido à criptografia DTLS.
- A resposta não foi encaminhada para o AP.

Isso explica por que:

- O AP nunca recebeu a Resposta de Eco CAPWAP.
- O AP continuou a retransmitir Solicitações de Eco.
- O contador de retransmissão excedeu o limite configurado.
- O AP reiniciou a máquina de estado CAPWAP.

As capturas de pacote identificam claramente o switch como o ponto onde o tráfego de controle CAPWAP foi interrompido



No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ct	Total Length	At	Id	Info
5895	2026-07-17 12:11:50.865681	10.197.34.153	255.255.255.255	CAPWA	--	--	0xc0...	--	--	370,292			CAPWAP-Control - Discovery Request [Malformed Packet]
5899	2026-07-17 12:11:50.865752	10.197.34.153	255.255.255.255	CAPWA	--	--	0xc0...	--	--	370,292			CAPWAP-Control - Discovery Request [Malformed Packet]
6568	2026-07-17 12:11:58.119507	192.168.100.120	10.105.60.132	DTLSv	--	--	0xc0...	--	--	1469			Application Data
6569	2026-07-17 12:11:58.119553	192.168.100.120	10.105.60.132	DTLSv	--	--	0xc0...	--	--	1469			Application Data
6572	2026-07-17 12:11:58.120206	10.105.60.132	192.168.100.120	DTLSv	--	--	0xc0...	--	--	1469			Application Data
6663	2026-07-17 12:11:58.401490	10.84.63.223	255.255.255.255	CAPWA	--	--	0xc0...	--	--	426,348			CAPWAP-Control - Discovery Request [Malformed Packet]

Porta de dados CAPWAP (UDP 5247) sendo descartada no switch de uplink AP

Este teste valida o comportamento do AP quando a porta de dados CAPWAP (UDP 5247) é descartada no switch de uplink do AP enquanto a porta de controle CAPWAP (UDP 5246) permanece operacional.

Ao contrário do cenário anterior, o AP continua a manter a conexão de controle CAPWAP com a WLC trocando com êxito mensagens de eco CAPWAP pela porta UDP 5246. No entanto, como os pacotes CAPWAP Data Keepalive não podem concluir a viagem de ida e volta, o AP finalmente declara o caminho de dados CAPWAP como inalcançável e inicia uma reinicialização CAPWAP.

Os logs de depuração do AP confirmam que o canal de controle CAPWAP permaneceu operacional durante o teste.

No início da captura, as solicitações de eco CAPWAP transmitidas pela porta UDP 5246 continuaram a receber respostas de eco válidas da WLC, confirmando a comunicação ininterrupta do plano de controle.

No entanto, às 14:30:15, o AP transmitiu um pacote CAPWAP Data Keepalive sobre a porta UDP

5247. Como nenhuma resposta de Data Keepalive correspondente foi recebida, o AP iniciou o mecanismo de repetição. As retransmissões podem ser observadas nestes carimbos de data/hora:

Carimbo de data/hora	Evento
14:30:15	Data Keepalive inicial transmitido
14:30:19	Repetir 1
14:30:25	Repetir 2
14:30:37	Repetir 3
14:30:49	Repetir 4
14:31:01	Repetir 5
14:31:13	Nova tentativa final

Embora as Respostas de Eco CAPWAP continuassem a ser recebidas durante esse período, o AP não recebeu nenhuma resposta para os pacotes de Data Keepalive. Após esgotar as tentativas de repetição, o AP relatou um Timeout de Data Keepalive Não Criptografado e iniciou uma reinicialização CAPWAP. Aproximadamente às 14:31:16, o AP encerrou a sessão CAPWAP existente e retornou ao processo de descoberta.

```
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: 10.105.60.132
[*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: 10.105.60.132
[*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: 10.105.60.132
[*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: 10.105.60.132
[*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: 10.105.60.132
[*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: 10.105.60.132
```

```
[*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 o canal de Dados CAPWAP, os rastreamentos indicam que o controlador não recebeu os pacotes de Data Keepalive esperados. Eventualmente, após o AP declarar a falha de Data Keepalive, o WLC registrou o término da sessão DTLS e o evento de desconexão do AP. A sequência observada nos rastreamentos RA confirma que o controlador permaneceu operacional até que o AP se desconecte voluntariamente devido ao timeout de Data Keepalive.

Rastreamentos de RA com 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.ad26
```

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)

Rastreamentos RA com MAC de rádio :

<#root>

```
2026/07/19 14:31:16.737070835 {wncd_x_R0-2}{2}: [capwapac-smgr-sess] [16638]: (debug): Mac: 889c.ad26.ea00
2026/07/19 14:31:16.737072831 {wncd_x_R0-2}{2}: [capwapac-smgr-srvr] [16638]: (debug): Mac: 889c.ad26.ea00
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.ea00
```

O EPC coletado no WLC valida o processamento de pacotes no lado do controlador. As capturas confirmam que os pacotes CAPWAP Control continuaram a ser trocados com êxito durante o

teste, mas não havia nenhum pacote de manutenção de atividade de dados recebido no WLC. Essa observação alinha-se com os logs de depuração do AP e demonstra que o mecanismo Data Keepalive falhou, apesar do canal de controle permanecer ativo.

Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ci	Total Length	Al	Id	Info
11827	2026-07-19 14:30:13.475973	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
11828	2026-07-19 14:30:13.476965	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	117			Application Data
11829	2026-07-19 14:30:13.476965	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	76			CAPWAP-Control - WTP Event Request
11830	2026-07-19 14:30:13.476965	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	65			Application Data
11831	2026-07-19 14:30:13.476965	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
11928	2026-07-19 14:30:16.714959	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	1469			Application Data
11929	2026-07-19 14:30:16.714959	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	1428			CAPWAP-Control - WTP Event Request [Malformed Packet]
11930	2026-07-19 14:30:16.715951	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	1449			Application Data
11931	2026-07-19 14:30:16.715951	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	1469			Application Data
11990	2026-07-19 14:30:18.024992	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	437			Application Data
11991	2026-07-19 14:30:18.024992	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	396			CAPWAP-Control - WTP Event Request
11992	2026-07-19 14:30:18.025984	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	65			Application Data
11993	2026-07-19 14:30:18.025984	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	85			Application Data
11994	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	437			Application Data
11995	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	396			CAPWAP-Control - WTP Event Request
11996	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	65			Application Data
11997	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	85			Application Data
12034	2026-07-19 14:30:18.236987	10.132.179.233	255.255.255.255	CAPWA..	--	0xc0	--	--	378,300			CAPWAP-Control - Discovery Request [Malformed Packet]
12036	2026-07-19 14:30:18.236987	10.132.179.233	255.255.255.255	CAPWA..	--	0xc0	--	--	378,300			CAPWAP-Control - Discovery Request [Malformed Packet]

Switch:

Capturas de pacotes coletadas no switch de uplink do AP mostram que os pacotes estavam presentes no switch, mas os mesmos não foram encaminhados para a wlc

Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ci	Total Length	Al	Id	Info
3303	2026-07-19 14:28:48.332827	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
3304	2026-07-19 14:28:48.332844	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5336	2026-07-19 14:29:18.342564	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5337	2026-07-19 14:29:18.342586	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5340	2026-07-19 14:29:18.343037	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5341	2026-07-19 14:29:18.343092	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8573	2026-07-19 14:29:48.353254	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8574	2026-07-19 14:29:48.353322	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8577	2026-07-19 14:29:48.353998	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8578	2026-07-19 14:29:48.354018	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10376	2026-07-19 14:30:18.363535	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10534	2026-07-19 14:30:21.364195	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10837	2026-07-19 14:30:27.366201	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
11465	2026-07-19 14:30:39.370239	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
12141	2026-07-19 14:30:51.374346	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
12959	2026-07-19 14:31:03.378437	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
13620	2026-07-19 14:31:15.382538	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
15834	2026-07-19 14:31:43.032731	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
16474	2026-07-19 14:31:46.000877	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
16886	2026-07-19 14:31:52.003518	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
17809	2026-07-19 14:32:04.007609	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
18576	2026-07-19 14:32:16.013802	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]

Desabilitação da Manutenção de Atividade de Dados do CAPWAP

Este recurso foi introduzido na ID de bug Cisco [CSCvs66015](#)

Esse recurso é útil na solução de problemas nesses cenários.

1. Solucionar problemas de desconexões de AP: Depois de desabilitar o capwap data keep-alive, podemos ver se o AP ainda está se desconectando devido ao capwap control keep-alive e identificar a causa raiz para as desconexões do AP keep-alive.
2. Evite desconexões devido ao capwap data-keepalive como uma solução alternativa até

identificar o motivo para o capwap data keep-alive drops.

3. APs farejadores em implantações flex de filial conectados através de link WAN com baixo throughput. Se quisermos coletar capturas de pacotes OTA configurando um dos APs para estar no modo sniffer, todos os pacotes capturados serão transmitidos para a WLC através do link WAN usando a porta de dados capwap. Ao fazer isso, sobrecarrega o link de WAN e afeta toda a filial.
4. Se desativar o capwap data keep-alive para AP no modo farejador e criar uma ACL na filial para descartar os pacotes de dados capwap desse AP concreto, o AP permanecerá conectado, pois o controle capwap está bem e, em seguida, você poderá coletar o OTA da switchport do AP sem sobrecarregar o link WAN com capturas de pacotes.

Dispense a manutenção de atividade de dados COS-AP para ativar/desativar a partir da WLC 9800. Por padrão, a manutenção de atividade de dados no WLC e no AP é habilitada.

Comando da WLC:

- 1) Exiba o status com a string "Dados não criptografados Keep Alive"

```
show ap config general
```

- 2) Habilitar/Desabilitar manutenção de atividade de dados com nome de aplicativo

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

Dispense a manutenção de atividade de dados COS-AP para ativar/desativar a partir do próprio AP. Por padrão, a manutenção de atividade de dados no AP é habilitada.

Comando AP:

- 1) Exiba o status com a sequência de caracteres "Dados não criptografados Keep Alive"

```
show capwap client config
```

- 2) Habilitar/Desabilitar a manutenção de atividade de dados no AP

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

Por exemplo:

Verificação de keepalive desabilitada no nível 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
```

Depurações de AP:

Na depuração de AP, podemos ver que não há troca de pacotes de manutenção de atividade de dados acontecendo entre o AP e a wlc, apenas vemos a troca de pacotes de controle.

```
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

```

Embora os pacotes de manutenção de atividade de dados estivessem sendo descartados, mas como desabilitamos a verificação de manutenção de atividade de dados, podemos ver que o AP permanece estável na wlc sem ser afetado pela queda dos pacotes de manutenção de atividade.

Monitoring > Wireless > AP Statistics

General

Join Statistics

AFC Statistics

URWB

Total APs : 1

Misconfigured APs

Tag : 0

Country Code : 0

LSC Falback : 0

URWB : 0

License Non-Compliance ⓘ

Non Compliant APs : 0

Multiple APs can be configured at once from Bulk AP Provisioning feature

AP Name	AP Model	Admin Status	Up Time	WLC Association Uptime	IP Address	AP Radio MAC	Ethernet MAC	Operation Status
AP12	C9130AXI-D		0 days 3 hrs 58 mins 7 secs	0 days 0 hrs 12 mins 25 secs	192.168.100.123	889c.ad26.ea00	e44e.2d2c.3d0c	Registered

1

100

1 - 1 of 1 items

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.