CAPWAP Keepalives op Catalyst 9800 WLC begrijpen en oplossen

Inhoud

Inleiding

Dit document beschrijft CAPWAP-controlebewaarders, gegevensbewaarders en hertransmissies,

context

CAPWAP biedt het communicatiekader tussen Cisco-toegangspunten en de draadloze LAN-controller op Cisco Catalyst 9800-platforms. Het maakt gebruik van afzonderlijke besturings- en gegevenskanalen, samen met gedefinieerde keepalive- en retransmissiemechanismen om de connectiviteit te behouden.

In dit artikel worden de belangrijkste indicatoren voor het oplossen van problemen toegelicht: CAPWAP-controlekeeper-alives, gegevensbewaarder-alives en hertransmissies, inclusief de bijbehorende timers, het faalgedrag en de belangrijkste indicatoren voor probleemoplossing.

Twee verschillende kanalen, twee verschillende mechanismen

CAPWAP loopt over twee UDP-kanalen en elk heeft zijn eigen levendigheidsmechanisme

NOT REQUIRED FOR THIS LANGUAGE	Standaardpoort (UDP)	Levendheidsmechanisme
controle	5246	ECHO-verzoek/ECHO-antwoord
gegevens	5247	Data Channel Keep-Alive

CAPWAP Control Keepalive (Echo / hartslag)

Doel

De CAPWAP-controlekeeper wordt gebruikt om te bevestigen dat het toegangspunt nog steeds bereikbaar is op het controlekanaal.

Het doel is heel eenvoudig: het verifieert dat de besturingsverbinding tussen het toegangspunt en de controller nog steeds springlevend en responsief is. Het wordt niet gebruikt voor het uitvoeren van configuratie-updates of clientgegevens. In plaats daarvan dient het als een levendigheidsmechanisme voor het CAPWAP-besturingspad over UDP-poort 5246.

Wie stuurt de Keepalive

Het toegangspunt is het apparaat dat actief de controle-keeper in leven brengt.

Indien nodig stuurt het toegangspunt een CAPWAP Echo Request naar de controller. De controller antwoordt vervolgens met een bijbehorende echorespons. Dit antwoord bevestigt dat de controller het verzoek heeft ontvangen en dat het controlekanaal in beide richtingen werkt.

Het antwoord komt overeen met het verzoek, waardoor het toegangspunt kan bevestigen dat het een geldig antwoord ontvangt op de keepalive die het heeft verzonden.

Dit gedrag is belangrijk omdat het laat zien dat de control keepalive niet primair een controller-driven polling mechanisme is. In plaats daarvan is de AP verantwoordelijk voor het controleren van de bereikbaarheid van het controlekanaal en reageert de controller dienovereenkomstig.

Het echo-interval is gebaseerd op inactiviteit, niet op een vast schema

Dit is een van de meest verkeerd begrepen aspecten van de CAPWAP-controle-keepalives.

Een veel voorkomende veronderstelling is dat het toegangspunt elke 30 seconden een echoverzoek verzendt, zoals een vaste periodieke hartslag. In de praktijk werkt het niet zo.

De controle keepalive is gebaseerd op controle-kanaal inactiviteit. Dit betekent dat het toegangspunt alleen een stand-alone echoverzoek verzendt wanneer het besturingskanaal gedurende het geconfigureerde interval niet actief is geweest. Als er al ander controleverkeer wordt uitgewisseld tussen het toegangspunt en de controller, is het niet nodig om een afzonderlijk echopakket te verzenden.

Elke geldige controlecommunicatie tussen het toegangspunt en de controller bewijst effectief dat het controlekanaal in leven is. Daarom wordt de keepalive-timer door het normale CAPWAP-besturingsverkeer gereset.

Voorbeelden van dergelijke verkeersleiding kunnen zijn:

- Configuratie-uitwisselingen
- Updates voor beheer van radiobronnen
- WLAN-gerelateerde controleberichten
- Client-gerelateerde besturingsgebeurtenissen
- Statistieken of statussynchronisatieberichten
- andere CAPWAP-controlepakketten die in het kader van de normale werking worden uitgewisseld

Als gevolg hiervan worden standalone Echo-verzoeken alleen gezien tijdens perioden waarin het controlekanaal anders stil is.

eenvoudig voorbeeld

U kunt de CAPWAP-echo-timers op het toegangspunt controleren met de opdracht Capwap-clienttimer tonen.

<#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
```

Timers

Het keepalive-controlemechanisme berust op twee belangrijke timingwaarden.

Item	standaardwaarde	Beschrijving
Echo-interval	30 seconden	De hoeveelheid inactiviteit van het besturingskanaal voordat het toegangspunt een zelfstandig echoverzoek verzendt
Controlemechanisme dode timer	90 seconden	De maximale hoeveelheid tijd die de controller toestaat zonder geldig controleverkeer te ontvangen voordat de controlesessie dood wordt verklaard

Wat gebeurt er als de controle Keepalive faalt

Als het controlekanaal langer stil blijft dan de toegestane time-out, verklaart de controller uiteindelijk dat de controlesessie verloren is gegaan.

Op dat moment behandelt de controller het toegangspunt als niet meer bereikbaar op het controlekanaal en begint de sessie af te breken. Dit omvat meestal het sluiten van de controleverbinding en het verwijderen van de status van de actieve controlesessie van het toegangspunt.

Het toegangspunt kan vervolgens proberen de connectiviteit te herstellen door de controller opnieuw te ontdekken en weer aan te sluiten, afhankelijk van het storingsscenario.

Implicaties voor probleemoplossing

Het begrijpen van dit keepalive-gedrag is essentieel tijdens het oplossen van problemen.

Ontbrekende echopakketten betekenen niet altijd een probleem

Als een pakketopname niet elke 30 seconden Echo-verzoeken weergeeft, duidt dat niet automatisch op een fout. Het kan eenvoudig betekenen dat er voldoende ander CAPWAP-besturingsverkeer stroomt, dus er is geen zelfstandige echo vereist.

Onregelmatige echo-afstand is meestal normaal

Echo's verschijnen vaak met niet-uniforme intervallen omdat ze worden veroorzaakt door inactiviteit. Dit is verwacht gedrag.

Focus op de algehele activiteit van het besturingskanaal

Wanneer de verbinding met het toegangspunt wordt verbroken, is het nuttiger om te vragen:

- Ontvangt de controller nog steeds CAPWAP-controleverkeer van het toegangspunt?
- Is het controlekanaal lang genoeg stil om de dode timer te activeren?
- Zijn er netwerkproblemen die alleen van invloed zijn op het controlepad?
- Onderbreken pakketverlies, firewallgedrag, NAT-problemen of vallen van besturingsvliegtuigen het UDP 5246-verkeer?

Het echte probleem is niet de afwezigheid van periodieke echopakketten op zichzelf. Het echte probleem is het verlies van controle-kanaal communicatie voor lang genoeg dat de controller verklaart de AP onbereikbaar.

CAPWAP Data Keepalive

Doel

De CAPWAP controle echo bevestigt dat het controlekanaal werkt, maar het bewijst niet dat het gegevenskanaal ook gezond is. Aangezien het regelpad en het gegevenspad onafhankelijk kunnen falen, gebruikt CAPWAP een afzonderlijke gegevensherstel op UDP-poort 5247.

Het doel van de gegevens die in leven worden gehouden, is:

- controleren of het toegangspunt nog steeds de controller op het gegevenskanaal kan bereiken
- de gegevenstunnelstatus van het toegangspunt behouden
- Helpt fouten te detecteren die alleen van invloed zijn op het gegevenspad

Wie stuurt het en hoe de controller reageert

Het toegangspunt verzendt de gegevens die worden bewaard, en de controller antwoordt met een reactie op de gegevens die worden bewaard.

Het antwoord kan worden gecodeerd of niet-gecodeerd, afhankelijk van of codering van gegevenskanalen is ingeschakeld.

Als de keepalive geldig is, gebruikt de controller deze om te bevestigen dat het gegevenspad van het toegangspunt nog steeds bereikbaar is. Als het pakket niet kan worden gekoppeld aan een geldige AP-sessie of als het antwoord niet kan worden verzonden, wordt de keepalive verwijderd en kan het gegevenspad uiteindelijk als mislukt worden beschouwd.

Hoe de controller het valideert

Alvorens de keepalive te accepteren, voert de controller basisvalidatie uit om ervoor te zorgen dat het pakket tot het juiste toegangspunt behoort.

De verwerkingsverantwoordelijke controleert of:

- de keepalive bevat geldige CAPWAP-informatie
- het MAC-adres van de AP-radio aanwezig is
- het pakket kan worden gekoppeld aan een AP-sessie

De controller probeert eerst de sessie te identificeren met behulp van het bron-IP-adres en de bron-UDP-poort. Als dat niet lukt, kan het terugvallen op het gebruik van het MAC-adres van de AP-radio.

Dit is belangrijk voor toegangspunten achter NAT of PAT, waarbij het gegevenskanaal kan aankomen vanuit een andere vertaalde UDP-poort dan het controlekanaal. In dergelijke gevallen kan de controller de daadwerkelijke datakanaalkoppeling van het toegangspunt leren en bijwerken.

Als het pakket lijkt te behoren tot een ander toegangspunt dan de sessie die al is gekoppeld aan die IP-poortcombinatie, wordt de keepalive afgewezen om onjuiste toewijzing van sessies te voorkomen.

Wat gebeurt er na validatie

Zodra de keepalive is geaccepteerd, verwerkt de controller deze op basis van de huidige

sessiestatus van het toegangspunt.

- Als de datasessie al is ingesteld, vernieuwt de keepalive gewoon de levendigheid.
- Als dit de eerste geldige gegevensopslag is, kan de controller deze gebruiken om de gegevens van het toegangspunt te leren of bij te werken en de gegevenstunnel te voltooien.

Deze eerste keepalive is vooral belangrijk omdat het de controller helpt de datatunnel correct te programmeren, inclusief gevallen waarin de AP achter NAT of PAT zit.

Nadat de datasessie volledig is vastgesteld, volgen toekomstige keepalives het normale steady-state pad en worden ze alleen gebruikt om de levendigheid te behouden.

belangrijk gedrag

Een geldige databewaarder doet meer dan de gezondheid van het gegevenspad bevestigen. Het vernieuwt ook de algehele sessielevendheid van het toegangspunt op de controller.

Dit betekent dat op de controller de levendigheid van het gegevenskanaal bijdraagt aan de algehele status van de AP-sessie. Als gevolg hiervan zijn de mechanismen voor controle en gegevenslevenheid gerelateerd, hoewel ze verschillende doelen dienen.

AP-side Data Keepalive Timers

Het toegangspunt bepaalt het interval voor het bewaren van gegevens en beslist wanneer de datatunnel als down moet worden beschouwd.

Item	standaardwaarde
Data keepalive-interval	30 seconden
Retransmissieback-off	3s, 6s, 12s, dan 15s
Data dead interval	180 seconden

Onder normale omstandigheden verzendt het toegangspunt elke 30 seconden een databewaarder.

Als het toegangspunt geen antwoord ontvangt, probeert het het opnieuw met behulp van een

back-offpatroon. Als de fout 180 seconden aanhoudt, wordt de datatunnel door het toegangspunt naar beneden geklaard.

CAPWAP-heruitzendingen

Kernprincipe: betrouwbaarheid werkt in beide richtingen

CAPWAP-besturingsberichten maken gebruik van een vraag-en-antwoordmodel, hoewel het via UDP wordt uitgevoerd. Om betrouwbaarheid te bieden, is het apparaat dat een verzoek verzendt ook verantwoordelijk voor het opnieuw verzenden ervan totdat de verwachte reactie is ontvangen.

Dit betekent dat hertransmissies symmetrisch zijn:

- Voor verzoeken van controller naar AP, zoals een configuratie-update, behandelt de controller doorgifte.
- Voor AP-controllerverzoeken, zoals Discovery, Join, Configuration Status, image-gerelateerde berichten en Echo-verzoeken, behandelt het AP doorgifte.

Dit is een belangrijk probleemoplossingspunt. Als u AP-naar-controller-heruitzendingen ziet in een pakketopname, betekent dit meestal dat de AP gewoon zijn eigen verzoek opnieuw probeert omdat deze niet de verwachte reactie heeft ontvangen. Dit is normaal tijdens het samenvoegen en kan ook optreden tijdens controle-echoactiviteit.

transmissiegedrag aan de controllerzijde

Op de controller wordt de hertransmissie afgehandeld door een speciale transmissiebetrouwbaarheidstoestandsmachine.

Eenvoudig gezegd: de controller:

1. Aanvaardt een verzoek dat erkenning vereist
2. plaatst deze in een per-AP-zendwachtrij
3. stuurt het verzoek
4. wacht op de passende reactie
5. Verwijdert het uit de wachtrij wanneer het antwoord arriveert, of verzendt het opnieuw wanneer de timer verloopt

Deze logica wordt voor elke AP-sessie afzonderlijk bijgehouden. De controller houdt ook een zendvenster en een aantal openstaande verzoekberichten bij.

Hoe de controller beslist of hij opnieuw verzendt

Elke keer dat de retransmission timer afloopt, beoordeelt de controller de in de wachtrij geplaatste verzoekitems en neemt een van deze beslissingen:

1. Reactie al buiten bestelling ontvangen

Als het antwoord voor dat verzoek al is ontvangen, zelfs als het buiten de volgorde is aangekomen, verzendt de controller het bericht niet opnieuw.

2. Limiet voor nieuwe poging overschreden

Als het verzoek al meer dan het toegestane aantal keren opnieuw is verzonden, behandelt de controller dit als een fout en wordt het verzendproces voor die AP-sessie afgebroken.

Op dat moment wordt de AP-sessie beëindigd.

3. Verzoek is nog niet oud genoeg

De controller verzendt niet onmiddellijk elk bericht in de wachtrij bij elke timergebeurtenis. Een verzoek moet ten minste gedurende het doorzendinterval in de wachtrij blijven voordat het opnieuw kan worden verzonden.

Standaard is dit herzendinterval 3 seconden.

4. Het verzoek opnieuw verzenden

Als het verzoek nog steeds in behandeling is, lang genoeg is verouderd en de limiet voor het opnieuw proberen niet heeft overschreden, verzendt de controller het opnieuw op het CAPWAP-controlekanaal en verhoogt de retry-teller.

Speciaal geval: bekabelde Daisy-Chain AP's

Voor mesh-implementaties met behulp van een bekabeld daisy-chain AP-pad, biedt de controller een groter herhalingsbudget.

In dit geval wordt de normale retry limiet effectief verdrievoudigd.

Met het standaard aantal herhalingen van 5 betekent dit dat de controller het tot 15 keer opnieuw

kan proberen voordat hij een fout declareert.

Deze uitzondering bestaat omdat deze topologieën meer tolerantie voor vertraging of berichtverlies kunnen vereisen.

AP-side retransmissiegedrag

De AP verzendt ook zijn eigen CAPWAP-verzoeken opnieuw, maar gebruikt een ander patroon dan de controller.

Terwijl de controller een vast herzendingsinterval gebruikt, gebruikt het toegangspunt exponentiële back-off. Dit betekent dat de wachttijd toeneemt na elke mislukte poging.

Bij de standaardinstellingen is de timing van het opnieuw proberen van het toegangspunt ongeveer:

- 6 seconden
- 12 seconden
- 24 seconden
- 48 seconden
- 96 seconden

Dit gedrag is van toepassing op door AP geïnitieerde CAPWAP-verzoeken, zoals:

- ontdekking
- zich aansluiten
- Configuratiegerelateerde uitwisselingen
- gecodeerde besturingstransacties
- Echo-verzoeken

Deze parameters voor het opnieuw proberen worden geleerd van de controller als onderdeel van de AP-join-configuratie.

Diagnostische vingerafdruk in pakketopnamen

Het retransmissiepatroon zelf is vaak een nuttige aanwijzing tijdens het oplossen van problemen.

hertransmissiepatroon	waarschijnlijke bron
Gelijkmatig verdeelde heruitzendingen, ongeveer elke 3 seconden	Doorgifte aan de controllerzijde
Heruitzendingen die zich verder uit elkaar verspreiden in de tijd, zoals 6s, 12s, 24s, 48s, 96s	AP-side retransmission met exponentiële back-off

Dit is een praktische manier om te bepalen welke kant opnieuw probeert, vooral tijdens join-mislukkingen of echogerelateerde problemen.

Wat gebeurt er als de retraites uitgeput zijn

Als heruitzendingen doorgaan zonder de verwachte reactie te ontvangen, geven beide partijen uiteindelijk op, maar hun herstelacties zijn anders.

Controller-zijde

Als de controller het retry-budget heeft opgebruikt, wordt het verzendproces afgebroken en wordt de AP-sessie beëindigd. Hierdoor worden de CAPWAP-besturings- en gegevenssessies gesloten.

AP-zijde

Als het toegangspunt zijn eigen herhalingspogingen uitput, verlaat het die controller en begint het opnieuw vanaf het begin, meestal door terug te keren naar de Discovery-fase en te proberen volledig opnieuw aan te sluiten.

Configuratieknoppen en standaardinstellingen

Het doorgiftegedrag wordt bepaald door twee hoofdinstellingen in het AP-join-profiel.

Opdracht	standaardwaarde	functie
capwap-rezendtelling	5	Maximumaantal hertransmissiepogingen
capwap-hertransmissieinterval	3 seconden	Base retransmission interval

Deze waarden beïnvloeden zowel de betrouwbaarheid van de verbinding als andere CAPWAP-

controlepogingen die door AP zijn geïnitieerd, waaronder echogerelateerde pogingen.

Geconsolideerde tijdopnemerreferentie

Deze tabel geeft een overzicht van de belangrijkste CAPWAP-timers die in dit artikel worden besproken.

Timer	standaardwaarde	vlak	eigenares	Beschrijving
Controle-echo-interval	30 seconden	controle	AP	Als het toegangspunt gedurende 30 seconden geen CAPWAP-besturingsverkeer verzendt, verzendt het een echoverzoek.
Dode timer voor hartslagregeling	90 seconden	controle	controleur	De controller verwacht geldig controleverkeer binnen dit venster. Als er niets wordt ontvangen, wordt de controlesessie als down beschouwd.
Controle-hertransmissieinterval	3 seconden	controle	controleur	De controller verzendt zijn eigen onbeantwoorde CAPWAP-verzoeken opnieuw met een vast interval.
Controle-hertransmissietelling	5 pogingen	controle	controleur	Maximale aantal herhalingen voor CAPWAP-verzoeken die door de controller zijn gestart. In bedrade daisy-chain scenario's kan dit oplopen tot 15 pogingen.
Terugzending via AP-besturingselement	6, 12, 24, 48, 96 seconden	controle	AP	De AP verzendt zijn eigen CAPWAP-verzoeken opnieuw met behulp van exponentiële back-off.
Data keepalive-interval	30 seconden	gegevens	AP	Onder normale omstandigheden verzendt het toegangspunt elke 30 seconden een databewaarder.

Timer	standaardwaarde	vlak	eigenares	Beschrijving
Terugwerkende kracht voor gegevensherstel	3, 6, 12, 15, 15 seconden	gegevens	AP	Als een reactie van de bewaarder van de gegevens wordt gemist, probeert het toegangspunt het opnieuw met behulp van een back-off, met een maximum van 15 seconden.
Dead interval in gegevenskanaal	180 seconden	gegevens	AP	Als het toegangspunt de gegevensuitwisseling niet binnen deze periode in stand houdt, wordt de gegevenstunnel uitgeschakeld.

Verschillen naast elkaar

Keepalive vs. hertransmissie

Hoewel ze soms verward zijn, dienen levend houden en doorgifte verschillende doelen.

aspect	Keepalive	hertransmissie
Hoofddoel	Controleert of de peer nog steeds bereikbaar is	Herstelt een specifiek verzoek als er geen antwoord is ontvangen
reikwijdte	Per sessie of per kanaal	Per bericht
Trigger	Time-out voor inactiviteit of levendigheid	Een verzoek blijft onbeantwoord
Volgmethode	op tijd gebaseerd	Op basis van aantal opnieuw proberen
Mislukking betekenis	Het kanaal of de sessie is niet meer bereikbaar	Een specifieke CAPWAP-uitwisseling is herhaaldelijk mislukt
Mislukkingsresultaat	Sessie kan worden afgebroken	De controller kan de sessie beëindigen of het toegangspunt kan opnieuw deelnemen

RA Trace Log Strings volgens mechanisme

Voor AP-specifieke tracering verzamelt u logs voor het AP en zoekt u naar deze exacte tekenreeksen.

Logboekverzameling

Gebruik:

- Foutopsporing draadloze Mac <AP-Radio-Mac>
- Toon logboekprofiel Draadloos filter MAC <AP-Radio-Mac> naar bestand bootflash:<file>

Controle keepalive / hartslag

Zoeken naar:

- Behandeling van Echo-verzoek
- Echorespons opbouwen
- Echo-antwoord op verzoek met volgnummer <N>.
- Heartbeat Timer opnieuw gestart met nieuwe waarde <ms>
- Hartslagtimer aangeraakt
- Vervaldatum hartslagtimer

Gegevenshersteller

Zoeken naar:

- Ontvangen gegevensbehoud
- reeds ingevoerde gegevensbeoordeling
- Gegevens DTLS is niet vastgesteld
- CAPWAP-gegevenstunnelinvoer bijwerken
- De gegevens kunnen niet worden verwerkt. Reden: CAPWAP-sessie is niet uitgevoerd of ingesteld
- Ongeldig keepalive-bericht, geen capwap-blok
- Ongeldig keepalive-bericht, geen WTP MAC
- Kan keepalive niet verwerken, CAPWAP-sessie niet gevonden
- Data keep-alive wordt ontvangen op een andere poort dan de controlepoort: <port>
- Data keep-alive wordt ontvangen voor verschillende AP <mac>
- De gegevens van de gegevenstunnel in de WTP-sessietabel voor externe host zijn niet bijgewerkt: <ip>

- CAPWAP-gegevenstunnelvermelding kan niet worden bijgewerkt

Bediening van het gegevensvliegtuig blijft in leven

Zoeken naar:

- Ontvangen gegevens in leven houden van <src> tot <dst>
- Verzonden <enc/plain> data keep-alive reactie
- Keep-alive pkt laten vallen vanaf IP: <ip>, onbekende sessie
- Keep-alive pkt van IP: <ip> laten vallen, DTLS-status van gegevens is niet opgehaald
- De reactie voor het bewaren van gegevens is niet verzonden
- Bericht voor taakverdeling gegevens levendig houden mislukt

hertransmissie

Zoeken naar:

- callback van timer opnieuw verzenden
- Seqnum <N> opnieuw verzenden omdat het in de wachtrij staat en nog moet worden teruggehaald
- Bericht opnieuw verzenden: <msg-name> poging tot opnieuw verzenden: <M>
- vermelding met volgnummer: <N> staat in de wachtrij voor <S> seconden. Niet opnieuw verzenden
- CAPWAP-sessie wordt beëindigd, max. heruitzendingen verlopen voor: <msg> ...
- Opschonen van CAPWAP-sessiebronnen op AP-verlof.

Afbreken van sessie

Zoeken naar:

- CAPWAP-sessie van toegangspunt beëindigen.
- Sluit de CAPWAP DTLS-sessie.
- CAPWAP-DTLS-controlesessie Sluiten
- CAPWAP-DTLS-gegevenssessie sluiten
- Laatste Control Packet ontvangen <S> seconden geleden.
- Laatste gegevens Keep Alive Packet ontvangen <S> seconden geleden.
- CAPWAP DTLS-sessie gesloten voor AP, oorzaak: <reden>

Voorbeelden:

Werkscenario

Verificatie van AP-foutopsporing

Deze AP-foutopsporingsopdracht kan worden gebruikt om de CAPWAP-besturing en de communicatie tussen het AP en de WLC te bewaken.

```
#debug capwap client event
```

Deze foutopsporingslogboeken tonen een succesvolle CAPWAP-communicatiereeks.

Om 13:11:44 zond het toegangspunt een CAPWAP Echo Request door naar de WLC via UDP-poort 5246. Tijdens hetzelfde interval verzond het toegangspunt ook een CAPWAP Data Keepalive-pakket via UDP-poort 5247. De logboeken bevestigen dat de WLC met succes op beide verzoeken heeft gereageerd.

De tijdstempels geven een normale CAPWAP-communicatiecyclus aan:

- 13:11:44.0917 – Verzoek van ECHO verzonden.
- 13:11:44.0918 – Gegevens worden verzonden.
- 13:11:44.0926 – Data Keepalive ontvangen van de WLC.
- 13:11:44.0940 – Echo Response ontvangen van de WLC.

Deze tijdstempels bevestigen dat zowel de CAPWAP-besturing als de gegevenskanalen functioneren zoals verwacht met een verwaarloosbare latentie voor retourvluchten.

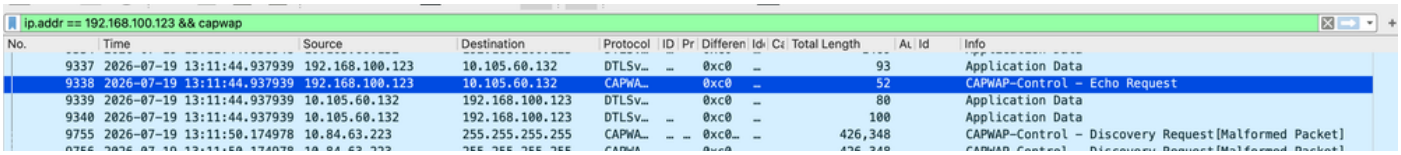
```
[*07/19/2026 13:11:14.0817] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0917] Echo Request: Send count 22
[*07/19/2026 13:11:44.0917] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: 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
```

CAPWAP Control Packet Validation (UDP-poort 5246)

pakketopname-analyse

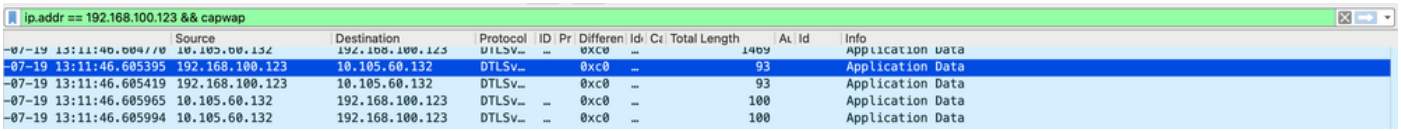
De pakketopname bevestigt dat het toegangspunt een CAPWAP Echo Request heeft gegenereerd om 13:11:44 via UDP-poort 5246.

De WLC heeft het pakket met succes ontvangen, het verzoek verwerkt en onmiddellijk de bijbehorende echorespons gegenereerd. Aangezien het CAPWAP-controlekanaal is beveiligd met DTLS-codering, wordt het antwoord weergegeven als gecodeerde toepassingsgegevens in de pakketopname.



Switch Packet Verification

De switch packet capture bevestigt dat de gecodeerde CAPWAP-besturingspakketten met succes zijn ontvangen van de WLC en zijn doorgestuurd naar het toegangspunt.

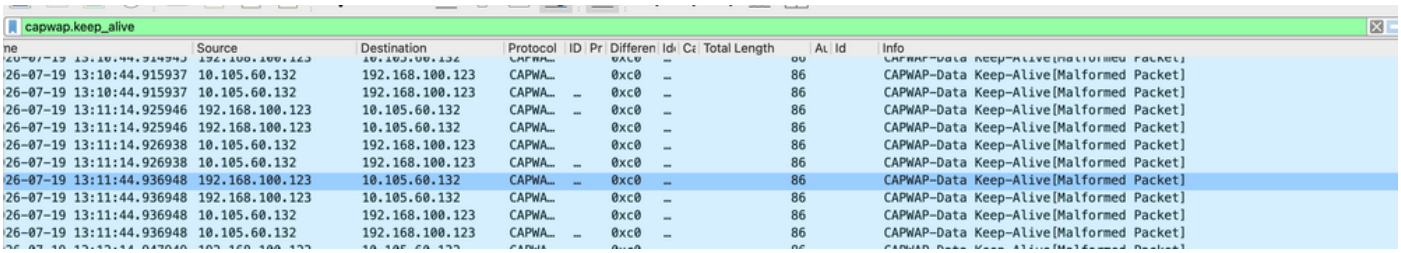


CAPWAP Data Keepalive-validatie (UDP-poort 5247)

Het toegangspunt verzendt periodiek CAPWAP Data Keepalive-pakketten via UDP-poort 5247 om de status van de CAPWAP-datatunnel te controleren.

Om 13:11:44 stuurde de AP een Data Keepalive-pakket naar de WLC. De WLC ontving het pakket met succes en reageerde onmiddellijk met de bijbehorende keepalive-respons.

Deze succesvolle uitwisseling bevestigt dat het CAPWAP-gegevenspad operationeel blijft en dat bidirectionele communicatie tussen het toegangspunt en de WLC normaal functioneert

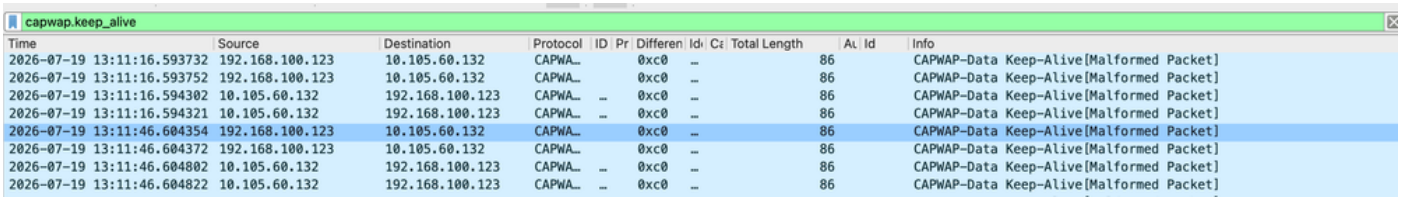


Switch Packet Verification

Met de switch packet capture wordt verder bevestigd dat de CAPWAP Data Keepalive-pakketten zonder onderbreking met succes zijn doorgestuurd tussen het toegangspunt en de WLC.

De waargenomen pakketstroom bevestigt dat:

- Data Keepalive-pakketten hebben de WLC bereikt.
- De WLC genereerde de verwachte keepalive-respons.
- De switch stuurde het antwoord terug naar de AP.
- Er is geen pakketverlies opgetreden op het doorstuurpad.



Controlepakketten (UDP 5246) die op de AP Uplink-Switch vallen

Deze test toont het gedrag van een toegangspunt aan wanneer de CAPWAP-controlepoort (UDP 5246) op de switch van de toegangspunt wordt neergezet.

Het doel is om het AP-, WLC- en netwerkgedrag te valideren wanneer CAPWAP-besturingspakketten het AP niet kunnen bereiken, ondanks het feit dat de WLC de verzoeken met succes verwerkt en beantwoordt.

In dit scenario:

- De AP blijft CAPWAP Echo Requests verzenden naar de WLC.
- De WLC ontvangt en verwerkt met succes elke Echo-aanvraag.
- De WLC genereert de bijbehorende echorespons.
- De switch AP uplink ontvangt het antwoord, maar stuurt het niet terug naar het toegangspunt.

- Aangezien het toegangspunt nooit de echorespons ontvangt, overschrijdt het uiteindelijk het maximale aantal heruitzendingen en start het de CAPWAP-toestandsmachine opnieuw op.

AP-foutopsporingsanalyse

Om 12:11:55.4568 verzond het toegangspunt een CAPWAP Echo Request naar de WLC via UDP-poort 5246.

Echo-aanvraag: aantal verzenden 0

In tegenstelling tot het normale werkscenario werd er geen Echo Response ontvangen. Als gevolg hiervan initieerde het toegangspunt heruitzendingen volgens de standaard CAPWAP-timer.

De heruitzendingen vonden plaats op deze tijdstempels:

tijd	gebeurtenis
12:12:00.2587	Aantal heruitzendingen = 1
12:12:03.2599	Aantal heruitzendingen = 2
12:12:06.2610	Aantal heruitzendingen = 3
12:12:09.2624	Aantal heruitzendingen = 4
12:12:12.2637	Aantal heruitzendingen = 5

Na de vijfde mislukte doorgifte verklaarde het toegangspunt de CAPWAP-controlesessie onbereikbaar.

Om 12:12:15.2647 meldde de AP:

Het maximale aantal heruitzendingen is overschreden en gaat terug naar de DISCOVER-modus.

Onmiddellijk daarna startte het toegangspunt de CAPWAP-statusmachine opnieuw op om een nieuw detectieproces te starten.

```
[*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
```

De WLC RA-sporen bevestigen dat de controller geen verwerkingsproblemen heeft ondervonden.

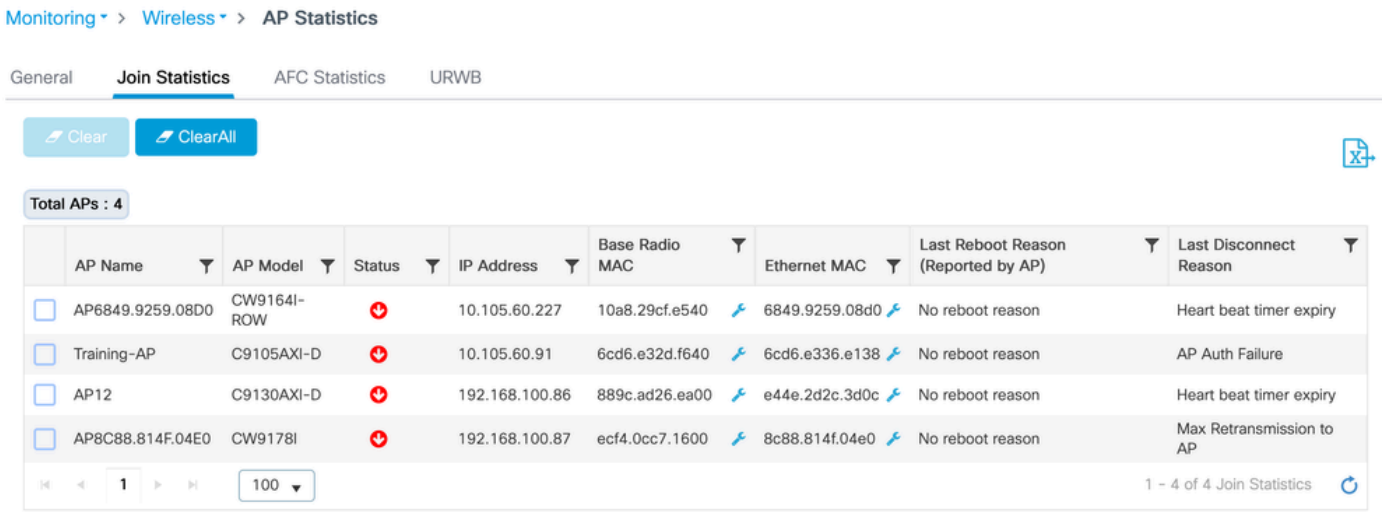
Om 12:11:58.731835712 ontving de WLC met succes het CAPWAP Echo Request dat door de AP werd verzonden. Deze logs tonen aan dat de WLC het verzoek succesvol heeft verwerkt en de juiste reactie heeft gegenereerd. Later, om 12:12:19.802183814, ontving de WLC een DTLS Close Notify van de AP. Het toegangspunt heeft de verbinding verbroken omdat het nooit de echo-antwoorden heeft ontvangen die door de controller zijn verzonden. Als gevolg hiervan beëindigde de WLC de DTLS-sessie en nam de AP-disassociatie op.

<#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>

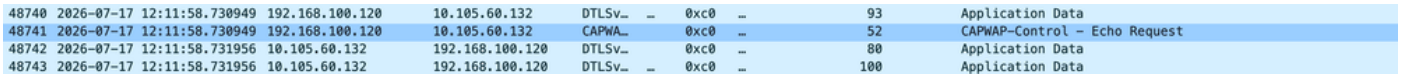
```
VK-WLC#show wireless stats ap history | i AP12


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
```

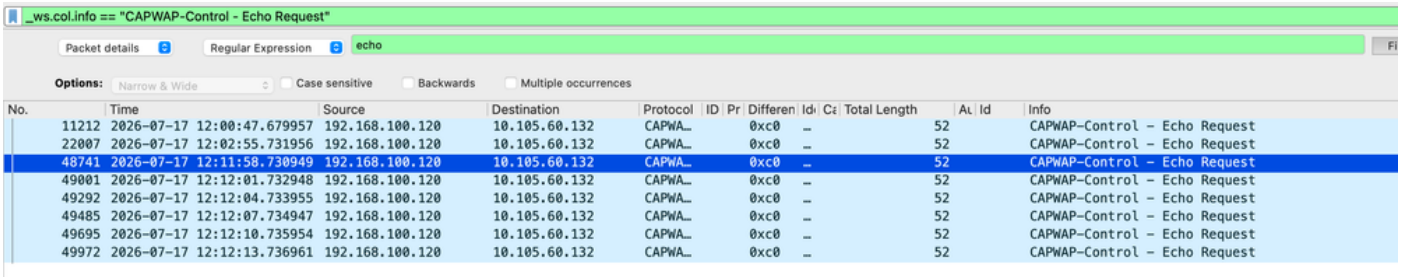


De WLC EPC bevestigt het volgende:

- Op hetzelfde tijdstempel, de CAPWAP Echo Request met succes bereikt de WLC.
- De WLC genereerde een gecodeerde CAPWAP Echo Response.
- Het antwoord wordt weergegeven als Toepassingsgegevens, omdat het CAPWAP-besturingsverkeer wordt beschermd door DTLS-codering.

De EPC bevestigt derhalve dat de voor de verwerking verantwoordelijke het antwoord met succes heeft verzonden. Dit elimineert de WLC als de bron van het probleem.





Pakketopnames verzameld op de AP-uplink-switch leveren het laatste bewijs.

De opnames tonen aan dat:

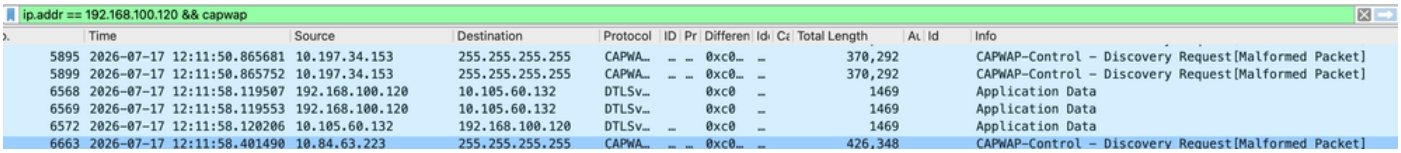
- De switch heeft met succes de gecodeerde echorespons ontvangen die door de WLC is verzonden.

- Het antwoord is zichtbaar als toepassingsgegevens, wat wordt verwacht vanwege DTLS-codering.
- Het antwoord werd niet doorgestuurd naar de AP.

Dit verklaart waarom:

- De AP heeft nooit de CAPWAP Echo Response ontvangen.
- De AP bleef ECHO-verzoeken doorsturen.
- De retransmissieteller overschreed uiteindelijk de geconfigureerde drempel.
- Het toegangspunt heeft het CAPWAP-statussysteem opnieuw opgestart.

De pakketopnames identificeren duidelijk de switch als het punt waar het CAPWAP-controleverkeer werd onderbroken



CAPWAP-gegevenspoort (UDP 5247) wordt verwijderd op de AP Uplink-Switch

Met deze test wordt het gedrag van het toegangspunt gevalideerd wanneer de CAPWAP-gegevenspoort (UDP 5247) op de switch van de AP-uplink wordt geplaatst terwijl de CAPWAP-controlepoort (UDP 5246) in gebruik blijft.

In tegenstelling tot het vorige scenario blijft de AP de CAPWAP-besturingsverbinding met de WLC behouden door CAPWAP Echo-berichten succesvol uit te wisselen via UDP-poort 5246. Aangezien de CAPWAP Data Keepalive-pakketten de retourvlucht echter niet kunnen voltooien, verklaart het toegangspunt het CAPWAP-gegevenspad uiteindelijk als onbereikbaar en start het een CAPWAP-herstart.

De foutopsporingslogboeken van het toegangspunt bevestigen dat het CAPWAP-controlekanaal tijdens de test operationeel bleef.

Aan het begin van de opname bleven CAPWAP Echo-verzoeken die via UDP-poort 5246 werden verzonden geldige Echo-antwoorden van de WLC ontvangen, waarmee ononderbroken communicatie tussen het besturingsvlak werd bevestigd.

Om 14:30:15 verzond het toegangspunt echter een CAPWAP Data Keepalive-pakket via UDP-poort 5247. Aangezien er geen overeenkomstige Data Keepalive-respons werd ontvangen, startte de AP het retry-mechanisme. De heruitzendingen kunnen worden waargenomen op deze

tijdstempels:

tijdstempel	gebeurtenis
14:30:15	Initiële Keepalive-gegevens verzonden
14:30:19	Opnieuw proberen 1
14:30:25	Opnieuw 2
14:30:37	Opnieuw proberen 3
14:30:49	4 Opnieuw proberen
14:31:01	5 opnieuw proberen
14:31:13	Laatste poging

Hoewel de CAPWAP-echorespons gedurende deze periode bleven worden ontvangen, ontving het toegangspunt geen respons voor de pakketten Data Keepalive. Na het uitputten van de herhalingspogingen meldde het toegangspunt een niet-versleutelde Time-out voor gegevensbehoud en startte het een herstart van CAPWAP. Om ongeveer 14:31:16 beëindigde het toegangspunt de bestaande CAPWAP-sessie en keerde het terug naar het detectieproces.

```
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)...
```

Voor het CAPWAP-gegevenskanaal geven de sporen aan dat de controller de verwachte pakketten voor gegevensbewaring niet heeft ontvangen. Uiteindelijk, nadat de AP de Data Keepalive-fout had verklaard, registreerde de WLC de beëindiging van de DTLS-sessie en de AP disjoin-gebeurtenis. De sequentie die in de RA-traces is waargenomen, bevestigt dat de controller operationeel bleef totdat het toegangspunt vrijwillig werd losgekoppeld vanwege de time-out voor het bewaren van gegevens.

RA traces met AP ethernet mac:

<#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)
```

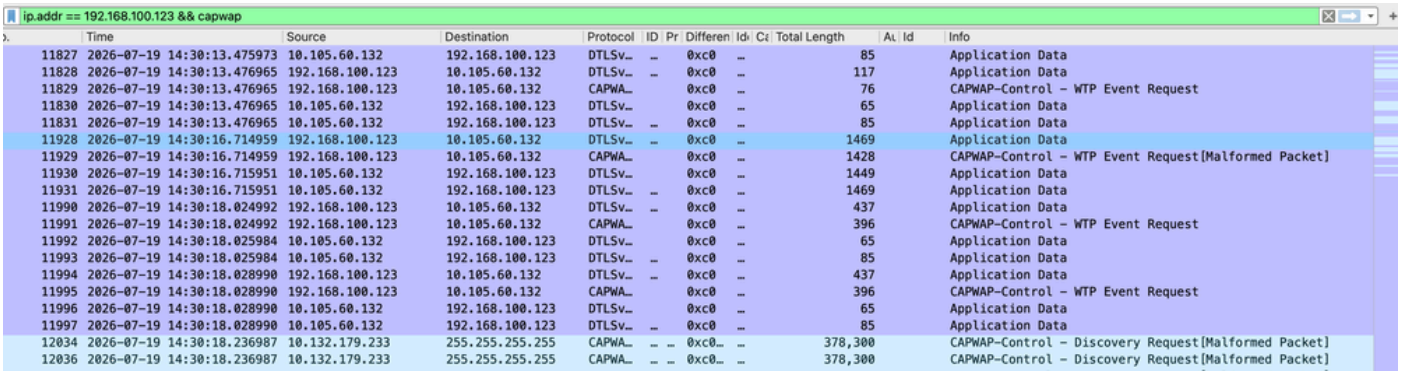
RA traces met Radio mac:

<#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
```

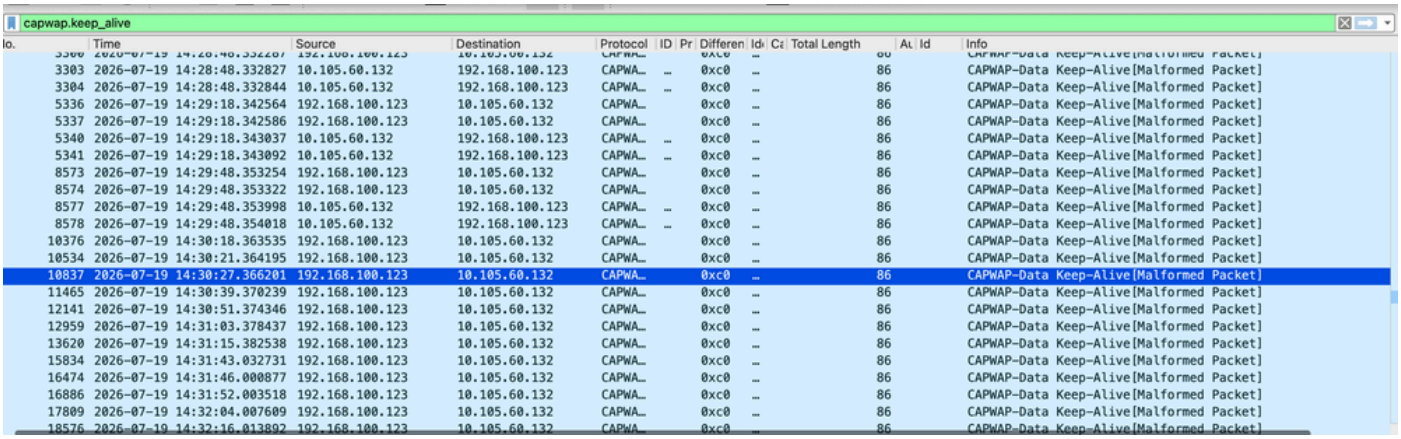
EPC verzameld op de WLC valideert de verwerking van pakketten aan de controllerzijde. De opnames bevestigen dat CAPWAP Control-pakketten succesvol bleven worden uitgewisseld tijdens de test, maar er was geen data keepalive-pakket ontvangen op wlc. Deze waarneming

stemt overeen met de AP-debuglogboeken en toont aan dat het Data Keepalive-mechanisme is mislukt, ondanks dat het controlekanaal actief blijft.



Switch:

Packet captures verzameld op de AP uplink switch toont hoewel de pakketjes aanwezig waren op de switch, maar dezelfde werden niet doorgestuurd naar de wlc



CAPWAP Data Keepalive uitschakelen

Deze functie werd geïntroduceerd onder Cisco bug ID CSCvs66015

Deze functie is handig bij het oplossen van problemen met deze scenario's.

1. Problemen met AP-verbroken verbindingen oplossen: Nadat u capwap-gegevens hebt uitgeschakeld om de verbinding levend te houden, kunnen we zien of AP nog steeds verbreekt vanwege capwap-controle om de verbinding levend te houden en de hoofdoorzaak voor AP-verbroken verbindingen te identificeren.
2. Vermijd ontkoppelingen als gevolg van capwap data-keepalive als een tijdelijke oplossing totdat de reden voor capwap data-keep-alive drops te identificeren.

3. Sniffer AP's in branch flex-implementaties die zijn verbonden via een WAN-koppeling met lage doorvoer. Als we OTA-pakketopnames willen verzamelen door een van de toegangspunten te configureren om in de snuffelmodus te staan, worden alle vastgelegde pakketten via een WAN-link naar WLC verzonden met behulp van de capwap-gegevenspoort. Als u dat doet, overweldigt het de WAN-link en heeft het invloed op de volledige tak.
4. Als u capwap data keep-alive voor AP uitschakelt in de snuffelmodus en een ACL in een tak maakt om capwap-gegevenspakketten van dat concrete AP te laten vallen, blijft AP verbonden omdat capwap-besturing prima is en dan kunt u OTA van AP-switchport verzamelen zonder overweldigende WAN-koppeling met pakketopnames.

COS-AP-gegevens activeren om 9800 WLC in-/uit te schakelen. Standaard zijn gegevens die in zowel WLC als AP worden bewaard ingeschakeld.

WLC, opdracht:

1) Geef de status weer met de tekenreeks "Unencrypted Data Keep Alive"

```
show ap config general
```

2) Gegevensbehoud inschakelen/uitschakelen met de naam van het toegangspunt

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

Activeer COS-AP-gegevensbehoud actief en schakel AP zelf in/uit. Standaard is het actief houden van gegevens in het toegangspunt ingeschakeld.

AP, opdracht:

1) Geef de status weer met de tekenreeks "Unencrypted Data Keep Alive"

```
show capwap client config
```

2) Gegevensbehoud inschakelen/uitschakelen in AP

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

Voorbeeld:

Gehandicapte keepalive-controle op ap-niveau:

```
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
```

AP-debugs:

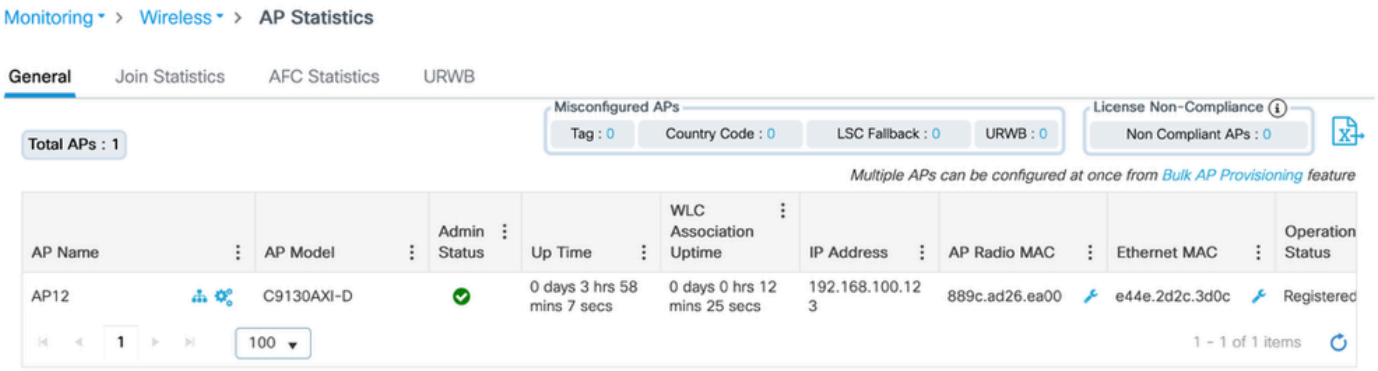
In ap debug kunnen we zien dat er geen data keepalive packet uitwisseling plaatsvindt tussen de AP en de wlc, we zien alleen de control packet uitwisseling.

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
```

Hoewel de pakketjes voor het bewaren van gegevens werden verwijderd, maar omdat we de controle voor het bewaren van gegevens hebben uitgeschakeld, kunnen we zien dat het toegangspunt stabiel blijft op de wlc zonder te worden beïnvloed door de daling van de pakketjes voor het bewaren van gegevens.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.