Comprensione e risoluzione dei problemi di CAPWAP Keepalives su Catalyst 9800 WLC

Sommario

Introduzione

Questo documento descrive i controlli CAPWAP keepalive, data keepalive e ritrasmissioni,

Contesto

CAPWAP fornisce la struttura di comunicazione tra i Cisco access point e il controller LAN wireless sulle piattaforme Cisco Catalyst 9800. Utilizza canali di controllo e dati separati, insieme a meccanismi di keepalive e ritrasmissione definiti per mantenere la connettività.

In questo articolo vengono illustrati i programmi keepalive di controllo CAPWAP, i programmi keepalive di dati e le ritrasmissioni, inclusi i timer associati, il comportamento di errore e gli indicatori chiave per la risoluzione dei problemi.

Due Canali Separati, Due Meccanismi Diversi

CAPWAP funziona su due canali UDP, ciascuno dei quali ha il proprio meccanismo di trasmissione

Channel	Porta predefinita (UDP)	Meccanismo di vitalità
Controllo	5246	Richiesta echo / Risposta echo
Dati	5247	Keep-Alive del canale dati

Controllo CAPWAP keepalive (eco/heartbeat)

Scopo

Il comando CAPWAP control keepalive viene usato per verificare che il punto di accesso sia ancora raggiungibile sul canale di controllo.

Il suo scopo è molto semplice: verifica che la connessione di controllo tra l'access point e il controller sia ancora attiva e reattiva. Non viene utilizzato per trasportare aggiornamenti della configurazione o dati client. Funge invece da meccanismo di livness per il percorso di controllo CAPWAP sulla porta UDP 5246.

Chi invia Keepalive

Il punto di accesso è il dispositivo che attiva il controllo keepalive.

Se necessario, l'access point invia una richiesta Echo CAPWAP al controller. Il controller risponde quindi con una risposta echo corrispondente. Questa risposta conferma che il controller ha ricevuto la richiesta e che il canale di controllo funziona in entrambe le direzioni.

La risposta corrisponde alla richiesta, che consente all'access point di confermare che sta ricevendo una risposta valida al messaggio keepalive inviato.

Questo comportamento è importante perché dimostra che il controllo keepalive non è principalmente un meccanismo di polling guidato dal controller. L'access point è invece responsabile del controllo della raggiungibilità del canale di controllo e il controller risponde di conseguenza.

L'intervallo dell'eco è basato sull'inattività e non su una pianificazione fissa

Questo è uno degli aspetti più comunemente fraintesi del controllo CAPWAP keepalive.

Si presume in genere che l'access point invii una richiesta echo ogni 30 secondi come un heartbeat periodico fisso. In pratica, non funziona così.

Il controllo keepalive è basato sull'inattività del canale di controllo. Questo significa che l'access point invia una richiesta echo standalone solo quando il canale di controllo è stato inattivo per l'intervallo configurato. Se il traffico di altri controlli è già stato scambiato tra il punto di accesso e il controller, non è necessario inviare un pacchetto echo separato.

Qualsiasi comunicazione di controllo valida tra l'access point e il controller dimostra in modo efficace che il canale di controllo è attivo. Per questo motivo, il normale traffico di controllo CAPWAP reimposta il timer keepalive.

Esempi di traffico di controllo possono includere:

- scambi di configurazione
- aggiornamenti di gestione risorse radio
- Messaggi di controllo relativi alla WLAN
- eventi di controllo correlati al client
- messaggi di sincronizzazione statistiche o dello stato
- altri pacchetti di controllo CAPWAP scambiati durante il normale funzionamento

Di conseguenza, le richieste echo standalone sono visibili solo nei periodi in cui il canale di controllo è silenzioso.

Esempio semplice

È possibile controllare i timer echo CAPWAP sull'access point utilizzando il 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
```

Timer

Il meccanismo di controllo keepalive si basa su due importanti valori di temporizzazione.

Articolo	Valore predefinito	Descrizione
Intervallo eco	30 secondi	Quantità di inattività del canale di controllo prima che l'access point invii una richiesta echo standalone
Timer inattivo controllo controller	90 secondi	Il periodo di tempo massimo consentito dal controller senza ricevere traffico di controllo valido prima di dichiarare la sessione di controllo inattiva

Cosa succede quando il controllo keepalive ha esito negativo

Se il canale di controllo rimane inattivo per un periodo di tempo superiore al timeout consentito, il controller dichiara infine che la sessione di controllo è stata persa.

A questo punto, il controller considera l'access point come non più raggiungibile sul canale di controllo e avvia il disassemblaggio della sessione. Ciò include in genere la chiusura della connessione di controllo e la rimozione dello stato della sessione di controllo attiva dell'access point.

L'access point può quindi tentare di ristabilire la connettività individuando di nuovo il controller e collegandolo di nuovo, a seconda dello scenario di errore.

Implicazioni della risoluzione dei problemi

La comprensione di questo comportamento keepalive è essenziale durante la risoluzione dei problemi.

I pacchetti echo mancanti non sempre rappresentano un problema

Se l'acquisizione di un pacchetto non visualizza le richieste echo ogni 30 secondi, non indica automaticamente un errore. Può semplicemente indicare che è in corso il flusso di altro traffico di controllo CAPWAP, quindi non è richiesta alcuna eco indipendente.

La Spaziatura Dell'Eco Irregolare È In Genere Normale

Gli echi spesso appaiono a intervalli non uniformi perché sono attivati dall'inattività. Si tratta di un comportamento normale.

Focus sull'attività complessiva del canale di controllo

Quando la risoluzione dei problemi di disconnessione dell'access point è più utile chiedere:

- Il controller riceve ancora traffico di controllo CAPWAP dall'access point?
- Il canale di controllo è silenzioso abbastanza a lungo da attivare il timer inattivo?
- Esistono problemi di rete che influiscono solo sul percorso di controllo?
- La perdita dei pacchetti, il comportamento del firewall, i problemi NAT o le perdite del control plane interrompono il traffico UDP 5246?

Il vero problema non è l'assenza di pacchetti echo periodici da soli. Il vero problema è la perdita della comunicazione del canale di controllo per un tempo sufficientemente lungo da far dichiarare l'access point irraggiungibile.

CAPWAP Data Keepalive

Scopo

L'eco del controllo CAPWAP conferma che il canale di controllo funziona, ma non dimostra che anche il canale dati è integro. Poiché il percorso di controllo e il percorso dei dati possono avere esito negativo in modo indipendente, CAPWAP utilizza un comando data keepalive separato sulla porta UDP 5247.

Lo scopo dei dati keepalive è:

- verificare che l'access point possa ancora raggiungere il controller sul canale dati
- mantieni lo stato del tunnel dati del punto di accesso
- rilevare gli errori che influiscono solo sul percorso dei dati

Chi lo invia e come risponde il controller

L'access point invia i dati keepalive, e il controller risponde con una risposta Data Keepalive.

La risposta può essere crittografata o non crittografata, a seconda che sia abilitata la crittografia del canale dati.

Se il comando keepalive è valido, il controller lo utilizza per verificare che il percorso dei dati dell'access point sia ancora raggiungibile. Se il pacchetto non può essere associato a una sessione AP valida o se non è possibile inviare la risposta, il pacchetto keepalive viene scartato e il percorso dei dati può essere considerato non riuscito.

Modalità di convalida del controller

Prima di accettare il comando keepalive, il controller esegue la convalida di base per verificare che il pacchetto appartenga all'access point corretto.

Il controllore verifica che:

- keepalive contiene informazioni CAPWAP valide
- l'indirizzo MAC radio AP è presente
- il pacchetto può corrispondere a una sessione AP

Il controller tenta innanzitutto di identificare la sessione utilizzando l'indirizzo IP di origine e la porta UDP di origine. Se l'operazione non riesce, è possibile ripristinare l'indirizzo MAC della radio dell'access point.

Questo è importante per i punti di accesso dietro NAT o PAT, dove il canale dati può arrivare da una porta UDP tradotta diversa rispetto al canale di controllo. In questi casi, il controller può apprendere e aggiornare l'effettiva tupla del canale dati del punto di accesso.

Se il pacchetto sembra appartenere a un punto di accesso diverso da quello della sessione già associata alla combinazione di porta IP, il comando keepalive viene rifiutato per impedire che la sessione venga mappata in modo errato.

Descrizione della procedura di convalida

Una volta accettato il comando keepalive, il controller lo elabora in base allo stato della sessione corrente dell'access point.

- Se la sessione di dati è già stabilita, il comando keepalive aggiorna semplicemente la vivacità.
- Se questo è il primo dato keepalive valido, il controllore può utilizzarlo per apprendere o aggiornare le informazioni del canale dati del punto di accesso e completare la creazione del tunnel dati.

Questa prima opzione di keepalive è particolarmente importante perché aiuta il controller a programmare correttamente il tunnel di dati, compresi i casi in cui l'access point si trova dietro NAT o PAT.

Una volta stabilita la sessione di dati, gli elementi keepalive futuri seguono il normale percorso di stato stazionario e vengono utilizzati solo per mantenere la vitalità.

Comportamento importante

Un'operazione keepalive di dati valida non solo conferma l'integrità del percorso dati. Aggiorna inoltre la durata complessiva della sessione dell'access point sul controller.

Ciò significa che, sul controller, la vivacità del canale dati contribuisce all'integrità complessiva della sessione AP. Di conseguenza, i meccanismi di controllo e di sopravvivenza dei dati sono correlati, anche se hanno scopi diversi.

Timer keepalive dati lato AP

L'access point controlla l'intervallo keepalive dei dati e decide quando il tunnel di dati deve essere considerato inattivo.

Articolo	Valore predefinito
Intervallo keepalive dei dati	30 secondi
Ritrasmissione backoff	3s, 6s, 12s, quindi 15s
Intervallo inattività dati	180 secondi

In condizioni normali, l'access point invia un messaggio keepalive dei dati ogni 30 secondi.

Se l'access point non riceve una risposta, riprova utilizzando un modello di backoff. Se il problema persiste per 180 secondi, l'access point dichiara inattivo il tunnel di dati.

Ritrasmissioni CAPWAP

Principio fondamentale: L'affidabilità funziona in entrambe le direzioni

CAPWAP control messaging utilizza un modello di richiesta e risposta, anche se viene eseguito su UDP. Per garantire l'affidabilità, il dispositivo che invia una richiesta è anche responsabile della ritrasmissione fino alla ricezione della risposta prevista.

Ciò significa che le ritrasmissioni sono simmetriche:

- Per le richieste da controller a access point, ad esempio un aggiornamento della configurazione, il controller gestisce la ritrasmissione.
- Per le richieste al controller da parte dell'access point, ad esempio individuazione, join, stato della configurazione, messaggi relativi alle immagini e richieste echo, l'access point gestisce la ritrasmissione.

Si tratta di un punto importante per la risoluzione dei problemi. Se durante l'acquisizione di un pacchetto vengono rilevate ritrasmissioni da punto di accesso al controller, in genere l'access point sta semplicemente tentando di eseguire nuovamente la richiesta perché non ha ricevuto la risposta prevista. Si tratta di un comportamento normale durante l'unione e può verificarsi anche durante l'attività eco del controllo.

Comportamento di ritrasmissione sul lato controller

Sul controller, la ritrasmissione è gestita da una macchina a stati di affidabilità di trasmissione dedicata.

In parole semplici, il controller:

1. accetta una richiesta che richiede conferma
2. lo inserisce in una coda di trasmissione per punto di accesso
3. invia la richiesta
4. attende la risposta corrispondente
5. rimuove la risposta dalla coda quando arriva oppure la ritrasmette quando scade il timer

Questa logica viene rilevata separatamente per ciascuna sessione AP. Il controller mantiene inoltre una finestra di trasmissione e un conteggio dei messaggi di richiesta in attesa.

Come il controller decide se ritrasmettere

Ogni volta che scade il timer di ritrasmissione, il controller esamina le voci di richiesta in coda e prende una delle seguenti decisioni:

1. Risposta già ricevuta fuori servizio

Se la risposta alla richiesta è già stata ricevuta, anche se è arrivata fuori sequenza, il controller non ritrasmette nuovamente il messaggio.

2. Limite tentativi superato

Se la richiesta è già stata ritrasmessa più volte del numero consentito, il controller la considera un errore e interrompe il processo di trasmissione per quella sessione AP.

A questo punto, la sessione AP viene terminata.

3. La richiesta non è ancora sufficientemente vecchia

Il controller non ritrasmette immediatamente ogni messaggio in coda a ogni evento del timer. Una richiesta deve rimanere nella coda almeno per l'intervallo di ritrasmissione prima di poter essere inviata di nuovo.

Per impostazione predefinita, questo intervallo di ritrasmissione è di 3 secondi.

4. Trasmetti nuovamente la richiesta

Se la richiesta è ancora in sospeso, ha superato il periodo di validità sufficiente e non ha superato il limite di tentativi, il controller la invia nuovamente sul canale di controllo CAPWAP e incrementa il contatore dei tentativi.

Caso speciale: AP a catena cablata

Per le distribuzioni mesh che utilizzano un percorso AP a catena cablata, il controller consente un budget per i tentativi maggiore.

In questo caso, il limite di tentativi normale è effettivamente triplicato.

Se il valore predefinito per il numero di tentativi è 5, il controller può eseguire un nuovo tentativo fino a 15 volte prima di dichiarare l'errore.

Questa eccezione esiste perché queste topologie possono richiedere una maggiore tolleranza per il ritardo o la perdita di messaggi.

Comportamento ritrasmissione lato access point

L'access point trasmette nuovamente le proprie richieste CAPWAP, ma utilizza un modello diverso da quello del controller.

Mentre il controller utilizza un intervallo di ritrasmissione fisso, l'access point utilizza un backoff esponenziale. Ciò significa che il tempo di attesa aumenta dopo ogni tentativo fallito.

Con le impostazioni predefinite, l'intervallo tra i tentativi del punto di accesso è approssimativamente il seguente:

- 6 secondi
- 12 secondi
- 24 secondi
- 48 secondi
- 96 secondi

Questo comportamento si applica alle richieste CAPWAP originate da AP, quali:

- Individuazione
- Partecipa
- scambi relativi alla configurazione
- transazioni di controllo crittografate
- Richieste echo

Questi parametri vengono appresi dal controller durante la configurazione del join AP.

Impronta digitale diagnostica nelle acquisizioni di pacchetti

Il modello di ritrasmissione è spesso utile per la risoluzione dei problemi.

Modello di ritrasmissione	Origine probabile
Ritrasmissioni equidistanti, circa ogni 3 secondi	Ritrasmissione lato controller
Ritrasmissioni che si diffondono nel tempo, ad esempio 6s,	ritrasmissione lato AP con backoff

Modello di ritrasmissione	Origine probabile
12s, 24s, 48s, 96s	esponenziale

Questo è un modo pratico per determinare quale parte sta riprovando, soprattutto in caso di errori di join o problemi correlati all'eco.

Operazioni eseguite quando i tentativi sono esauriti

Se le ritrasmissioni continuano senza ricevere la risposta prevista, entrambe le parti alla fine si arrendono, ma le loro azioni di recupero sono diverse.

Lato controller

Se il controller esaurisce il budget per i tentativi, interrompe il processo di trasmissione e termina la sessione AP. In questo modo le sessioni di dati e di controllo CAPWAP verranno chiuse.

Lato AP

Se l'access point esaurisce i propri tentativi, abbandona il controller e ricomincia dall'inizio, in genere tornando alla fase di individuazione e tentando un full rejoin.

Manopole e impostazioni predefinite della configurazione

Il comportamento di ritrasmissione è controllato da due impostazioni principali nel profilo di join AP.

Comando	Valore predefinito	Funzione
conteggio ritrasmissioni capwap	5	Numero massimo di tentativi di ritrasmissione
intervallo di ritrasmissione capwap	3 secondi	Intervallo di ritrasmissione di base

Questi valori influiscono sia sull'affidabilità del join che su altri tentativi di controllo CAPWAP originati da AP, inclusi i tentativi correlati all'eco.

Riferimento timer consolidato

La tabella contiene un riepilogo dei principali timer CAPWAP discussi in questo articolo.

Timer	Valore predefinito	Piano	Proprietario	Descrizione
Intervallo eco di controllo	30 secondi	Controllo	AP	Se l'access point non trasmette il traffico di controllo CAPWAP per 30 secondi, invia una richiesta echo.
Controlla timer inattività heartbeat	90 secondi	Controllo	Controller	Il controller prevede un traffico di controllo valido all'interno di questa finestra. Se non viene ricevuto alcun messaggio, la sessione di controllo viene considerata inattiva.
Intervallo di ritrasmissione controllo	3 secondi	Controllo	Controller	Il controller ritrasmette le proprie richieste CAPWAP senza risposta a un intervallo fisso.
Conteggio ritrasmissioni controllo	5 tentativi	Controllo	Controller	Numero massimo di tentativi per le richieste CAPWAP originate dal controller. Negli scenari con catena a margherita cablata, questo valore può aumentare fino a 15 tentativi.
Ritrasmissione backoff controllo AP	6, 12, 24, 48, 96 secondi	Controllo	AP	L'access point ritrasmette le proprie richieste CAPWAP utilizzando un backoff esponenziale.
Intervallo keepalive dei dati	30 secondi	Dati	AP	In condizioni normali, l'access point invia un data keepalive ogni 30 secondi.
Riprova backoff di Data keepalive	3, 6, 12, 15, 15 secondi	Dati	AP	Se una risposta keepalive dei dati viene persa, l'access point tenta di utilizzare il backoff, limitandolo a 15 secondi.
Intervallo inattività	180 secondi	Dati	AP	Se l'access point non riesce a mantenere lo

Timer	Valore predefinito	Piano	Proprietario	Descrizione
del canale dati				scambio di dati keepalive entro questo periodo, dichiara inattivo il tunnel di dati.

Differenze affiancate

Keepalive e ritrasmissione

Anche se a volte sono confusi, keepalive e ritrasmissione servono a scopi diversi.

Aspetto	Mantenimento attività	Ritrasmissione
Scopo principale	Verifica che il peer sia ancora raggiungibile	Riprova una richiesta specifica quando non viene ricevuta alcuna risposta
Ambito	Per sessione o per canale	Per messaggio
Fattore scatenante	Timeout di inattività o attività	Una richiesta rimane senza risposta
Metodo di verifica	Basato sul tempo	Basato sul conteggio dei tentativi
Significato errore	Impossibile raggiungere il canale o la sessione	Uno scambio CAPWAP specifico si è verificato più volte
Risultato errore	La sessione può essere dichiarata inattiva	Il controller può terminare la sessione oppure l'access point può riavviare il join

Stringhe del log di traccia RA per meccanismo

Per il trace specifico del punto di accesso, raccogliere i log per il punto di accesso e cercare queste stringhe esatte.

Raccolta registri

Utilizzo:

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

Controllo keepalive/heartbeat

Cerca:

- Gestione richiesta echo
- Genera risposta echo
- Risposta echo inviata per la richiesta con numero di sequenza <N>.
- Il timer di heartbeat è stato riavviato con il nuovo valore <ms>
- Tocco timer heartbeat richiamato
- Scadenza timer heartbeat

Data keepalive

Cerca:

- Data keepalive ricevuto
- set di dati già stabilito
- DTLS dati non stabilito
- Aggiornamento della voce del tunnel di dati CAPWAP
- Impossibile elaborare i dati keepalive. Motivo: Sessione CAPWAP non in stato di esecuzione o di configurazione
- Messaggio keepalive non valido, nessun blocco capwap
- Messaggio keepalive non valido, nessun MAC WTP
- Impossibile elaborare keepalive. Sessione CAPWAP non trovata
- Data keep-alive ricevuto su una porta diversa dalla porta di controllo: <porta>
- Data keep-alive ricevuto per punto di accesso <mac> diverso
- Impossibile aggiornare le informazioni sulla tupla di dati nella tabella di sessione WTP per l'host remoto: <ip>
- Impossibile aggiornare la voce del tunnel dati CAPWAP

Gestione keepalive del piano dati

Cerca:

- Dati ricevuti da keep-alive da <src> a <dst>
- Risposta keep-alive dei dati inviata <enc/plain>
- Eliminazione del pacchetto keep-alive dall'indirizzo IP: <ip>, sessione sconosciuta
- Eliminazione del pacchetto keep-alive dall'indirizzo IP: <ip>,, impossibile ottenere lo stato DTLS dei dati
- Impossibile inviare la risposta keep-alive dei dati
- Impossibile caricare il messaggio keep-alive dei dati

Ritrasmissione

Cerca:

- ritrasmissione timer callback
- Ritrasmissione del numero di sequenza <N> perché è in coda e non è ancora stato recuperato
- Ritrasmissione del messaggio: Tentativo di ritrasmissione di <msg-name>: <M>
- voce con numero seq: <N> è in coda per <S> secondi. Nessuna ritrasmissione
- Sessione CAPWAP terminata. Numero massimo di ritrasmissioni scadute per: <messaggio> ...
- Pulizia delle risorse della sessione CAPWAP al congedo da AP.

Disinstallazione sessione

Cerca:

- Chiusura della sessione AP CAPWAP.
- Chiudere la sessione CAPWAP DTLS.
- chiusura sessione di controllo capwap-dtls
- chiusura sessione dati capwap-dtls
- Ultimo pacchetto di controllo ricevuto <S> secondi fa.
- Ultimo pacchetto Keep Alive dei dati ricevuto <S> secondi fa.
- Sessione CAPWAP DTLS chiusa per il punto di accesso. Causa: <motivo>

Esempi:

Scenario di lavoro

Verifica debug AP

Questo comando debug AP può essere usato per monitorare il controllo CAPWAP e la

comunicazione keepalive dei dati tra l'AP e il WLC.

```
#debug capwap client event
```

I log di debug mostrano che la sequenza di comunicazione CAPWAP è riuscita.

Alle 13:11:44, l'access point ha trasmesso una richiesta Echo CAPWAP al WLC sulla porta UDP 5246. Durante lo stesso intervallo, l'access point ha anche trasmesso un pacchetto CAPWAP Data Keepalive sulla porta UDP 5247. I log confermano che il WLC ha risposto correttamente a entrambe le richieste.

I timestamp indicano un normale ciclo di comunicazione CAPWAP:

- 13:11:44.0917 - Richiesta echo trasmessa.
- 13:11:44.0918 - Trasmissione di Data Keepalive.
- 13:11:44.0926 - Dati conservati ricevuti dal WLC.
- 13:11:44.0940 - Risposta echo ricevuta dal WLC.

Questi timestamp confermano che sia il controllo CAPWAP che i canali dati funzionano come previsto con una latenza di andata e ritorno trascurabile.

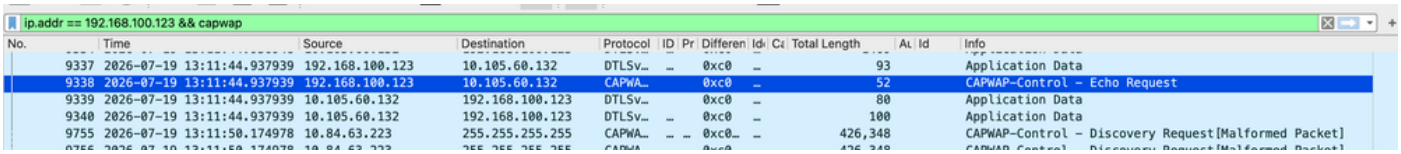
```
[*07/19/2026 13:11:14.0817] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0917] Echo Request: Send count 22
[*07/19/2026 13:11:44.0917] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: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

Convalida pacchetti CAPWAP Control (porta UDP 5246)

Analisi acquisizione pacchetti

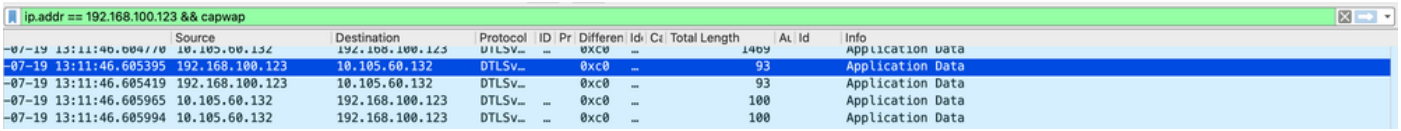
L'acquisizione del pacchetto conferma che l'access point ha generato una richiesta Echo CAPWAP alle 13:11:44 sulla porta UDP 5246.

Il WLC ha ricevuto il pacchetto, ha elaborato la richiesta e ha generato immediatamente la risposta echo corrispondente. Poiché il canale di controllo CAPWAP è protetto tramite crittografia DTLS, la risposta viene visualizzata come dati dell'applicazione crittografati nell'acquisizione del pacchetto.



Verifica pacchetto switch

L'acquisizione dei pacchetti dello switch conferma che i pacchetti di controllo CAPWAP crittografati sono stati ricevuti correttamente dal WLC e inoltrati all'access point.

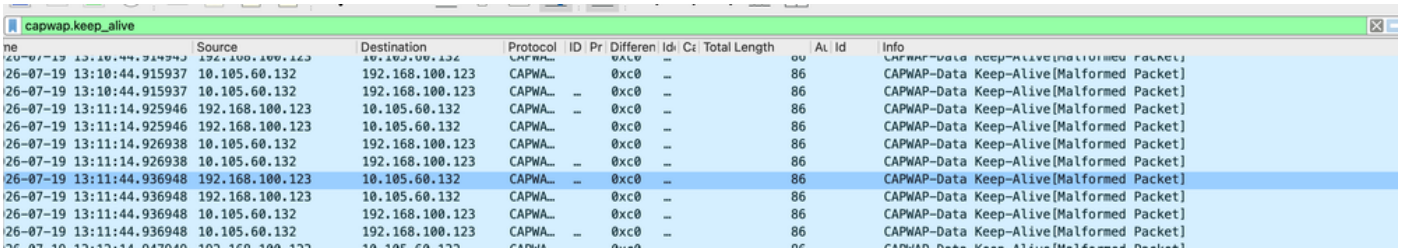


Convalida CAPWAP Data Keepalive (porta UDP 5247)

L'access point trasmette periodicamente pacchetti CAPWAP Data Keepalive sulla porta UDP 5247 per verificare lo stato del tunnel di dati CAPWAP.

Alle 13:11:44, l'access point ha trasmesso un pacchetto Data Keepalive verso il WLC. Il WLC ha ricevuto il pacchetto con esito positivo e ha risposto immediatamente con la corrispondente risposta keepalive.

Il buon esito di questo scambio conferma che il percorso dei dati CAPWAP rimane operativo e che la comunicazione bidirezionale tra l'access point e il WLC funziona normalmente

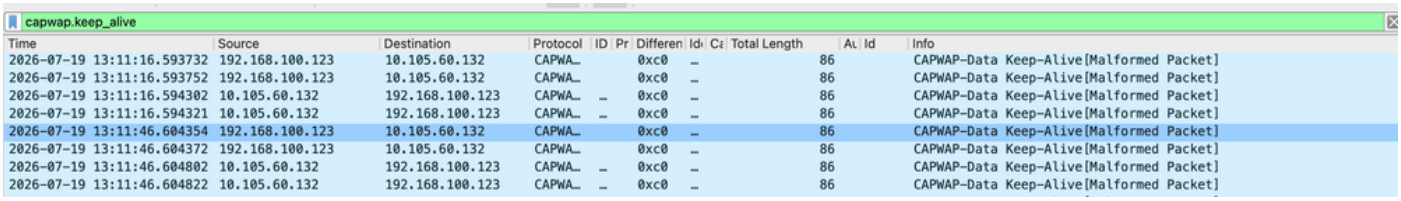


Verifica pacchetto switch

L'acquisizione dei pacchetti dello switch convalida ulteriormente che i pacchetti CAPWAP Data Keepalive sono stati inoltrati correttamente tra l'AP e il WLC senza interruzione.

Il flusso di pacchetti osservato conferma che:

- I pacchetti Data Keepalive hanno raggiunto il WLC.
- Il WLC ha generato la risposta keepalive prevista.
- Lo switch ha inoltrato la risposta al punto di accesso.
- Nessuna perdita di pacchetti nel percorso di inoltro.


capwap.keep_alive

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

Pacchetti di controllo (UDP 5246) ignorati sullo switch Uplink AP

Questo test mostra il comportamento di un access point quando la porta di controllo CAPWAP (UDP 5246) viene rilasciata sullo switch di uplink dell'access point.

L'obiettivo è quello di convalidare il comportamento di AP, WLC e rete quando ai pacchetti di controllo CAPWAP viene impedito di raggiungere l'AP, malgrado il WLC riesca a elaborare e a rispondere correttamente alle richieste.

In questo scenario:

- L'access point continua a trasmettere le richieste echo CAPWAP verso il WLC.
- Il WLC riceve ed elabora correttamente ogni richiesta echo.
- Il WLC genera la risposta echo corrispondente.
- Lo switch di uplink AP riceve la risposta ma non la inoltra all'access point.
- Poiché l'access point non riceve mai la risposta echo, supera il numero massimo di ritrasmissioni e riavvia la macchina a stati CAPWAP.

Analisi di debug AP

Alle 12:11:55.4568, l'access point ha trasmesso una richiesta CAPWAP Echo verso il WLC sulla porta UDP 5246.

Richiesta echo: Conteggio invii 0

A differenza dello scenario di lavoro normale, non è stata ricevuta alcuna risposta echo. Di conseguenza, l'access point ha iniziato le ritrasmissioni in base al timer CAPWAP predefinito.

Le ritrasmissioni si sono verificate in corrispondenza dei seguenti timestamp:

Ora	Evento
12:12:00.2587	Conteggio ritrasmissioni = 1
12:12:03.2599	Conteggio ritrasmissioni = 2
12:12:06.2610	Conteggio ritrasmissioni = 3
12:12:09.2624	Conteggio ritrasmissioni = 4
12:12:12.2637	Conteggio ritrasmissioni = 5

Dopo la quinta ritrasmissione non riuscita, l'access point ha dichiarato che la sessione di controllo CAPWAP non è raggiungibile.

Alle 12:12:15.2647, l'AP ha riferito:

È stato superato il numero massimo di ritrasmissioni. Verrà ripristinata la modalità DISCOVER.

Subito dopo, l'access point ha riavviato la macchina a stati CAPWAP per avviare un nuovo processo di rilevamento.

```
[*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
```

Le tracce RA WLC confermano che il controller non ha riscontrato problemi di elaborazione.

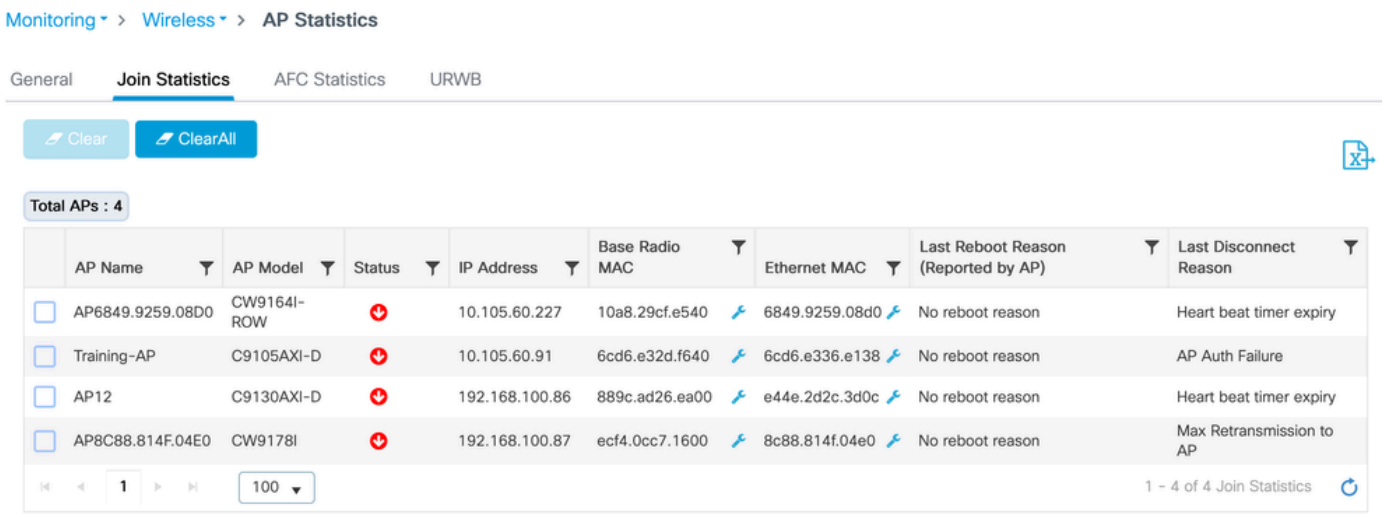
Alle 12:11:58.731835712, il WLC ha ricevuto la richiesta Echo CAPWAP trasmessa dall'access point. Questi log dimostrano che il WLC ha elaborato la richiesta con successo e ha generato la risposta appropriata. In seguito, alle 12:12:19.802183814, il WLC ha ricevuto una notifica di chiusura DTLS dall'access point. L'access point si è disconnesso perché non ha mai ricevuto le risposte echo trasmesse dal controller. Di conseguenza, il WLC ha terminato la sessione DTLS e registrato la disassociazione dell'access point.

<#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>

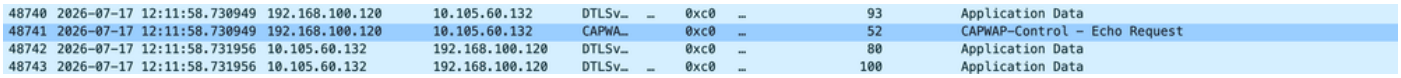
```
VK-WLC#show wireless stats ap history | i AP12


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
```

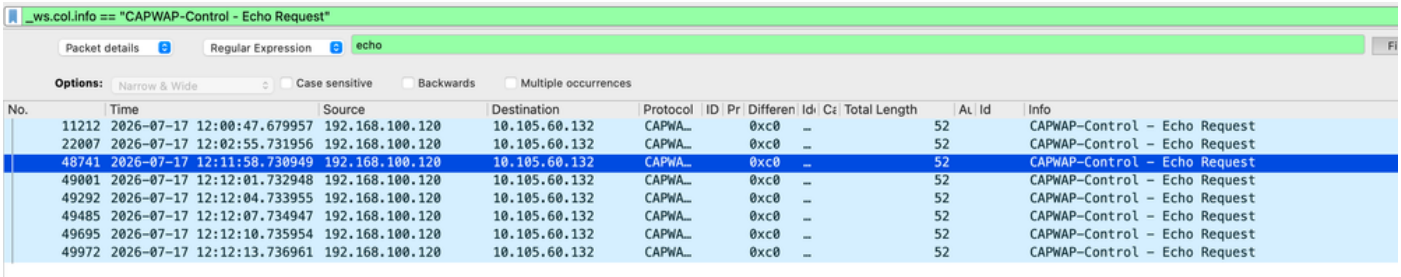


L'EPC del WLC conferma che:

- Allo stesso tempo, la richiesta Echo CAPWAP ha raggiunto il WLC.
- Il WLC ha generato una risposta echo CAPWAP crittografata.
- La risposta viene visualizzata come Dati applicazione, poiché il traffico di controllo CAPWAP è protetto dalla crittografia DTLS.

L'EPC conferma pertanto che il controllore ha trasmesso la risposta con esito positivo, eliminando il WLC come origine del problema.





Le acquisizioni dei pacchetti raccolte sullo switch uplink dell'access point forniscono l'evidenza finale.

Le immagini acquisite dimostrano che:

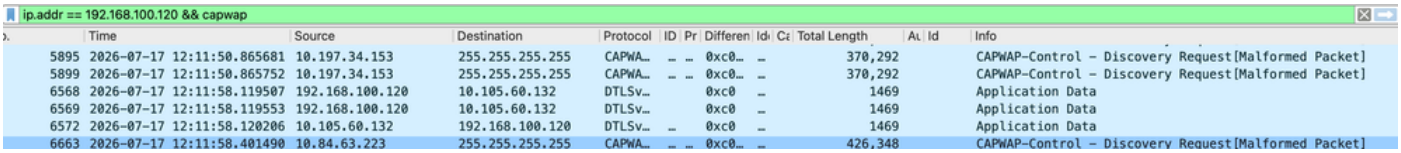
- Lo switch ha ricevuto correttamente la risposta echo crittografata trasmessa dal WLC.

- La risposta è visibile come Dati applicazione, il che è previsto a causa della crittografia DTLS.
- La risposta non è stata inoltrata al punto di accesso.

Questo spiega perché:

- L'access point non ha mai ricevuto la risposta echo CAPWAP.
- L'AP ha continuato a ritrasmettere le richieste echo.
- Il contatore di ritrasmissione ha infine superato la soglia configurata.
- L'access point ha riavviato la macchina a stati CAPWAP.

Le immagini acquisite identificano chiaramente lo switch come il punto in cui il traffico di controllo CAPWAP è stato interrotto


ip.addr == 192.168.100.120 && capwap

	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ca	Total Length	Au	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]

CAPWAP Data Port (UDP 5247) scaricata sullo switch Uplink AP

Questo test convalida il comportamento dell'access point quando la porta dati CAPWAP (UDP 5247) viene rilasciata sullo switch uplink AP mentre la porta di controllo CAPWAP (UDP 5246) rimane operativa.

A differenza dello scenario precedente, l'AP continua a mantenere la connessione di controllo CAPWAP con il WLC scambiando correttamente i messaggi Echo CAPWAP sulla porta UDP 5246. Tuttavia, poiché i pacchetti CAPWAP Data Keepalive non sono in grado di completare il round trip, l'access point dichiara infine il percorso dei dati CAPWAP come non raggiungibile e avvia un riavvio di CAPWAP.

I log di debug dell'access point confermano che il canale di controllo CAPWAP è rimasto operativo per tutto il test.

All'inizio dell'acquisizione, le richieste echo CAPWAP trasmesse sulla porta UDP 5246 hanno continuato a ricevere risposte echo valide dal WLC, confermando la comunicazione ininterrotta tra il control plane.

Tuttavia, alle 14:30:15, l'access point ha trasmesso un pacchetto CAPWAP Data Keepalive sulla porta UDP 5247. Poiché non è stata ricevuta alcuna risposta Data Keepalive corrispondente, l'access point ha avviato il meccanismo dei nuovi tentativi. Le ritrasmissioni possono essere

osservate ai seguenti timestamp:

Timestamp	Evento
14:30:15	Initial Data Keepalive trasmesso
14:30:19	Nuovo tentativo 1
14:30:25	Riprova 2
14:30:37	Riprova 3
14:30:49	Riprova 4
14:31:01	Riprova 5
14:31:13	Nuovo tentativo finale

Sebbene le risposte echo CAPWAP continuino a essere ricevute durante questo periodo, l'access point non ha ricevuto alcuna risposta per i pacchetti Data Keepalive. Dopo aver esaurito i tentativi, l'access point ha segnalato un timeout di Data Keepalive non crittografato e ha avviato un riavvio di CAPWAP. Verso le 14:31:16, l'access point ha terminato la sessione CAPWAP esistente e ha restituito il processo di individuazione.

```
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)...
```

Per il canale dati CAPWAP, le tracce indicano che il controller non ha ricevuto i pacchetti Data Keepalive previsti. Alla fine, dopo che l'access point ha dichiarato l'errore Data Keepalive, il WLC ha registrato la chiusura della sessione DTLS e l'evento disjoin dell'access point. La sequenza osservata nelle tracce RA conferma che il controller è rimasto operativo finché l'access point non si è disconnesso volontariamente a causa del timeout di Data Keepalive.

Tracce RSA con MAC Ethernet AP:

<#root>

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

 Last Data Keep Alive Packet received 90 seconds ago.


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

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

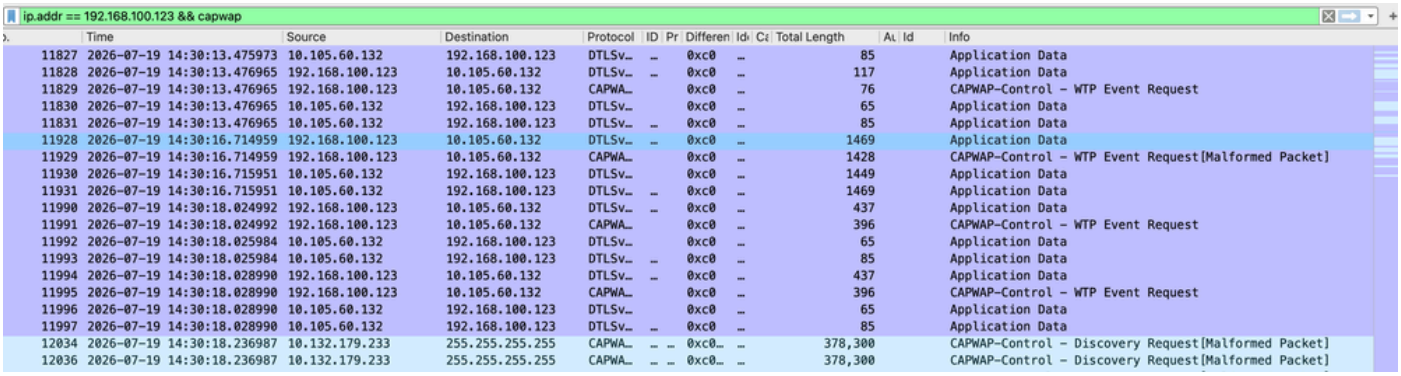
Tracce RA con Radio Mac:

<#root>

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

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


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

L'EPC raccolto sul WLC convalida l'elaborazione dei pacchetti sul lato controller. Le acquisizioni confermano che i pacchetti di controllo CAPWAP hanno continuato a essere scambiati correttamente durante il test, ma che non è stato ricevuto alcun pacchetto keepalive dei dati sul WLC. Questa osservazione è in linea con i log di debug dell'AP e dimostra che il meccanismo

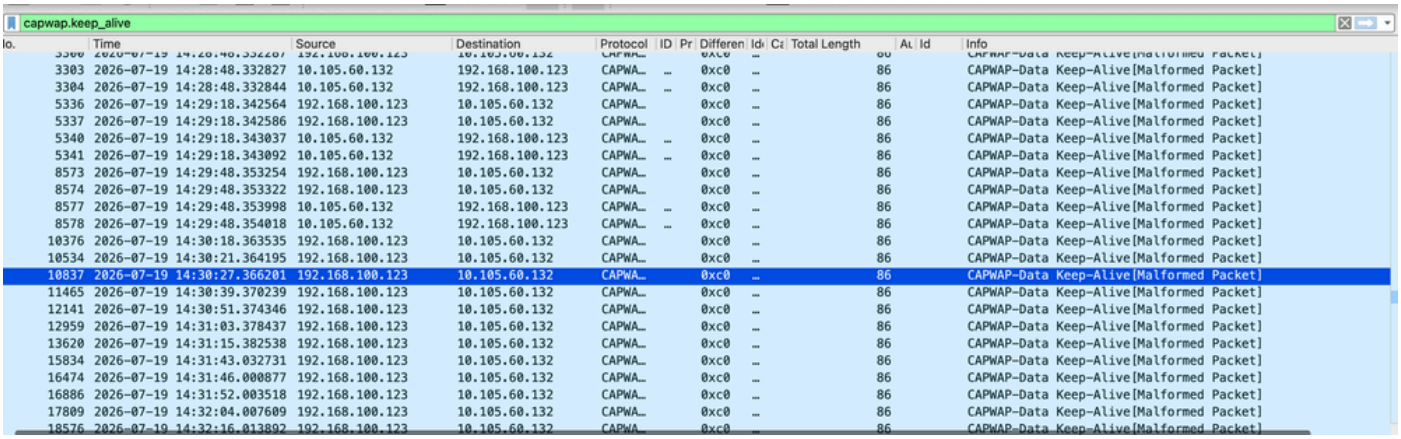
Data Keepalive non è riuscito nonostante il canale di controllo sia rimasto attivo.


ip.addr == 192.168.100.123 && capwap

	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ca	Total Length	Au	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	10.105.60.132	192.168.100.123	DTLSv…			0xc0	…		1449			Application Data
11931	2026-07-19 14:30:16.715951	10.105.60.132	192.168.100.123	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	10.105.60.132	192.168.100.123	DTLSv…			0xc0	…		65			Application Data
11993	2026-07-19 14:30:18.025984	10.105.60.132	192.168.100.123	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	10.105.60.132	192.168.100.123	DTLSv…			0xc0	…		65			Application Data
11997	2026-07-19 14:30:18.028990	10.105.60.132	192.168.100.123	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:

Le acquisizioni dei pacchetti raccolte sullo switch uplink AP mostrano che i pacchetti erano presenti sullo switch ma non sono stati inoltrati al wlc


capwap.keep_alive

	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ca	Total Length	Au	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	10.105.60.132	192.168.100.123	CAPWA…	…		0xc0	…		86			CAPWAP-Data Keep-Alive[Malformed Packet]
5341	2026-07-19 14:29:18.343092	10.105.60.132	192.168.100.123	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	10.105.60.132	192.168.100.123	CAPWA…	…		0xc0	…		86			CAPWAP-Data Keep-Alive[Malformed Packet]
8578	2026-07-19 14:29:48.354018	10.105.60.132	192.168.100.123	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]

CAPWAP - Data Keepalive disabilitato

Questa funzione è stata introdotta con l'ID bug Cisco CSCvs6015

Questa funzione è utile per la risoluzione dei problemi relativi a questi scenari.

1. Risoluzione dei problemi di disconnessione dei punti di accesso: Dopo aver disattivato Capwap data keep-alive, è possibile verificare se il punto di accesso si sta ancora disconnettendo a causa di Capwap control keep-alive e identificare la causa principale delle disconnessioni del punto di accesso keep-alive.
2. Evitare le disconnessioni dovute a capwap data-keepalive come soluzione fino a quando non si identifica il motivo per cui i dati capwap devono essere conservati.
3. Sniffer AP in installazioni flex di filiali collegate tramite collegamento WAN con throughput

ridotto. Se si desidera raccogliere le acquisizioni di pacchetti OTA configurando uno degli access point in modalità sniffer, tutti i pacchetti acquisiti vengono trasmessi al WLC attraverso il collegamento WAN utilizzando la porta dati capwap. In questo modo, si sovraccarica il collegamento WAN e si ha un impatto sulla filiale completa.

4. Se si disabilita il keep-alive dei dati capwap per l'access point in modalità sniffer e si crea un ACL in un branch per eliminare i pacchetti di dati capwap dall'access point specifico, l'access point rimane connesso perché il controllo capwap funziona correttamente e quindi è possibile raccogliere l'OTA dalla porta dello switch dell'access point senza sovraccaricare il collegamento WAN con le acquisizioni dei pacchetti.

Attivare l'opzione COS-AP data keepalive per abilitare/disabilitare il protocollo da 9800 WLC. Per impostazione predefinita, i dati keepalive sono abilitati sia nel WLC che nell'access point.

Comando WLC:

1) Visualizzare lo stato con la stringa "Unencrypted Data Keep Alive"

```
show ap config general
```

2) Abilita/Disabilita keepalive dei dati con nome ap

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

Attivare l'abilitazione/disabilitazione dei dati keepalive COS-AP dallo stesso access point. Per impostazione predefinita, il comando data keepalive è abilitato nell'access point.

Comando AP:

1) Visualizzare lo stato con la stringa "Unencrypted Data Keep Alive"

```
show capwap client config
```

2) Abilitare/Disabilitare i dati keepalive nell'access point

```
capwap ap unencrypted_data_keepalive enable
```

```
capwap ap unencrypted_data_keepalive disable
```

Ad esempio:

Controllo keepalive disattivato a livello 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
```

Debug dell'AP:

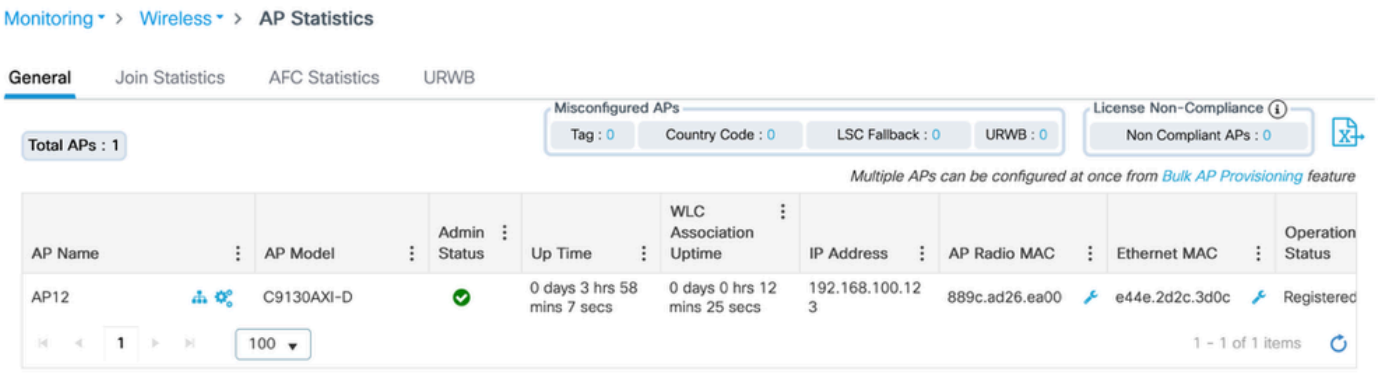
Durante il debug del pacchetto ap, è possibile verificare che lo scambio di pacchetti keepalive tra l'access point e il wlc non ha luogo, è sufficiente controllare lo scambio di pacchetti.

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
```

Anche se i pacchetti keepalive dei dati sono stati scartati, ma dal momento che abbiamo disabilitato il controllo keepalive dei dati, possiamo vedere che l'AP rimane stabile sul wlc senza essere influenzato dal calo dei pacchetti keepalive.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).