

Catalyst 9800 WLCでのCAPWAPキープアライブの説明とトラブルシューティング

内容

[はじめに](#)

[CONTEXT](#)

[2つの異なるチャネル、2つの異なるメカニズム](#)

[CAPWAP再送信](#)

[統合タイマーリファレンス](#)

[横に並んだ相違点](#)

[メカニズム別のRAトレースログ文字列](#)

[例:](#)

[正常動作シナリオ](#)

[CAPWAP制御パケットの検証 \(UDPポート5246\)](#)

[CAPWAPデータキープアライブ検証 \(UDPポート5247\)](#)

[制御パケット\(UDP 5246\)がAPアップリンクスイッチでドロップされる](#)

[APアップリンクスイッチでCAPWAPデータポート\(UDP 5247\)がドロップされる](#)

[CAPWAPデータキープアライブの無効化](#)

はじめに

このドキュメントでは、CAPWAP制御キープアライブ、データキープアライブ、および再送信について説明します。

CONTEXT

CAPWAPは、Cisco Catalyst 9800プラットフォーム上のCiscoアクセスポイントとワイヤレスLANコントローラ間の通信フレームワークを提供します。これは、定義されたキープアライブおよび再送信メカニズムとともに、個別の制御チャネルとデータチャネルを使用して接続を維持します。

この記事では、CAPWAP制御キープアライブ、データキープアライブ、および再送信について、関連するタイマー、障害の動作、および主なトラブルシューティングインジケータを含めて説明します。

2つの異なるチャネル、2つの異なるメカニズム

CAPWAPは2つのUDPチャンネルで実行され、それぞれに独自の活性メカニズムがあります

チャンネル	デフォルトポート(UDP)	活力機構
Control	5246	エコー要求/エコー応答
データ	5247	データチャンネルキープアライブ

CAPWAP制御キープアライブ (エコー/ハートビート)

目的

CAPWAP制御キープアライブは、アクセスポイントが制御チャンネルでまだ到達可能であることを確認するために使用されます。

その目的は非常にシンプルです。APとコントローラの間の制御接続がまだ有効で応答できることを確認します。設定の更新やクライアントデータの伝送には使用されません。代わりに、UDPポート5246経由のCAPWAP制御パスの活性メカニズムとして機能します。

キープアライブの送信者

アクセスポイントとは、コントロールキープアライブをアクティブに開始するデバイスです。

必要に応じて、APはコントローラにCAPWAPエコー要求を送信します。コントローラは、対応するエコー応答を返します。この応答は、コントローラが要求を受信したこと、および制御チャンネルが両方向で機能していることを確認します。

この応答は要求に一致するため、APは送信したキープアライブに対する有効な応答を受信していることを確認できます。

この動作は、コントロールキープアライブが主にコントローラ駆動型のポーリングメカニズムではないことを示すため、重要です。代わりに、APが制御チャンネルの到達可能性をチェックし、コントローラがそれに応じて応答します。

エコー間隔は、固定スケジュールではなく、非アクティブに基づいています

これは、CAPWAP制御キープアライブに関して最もよく誤解されている側面の1つです。

一般的には、APは固定定期的ハートビートのように30秒ごとにエコ要求を送信すると想定されています。実際には、その仕組みではありません。

コントロールキープアライブは、コントロールチャネルの非アクティビティに基づいています。つまり、コントロールチャネルが設定された間隔アイドル状態であった場合にのみ、APはスタンダロンのエコ要求を送信します。APとコントローラの間で他の制御トラフィックがすでに交換されている場合は、別のエコパケットを送信する必要はありません。

APとコントローラの間で有効な制御通信があれば、制御チャネルが有効であることを効果的に証明できます。そのため、通常のCAPWAP制御トラフィックによってキープアライブタイマーがリセットされます。

このような制御トラフィックの例には、次のものがあります。

- 設定の交換
- Radio Resource Management(RRM)アップデート
- WLAN関連のコントロールメッセージ
- クライアント関連の制御イベント
- 統計情報または状態同期メッセージ
- 通常動作の一部として交換されるその他のCAPWAP制御パケット

その結果、スタンダロンのエコ要求は、制御チャネルが他の点では静かな期間にのみ見られます。

簡単な例

AP上のCAPWAPエコタイマーを確認するには、show capwap client timerコマンドを使用します。

```
<#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

タイマー

制御キープアライブメカニズムは、2つの重要なタイミング値に依存しています。

項目	デフォルト値	説明
エコー間隔	30 秒	APがスタンドアロンのエコー要求を送信するまでのコントロールチャンネルの非アクティブな時間
コントローラ制御デッドタイマー	90 seconds	制御セッションのデッドを宣言する前に、コントローラが有効な制御トラフィックを受信せずに許可する最大時間

制御キープアライブが失敗した場合

コントロールチャンネルが許可されたタイムアウトよりも長く無音になると、コントローラは最終的にコントロールセッションが失われるように宣言します。

この時点で、コントローラはAPをコントロールチャンネルで到達不能と見なし、セッションティアダウンを開始します。これには通常、コントロール接続のクローズと、APのアクティブなコントロールセッションステートの削除が含まれます。

その後、APは障害のシナリオに応じて、コントローラを再検出して再加入することで、接続の再確立を試みます。

トラブルシューティングの影響

このキープアライブ動作を理解することは、トラブルシューティングの際に不可欠です。

エコーパケットが欠落していても、必ずしも問題があるとは限りません

パケットキャプチャで30秒ごとにエコー要求が表示されない場合、障害は自動的には示されません。これは単に、他に十分な数のCAPWAP制御トラフィックが流れていることを意味するだけな

ので、スタンドアロンのエコーは必要ありません。

通常、不規則なエコー間隔は正常です

エコーは非アクティブによってトリガーされるため、不均等な間隔で表示されることがあります。これは正常な動作です。

全体的な制御チャネルのアクティビティに集中

APの接続解除をトラブルシューティングする際には、次の点を確認するとより便利です。

- ・ コントローラはAPからCAPWAP制御トラフィックを受信し続けていますか。
- ・ コントロールチャネルはdeadタイマーをトリガーするのに十分な期間サイレントですか。
- ・ 制御パスだけに影響を与えるネットワークの問題はありますか。
- ・ パケット損失、ファイアウォールの動作、NATの問題、またはコントロールプレーンのドロップがUDP 5246トラフィックを中断していますか。

実際の問題は、定期的なエコーパケットが単独で存在しないことではありません。実際の問題は、コントローラがAPを到達不能と宣言するまで制御チャネル通信が失われることです。

CAPWAPデータキープアライブ

目的

CAPWAP制御エコーは制御チャネルが機能していることを確認しますが、データチャネルも正常であることを証明するものではありません。コントロールパスとデータパスはそれぞれ独立して失敗する可能性があるため、CAPWAPはUDPポート5247で個別のデータキープアライブを使用します。

データキープアライブの目的は次のとおりです。

- ・ apがデータチャネル上のコントローラにまだ到達できることを確認する
- ・ apのデータトンネル状態を維持する
- ・ データパスのみに影響する障害の検出を支援する

送信者とコントローラの応答方法

APがデータキープアライブを送信し、コントローラがデータキープアライブ応答で応答します。

応答は、データチャネル暗号化が有効かどうかに応じて、暗号化または非暗号化にすることができます。

キープアライブが有効であれば、コントローラはそれを使用して、APのデータパスがまだ到達可能であることを確認します。パケットが有効なAPセッションに一致しない場合、または応答を送信できない場合、キープアライブはドロップされ、最終的にデータパスは失敗したと見なすことができます。

コントローラによる検証方法

コントローラは、キープアライブを受け入れる前に、パケットが正しいAPに属していることを確認するための基本的な検証を実行します。

コントローラは次のことを確認します。

- キープアライブに有効なCAPWAP情報が含まれている
- apの無線MACアドレスが存在する
- パケットをAPセッションに一致させることができる

コントローラはまず、送信元IPアドレスと送信元UDPポートを使用してセッションの識別を試みます。これに失敗すると、AP無線MACアドレスの使用にフォールバックできます。

これは、データチャネルがコントロールチャネルとは異なる変換されたUDPポートから到着できる、NATまたはPATの背後にあるAPにとって重要です。このような場合、コントローラはAPの実際のデータチャネルタプルを学習して更新できます。

パケットが、そのIPポートの組み合わせにすでに関連付けられているセッションとは異なるAPに属していると考えられる場合、不正なセッションマッピングを防ぐために、キープアライブは拒否されます。

検証後の動作

キープアライブが受け入れられると、コントローラはAPの現在のセッション状態に基づいてキープアライブを処理します。

- データセッションがすでに確立されている場合、キープアライブは活性を更新するだけです。
- これが最初の有効なデータキープアライブである場合、コントローラはこれを使用してAPのデータチャネル情報を学習または更新し、データトンネルの確立を完了できます。

この最初のキープアライブは、APがNATまたはPATの背後にある場合を含め、コントローラがデータトンネルを正しくプログラムするのに役立つため、特に重要です。

データセッションが完全に確立されると、以降のキープアライブは通常の定常状態パスに従い、活性を維持するためだけに使用されます。

重要な動作

有効なデータキープアライブでは、データパスの状態を確認する以上の処理が行われます。また、コントローラ上でのAPの全体的なセッション活性も更新されます。

つまり、コントローラでは、データチャネルの活性がAPセッション全体の健全性に寄与します。その結果、制御とデータの活性メカニズムは、目的は異なっても関連しています。

AP側のデータキープアライブタイマー

APはデータキープアライブインターバルを制御し、データトンネルがダウンしたと見なす必要があるタイミングを決定します。

項目	デフォルト値
データキープアライブ間隔	30 秒
再送信バックオフ	3秒、6秒、12秒、次に15秒
データデッド間隔	180 seconds

通常の状況では、APは30秒ごとにデータキープアライブを送信します。

APが応答を受信しない場合、APはバックオフパターンを使用して再試行します。障害が180秒間続くと、APはデータトンネルダウンを宣言します。

CAPWAP再送信

原理：両方向で動作する信頼性

CAPWAP制御メッセージングは、UDP上で動作するにもかかわらず、要求と応答のモデルを使用

します。信頼性を提供するため、要求を送信したデバイスは、期待される応答が受信されるまで要求を再送信する役割も担います。

これは、再送信が対称であることを意味します。

- 設定の更新など、コントローラからAPへの要求の場合、コントローラが再送信を処理します。
- ディスカバリ、加入、設定ステータス、イメージ関連のメッセージ、およびエコ要求などのAPからコントローラへの要求では、APが再送信を処理します。

これは重要なトラブルシューティングのポイントです。パケットキャプチャでAPからコントローラへの再送信が発生する場合、通常は、期待される応答を受信しなかったために、APが単に自身の要求を再試行していることを意味します。これは加入中は正常で、制御エコアクティビティ中にも発生する可能性があります。

コントローラ側の再送信動作

コントローラでは、再送信は専用の送信信頼性状態マシンによって処理されます。

簡単に言うと、コントローラは次のことを実行します。

1. 確認応答を必要とする要求を受け入れます
2. ap単位の送信キューに配置する
3. 要求を送信する
4. 一致する応答を待つ
5. 応答が到着したときにパケットをキューから削除するか、タイマーが切れたときに再送信します

このロジックは、APセッションごとに個別に追跡されます。コントローラは、送信ウィンドウと未処理の要求メッセージの数も保持します。

コントローラが再送信するかどうかを決定する方法

再送信タイマーが期限切れになるたびに、コントローラはキューに入れられた要求エントリを確認し、次のいずれかの決定を行います。

1. 応答は既に順序が正しくありません

その要求に対する応答がすでに受信されている場合、それが誤った順序で到着した場合でも、コントローラはメッセージを再送信しません。

2. Retry limit exceeded

要求がすでに許容回数を超えて再送信されている場合、コントローラはこれを障害として扱い、そのAPセッションの送信プロセスを中断します。

この時点で、APセッションが終了します。

3. 要求の古さがまだ足りません

コントローラは、すべてのタイマーイベントで、キューに入れられたすべてのメッセージをただちに再送信するわけではありません。要求は、再送信の資格が得られるまでに、少なくとも再送信間隔の間はキューに留まっている必要があります。

デフォルトでは、この再送信間隔は3秒です。

4. 要求を再送信する

要求がまだ保留中で、十分な時間が経過し、再試行制限を超えていない場合、コントローラはCAPWAP制御チャネルでそれを再送信し、再試行カウンタを増やします。

特殊なケース：有線デイジーチェーンAP

有線のデイジーチェーンAPパスを使用したメッシュ導入では、コントローラはより大きなリトライ予算を可能にします。

この場合、通常のリトライ制限は実質的に3倍になります。

デフォルトのリトライ回数が5の場合、コントローラは失敗を宣言する前に最大15回リトライできます。

この例外が存在するのは、これらのトポロジでは遅延やメッセージ損失に対する許容度が高くなる場合があるためです。

AP側の再送信動作

APは自身のCAPWAP要求も再送信しますが、コントローラとは異なるパターンを使用します。

コントローラでは固定再送信間隔を使用し、APでは指数関数的なバックオフを使用します。これは、試行が失敗するたびに待機時間が長くなることを意味します。

デフォルトの設定では、AP再試行タイミングは約：

- 6 seconds
- 12 秒
- 24 seconds
- 48 seconds
- 96 seconds

この動作は、次のようなAP発信CAPWAP要求に適用されます。

- ディスカバリ
- 加入
- 設定関連の交換
- 暗号化制御トランザクション
- エコー要求

これらの再試行パラメータは、AP加入設定の一部としてコントローラから取得されます。

パケットキャプチャの診断フィンガープリント

再送信パターン自体は、トラブルシューティング時に役立つ手がかりとなることがよくあります。

再送信パターン	考えられる原因
約3秒ごとに均等な間隔で再送信	コントローラ側の再送信
6秒、12秒、24秒、48秒、96秒など、時間の経過とともに広がる再送信	指数関数的なバックオフを伴うAP側の再送信

これは、特に接続障害やエコー関連の問題の発生時に、再試行している側を判別するための実用的な方法です。

リトライが枯渇した場合の動作

期待される応答を受信せずに再送信が続くと、両側が最終的に応答を断念しますが、復旧処理は異なります。

コントローラ側

コントローラは、再試行バジェットを使い果たした場合、送信プロセスを中断し、APセッションを終了します。その結果、CAPWAP制御およびデータセッションが閉じられます。

AP側

APはそれ自体の再試行回数を使い切ると、そのコントローラを放棄し、最初からやり直します。通常は、ディスカバリフェーズに戻り、完全な再加入を試行します。

設定ノブとデフォルト

再送信動作は、AP加入プロファイルの2つの主要な設定によって制御されます。

コマンド	デフォルト値	機能
CAPWAP再送信数	5	再送信の最大試行回数
CAPWAP再送信間隔	3 秒	基本再送信間隔

これらの値は、接続の信頼性と、エコー関連の再試行を含む、APから発信されたその他のCAPWAP制御の再試行の両方に影響します。

統合タイマーリファレンス

次の表は、このドキュメントで説明した主なCAPWAPタイマーをまとめたものです。

タイマー	デフォルト値	平面	主催者 (Owner)	説明
制御エコー間隔	30 秒	Control	AP	APがCAPWAP制御トラフィックを30秒間送信しない場合、APはエコー要求を送信します。
ハートビートのデッドタイマーの制御	90 seconds	Control	コントローラ	コントローラは、このウィンドウ内で有効な制御トラフィックを想定しています。何も受信されない場合、制御セッションはダウンしていると見なされます。
制御再送信間	3 秒	Control	コントローラ	コントローラは、応答のない独自のCAPWAP要

タイマー	デフォルト値	平面	主催者 (Owner)	説明
隔			ラ	求を一定の間隔で再送信します。
再送信回数の制御	5回	Control	コントローラ	コントローラから発信されたCAPWAP要求の最大再試行回数。有線のデイジーチェーンのシナリオでは、これは15回まで試行される可能性があります。
AP制御再送信バックオフ	6、12、24、48、96秒	Control	AP	APは、指数関数的なバックオフを使用して、自身のCAPWAP要求を再送信します。
データキープアライブ間隔	30 秒	データ	AP	通常の場合では、APは30秒ごとにデータキープアライブを送信します。
データキープアライブリトライバックオフ	3、6、12、15、15秒	データ	AP	データキープアライブ応答が失われた場合、APはバックオフを使用して15秒の制限で再試行します。
データチャネルデッド間隔	180 seconds	データ	AP	この期間内にAPがデータキープアライブ交換を正常に維持できなかった場合、APはデータトンネルダウンを宣言します。

横に並んだ相違点

キープアライブと再送信

混同されることもありますが、キープアライブと再送信の目的は異なります。

アспект	キープアライブ	再送信
主な目的	ピアがまだ到達可能であることを確認します。	応答を受信しないときに特定の要求を再試行する
対象範囲	セッション単位またはチャネル単	メッセージごと

アспект	キープアライブ	再送信
	位	
トリガー	非アクティブまたは活性タイムアウト	要求に対する応答がありません
トラッキング方式	時間ベース	再試行回数ベース
失敗の意味	チャネルまたはセッションに到達できなくなった	特定のCAPWAP交換が繰り返し失敗した
失敗の結果	セッションがダウンしていると宣言できる	コントローラがセッションを終了するか、APが加入を再開できる

メカニズム別のRAトレースログ文字列

AP固有のトレースの場合は、APのログを収集して、これらの正確な文字列を検索します。

ログ収集

利用:

- debug wireless mac <AP無線MAC>
- show logging profile wireless filter mac <ap-radio-mac> to-file bootflash:<ファイル>

キープアライブ/ハートビートの制御

検索:

- エコー要求の処理
- エコー応答の生成
- シーケンス番号<N>の要求に対するエコー応答が送信されました。
- ハートビートタイマーが新しい値<ms>で再起動しました
- ハートビートタイマタッチが呼び出されました
- ハートビートタイマーの期限切れ

データキープアライブ

検索：

- データキープアライブの受信
- データサービスはすでに確立されています
- データDTLSが確立されていない
- CAPWAPデータトンネルエントリの更新
- データキープアライブを処理できませんでした。理由：CAPWAPセッションが実行状態または構成状態でない
- 無効なキープアライブメッセージ、capwapブロックなし
- Invalid keepaliveメッセージ、no WTP MAC
- キープアライブの処理に失敗しました。CAPWAPセッションが見つかりません。
- データのキープアライブが制御ポート<port>以外の異なるポートで受信される
- 異なるAP <mac>でデータキープアライブが受信される
- リモートホスト<ip>のWTPセッションテーブルのデータタプル情報を更新できませんでした。
- CAPWAPデータトンネルエントリを更新できませんでした

データプレーンのキープアライブ処理

検索：

- <src>から<dst>にデータのキープアライブを受信
- <enc/plain>データキープアライブ応答を送信
- IPからキープアライブパケットをドロップしています：<ip>、不明なセッション
- IP <ip>からキープアライブパケットをドロップしています。データのDTLSステータスを取得できませんでした。
- データのキープアライブ応答を送信できませんでした
- Loadbalancing data keep-aliveメッセージが失敗しました

再送信

検索：

- 再送信タイマーコールバック
- seqnum <N>はキュー内にあるがまだackを取得していないため、再送信します。
- Retransmitting message: <msg-name> retransmit attempt: <M> (再送メッセージ：<msg-name> retransmit attempt: <M>)
- シーケンス番号<N>のエントリが<S>秒間キューに入っています。再転送しない
- CAPWAPセッションが終了し、<msg>の最大再送信期限が切れました...
- AP脱退でのCAPWAPセッションリソースのクリーンアップ

セッションティアダウン

検索：

- AP CAPWAPセッションを終了しています。
- CAPWAP DTLSセッションを閉じます。
- capwap-dtls制御セッションの終了
- capwap-dtlsデータセッションの終了
- 最後の制御パケットが<S>秒前に受信されました。
- 最後のデータキープアライブパケットが<S>秒前に受信されました。
- APに対してCAPWAP DTLSセッションが閉じられました。原因：

例:

正常動作シナリオ

APデバッグの検証

このAP debugコマンドを使用すると、APとWLCの間のCAPWAP制御およびデータキープアライブ通信を監視できます。

```
#debug capwap client event
```

次のデバッグログは、正常なCAPWAP通信シーケンスを示しています。

13:11:44に、APはCAPWAPエコー要求をUDPポート5246経由でWLCに送信しました。同じインターバルの間に、APはCAPWAPデータキープアライブパケットをUDPポート5247経由で送信しました。ログは、WLCが両方の要求に正常に応答したことを示しています。

タイムスタンプは、通常のCAPWAP通信サイクルを示します。

- 13:11:44.0917 – エコー要求が送信されました。
- 13:11:44.0918 : データキープアライブが送信されました。
- 13:11:44.0926 - WLCから受信したデータキープアライブ
- 13:11:44.0940 - WLCから受信したエコー応答。

これらのタイムスタンプは、CAPWAP制御チャネルとデータチャネルの両方が期待通りに機能し

ており、ラウンドトリップ遅延が無視できる程度であることを確認します。

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

CAPWAP制御パケットの検証 (UDPポート5246)

パケットキャプチャ分析

パケットキャプチャにより、APがUDPポート5246経由で13:11:44にCAPWAPエコー要求を生成したことが確認できます。

WLCはパケットを正常に受信し、要求を処理し、対応するエコー応答を即座に生成しました。CAPWAP制御チャネルはDTLS暗号化を使用して保護されるため、応答は暗号化されたアプリケーションデータとしてパケットキャプチャに表示されます。

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

スイッチパケットの検証

スイッチパケットキャプチャは、暗号化されたCAPWAP制御パケットがWLCから正常に受信され、APに転送されたことを示します。

No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cs	Total Length	At	Id	Info
97-19	13:11:46.605395	192.168.100.123	10.105.60.132	DTLSv...	...	0xc0	...	...	...	93	...	...	Application Data
13:11:46.605419	192.168.100.123	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	...	...	93	...	...	Application Data
13:11:46.605965	10.105.60.132	192.168.100.123	192.168.100.123	DTLSv...	...	0xc0	...	...	...	100	...	...	Application Data
13:11:46.605994	10.105.60.132	192.168.100.123	192.168.100.123	DTLSv...	...	0xc0	...	...	...	100	...	...	Application Data

CAPWAPデータキープアライブ検証 (UDPポート5247)

APは定期的にUDPポート5247を介してCAPWAPデータキープアライブパケットを送信し、CAPWAPデータトンネルの健全性を確認します。

13:11:44に、APからWLCに向けてデータキープアライブパケットが送信されました。WLCはパケットを正常に受信し、対応するキープアライブ応答を即座に返しました。

この正常な交換により、CAPWAPデータパスが引き続き動作可能であり、APとWLCの間の双方向通信が正常に機能していることが確認されます

capwap_keep_alive											
Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cs	Total Length	At	Id
26-07-19 13:10:44.915937	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:10:44.915937	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:44.936948	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:44.936948	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
26-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-

スイッチパケットの検証

スイッチパケットキャプチャでは、CAPWAPデータキープアライブパケットがAPとWLCの間で中断なく正常に転送されたことをさらに検証します。

確認されたパケットフローにより、次のことが確認されます。

- データキープアライブパケットがWLCに正常に到達しました。
- WLCが期待されるキープアライブ応答を生成しました。
- スイッチは応答をAPに転送しました。
- 転送パスでパケット損失は発生しませんでした。

capwap_keep_alive											
Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cs	Total Length	At	Id
2026-07-19 13:11:16.593732	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:16.593752	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:16.594302	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:16.594321	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:46.604354	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:46.604372	192.168.100.123	10.105.60.132	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:46.604802	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-
2026-07-19 13:11:46.604822	10.105.60.132	192.168.100.123	CAPWA	0xc0	-	-	-	-	86	-	-

制御パケット(UDP 5246)がAPアップリンクスイッチでドロップされる

このテストでは、APアップリンクスイッチでCAPWAPコントロールポート(UDP 5246)がドロップされたときのAPの動作を確認します。

目的は、WLCが要求の処理と応答に成功したにもかかわらず、CAPWAP制御パケットがAPに到達できない場合のAP、WLC、およびネットワークの動作を検証することです。

このシナリオでは次のようになっています。

- APはWLCに対してCAPWAPエコ要求の送信を続行します。
- WLCは、各エコ要求を正常に受信して処理します。
- WLCは、対応するエコ応答を生成します。
- APアップリンクスイッチは応答を受信しますが、APに転送しません。
- APはエコ応答を受信しないため、最終的に最大再送信回数を超え、CAPWAPステートマシンを再起動します。

APデバッグ分析

12:11:55.4568の時点で、APはCAPWAPエコ要求をUDPポート5246経由でWLCに送信しています。

エコ要求：送信カウント0

通常の動作シナリオとは異なり、エコ応答は受信されませんでした。その結果、APはデフォルトのCAPWAPタイマーに従って再送信を開始します。

再送信は次のタイムスタンプで行われました。

[Time]	[Event]
12:12:00.2587	再送信カウント= 1
12:12:03.2599	再送信カウント= 2
12:12:06.2610	再送信カウント= 3
12:12:09.2624	再送信カウント= 4
12:12:12.2637	再送信カウント= 5

5回目の再送信の失敗の後、APはCAPWAP制御セッションを到達不能と宣言しました。

12:12:15.2647の時点で、APは次を報告しました。

最大再送信数を超えました。DISCOVERモードに戻ります。

その直後に、APはCAPWAPステートマシンを再起動して、新しいディスカバリプロセスを開始しました。

```
[*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
```

WLC RAトレースにより、コントローラで処理の問題が発生しなかったことが確認されます。

12:11:58.731835712の時点で、WLCはAPによって送信されたCAPWAPエコー要求を正常に受信しています。これらのログは、WLCが要求を正常に処理し、適切な応答を生成したことを示しています。その後、12:12:19.802183814でWLCがAPからDTLS Close Notifyを受信しました。コントローラから送信されたエコー応答を受信しなかったため、APは切断されました。その結果、WLCはDTLSセッションを終了し、APのアソシエーション解除を記録しました。

<#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

Monitoring > Wireless > AP Statistics

GeneralJoin StatisticsAFC StatisticsURWB

ClearClearAll

Total APs : 4

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

1 - 4 of 4 Join Statistics

WLC EPCは次のことを確認します。

- 同じタイムスタンプで、CAPWAPエコー要求はWLCに正常に到達しました。
- WLCは暗号化されたCAPWAPエコー応答を生成しました。
- CAPWAP制御トラフィックはDTLS暗号化によって保護されているため、応答はApplication Dataと表示されます。

したがって、EPCはコントローラが応答を正常に送信したことを確認します。 これにより、WLCが問題の原因でなくなります。

48740 2026-07-17 12:11:58.730949 192.168.100.120 10.105.60.132 DTLSv... 93 Application Data

48741 2026-07-17 12:11:58.730949 192.168.100.120 10.105.60.132 CAPWA... 52 CAPWAP-Control - Echo Request

48742 2026-07-17 12:11:58.731956 10.105.60.132 192.168.100.120 DTLSv... 80 Application Data

48743 2026-07-17 12:11:58.731956 10.105.60.132 192.168.100.120 DTLSv... 100 Application Data

_ws.col.info == "CAPWAP-Control - Echo Request"

Packet detailsRegular Expressionecho

Options: Narrow & WideCase sensitiveBackwardsMultiple occurrences

No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cz	Total Length	At	Id	Info
11212	2026-07-17 12:00:47.679957	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
22007	2026-07-17 12:02:55.731956	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
48741	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
49001	2026-07-17 12:12:01.732948	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
49292	2026-07-17 12:12:04.733955	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
49485	2026-07-17 12:12:07.734947	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
49695	2026-07-17 12:12:10.735954	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request
49972	2026-07-17 12:12:13.736961	192.168.100.120	10.105.60.132	CAPWA...	0xc0	...	...	...	...	52	...	...	CAPWAP-Control - Echo Request

APアップリンクスイッチで収集されたパケットキャプチャが、最終的な証拠となります。

キャプチャは次のことを示しています。

- スイッチは、WLCによって送信された暗号化されたエコー応答を正常に受信しました。
- 応答はアプリケーションデータとして表示されます。これは、DTLS暗号化が原因で発生します。
- 応答はAPに転送されませんでした。

その理由は次のとおりです。

- APはCAPWAPエコー応答を受信しませんでした。
- APはエコー要求の再送信を続行しました。
- 再送信カウンタが、最終的に設定されたしきい値を超えました。
- APはCAPWAPステートマシンを再起動しました。

パケットキャプチャは、CAPWAP制御トラフィックが中断されたポイントとしてスイッチを明確に特定します

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

APアップリンクスイッチでCAPWAPデータポート(UDP 5247)がドロップされる

このテストでは、CAPWAPコントロールポート(UDP 5246)が稼働している状態で、APアップリンクスイッチでCAPWAPデータポート(UDP 5247)がドロップされた場合のAPの動作を検証します。

前のシナリオとは異なり、APはUDPポート5246経由でCAPWAPエコーメッセージを正常に交換することで、WLCとのCAPWAP制御接続を維持し続けます。ただし、CAPWAPデータキープアライブパケットはラウンドトリップを完了できないため、APは最終的にCAPWAPデータパスを到達不能と宣言し、CAPWAPの再起動を開始します。

APデバッグログは、CAPWAP制御チャネルがテストを通じて正常に動作していたことを確認します。

キャプチャの開始時に、UDPポート5246を介して送信されたCAPWAPエコー要求はWLCからの有効なエコー応答の受信を継続し、コントロールプレーン通信が中断されないことを確認しました。

ただし、14:30:15の場合、APではCAPWAPデータキープアライブパケットをUDPポート5247経由で送信しています。 対応するデータキープアライブ応答が受信されなかったため、APは再試行メカニズムを開始しました。 再送信は、次のタイムスタンプで確認できます。

タイムスタンプ	[Event]
14:30:15	最初のデータキープアライブの送信
14:30:19	再試行1
14:30:25	再試行2
14:30:37	再試行3
14:30:49	再試行4
14:31:01	再試行5
14:31:13	最終的な再試行

この間、CAPWAPエコー応答は受信され続けましたが、APはデータキープアライブパケットに対する応答を受信しませんでした。 再試行の試行回数を超過すると、APからUnencrypted Data Keepalive Timeoutが報告され、CAPWAPの再起動が開始されました。 約14:31:16に、APは既存のCAPWAPセッションを終了し、ディスカバリプロセスに戻りました。

```
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)...
```

CAPWAPデータチャネルの場合、トレースは、コントローラが予期されるデータキープアライブパケットを受信しなかったかのどちらかを示します。最終的に、APがデータキープアライブ障害を宣言した後、WLCはDTLSセッションの終了とAPの切断イベントを記録しました。RAトレースで確認されるシーケンスにより、データキープアライブタイムアウトが原因でAPが自発的に接続解除されるまで、コントローラは動作し続けたことが確認されます。

AP ethernet macを使用したRAトレース：

<#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)

Radio MACを使用したRAトレース：

<#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
```

WLC上で収集されたEPCによって、コントローラ側のパケット処理が検証されます。キャプチャは、CAPWAP制御パケットがテスト全体を通じて正常に交換され続けたが、WLCでデータキープ

アライブパケットが受信されなかったことを示しています。この観察結果は、APのデバッグログと一致し、コントロールチャネルがアクティブのままであるにもかかわらず、データキープアライブメカニズムが失敗したことを示しています。

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

スイッチ：

APアップリンクスイッチで収集されたパケットキャプチャは、パケットがスイッチに存在するものの、同じものがWLCに転送されなかったことを示します

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

CAPWAPデータキープアライブの無効化

この機能は、Cisco Bug ID CSCvs66015

この機能は、これらのシナリオのトラブルシューティングに役立ちます。

1. APの切断のトラブルシューティング：CAPWAPデータキープアライブを無効にした後、APがCAPWAP制御キープアライブにより切断し続けているかどうかを確認し、APキープアライブ切断の根本原因を特定できます。
2. CAPWAPデータキープアライブのドロップの原因を特定するまでの回避策として、CAPWAPデータキープアライブによる切断を避けてください。

3. ブランチのフレックス展開におけるスニファAPは、低スループットのWANリンクを介して接続されます。APの1つをスニファモードに設定してOTAパケットキャプチャを収集する場合、キャプチャされたすべてのパケットは、capwapデータポートを使用して、WANリンク経由でWLCに送信されます。その場合、WANリンクに過大な負荷がかかり、ブランチ全体に影響を及ぼします。
4. スニファモードでAPのcapwapデータキープアライブを無効にし、ブランチでACLを作成して、具体的なAPからのcapwapデータパケットをドロップする場合、capwap制御が適切であるためAPは接続されたままになり、パケットキャプチャでWANリンクを圧迫することなくAPスイッチポートからOTAを収集できます。

9800 WLCからのCOS-APデータキープアライブのイネーブル/ディセーブルをトリガーします。デフォルトでは、WLCとAPの両方のデータキープアライブがイネーブルになっています。

WLCコマンド：

- 1)文字列「Unencrypted Data Keep Alive」でステータスを表示します。

```
show ap config general
```

- 2) AP名によるデータキープアライブのイネーブル/ディセーブル

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

AP自体からCOS-AP data keepalive enable/disableをトリガーします。デフォルトでは、APのデータキープアライブは有効になっています。

APコマンド：

- 1)文字列「Unencrypted Data Keep Alive」でステータスを表示します。

```
show capwap client config
```

- 2) APでのデータキープアライブのイネーブル/ディセーブル

```
capwap ap unencrypted_data_keepalive enable
```

```
capwap ap unencrypted_data_keepalive disable
```

例：

APレベルでキープアライブチェックを無効にした場合：

```
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 のデバッグ：

APのデバッグでは、APとWLCの間でデータキープアライブパケット交換が発生していないことがわかります。制御パケット交換だけが確認できます。

```
AP12#debug capwap client keepalive ( クライアントキープアライブのデバッグ )
```

```
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
```

データキープアライブパケットがドロップされていても、データキープアライブチェックを無効にしているため、APはキープアライブパケットのドロップの影響を受けることなくWLC上で安定しています。

Monitoring > Wireless > AP Statistics

General

Join Statistics

AFC Statistics

URWB

Misconfigured APs

Tag : 0

Country Code : 0

LSC Falback : 0

URWB : 0

License Non-Compliance ⓘ

Non Compliant APs : 0



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

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

1 - 1 of 1 items

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。