インテリジェントキャプチャの管理

インテリジェントキャプチャについて

Cisco DNA Center では、デバイスやクライアントの正常性に関するすべての情報は、通常シスコ ワイヤレス コントローラから入手できます。インテリジェントキャプチャ機能は Cisco DNA Center とアクセスポイント（AP）間の直接通信リンクをサポートしているため、各 AP は Cisco DNA Center と直接通信できます。Cisco DNA Center はこのチャネルを使用して、パケットキャプチャデータ、AP とクライアントの統計情報、およびスペクトルデータを受信できます。インテリジェントキャプチャ機能は、Cisco DNA Center と AP 間の直接通信リンクを利用することで、ワイヤレスコントローラからはアクセスできないデータに AP からアクセスできるようにします。

（注）
- インテリジェントキャプチャは、ローカルモードまたは FlexConnect モードの AP でのみサポートされます。
- インテリジェントキャプチャは、SDA 展開ではサポートされていません。

インテリジェントキャプチャ対応デバイス

インテリジェントキャプチャをサポートするシスコ ワイヤレス コントローラを次の表に示します。

サポート対象の Cisco Catalyst ワイヤレスコントローラ	
デバイス	サポート対象の最小ソフトウェアバージョン
Cisco 3504 ワイヤレス コントローラ	AireOS 8.8.125.0
Cisco 5520 ワイヤレス コントローラ	AireOS 8.8.125.0
Cisco 8540 ワイヤレス コントローラ	AireOS 8.8.125.0

インテリジェントキャプチャをサポートする Cisco Catalyst ワイヤレスコントローラを次の表に示します。

サポート対象の Cisco Catalyst ワイヤレスコントローラ	
デバイス	サポート対象の最小ソフトウェアバージョン
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	IOS-XE Gibraltar 16.12.1.s

インテリジェントキャプチャをサポートする Cisco AP を次の表に示します。

サポート対象の Cisco AP		
デバイス	サポート対象 AireOS ソフトウェアの最小バージョン	サポート対象 IOS-XE ソフトウェアの最小バージョン
Aironet 1540 AP[1]	8.10.105.0	16.12.1.s
Aironet 1560 AP	8.10.105.0	16.12.1 s
Aironet 1815 AP [1]	8.10.105.0	16.12.1 s
Aironet 1830 AP [1]	8.10.105.0	16.12.1 s
Aironet 1840 AP [1]	8.10.105.0	16.12.1 s
Aironet 1850 AP [1]	8.10.105.0	16.12.1 s
Aironet 2800 シリーズ AP	8.8.125.0 または 8.10	16.12.1s
Aironet 3800 シリーズ AP	8.8.125.0 または 8.10	16.12.1s
Aironet 4800シリーズ AP [2]	8.8.125.0 または 8.10	16.12.1s
Catalyst 9105 AP[1]	8.10 MR3	17.3.1
Catalyst 9115 AP [1]	8.10.105.0	16.12.1 s

サポート対象の **Cisco AP**		
デバイス	サポート対象 **AireOS** ソフトウェアの最小バージョン	サポート対象 **IOS-XE** ソフトウェアの最小バージョン
Catalyst 9120 AP	8.10.105.0 8.10.112.0（スペクトル解析向け）	16.12.1s 17.2.1（スペクトル解析向け）
Catalyst 9130 AP [2]	8.10 MR3	17.3.1
Catalyst IW6300 Heavy Duty シリーズ AP	8.10.105.0	17.1.1s
Catalyst ESW6300 組み込みサービス AP	8.10.105.0	17.1.1s

[1] スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、Catalyst 9105 AP、および Catalyst 9115 AP ではサポートされていません。

[2] データパケットキャプチャは、Aironet 4800 AP および Catalyst 9130 AP のみでサポートされます。

インテリジェントキャプチャのベストプラクティス

インテリジェントキャプチャ機能を Cisco DNA Center で確実に最適化するためのベストプラクティスを以下で紹介します。

- 新しいワイヤレス コントローラ デバイスを Cisco DNA Center に追加したら、インテリジェントキャプチャのグローバル設定を無効にしてから、設定を再度有効にします。これで、新しいワイヤレスコントローラにインテリジェントキャプチャが設定されます。
- Cisco DNA Center からワイヤレス コントローラ デバイスを削除する前に、すべてのインテリジェントキャプチャ設定を無効にします。
- 管理対象のワイヤレスコントローラのアップグレードや Cisco DNA Center の再イメージ化の前に、すべてのインテリジェントキャプチャ設定を無効にします。アップグレード完了後に設定を再度有効にします。

クライアントデバイス向けのライブおよびスケジュール済みキャプチャセッション

クライアントデバイス向けのキャプチャセッションについて

クライアントデバイスに対して、次の種類のキャプチャセッションを実行できます。

オンボーディングパケットキャプチャセッションは、クライアントデバイスがワイヤレスネットワークに参加するために使用するパケット（802.11 管理フレーム、DHCP、EAP パケットなど）をキャプチャし、クライアントの RF 統計（5 秒のサンプル）を収集します。このデータは [Client 360] > [Intelligent Capture] ページに表示されます。セッションは、すぐに開始することも（[Run Now]）、後で実行するようにスケジュールすることもできます。セッションのデフォルトの持続時間は 30 分で、最大 8 時間に設定されています。デフォルトでは、最後にクライアントに接続されたワイヤレスコントローラでキャプチャが有効になっています。クライアント ローミング シナリオに対応するワイヤレスコントローラを 3 つまで選択できます。

オンボーディング キャプチャ セッションの制限事項

オンボーディング キャプチャ セッションの制限事項は次のとおりです。

- キャプチャセッション（ライブおよびスケジュール済み）には合計 16 個のタイムスロットが割り当てられています。セッション内の各クライアントは1つのタイムスロットを使用します。

  ライブキャプチャセッションの最大数は 16 であるため、16 のライブキャプチャセッションが同時に実行されている場合は、スケジュール済みキャプチャセッションに使用できるスロットはありません。

  同時に実行可能なスケジュール済みキャプチャセッションは、最大 12 です。このため、常に 4 個（16 - 12）のスロットがライブキャプチャセッション用に確保されています。

  たとえば、17個目のライブキャプチャセッションを開始しようとすると、この最大値を超えるため、次のエラーメッセージが表示されます。エラーメッセージのダイアログボックスで [Yes] をクリックし、次に終了するライブキャプチャセッションを選択します。

（注） 16個のタイムスロット制限は、ワイヤレスコントローラによって適用されます。

キャプチャセッションが Cisco DNA Center で設定されている場合、Cisco DNA Centerが認識していないライブキャプチャセッションやスケジュール済みのキャプチャセッションはすべて削除されます（ワイヤレスコントローラで直接設定された部分的なパケット キャプチャ セッションなど）。

- オンボーディングイベント期間中は、オンボーディングイベントに関連した最大 100 パケットのキャプチャが可能です。
- Cisco DNA Center に格納するすべてのスケジュール済みオンボーディング パケット ファイルの合計サイズには、3.5 GB の制限があります。制限を超えると、合計サイズが 3.5 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

クライアント統計情報について

グローバル設定のオンボーディング パケット キャプチャ セッションを使用すると、サポート対象の AP でクライアント統計情報を 5 秒間隔で収集できます。

クライアント統計情報は、クライアントが接続されている AP で AP 統計が有効になっている場合にも 30 秒間隔で収集されます。

収集されたクライアント統計情報は、**[Client 360]** > **[Intelligent Capture]** ウィンドウの 4 つの RF 統計情報チャートに表示されます。

クライアントデバイスのライブキャプチャセッションの有効化

以下の手順により、特定のクライアントデバイスに対してライブキャプチャセッションを有効にし、オンボーディングイベントと RF 統計情報のデータパケットを表示できます。

ステップ 1 [Health]左上隅にあるメニューアイコンをクリックして次を選択します：**アシュアランス** > 。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

[クライアントの健全性（Client Health）] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- **[クライアントデバイス（Client Devices）]** 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索（Search）] フィールド（右上端）に次のいずれかを入力します。ユーザ ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレス。

クライアント デバイスの 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンがクライアント名の横に表示される場合は、クライアントまたはアクセスポイントがインテリジェント キャプチャ データを送信できない Cisco DNA Center （33 ページ） で詳細を確認してください。

図 *1* : クライアントの *[Intelligent Capture]* ウィンドウ

ステップ 5 タイムラインスライダは、次の機能に使用できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。ライブキャプチャの結果については、オンボーディングイベントの折れ線グラフが表示されます。緑色はオンボーディングイベント、赤色は異常イベントを示します。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注） タイムラインには、最長で過去 2 週間のデータを表示できます。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

ステップ 6 ライブキャプチャセッションを実行するには、次の手順を実行します。

a) ライブキャプチャセッションを開始するには、右上隅にある [Start Live Capture] をクリックします。

ライブキャプチャセッション中、[Onboarding Events] と [RF Statistics] ダッシュレットのデータパケットが収集されます。

b) ライブキャプチャセッションを停止するには、[Stop Capturing] ボタンをクリックします。

（注） ライブキャプチャセッションは3時間実行されます。3時間が経過すると、セッションを延長するためのダイアログボックスが表示されます。

c) 実行中のライブキャプチャセッションは、クライアントの [Intelligent Capture Settings] ウィンドウで確認できます。

ステップ7 ネットワーク接続の確立に関連付けられているイベントを表示するには、[Onboarding Events ダッシュレットを使用します。

[Onboarding Events] ダッシュレット	
アイテム	**説明**
[All] および Anomaly PCAP フィルタ	オンボーディングイベントをフィルタ処理できます。次のオプションがあります。 • [All]：すべてのイベントを表示します。これはデフォルトです。 • Anomaly PCAP：異常イベントのみをフィルタ処理します。 （注） クライアントがネットワークに参加する際に問題が発生した場合は、特定のイベントの横に「PCAP」という語が赤色で表示されます。 クライアントが問題なくネットワークに参加できる場合は、特定のイベントの横に「PCAP」という語が灰色で表示されます。
Export PCAP	指定されたイベントの範囲のパケットをダウンロードできます。 **1.** [Export PCAP] をクリックします。 **2.** PCAP に含める最初と最後のイベントを指定します。 **3.** ダウンロードを開始するには、[Download PCAP] ボタンをクリックします。 （注） ヒューリスティックを使用してイベントに属するパケットを判断するため、最初のイベントの1分前と最後のイベントの1分後のパケットがダウンロードに含まれます。これにより、すべての関連するパケットがダウンロードされたPCAPに含まれるようになります。 各エクスポートに含まれるのは、最もタイムスタンプが古いものから2000パケットまでに制限されます。

[Onboarding Events] ダッシュレット	
アイテム	説明
オンボーディング、不完全、および異常イベントのリスト	オンボーディング、不完全、および異常イベントのリストを時系列順に表示します。イベントは、以下を示すために色分けされています。 ● : 正常なオンボーディングイベント。 ● : 不完全なイベント。 ● : 異常イベント。 （注） アイコン付きのイベントは、このイベントのデータパケットがダウンロードまたは分析のためにキャプチャされていることを示します。 親イベントグループをクリックすると、グループを展開して、そのグループの個々のイベントを表示できます。

[Onboarding Events] ダッシュレット	
アイテム	説明
Event Details	イベントグループまたは個々のイベントをクリックすると、次のセクションでさらに詳細情報を表示できます。 [Client Location]：イベント中のクライアントの場所のマップとクライアントの移動のマップが表示されます。 [Auto Packet Analyzer]：このセクションは、ライブキャプチャ、スケジュールされたキャプチャ、または異常キャプチャセッションがイベントのパケットをキャプチャした場合に表示されます。イベントの横に表示される アイコンは、イベントによってパケットがキャプチャされたことを示します。 [Auto Packet Analyzer] セクションには、次の情報を含むグラフが表示されます。 • イベントを囲むパケット（最大 100 個）は、次の 2 つのグループに分けられます。グレーのセクションは、オンボーディングセッション開始前のパケットを示します。白のセクションは、オンボーディングセッション内のパケットを示します。 認証解除パケットと予期しないパケットのパターンは赤色の三角形で表されます。これらは、クライアントのオンボーディングエクスペリエンスを低下させる可能性のある重要な意味を持つパケットです。 [Download Packets] をクリックすると詳細分析のためにパケットをダウンロードできます。 • パケット（クライアントまたは AP からのパケット） • オンボードパケットのステージ識別子 • パケット間ギャップ（ms） • パケットごとの RSSI（dBm） • 関連付けられている AP [RF Statistics]：イベントを囲む 10 分間隔の RF 統計データを使用したグラフが表示されます。 RF 統計データは、RSSI および SNR 測定値（デシベル単位）、Rx 平均データレートと Rx 最終データレート、Tx パケットと Rx パケット、および Tx パケットの再試行で構成されます。 （注） [Anomaly Capture] が有効になっている場合、ライブまたはスケジュールされたキャプチャが実行されていない場合でも、異常イベントのパケットはキャプチャされます。

ステップ 8 [Client Location] ダッシュレットでは、フロアマップを表示して次の情報を確認できます。

- フロア上のクライアントと AP の場所。
- カバレッジの強度を色の濃淡で視覚化したヒートマップ
- フロアマップ上のクライアントのリアルタイムロケーション。クライアントが別の場所に移動すると、その移動が表示されます。
- RF 統計情報（RSSI、SNR、データレート、スループット、およびパケットドロップレート）を使用して接続が色分け表示されたクライアント証跡トラッキング。

  マップ上の色は、クライアントの正常性を示します。

  ● : 良い ● : 平均 ● : 悪い
- 選択したオンボーディングイベントの時間を含む 1 分間のクライアントのトラッキング。
- マップの下のリプレイおよび停止/開始のコントロールを使用すると表示をコントロールできます。

（注） クライアントロケーション機能を使用するには、CMX が Cisco DNA Center と統合されている必要があります。詳細については、「ワイヤレスマップ向け Cisco CMX の統合」の章を参照してください。

ステップ 9 [RF Statistics] ダッシュレットでは、RF 情報の詳細を確認できます。

クライアントの AP クライアント統計情報は、4 つのチャートに表示さます。クライアント統計情報について （5 ページ）を参照してください。データは色分けされていて、次の情報が含まれています。

- RSSI および SNR の測定値（デシベル単位）。
- Rx 平均データレート（直近の 5 秒間）および Rx 最新データレート。
- Tx パケットおよび Rx パケット。
- Tx パケットの再試行。

チャートでは、次の操作を実行できます。

- チャートにカーソルを重ねると、特定の時点の統計を表示できます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルト表示に変更するには、  アイコンをクリックします。

ステップ 10 クライアントデバイスのデータパケットキャプチャを実行するには、「クライアントデバイスのデータパケットキャプチャの実行 （14 ページ）」を参照してください。

クライアントデバイス向けキャプチャセッションのスケジュールと管理

スケジュール済みのキャプチャセッションを停止、編集、削除するには、次の手順を実行します。

クライアントキャプチャセッションは、次のデータを収集します。

- オンボーディングイベントのデータパケットおよび **[Client 360]** > **[Intelligent Capture]** ウィンドウに表示される [RF Statistics] チャートデータ（5 秒のサンプル）。クライアントデバイスのライブキャプチャセッションの有効化 （5 ページ） を参照してください。
- **[Device 360]** > **[Intelligent Capture]** ウィンドウに表示されるチャートおよび表のデータ。RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理 （27 ページ） を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 クライアント キャプチャ セッションをスケジュールするには、[+ Schedule Client Capture] をクリックします。

[Schedule Client Capture] スライドインペインで、次の設定を行います。

a) [Start Time] エリアで、キャプチャセッションを開始するタイミングを指定します。[Run Now]、[Run Later] のどちらかを選択できます。
b) [Duration] ドロップダウンリストをクリックして期間を指定します。
c) [Select Client Devices] ドロップダウンリストをクリックすると、カテゴリの一致を返す検索文字列を入力できます（クライアント ユーザー ID、ホスト名、MAC アドレス）。

（注） 検索では、カテゴリごとに最大 10 個の一致が返されるため、エントリが見つからない場合は検索文字列を再調整します。

（注） キャプチャセッションの詳細については、クライアントデバイス向けのキャプチャセッションについて （4 ページ） を参照してください。

d) [Save] をクリックします。

ステップ 3 実行中のキャプチャセッションを停止するには、次の手順を実行します。

a) [In-progress Captures] タブをクリックします。
b) テーブルからクライアントを選択します。
c) [Stop Capture] をクリックします。

ステップ 4 将来の時間にスケジュールされたキャプチャセッションを編集するには、次の手順を実行します。

a) [Scheduled Captures] タブをクリックします。
b) テーブルからクライアントを選択します。

c) [Edit Schedule] をクリックします。

ステップ 5 完了したキャプチャセッションを削除するには、次の手順を実行します。

a) [Completed Captures] タブをクリックします。
b) テーブルからクライアントを選択します。
c) [Delete Schedule] をクリックします。

クライアントデバイス向けデータパケットキャプチャ

クライアントデバイス向けデータパケットキャプチャについて

データパケットキャプチャを使用すると、ネットワークデータをPCAPファイルにキャプチャできます。このファイルはWiresharkでダウンロードして表示できます。詳細については、クライアントデバイスのデータパケットキャプチャの実行 （14 ページ）を参照してください。

データパケットキャプチャの制限事項

データパケットキャプチャには、次の制限事項があります。

- データパケットキャプチャは、Cisco Aironet 4800 APおよびCisco Catalyst 9130、9136、9166 APでのみサポートされます。データパケットキャプチャが有効になっていて、クライアントがパケットキャプチャに対応していないAPにローミングした場合、クライアントがパケットキャプチャ対応のAPに再接続するまで、パケットキャプチャは停止します。
- 一度に実行できるデータ パケット キャプチャ セッションは1つだけです。
- すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Centerとシスコ ワイヤレス コントローラの間でクロックを同期させる必要があります。ワイヤレスコントローラがNetwork Time Protocol（NTP）サーバーに接続されていることを確認します。
- 各データ パケット キャプチャ セッションで最大1 GBのローリングデータをキャプチャできます。ダウンロードを高速化するために、1 GBのデータが10個の100 MBのファイルに分割されます。

NAM 統合について

ソフトウェアバージョン6.4(2)以降を実行中のNetwork Analysis Module（NAM）またはvNAMサーバーをご使用の場合は、お使いのNAMサーバーをCisco DNA Centerと統合できます。インストールと設定の詳細については、*Cisco Prime* 仮想ネットワーク解析モジュール（*vNAM*）インストールおよびコンフィギュレーション ガイド [英語] を参照してください。

クライアントに対して NAM 統合とフルパケットキャプチャを有効にすると、**[Client 360]** > **[Intelligent Capture]** ウィンドウの [Wireless Packet Application Analysis] チャートにデータが提供されます。このテーブルとチャートには、クライアントが使用するアプリケーション、その QoS 設定、パケット損失、ワイヤレス遅延、およびジッターに関する情報が表示されます。

NAM サーバーを Cisco DNA Center と統合するには、次の手順を実行します。

1. NAM データポートで IP アドレスを設定します。
2. gRPC コレクタを設定します。

（注） NAM 統合は、IPv6 アドレスを使用する Cisco DNA Center クラスタではサポートされません。

NAM データポートでの IP アドレス設定

NAM や vNAM のデータポートに有効な IP アドレスを設定するには、次の手順を実行します。この手順は、NAM と統合するために必要です。

（注） データポートはパケットを受信するためだけのもので、要求には応答しません。したがって、IP アドレスを正しく設定していても、データポートに ping を実行するとタイムアウトになります。IP アドレスが有効で、Cisco DNA Center から到達可能であることを確認します。

ステップ 1 NAM サーバーの CLI にログインします。

ステップ 2 コマンド **show data-port ip-addresses** を入力します。
コマンドにより、ポート番号と IP アドレスが表示されます。

```
Device# show data-port ip-addresses
Port number: 1
IPv4 address: 172.20.125.125
```

ステップ 3 **show data-port ip-addresses** コマンドで何も表示されない場合、コマンド **data-port 1 ip-address** *ip-address* を入力して、IP アドレスをポート 1 に割り当てます。

ステップ 4 **show data-port ip-addresses** コマンドを再度実行し、そのデータポート 1 が IP アドレスに割り当てられたことを確認します。

ステップ 5 データ ポート 1 またはその他の表示されているポートの IP アドレスの 1 つを記録します。

ステップ 6 **cdb-export** が Cisco DNA Center で有効であることを確認します。そのためには、**show cdb-export all** コマンドを入力します。何も表示されない場合は、コマンド **cdb-export collector 1 ip-address** *IP-address-of-Cisco-DNA-Center* を入力します。

ステップ 7 コマンド **autocreate-data-source erspan** を入力して、Cisco DNA Center からのデータパケットが処理されていることを確認します。

ステップ 8 NAM や vNAM サーバーと Cisco DNA Center で時間が同期していることを確認します。NAM ユーザーインターフェイスから **[Administration]** > **[System]** > **[System Time]** の順に選択することにより、時刻を同期できます。

gRPC コレクタの設定

この手順を gRPC コレクタに対して実行して NAM を統合します。gRPC は、オープンソースの高パフォーマンス RPC（リモートプロシージャコール）フレームワークです。

始める前に

NAM データポートで IP アドレスを設定します。NAM データポートでの IP アドレス設定 （13 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Data Platform]**。

[Data Centers] ウィンドウが表示されます。

ステップ 2 [Collectors] タブをクリックします。

[Collectors] ウィンドウが表示されます。

ステップ 3 [GRPC-COLLECTOR] をクリックします。

[GRPC-COLLECTOR] ウィンドウが表示されます。

ステップ 4 **[+ Add]** をクリックします。

[gRPC Collector Configuration] ウィンドウが表示されます。

ステップ 5 [GRPC-COLLECTOR] 設定を 1 つだけ追加します。次の手順を実行します。

a) [ConfigData] エリアで [Agent Export] チェックボックスをオンにして、ネットワークパケットデータの NAM へのエクスポートを有効にします。

b) [Agent IP Address] フィールドに、記録したデータポートの IP アドレスを入力します（NAM データポートでの IP アドレス設定 （13 ページ） の ステップ 5 （13 ページ） を参照してください）。

c) [Configuration Name] フィールドに、GRPC-コレクタ設定の一意の名前を入力します。

d) [Save Configuration] をクリックします。

クライアントデバイスのデータパケットキャプチャの実行

この手順では、クライアントデバイスのデータパケットキャプチャを実行する方法を示します。

始める前に

アクセスされたアプリケーションとポート、QoSデータ、パケット損失、ワイヤレス遅延、およびジッターに関する情報を取得するには、NAM 統合を有効にする必要があります。詳細については、「NAM 統合について （12 ページ）」を参照してください。

ステップ 1 [Health]左上隅にあるメニューアイコンをクリックして次を選択します：**アシュアランス** > 。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

[クライアントの健全性（Client Health）] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- **[クライアントデバイス（Client Devices）]**表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索（Search）] フィールド（右上端）に次のいずれかを入力します。ユーザ ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレス。

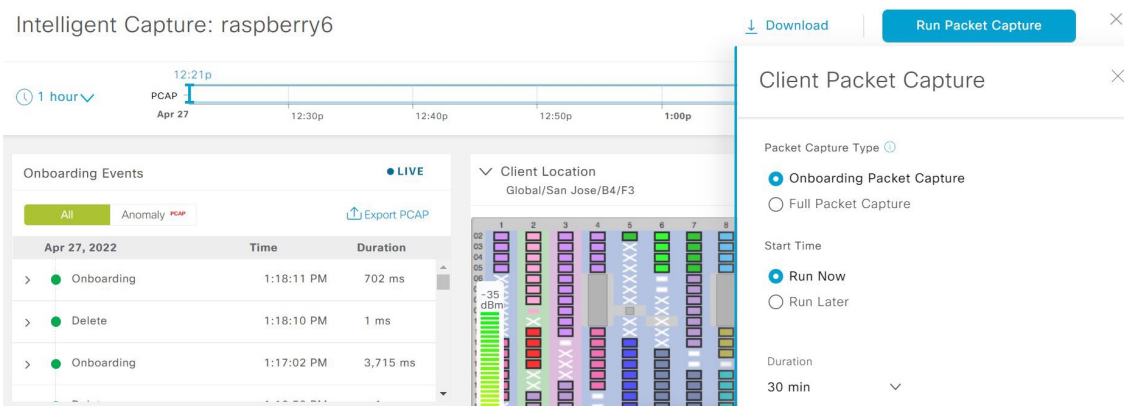
クライアント デバイスの 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンがクライアント名の横に表示される場合は、クライアントまたはアクセスポイントがインテリジェント キャプチャ データを送信できない Cisco DNA Center （33 ページ） を参照してください。

図 2 : クライアントの *[Intelligent Capture]* ウィンドウ



ステップ 5 タイムラインスライダは、次の機能に使用できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注）　タイムラインには、最長で過去 2 週間のデータを表示できます。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

ステップ 6 データパケットキャプチャを実行するには、[Data Packet Capture] エリア（右上隅）で次の機能を使用します。

[Data Packet Capture] エリア	
アイテム	説明
[Run Packet Capture] ボタン	[Run Packet Capture] をクリックして、[Client Packet Capture] スライドインペインを開き、次の手順を実行します。 **1.** [Onboarding Packet Capture] または [Full Packet Capture] オプションボタンをクリックして、[Packet Capture Type] を選択します。 **2.** [Start Time] を選択します。[Run Now]、[Run Later] のどちらかを選択できます。 **3.** [Duration] ドロップダウンリストから、パケットキャプチャの期間を選択します。デフォルトは 30 分です。 **4.** パケットキャプチャを有効にする必要がある [Wireless Controllers] を選択します。ワイヤレスコントローラは最大 3 つまで選択できます。 **5.** [Save] をクリックします。 [Packet Capture Type]：このボタンを使用して、クライアントのデータパケットキャプチャを開始します。データ パケット キャプチャ ファイルは、トラブルシューティングと [Wireless Packet Application Analysis] ダッシュレットに使用されます。データパケットキャプチャがクライアントに対して現在実行されている場合は、[Data Packet Capturing Stop] をクリックして停止します。 （注） すべてのオンボーディング パケット キャプチャ セッションは、**アシュアランス** > **[Intelligent Capture Settings]** > **[Client Schedule Capture]** の下に表示されます。 一度に実行できるデータ パケット キャプチャ セッションは 1 つだけです。データパケットキャプチャの実行中に [Run Data Packet Capture] をクリックすると、現在のキャプチャを終了するか、または新しいキャプチャを開始するかのオプションが表示されたダイアログボックスが現れます。 When a Data Packet Capture session is configured on Cisco DNA Center, any Data Packet Capture session that Cisco DNA Center is not aware of is removed（such as full packet capture sessions that were directly configured on the wireless controller). （注） すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Center とシスコ ワイヤレス コントローラの間でタイムゾーンを同期させる必要があります。ワイヤレスコントローラが Network Time Protocol（NTP）サーバーに接続されていることを確認します。 （注） 新しいキャプチャセッションが開始されるたびに、新しい一連の PCAP ファイルが開始されます。

[Data Packet Capture] エリア	
アイテム	**説明**
[Download] ボタン	フルパケットPCAPファイルがセッションからキャプチャされたら、このボタンクリックしてPCAPファイルをダウンロードします。データパケットファイルをダウンロードするには、[Download]列にあるアイコンをクリックします。次のいずれかのファイルをダウンロードできます。 • ワイヤレスデータ：AP とクライアント間のパケットの 802.11 ファイル。 • 有線データ：AP とスイッチまたはワイヤレスコントローラ間のパケットのイーサネットファイル。 （注） データ パケット キャプチャ ファイルには、100 MB の制限があります。すべてのデータ パケット キャプチャ ファイルの合計は、3.5 GB を超えることはできません。 （注） 過去 7 日間の PCAP ファイルのみダウンロードできます。

ステップ 7 クライアントデバイスのデータパケットキャプチャを実行するには、[Run Packet Capture] をクリックして、[Client Packet Capture] スライドインペインを有効にします。

Client Packet Capture	
アイテム	**説明**
[Packet Capture Type]	[Packet Capture Type] を選択します。それぞれのタブから、次のパケットキャプチャのいずれかを選択できます。 • **[Onboarding Packet Capture]** • **[Full Packet Capture]** • **[OTA Sniffer]**

Client Packet Capture	
アイテム	説明
[Onboarding and Full Packet Capture] タブ	[Onboarding Packet Capture] タブまたは [Full Packet Capture] タブをクリックして、次の手順を実行します。 **1.** [Start Time] を選択します。[Run Now]、[Run Later] のどちらかを選択できます。 **2.** [Duration] ドロップダウンリストから、パケットキャプチャの期間を選択します。デフォルトは 30 分です。 **3.** パケットキャプチャを有効にする [Wireless Controllers] を選択します。ワイヤレスコントローラは最大 3 つまで選択できます。 **4.** [Save] をクリックします。 （注） すべてのオンボーディングパケットキャプチャセッションは、**アシュアランス** > **[Intelligent Capture Settings]** > **[Client Schedule Capture]** の下に表示されます。 一度に実行できるデータパケットキャプチャセッションは 1 つだけです。データパケットキャプチャの実行中に [Run Data Packet Capture] をクリックすると、現在のキャプチャを終了するか、または新しいキャプチャを開始するかのオプションが表示されたダイアログボックスが現れます。 When a Data Packet Capture session is configured on Cisco DNA Center, any Data Packet Capture session that Cisco DNA Center is not aware of is removed（such as full packet capture sessions that were directly configured on the wireless controller).

Client Packet Capture	
アイテム	説明
[OTA Sniffer] タブ	[OTA Sniffer] タブをクリックして、次の手順を実行します。 **1.** パケットキャプチャを実行する AP の横にあるチェックボックスをオンにします。 Cisco DNA Center は、OTA スニファ機能がサポートする無線のみが表示されます。 **2.** ドロップダウンリストから [Sniffer] モードを選択します。その他のオプションは、[Radio Mode] または [AP Mode] です。 それぞれのドロップダウンリストから、[Radio]、[Band]、[Channel Width]、および [Channel] を選択します。 （注） デュアル無線をサポートする AP の場合は、次のように、プライマリ無線またはセカンダリ無線を使用して OTA スニファ データ パケット キャプチャを実行します。 • AP でデュアル無線モードが無効になっている場合は、プライマリ無線を使用してデータパケットキャプチャを実行します。 • AP でデュアル無線モードが有効になっている場合は、セカンダリ無線を使用してデータパケットキャプチャを実行します。 **3.** [Run] をクリックします。 **4.** [Packet Captures] スライドインペインで、OTA スニファデータキャプチャを表示およびダウンロードできます。 （注） すべての OTA スニファ データ キャプチャ セッションが、**アシュアランス** > **[Intelligent Capture Settings]** > **[OTA Sniffer Capture]**の下に表示されます。

Client Packet Capture	
アイテム	説明
ダウンロード	フルパケットPCAPファイルがセッションからキャプチャされたら、このボタンクリックしてPCAPファイルをダウンロードします。データパケットファイルをダウンロードするには、[Download]ボタンのアイコンをクリックします。次のいずれかのファイルをダウンロードできます。 • ワイヤレスデータ：APとクライアント間で移動するパケットの802.11ファイル。 • 有線データ：APとスイッチまたはワイヤレスコントローラ間で移動するパケットのイーサネットファイル。 （注） データ パケット キャプチャ ファイルには、100 MB の制限があります。すべてのデータ パケット キャプチャ ファイルの合計は、3.5 GB を超えることはできません。過去 7 日間の PCAP ファイルのみダウンロードできます

ステップ 8 [Wireless Packet Application Analysis] ダッシュレットを使用して、データパケットキャプチャの詳細を確認します。

データパケットキャプチャが実行されている場合、このダッシュレットには、アクセスされたアプリケーションとポート、QoS データ、パケット損失、ワイヤレス遅延、およびジッターなど、分析されたパケットに関する詳細が表示されます。

（注） このダッシュレットにデータを表示するには、NAM の統合を設定する必要があります。NAM 統合について （12 ページ）を参照してください。

クライアントの データパケットキャプチャ履歴の表示

クライアントのデータ パケット キャプチャ セッションの履歴（最初のパケットと最後のデータパケットがキャプチャされた時刻、キャプチャされたデータパケットの合計サイズ、パケットのタイプなど）を表示するには、以下の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 [Client Data Packet Capture] タブをクリックします。

[Client Data Packet Control] ウィンドウが表示されます。

ステップ 3 [Intelligent Capture Settings - Client Data Packet Capture] ウィンドウには、次の情報が表示されます。

オプション	説明
[Identifier]	クライアントのユーザー ID またはホスト名が表示されます。ユーザー ID またはホスト名をクリックすると、[Intelligent Capture: Client Device] ウィンドウが開きます。
[MAC Address]	クライアントデバイスの MAC アドレスが表示されます。
[First Packet Time]	最初のデータパケットがキャプチャされた時刻が表示されます。
[Last Packet Time]	最後のデータパケットがキャプチャされた時刻が表示されます。
[Total Size]	キャプチャされたデータの合計サイズが表示されます。
[Currently Running]	データパケットキャプチャが実行中かどうかを表示します。
[Type of Packet]	パケットのタイプ（[Wired]、[Wireless] など）が表示されます。

アクセスポイント向けインテリジェントキャプチャ

アクセスポイントのインテリジェントキャプチャについて

AP インテリジェントキャプチャ機能を使用すると、1 つ以上の AP で次のデータをキャプチャできます。

- **AP 統計情報キャプチャ**には、次の情報が含まれます。
  - **[Device 360]** > **[Intelligent Capture]** ウィンドウの [RF Statistics] タブに表示される AP 無線および WLAN 統計情報。
  - 選択した AP に関連付けられているすべてのクライアントの **[Client 360]** > **[Intelligent Capture]** ウィンドウで [RF Statistics] エリアに表示される AP クライアントの統計情報（サンプリング時間は 30 秒）。
- **異常キャプチャ**は、選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント（グローバルまたは選択した AP に関連付けられているすべてのクライアント）をキャプチャして、ダウンロードまたは表示できます。

キャプチャの制限事項

Cisco DNA Center に格納する異常をトリガーしたパケットファイルの合計サイズには、1.05 GB の制限があります。制限を超えると、合計サイズが 1.05 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

アクセスポイントのインテリジェントキャプチャの有効化と管理

1 つまたは複数のアクセス ポイント（AP）を有効にして次のデータをキャプチャするには、以下の手順を実行します。

- **AP 統計情報**：AP 無線の統計情報、WLAN 統計情報、および AP クライアントの統計情報が含まれます。Cisco DNA Center は、AP 統計情報のキャプチャに関して最大 1000 の AP をサポートできます。
- **異常キャプチャ**：選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント（グローバルまたは選択した AP に関連付けられているすべてのクライアント）をキャプチャして、ダウンロードまたは表示できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 [Access Points] タブをクリックします。

[Access Point] ウィンドウが表示されます。

ステップ 3 AP 統計情報キャプチャを有効または無効にするには、次のいずれかを実行します。

- 有効な AP がない場合は、[Configure AP Enablement] エリアが表示されます。[Specific] または [Global] のいずれかのオプションを選択し、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[AP Stats Capture] ウィンドウが表示されます。[AP Stats Capture] ウィンドウで、次のいずれかのオプションを選択します。

オプション	説明
None - disable all APs	1 つ以上の AP が有効になっている場合は、「None - disable all APs」 と表示されます。 現在有効になっているすべての AP で 統計情報キャプチャを無効にできます。

オプション	説明
Specific - select specific APs and enable	選択した AP の 統計情報キャプチャを有効にできます。次の手順を実行します。 **1.** [Specific - select specific APs and enable] オプションボタンをクリックします。 **2.** 左側のペインで、[Global] を展開し、サイト > ビルディング > フロア の順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。 **3.** 選択した AP の統計情報キャプチャを有効にするには、次の手順を実行します。 • [Disabled APs] タブをクリックします。統計情報キャプチャが現在無効になっている AP のリストが表示されます。 • 統計情報キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。 **4.** 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 （注） 互換性のない AP の条件は次のとおりです。 • 動作モードが [local] または [FlexConnect] に設定されていない。 • AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。
Global - enable all capable APs	すべての対応 AP で統計情報キャプチャを有効にできます。

ステップ 4 異常キャプチャを有効または無効にするには、[Anomaly Capture] タブをクリックして、次のいずれかを実行します。

- 有効になっている AP がない場合は、[Configure AP Enablement] エリアが表示されます。次のいずれかのオプションを選択してから、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[Anomaly Capture] ウィンドウが表示されます。[Anomaly Capture] ウィンドウで、次のいずれかのオプションを選択します。

オプション	説明
None - disable all APs	1 つ以上の AP が有効になっている場合は、「None - disable all APs」 と表示されます。 現在有効になっているすべての AP で異常キャプチャを無効にできます。

オプション	説明
Specific - select specific APs and enable or disable	選択した AP の異常キャプチャを有効または無効にできます。次の手順を実行します。 **1.** [Specific - select specific APs and enable or disable] オプションボタンをクリックします。 **2.** 左側のペインで、[Global] を展開し、サイト > ビルディング > フロア の順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。 **3.** 選択した AP の異常キャプチャを有効にするには、次の手順を実行します。 • [Disabled APs] タブをクリックします。異常キャプチャが現在無効になっている AP のリストが表示されます。 （注） 以前に AP を有効にしようとして失敗した場合、[Config Status] 列にエラーメッセージが表示されます。 • 異常キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。 **4.** 選択した AP の異常キャプチャを無効にするには、次の手順を実行します。 • [Enabled APs] タブをクリックします。異常キャプチャが現在有効になっている AP のリストが表示されます。 • 異常キャプチャを無効にする AP の横にあるチェックボックスをオンにして、[Disable] をクリックします。 **5.** 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 （注） 互換性のない AP の条件は次のとおりです。 • 動作モードが [local] または [FlexConnect] に設定されていない。 • AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。 **6.** インテリジェントキャプチャをサポートしている AP のリストを表示するには、[Not-Ready APs] タブの横にある情報アイコンをクリックします。

オプション	説明
Global - enable all capable APs	すべての対応 AP の異常キャプチャを有効にできます。

RF統計情報の表示とアクセスポイントのスペクトル解析データの管理

RF 統計情報を表示し、特定のアクセスポイントのスペクトル解析データを開始および管理するには、次の手順を実行します。

ステップ 1 [Health]左上隅にあるメニューアイコンをクリックして次を選択します：**アシュアランス** > 。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Network Health] タブをクリックします。

[Network Health] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名（ハイパーリンクされた識別子）をクリックし、AP の詳細を表示します。
- [Search] フィールド（右上隅にあります）で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンが AP 名の横に表示される場合は、「クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center （33 ページ）」を参照してください。

ステップ 5 [RF Statistics] タブをクリックすると、RF 統計情報の詳細が表示されます。

（注） [AP Stats Capture] が有効になっていない場合は、有効にします。アクセスポイントのインテリジェントキャプチャの有効化と管理 （23 ページ）を参照してください。

ステップ 6 [RF Statistics] タブでは、次の操作を実行できます。

a) タイムラインを使用すると、指定された時間の RF 統計情報を表示し、データの範囲を指定できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]（デフォルト）、[3 hours]、および [5 hours] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。タイムラインスライダは、APの正常性を表示するために色分けされています。特定の時刻にカーソルを合わせると、デバイスの正常性スコア、システムリソース、データプレーンなどの詳細を表示できます。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

b) タイムラインの下にある無線周波数セレクタを使用すると、周波数帯域に基づいてダッシュレットのデータをフィルタ処理できます。ドロップダウンリストをクリックして、サポートされている無線の数に応じて [Radio 0 (2.4 GHz or 5 GHz)]、[Radio 1 (5 GHz)]、または [Radio 2 (6 GHz)] を選択します。

c) このダッシュレットで、RF 統計情報の詳細を確認できます。

（注） ダッシュレットに表示されるチャートでは、次の操作を実行できます。

- 詳細を表示するには、チャートにカーソルを合わせます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルトに変更するには、 をクリックします。
- チャートの下の色分けされたデータタイプをクリックすると、チャートに表示されているそのデータタイプを無効化または有効化できます。

ダッシュレット	説明
[Clients] ダッシュレット	この AP を使用しているクライアントの数が表示されます。データソースは AP WLAN 統計情報からのものです。
[Top Clients with Tx Failed Packets by SSID] ダッシュレット	テーブル内の SSID のリストが表示されます。テーブルのデータソースは、AP WLAN 統計情報からのものです。棒グラフのデータソースは、AP クライアントの統計情報からのものです。 SSID を選択すると、その SSID の送信に失敗したパケットの上位のクライアントが表示されます。
[Channel Utilization] ダッシュレット	APおよびその他のワイヤレスおよびワイヤレス以外のデバイスで使用されているチャネル使用率が表示されます。棒グラフのデータソースは、AP無線統計情報からのものです。

ダッシュレット	説明
[Channel Utilization by this Radio] ダッシュレット	AP によって使用されている現在のチャネル使用率、SSID のリスト、接続されているクライアントの数、およびクライアントの過去15分間に送受信されたパケット数が表示されます。 テーブルのデータソースは、AP WLAN 統計情報からのものです。円グラフのデータソースは、AP 無線統計情報からのものです。
[Frame Count] ダッシュレット	管理フレームとデータフレームの数が表示されます。データソースは AP 無線統計情報からのものです。
[Frame Errors] ダッシュレット	送受信エラーの数が表示されます。データソースは AP 無線統計情報からのものです。
[Tx Power and Noise Floor] ダッシュレット	送信電力とノイズフロアが表示されます。データソースは AP 無線統計情報からのものです。
[Multicast/Broadcast Counter] ダッシュレット	各 SSID のマルチキャストおよびブロードキャストの数が表示されます。データソースは AP WLAN 統計情報からのものです。

ステップ 7 [Spectrum Analysis] タブをクリックします。

ステップ 8 [Start Spectrum Analysis] タブをクリックし、ペクトル解析セッションを開始します。

（注）
- スペクトル解析期間は 10 分です。
- 同時スペクトル解析セッションの最大数は 10 です。

ステップ 9 [Spectrum Analysis] タブでは、次の操作を実行できます。

a) タイムラインを使用すると、指定された時間のスペクトル解析データを、データの範囲を指定して表示できます。

タイムラインスライダ	
アイテム	説明
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]（デフォルト）、[3 hours]、および [5 hours] です。

タイムラインスライダ	
アイテム	説明
タイムラインスライダ	タイムラインスライダは、表示されるデータの時間枠を決定します。タイムラインスライダは、APの正常性を表示するために色分けされています。特定の時刻にカーソルを合わせると、デバイスの正常性スコア、システムリソース、データプレーンなどの詳細を表示できます。 スペクトル解析の場合、時間範囲は 5 分の枠に設定されます。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注）　タイムラインには、最長で過去 2 週間のデータを表示できます。 境界線をクリックしてドラッグすると、特定の時間のデータが表示されます。

b) タイムラインの下にある無線周波数セレクタを使用すると、周波数帯域に基づいてチャートのデータをフィルタ処理できます。[2.4 GHz]、[5 GHz]、または [6 GHz] をクリックします。

（注）　[Radio Mode] と [Channel]（[Spectrum Analysis] チャートの上）にデータが表示されない場合、その AP には選択された帯域を使用している無線がないことを示します。これは、AP に [5 GHz] の無線を出力するクライアントがあるが、無線周波数セレクタが [2.4 GHz] に設定されている場合に発生します。

詳細については、スペクトル解析時の Cisco AP 機能について （32 ページ）を参照してください。

c) [Spectrum Analysis] チャートには、次の機能が用意されています。

スペクトル解析チャート	
アイテム	説明
上位チャート（パーシステンス）	このチャートは、RF 環境で検知された各信号の振幅（電力）とチャネル周波数をリアルタイムで提供します。X 軸は振幅を表し、Y 軸はチャネル周波数を表します。 チャート内の色は、選択された 5 分間で同じ振幅およびチャネル周波数で検知される信号の数を表します。 • 青色は、オーバーラップする信号の数が少ない（または信号が同じ振幅と周波数で検知される）ことを示します。 • 赤色は、オーバーラップする信号の数が多いことを示します。 より多くの信号が検知されるにつれ、色の強度が増加します（青色 > 緑色 > 黄色 > オレンジ色 > 赤色）。チャート内の線がオーバーラップし、交差すると、色が変わります。 色の透過性は、信号データの経過時間を表し、古いデータはより透過的になります。 リアルタイムで RF 環境を表示するには、[Real-TimeFFT（Fast Fourier Transform）] をクリックして有効にします。リアルタイム FFT を有効にすると、永続化チャートが制限されて 5 分間のデータストリームのコレクションではなく、「1 つ」の最新データストリームが表示されます。 特定の範囲のチャネルのデータをズームインして表示するには、マウスをクリックしてドラッグし、範囲を選択します。チャートが更新され、選択した特定のチャネルのデータが表示されます。 チャート全体をズームアウトして表示するには、右上隅の虫めがねをクリックします。
ボトムチャート（ウォーターフォール）	このチャートは、データの時間的な解釈を提供します。このチャートは、パーシステンスチャートと同じ情報を提供しますが、フォーマットは異なります。X 軸は時間を表し、Y 軸はチャネル周波数を表します。チャート内の行は、イベントが発生した正確な順序を表します。これにより、問題が発生した場合に根本原因をトラブルシュートすることができます。 チャート内の色は、振幅を表します。青色は低い値（-100 dBm）を示し、赤色は高い値（-20 dBm）を示します。

d) [Interference and Duty Cycle] チャートには、次の情報が表示されます。

- 検出された干渉とその重大度：
  - 干渉は、半径が干渉の帯域幅を表す円としてプロットされます。X 軸は干渉が検出された周波数を表し、Y 軸は重大度を表します。

- [Severity] は、干渉と範囲の影響を測定します。範囲は 0（影響がないことを示す）から 100（大きな影響を示す）です。
- 干渉タイプは RF 署名から決定され、Cisco CleanAir テクノロジーによって識別され ます。

- 各チャネルのデューティサイクル。

スペクトル解析時の Cisco AP 機能について

Cisco Aironet 2800 シリーズ、3800 シリーズ、および 4800 シリーズ アクセスポイント（AP）には、フレキシブル ラジオ アサインメント（FRA）を備えたデュアルバンド無線がスロット 0 に搭載されています。この FRA 無線は 2.4 GHz で動作しますが、5 GHz で動作するように割り当てることができます。このモードは、AP の動作モードとは異なるように変更できます。AP の FRA 無線を 5 GHz で動作するように設定すると、クライアント無線は 2.4 GHz 帯域で動作できなくなります。

（注） スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、および Catalyst 9115 AP ではサポートされていません。

（注） AP に正しいソフトウェアバージョンがインストールされていることを確認します。インテリジェントキャプチャ対応デバイス （2 ページ） に記載された「**サポート対象の Cisco AP**」の表を参照してください。

スペクトル解析のための無線スロットの割り当ては次のとおりです。

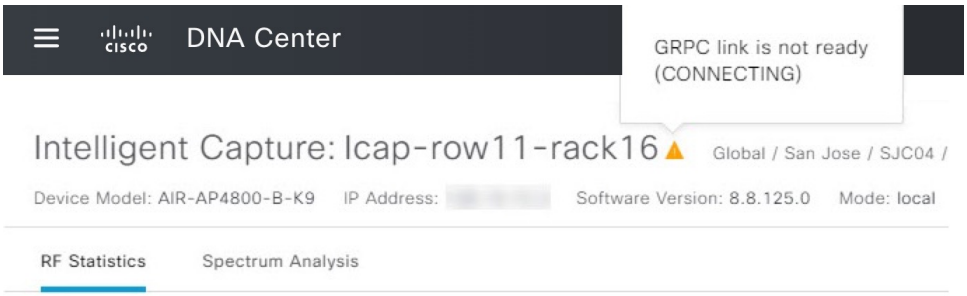
デバイス モデル	スペクトル解析の無線スロットの割り当て
Aironet 2800 シリーズ AP Aironet 3800 シリーズ AP Aironet 1560 AP Catalyst IW6300 Heavy Duty シリーズ AP Catalyst IW6300 Heavy Duty シリーズ AP	無線スロット 0 および 1 が有効になっています。

デバイス モデル	スペクトル解析の無線スロットの割り当て
Aironet 4800 シリーズ AP Catalyst 9120 AP Catalyst 9130 AP	これらの AP には、3 つの無線スロットがあります。 データパケットキャプチャが実行されている場合は、無線スロット 0 および 1 が有効になります。 データパケットキャプチャが実行されていない場合は、無線スロット 2 が有効になります。 （注） AP スペクトル解析データは、2.4 GHz チャネル帯域では表示されません。また、2.4 GHz 帯域を提供する AP 無線がない場合、[Radio Mode] フィールドと [Channel] フィールドは空になります。こうした状況になるのは、FRA 無線が 5 GHz で動作するように設定され、パケットキャプチャが有効になっている場合です。

インテリジェントキャプチャのトラブルシューティング

クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center

問題：クライアントまたはアクセスポイントがインテリジェント キャプチャ データを Cisco DNA Center に送信できません。警告（⚠）アイコンが「**GRPC link is not ready (CONNECTING)**」というメッセージと共に表示されます。



バックグラウンド：AP がインテリジェント キャプチャ データを Cisco DNA Center に送信するためには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ または シスコ ワイヤレス コントローラ のインテリジェント キャプチャ ポート番号を 32626 に設定する必要があります。通常、Catalyst 9800 シリーズ ワイヤレス コントローラ または ワイヤレスコントローラ が Cisco DNA Center によって検出されると、ポート番号は自動的に 32626 に設定されます。

ただし、Cisco DNA Center のアップグレードパスによっては、ポート番号が適切に設定されない場合があります。

解決策：この問題を解決するには、次の作業を実行します。

1. Catalyst 9800 シリーズ ワイヤレス コントローラ または ワイヤレスコントローラ でインテリジェント キャプチャ サーバーのポート番号が 32626 に設定されていることを確認します。
2. ポート番号が 32626 に設定されていない場合は、手動で設定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。