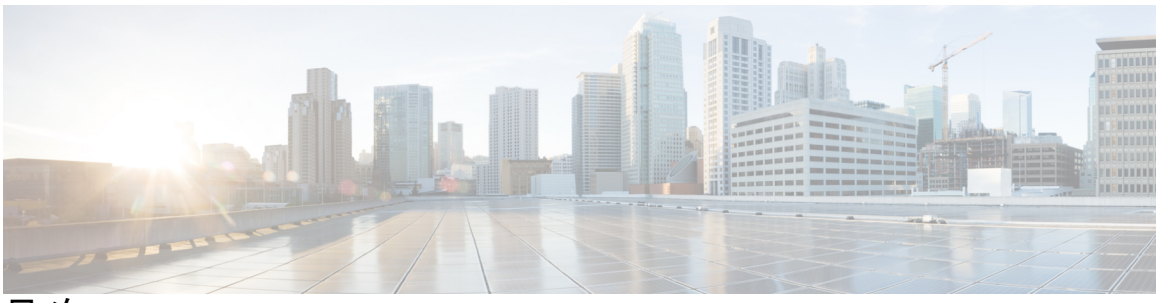
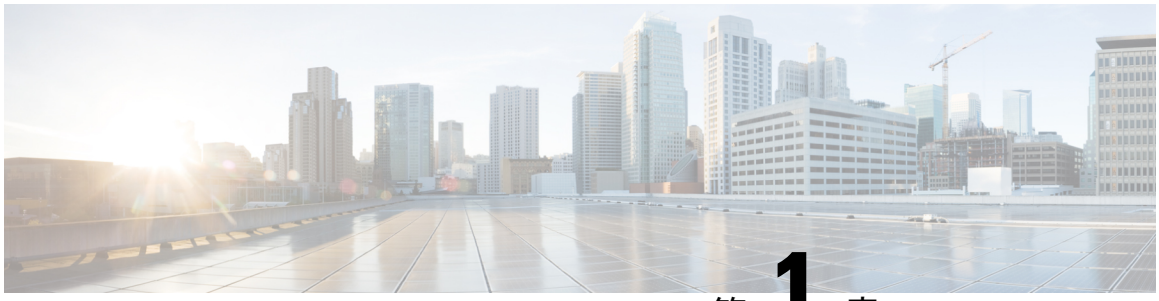
Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント設定ガイド、Cisco IOS XE 17.17.x

最終更新：2025 年 12 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次



第 1 章

はじめに

Cisco Catalyst IW9165E アクセスポイント

Cisco Catalyst IW9165E アクセスポイントは、移動する車両や産業機械に非常に信頼性の高い接続を提供するように設計された高耐久性のワイヤレスデバイスです。

これらのアクセスポイントは、外部アンテナを備えた 2x2 Wi-Fi 6E 設計を特徴としており、過酷な環境で高度なワイヤレス性能を確実に実現します。低消費電力に最適化されており、IP30 定格の堅牢設計で、産業用アプリケーションに最適です。

Catalyst IW9165E アクセスポイントは、小型形状と堅牢な構造により、産業設備に円滑に統合できるように特別に設計されています。主要機能は次のとおりです。

- Wi-Fi 6E テクノロジー：最新のワイヤレス規格をサポートし、性能と信頼性を向上させます。
- 外部アンテナ：信号強度とカバー域を強化します。
- 耐久性に優れた設計：過酷な環境での使用に適した IP30 定格です。
- 低消費電力：エネルギー効率のために最適化されています。
- 小型形状：産業機械や移動する車両への統合を簡素化します。

これらの属性により、Catalyst IW9165E AP は、要求の厳しい産業環境でワイヤレス接続を実現する信頼性の高い選択肢となっています。

Cisco Catalyst IW9165E 高耐久性アクセスポイント（AP）およびワイヤレスクライアント（以降、「Catalyst IW9165E」）は、外部アンテナを備えた 2x2 Wi-Fi 6E 設計をサポートしています。また、移動する車両や機械に超高信頼ワイヤレス接続を追加するように設計されています。低消費電力、堅牢な IP30 設計、小型形状により、Catalyst IW9165E は産業設備に非常に簡単に統合できます。

Cisco Unified Industrial Wireless ソフトウェアリリース情報

機能と動作モード

Cisco Unified Industrial Wireless（UIW）ソフトウェアリリースにより、Catalyst IW9165E の機能が強化され、さまざまな産業用ネットワークのニーズに合わせて複数のモードで動作できるようになります。これらの更新は、さまざまなインフラストラクチャセットアップで高可用性、低遅延、および円滑な接続を実現するように設計されており、Catalyst IW9165E が産業用ワイヤレスネットワーキング向けの多用途ソリューションになります。

表 *1:* 動作モードと機能

モード	導入されたリリース	機能	用途
CURWB	17.12.1	低遅延、ゼロパケット損失、無瞬断のハンドオフを実現するシスコの超高信頼ワイヤレスバックホール（CURWB）を提供します。	ミッションクリティカルな産業用アプリケーション。
WGB	17.13.1	有線クライアントを Wi-Fi クライアントとしてシスコの AP インフラストラクチャに接続します。	シスコベースのワイヤレス環境。

モード	導入されたリリース	機能	用途
uWGB	17.13.1	有線クライアントを Wi-Fi クライアントとしてサードパーティの AP インフラストラクチャに接続します。	サードパーティのワイヤレス環境。 どちらのモード（WGB と uWGB）も、WGB の背後にある有線クライアントをインフラストラクチャの AP にブリッジするために役立ちます。
CAPWAP	17.14.1	CAPWAP プロトコルを使用して Lightweight AP として動作します。	柔軟な AP の管理と展開。

（注） IW9165E では、ハードウェアを交換せずに、ソフトウェアを更新するだけで動作モードを CAPWAP、WGB、または URWB に変更できます。

CAPWAP モード

CAPWAP モードは、AP がワイヤレスコントローラやネットワーク インフラストラクチャと連携する方法を定義する動作設定です。これらのモードは、ネットワーク内の AP の動作と機能を決定します。

CAPWAP モードは、AP がネットワーク環境で採用できるさまざまな動作設定を示すカテゴリです。各モードは、AP がクライアントトラフィックを処理し、コントローラと連携し、追加のネットワーク機能を実行する方法を決定します。

動作モード

CAPWAP 環境のアクセスポイントは、次のモードで動作できます。

表 *2 : CAPWAP* モード

モード	説明	主な機能	使用例
ローカルモード	AP が、クライアントにサービスを提供し、CAPWAP トンネルを介してトラフィックを集中管理するデフォルトモード。	• 2 つの CAPWAP トンネルを作成します。 • Centralスイッチング（コントローラへのデータブリッジ）。	一元化されたトラフィック管理。
FlexConnect	AP はトラフィックをローカルに切り替えますが、コントローラはそれを管理するため、コントローラの接続が失われても確実に動作します。	• ローカル トラフィック スイッチング。 • 自律型 AP のように動作します。 • コントローラの切断に対する復元力があります。	分散拠点またはリモートサイトでの復元力とローカルトラフィック処理。
ファブリック	AP が、ファブリックエッジへの VxLANトンネルを確立し、ネットワークのセグメンテーションを確保します。	• AP へのセグメンテーションを維持します。 • VxLAN トラフィックに SGT を挿入します。 • EN ノードと PEN ノードをサポートしています。	ファブリックベースのネットワークでのセグメンテーションとセキュアな通信。
スニファ	AP は、Wireshark などのツールを使用した分析のために、特定のチャネル上の無線トラフィックをキャプチャします。	• パケットをリモート分析ツールに転送します。 • 中継中にトラフィックに SGT をタグ付けします。	ネットワークのトラブルシューティングとパケット分析。

モード	説明	主な機能	使用例
監視	AP は、クライアントトラフィックを処理せずに、LBS、不正 AP 検出、および IDS のセンサーとして機能します。	• 専用の電波監視。 • クライアントにサービスを提供しません。	セキュリティ監視と侵入検知。
サイトサーベイ	サイトサーベイの RF パラメータを設定するために使用される AP。	RF 分析を支援します。詳細については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』の「AP Survey Mode」を参照してください。	ワイヤレスプランニングの RF 分析。

（注） スニファモード：エラーを回避するために、サーバーとコントローラの両方が同じ VLAN 上にあることを確認してください。

各モードの機能

- ローカルモード：デフォルトモード、2 つの CAPWAP トンネル、中央スイッチング。
- FlexConnect モード：ローカルスイッチング、自律型 AP のように動作、コントローラを利用できない場合でも機能。
- ファブリックモード：ファブリックエッジへの VxLAN トンネル、セグメンテーションをサポート、SGT タギング。
- スニファモード：パケットをキャプチャ、分析ツールに送信、トラフィックに SGT をタグ付け。
- 監視モード：センサーとして機能、クライアントトラフィックなし、LBS をサポート、IDS、不正 AP 検出。
- サイトサーベイモード：サイトサーベイ中の RF 設定に使用。

サポートされない機能

- 2.4 GHz 無線機、および
- 無線の走査

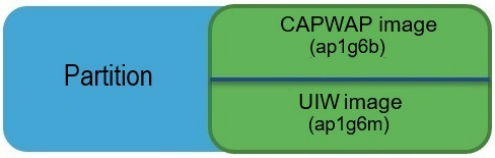
コントローラでの AP の設定方法について詳しくは、『Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア コンフィギュレーション ガイド』を参照してください。

イメージの決定

始める前に

動作モードに基づいて、IW9165E の正しい AP ソフトウェアイメージを選択します。これにより、デバイスの適切な機能および互換性を確保できます。

IW9165E のソフトウェアイメージは、デバイスの同じセクション内にあるさまざまなフォルダに保存されます。各イメージは、CAPWAP、URWB、WGB/uWGB などの特定の AP モードに対応します。



手順

ステップ 1 ソフトウェアイメージを見つけます。

IW9165E 上のソフトウェアイメージが保存されているセクションに移動します。イメージを含む適切なフォルダにアクセスできることを確認してください。

ステップ 2 AP のモードを識別します。

IW9165E の動作モードを決定します。デバイスは、次のいずれかのモードで動作できます。

- CAPWAP
- URWB
- WGB または uWGB

ステップ 3 対応するソフトウェアイメージを選択します。

デバイスの動作モードに適合するソフトウェアイメージを選択します。適切なソフトウェアイメージについては、次の表を参照してください。

表 3:

IW9165E のモード	ソフトウェアイメージ
CAPWAP	`ap1g6b-k9w8-xxx.tar`

IW9165E のモード	ソフトウェアイメージ
URWB	UIW イメージ ap1g6m-k9c1-xxx.tar
WGB または uWGB	

AP で動作中のソフトウェアの確認

IW9165E で実行されているイメージを判別するには、**show version** コマンドを使用します。

手順

ステップ 1 出力が「**Cisco AP Software, (ap1g6b)**」と表示される場合、AP は CAPWAP モードで動作しています。

例：

```
Cisco AP Software, (ap1g6b), C9165, RELEASE SOFTWARE Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2024 by Cisco Systems, Inc. Compiled Tue Feb 20
 23:04:29 GMT 2024
```

ステップ 2 出力が「**Cisco AP Software (ap1g6m)**」と表示される場合、AP は URWB モードまたは WGB/uWGB モードで動作しています。

例：

```
Cisco AP Software, (ap1g6m), C9165, RELEASE SOFTWARE Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2024 by Cisco Systems, Inc. Compiled Tue Feb 20
 23:04:29 GMT 2024
```

イメージの変換

始める前に

Wi-Fi（CAPWAP）、URWB、および WGB モード間で IW9165E AP のイメージを変換するには、このタスクを実行します。IW9165E AP を異なる運用環境やネットワーク要件に適応させるには、イメージ変換が必要です。

警告 イメージを変換すると、工場出荷時の状態への完全なリセットが実行され、デバイス上のすべての設定とデータが削除されます。

手順

ステップ 1 **configure boot mode urwb** コマンドを使用して、CAPWAP モードから URWB モードに、または WGB/uWGB モードから URWB モードに変換します。

```
Device#configure boot mode urwb
```

または

ステップ 2 **configure boot mode capwap** コマンドを使用して、URWB モードから CAPWAP モードに、または WGB/uWGB モードから CAPWAP モードに変換します。

```
Device#configure boot mode capwap
```

または

ステップ 3 **configure boot mode wgb** コマンドを使用して、CAPWAP モードから WGB/uWGB モードに、または URWB モードから WGB/uWGB モードに変換します。

```
Device#configure boot mode wgb
```

（注）
これらのコマンドを実行すると、AP が再起動し、新しい設定が有効になります。

AP コンソールポートへのコンピュータの接続

始める前に

このタスクは、有線ネットワーク経由でのアクセスポイントへの直接アクセスが使用できない場合や不要な場合に適用できます。このタスクを実行するには、DB-9/RJ-45 シリアルケーブルと端末エミュレータ アプリケーションが必要です。

アクセスポイントを有線 LAN に接続せずにローカルで設定するには、このタスクを実行します。これにより、CLI にアクセスして必要な設定コマンドを実行できます。

手順

ステップ 1 シリアルケーブルを AP とコンピュータに接続します。

- 9 ピン DB-9/RJ-45 メスシリアルケーブルを AP の RJ-45 シリアルポートに接続します。
- ケーブルの反対側をコンピュータの COM ポートに接続します。

ステップ 2 端末エミュレータを設定します。

- コンピュータで端末エミュレータ アプリケーションを起動します。
- 端末エミュレータを次のように設定します。

パラメータ	値
ボーレート	115200 bps
データビット	8 ビット
パリティ	パリティなし
ストップビット	1 ストップビット
フロー制御	フロー制御なし

ステップ 3 AP にログインします。

- 接続時に、次の 2 つのコマンドプロンプトモードを使用できます。
  - 標準コマンドプロンプト（>）
  - 特権コマンドプロンプト（#）
- ログインしてすぐは、CLI がデフォルトで、特権のないコマンドを実行するための**標準コマンドプロンプト（>）**になります。
- **特権コマンドプロンプト（#）**に切り替えるには、`enable` コマンド（またはその省略形の `en`）を入力し、有効化パスワードを入力します。

ステップ 4 デフォルトのログイン情報を使用してログインします。

- ユーザー名：`cisco`
- パスワード：`cisco`

（注）
初期設定が完了したら、必ず、AP からシリアルケーブルを取り外してください。

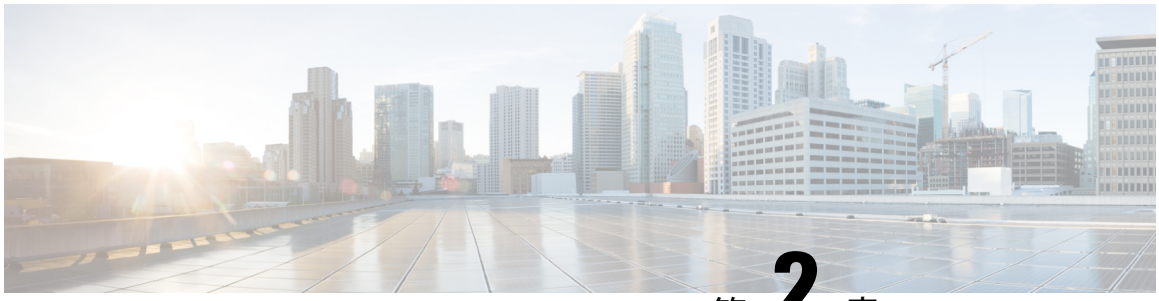
関連資料

Cisco Catalyst IW9165 高耐久性シリーズのすべてのサポート情報を確認するには、https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html [英語] を参照してください。

サポートページで提供されるドキュメントに加えて、以下のガイドの参照が必要になります。

- IW9165E ハードウェアの詳細については、『Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント ハードウェア設置ガイド』を参照してください。
- AP の機能および仕様をすべて網羅したリストは、『Cisco Catalyst IW9165 シリーズ データシート』に記載されています。
- Cisco URWB モード設定の詳細については、関連するドキュメントを参照してください。

  https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html。
- Cisco Catalyst 9800 シリーズ ワイヤレスコントローラの設定方法について詳しくは、『Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア コンフィギュレーション ガイド』を参照してください。



第 2 章

ワークグループ ブリッジ

概要と基本

ワークグループ ブリッジ

ワークグループブリッジ（WGB）は、1台の有線デバイスまたは有線デバイスのグループがワイヤレスネットワークに接続することを可能にするワイヤレスネットワーキングの機能です。

ワークグループブリッジ（WGB）モードとユニバーサル ワークグループ ブリッジ（uWGB）モードは両方とも WGB の一部であり、有線ネットワークとワイヤレスネットワークの間の円滑な接続性を実現します。

Unified Industrial Wireless（UIW）リリース 17.13.1 以降では、これらのモードの両方が、Cisco Catalyst IW9165E 高耐久性アクセスポイント（AP）およびワイヤレスクライアントでサポートされます。

WGB モード

WGB モードは、WGB のイーサネットポートに接続される有線クライアントへのワイヤレス接続を提供します。

- 有線ネットワークをワイヤレスセグメントにブリッジします。
- 接続されたイーサネット有線クライアントの MAC アドレスを学習し、これらの識別子をコントローラと共有します。これは、Internet Access Point Protocol（IAPP）メッセージングを使用して AP インフラストラクチャを介して行われます。

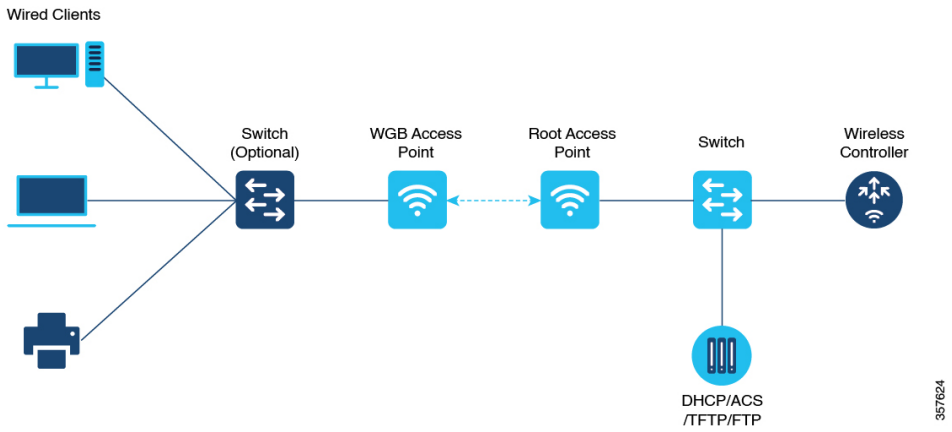
- ルート AP への単一のワイヤレス接続を確立します。ルート AP は WGB をワイヤレスクライアントとして扱います。

このモードは、ネイティブワイヤレス機能を持たない有線デバイスのワイヤレス接続を必要とする環境に最適です。

WGB モードの使用例

工場フロアで、ワイヤレス接続が組み込まれていない、センサーや PLC などの有線デバイスが使用されています。これらのデバイスはイーサネットを使用して WGB に接続し、WGB がそれらを、ルート AP への単一の接続を介してワイヤレス インフラストラクチャにブリッジします。

図 *1 : WGB* モードの実装



uWGB モード

uWGB モードは、WGB モードを補完するカテゴリであり、有線クライアントとワイヤレス インフラストラクチャ間でワイヤレスブリッジとして機能するように設計されています。

- シスコ製とシスコ製以外の両方のワイヤレスネットワークをサポートしています。
- ワイヤレスインターフェイスを使用して AP に接続し、アソシエーションに無線 MAC アドレスを使用します。
- uWGB に接続された有線クライアントの、ワイヤレスネットワークへの円なアクセスを確保します。

uWGB モードの使用例

小売店が、ワイヤレスネットワークへの接続を必要とする有線デバイスを備えた販売時点管理（POS）システムを採用しています。uWGB は、これらのデバイスを店舗のワイヤレス インフラストラクチャに接続し、シスコ製とシスコ製以外の両方のワイヤレスネットワークをサポートします。uWGB は、ワイヤレスインターフェイスを使用して AP にアソシエートされ、有線 POS デバイスとワイヤレスネットワーク間の使用例な通信を実現します。

これらのモードの両方を使用して、ワイヤレス機能を有線デバイスに効率的に拡張し、ネットワークの拡張性と柔軟性の両方を向上させます。

WGB モードと uWGB モードの主な機能の比較

次の表に、これら 2 つのモードの違いを簡単にまとめます。

機能	WGB モード	uWGB モード
接続	シスコ製のワイヤレスネットワークのみ	シスコ製とシスコ製以外のワイヤレスネットワーク
インターフェイスの使用法	イーサネットポートを使用して MAC アドレスを学習	アソシエーションに無線 MAC アドレスを使用

WGB モードに関する推奨事項

最適な性能を確保し、潜在的なネットワークの問題を回避するために、WGB モードと uWGB モードの両方の制限および制約事項を理解してください。

- WGB は Cisco Lightweight AP とのみアソシエートできます。
- 速度とデュプレックスの設定は、ローカルに接続されたエンドポイントの機能に基づいて自動的にネゴシエートされます。これらの設定は、AP の有線 0 および有線 1 インターフェイスでは手動で設定できません。
- WGB がフォーリンコントローラにローミングすると、有線クライアントは WGB ネットワークに接続できます。この場合、アンカーコントローラには有線クライアントの IP アドレスが表示されますが、フォーリンコントローラには表示されません。
- コントローラから WGB レコードの認証を解除すると、その WGB に接続されている有線クライアントのすべてのエントリが消去されます。
- WGB に接続された有線クライアントは、次をサポートしません。
  - MAC フィルタリング、
  - リンクテスト、
  - アイドルタイムアウト、および
  - Web 認証
- WGB は、適応型 802.11r で設定された WLAN とアソシエートできません。

IPv4 および IPv6 サポート

- WGB は、IPv4 が有効になっている場合でも、有線クライアントに対してのみ IPv6 トラフィックをサポートします。

- WGB がアップリンクと正常にアソシエートされている場合でも、WGB の IPv6 管理は正しく機能しません。WGB 管理 IPv6 アドレスへの IPv6 ping および SSH は機能しません。

（注） IPv6 がすでに有効になっており、IPv6 アドレスが割り当てられている場合でも、WGB で IPv6 を再度有効にしてください。

チャネル帯域幅の問題

インフラストラクチャ AP が非動的周波数選択（非 DFS）チャネルで動作しているときに、そのチャネル帯域幅が変更された場合、WGB は引き続き元のチャネル帯域幅を使用します。

（注） WGB が正しいチャネル帯域幅を使用して AP に接続していることを確認してください。

uWGB モードに関する推奨事項

- TFTP および SFTP は、uWGB モードではサポートされていません。ソフトウェアアップグレードは WGB モードでのみ実行できます。詳細については、「uWGB イメージのアップグレード」を参照してください。
- uWGB モードは、wired0 インターフェイスに接続された有線クライアントをサポートしています。ただし、wired1 インターフェイスに接続された有線クライアントはサポートしていません。
- uWGB には任意のルーティング不可能な IP アドレスを設定する必要があります。エンドデバイスと同じ範囲の静的または動的 IP アドレスを使用すると、予期しない動作が発生する可能性があります。
- UIW リリース 17.13.1 以降、uWGB モードの AP は、SSH を使用して管理されます。有線クライアントが AP に接続されていない場合、イメージのアップグレードを実行できます。
  - 有線クライアントが検出されると、uWGB モードの AP は、同じ uWGB モードのままになります。AP のイメージをアップグレードすることはできません。
  - 有線クライアントが検出されなかった場合、uWGB モードの AP は WGB モードに切り替わります。AP のイメージを管理したり、アップグレードしたりすることができます。

ログイン情報をリセットするためのガイドライン

ログイン情報要件

ネットワークデバイスのセキュリティを確保するために、初期のログイン情報をリセットします。初回ログイン後に新しいログイン情報を設定するには、次のガイドラインに従ってください。

表 *4:* ユーザー名とパスワードに関する推奨事項

ルールタイプ	詳細
ユーザー名の長さ	1 ～ 32 文字にする必要がある
パスワードの長さ	8 ～ 120 文字にする必要がある
パスワードに必須のもの	• 1 つ以上の大文字 • 1 つの小文字 • 1 つの数字、および • 1 つの記号
パスワードに使用可能なもの	• 英数字、および • 特殊文字（ASCII 10 進コード 33 ～ 126）
パスワードに使用できないもの	• "（二重引用符）、 • '（一重引用符）、および • ?（疑問符）
パスワードで不可なこと	• 3 つの連続文字をシーケンスに含める（ABC/CBA）、 • 3つ連続する同一文字（AAA）を含める、 • ユーザー名と同じものまたはユーザー名を逆にしたものにする
パスワードで必要なこと	新しいパスワードは、現在のパスワードと 4 文字以上異なる必要がある

デフォルトのログイン情報の例：

ユーザー名：**Cisco** パスワード：**Cisco** 有効化パスワード：**Cisco**

ユーザーログイン情報の例：

現在のパスワード：**Cisco** 現在の有効化パスワード：**Cisco** 新しいユーザー名：**demouser** 新しいパスワード：**DemoP@ssw0rd** 確認用の新しいパスワード：**DemoP@ssw0rd** 新しい有効化パスワード：**DemoE^aP@ssw0rd** 確認用の新しい有効化パスワード：**DemoE^aP@ssw0rd**

（注） 提示されている例では、わかりやすくするために、パスワードがプレーンテキストで表示されています。実際のシナリオでは、パスワードはアスタリスク（*）でマスクされます。

LED インジケータを使用した AP のステータスの確認

LEDパターンは、デバイスの動作ステータスと信号強度を表示するインジケータの点灯シーケンスです。

これらのパターンでは、点滅や点灯などの視覚的合図を使用して、特定の状態や評価指標を伝えます。IW9165E デバイスの場合、LED パターンは、システムステータスと信号品質を識別するために役立ちます。

IW9165E LED インジケータ

IW9165E デバイスは、前面パネルに 2 つの LED を備えています。

1. システム ステータス LED
2. RSSI ステータス LED

表 *5:* 視覚的リファレンス：*LED* ステータスインジケータ

LED	色またはパターン	説明
システム ステータス LED	赤色の点滅	WGBのアソシエートが解除されています。
	緑色の点灯	WGB が親 AP にアソシエートされています。
RSSI ステータス LED	緑色の点灯	RSSI が - 71 dBm 以上です。
	緑色の点滅	RSSI が -81 ～ -70 dBm です。
	黄色の点灯	RSSI が -95 ～ -81 dBm です。
	オフ	RSSI が指定範囲外です。

初期セットアップとコア設定

WLAN プロファイルの設定

手順

この手順の目的は、WLAN を設定し、関連する設定を指定することにより、ワークグループブリッジ（WGB）がワイヤレスネットワークに参加できるようにすることです。この設定を完了すると、確実に、WGB がアクセスポイント（AP）とのセキュアで信頼性の高い通信を確立できるようになります。これにより、適切なネットワーク接続を維持できます。

ステップ 1 **wlan** *profile-name* コマンドを使用して、WLAN 設定サブモードを開始します。

```
Device# wlan test-wlan
```

ここで、*profile-name* は、設定する WLAN の名前です。

ステップ 2 **ccx aironet-iesupport** コマンドを使用して、Cisco Client Extensions（CCX）オプションを設定し、WLAN での Aironet 情報要素（IE）のサポートを有効にします。

```
Device# ccx aironet-iesupport
```

（注）
この設定は、WGB を AP にアソシエートするために必須です。

ワイヤレス ポリシー プロファイルの設定

ワイヤレス ポリシー プロファイルを設定し、AP で WGB の VLAN クライアントサポートを有効にするには、このタスクを実行します。これにより、ネットワーク内の WGB の円滑なクライアント接続と適切な VLAN 割り当てが確保されます。

始める前に

- 設定する前に、デバイスに対する管理アクセス権を持っていることを確認してください。
- 割り当てる VLAN ID が存在し、ネットワーク インフラストラクチャで設定されていることを確認してください。

手順

ステップ 1 **wireless profile policy** *profile-policy* コマンドを使用して、目的のプロファイルのワイヤレス ポリシー コンフィギュレーション モードにアクセスします。

```
Device# wireless profile policy Corp-Policy
```

ステップ 2 **vlan** *vlan-id* コマンドを使用して、WLAN ポリシープロファイルを、対応する VLAN ID にマッピングします。

```
Device# vlan 20
```

ステップ 3 **wgb vlan** コマンドを使用して、WGB の VLAN クライアントサポートを有効にします。

```
Device# wgb vlan
```

IP アドレスの設定

IPv4 アドレスの設定

DHCP または静的設定のいずれかを使用してデバイスで IPv4 アドレスを設定するには、このタスクを実行します。このタスクを実行することにより、適切なネットワーク接続とデバイス管理を確保できます。

手順

ステップ 1 次のいずれかのオプションを使用して、デバイスで IPv4 アドレスを設定します。

オプション	説明
IPv4 アドレスの動的取得	**configure ap address ipv4 dhcp** コマンドを使用します。 `Device# configure ap address ipv4 dhcp`
静的 IPv4 アドレスの手動割り当て	**configure ap address ipv4 static** *ipv4_addr netmask gateway* コマンドを使用します。 `Device# configure ap address ipv4 static 192.168.10.25 255.255.255.0 192.168.10.1`

ステップ 2 （オプション）**show ip interface brief** コマンドを使用して、現在の IP アドレス設定を表示します。

```
Device# show ip interface brief
```

IPv6 アドレスの設定

デバイスの IPv6 アドレスを設定するには、このタスクを実行します。

手順

ステップ 1 次のいずれかのオプションを使用して、デバイスで IPv6 アドレスを設定または取得します。

オプション	説明
IPv6 アドレスの動的取得	**configure ap address ipv6 dhcp** コマンドを使用します。 `Device# configure ap address ipv6 dhcp`
IPv6 アドレスの自動取得	**configure ap address ipv6 auto-config enable** コマンドを使用します。 `Device# configure ap address ipv6 auto-config enable` （注） IPv6 自動設定を有効にすると、ステートレスアドレス自動設定（SLAAC）もアクティブになりますが、SLAAC は WGB の CoS には適用されません。このコマンドでは、SLAAC の代わりに DHCPv6 を使用して IPv6 アドレスを設定します。 **configure ap address ipv6 auto-config disable** コマンドを使用して、AP で IPv6 自動設定を無効にします。
静的 IPv6 アドレスの手動割り当て	**configure ap address ipv6 static** *ipv6_addr prefix-length gateway* コマンド使用します。 `Device# configure ap address ipv6 static 2001:db8:abcd:100::25 64 2001:db8:abcd:100::1` 静的 IPv6 アドレスを設定すると、アップリンク接続がない場合でも、有線インターフェイスを介して AP を管理できます。

ステップ 2 （オプション）**show ipv6 interface brief** コマンドを使用して、現在の IP アドレス設定を確認します。

```
Device# show ipv6 interface brief
```

無線インターフェイスでの WGB の設定

ワークグループブリッジ（WGB）は、非ワイヤレスの有線デバイスがワイヤレスネットワークにアクセスする方法を提供します。ブリッジとして機能することにより、WGB は、有線エンドポイントを WLAN に接続して、ネイティブ Wi-Fi 機能を持たない機器にワイヤレス接続を拡張します。この機能を有効にするには、最初に、ワイヤレスパラメータを定義する SSID プロファイルを作成する必要があります。次に、WGB が無線インターフェイスで設定されます。その後、 SSID プロファイルがインターフェイスに関連付けられ、接続が確立されます。

process_summary

WGB は、非ワイヤレスデバイスがワイヤレスネットワークに接続することを可能にします。この設定には、SSID プロファイルの作成、無線インターフェイスでの WGB の設定、および SSID プロファイルのインターフェイスへの関連付けが含まれます。

process_workflow

1. SSID プロファイルの作成

   ネットワーク要件に基づいて認証方式を選択します。

2. 無線インターフェイスの設定

   無線インターフェイスの設定にアクセスします。必要な設定を適用して WGB 機能を有効にします。

3. 無線への SSID プロファイルの関連付け

   先に作成した SSID プロファイルを無線インターフェイスにつなぎます。これにより、接続が確立します。

4. 無線インターフェイスの有効化

   無線インターフェイスをアクティブ化して WGB の設定を完了します。これにより、動作が開始されます。

SSID プロファイルの作成

始める前に

ネットワークの認証要件を満たし、ユーザーのセキュアなアクセスを確保する SSID プロファイルを設定するには、このタスクを実行します。

手順

ネットワーク要件に基づいて SSID プロファイルの認証プロトコルを選択します。

次のオプションがあります。

- [Open authentication]：ユーザーログイン情報を必要としないアクセスを可能にします。オープン認証を使用した SSID プロファイルの設定 （21 ページ）
- [PSK authentication]：セキュアなアクセスのための暗号化を提供します。PSK 認証を使用した SSID プロファイルの設定 （21 ページ）
- [Dot1x authentication]：ユーザー検証に一元化認証サーバーを利用します。Dot1x 認証を使用した SSID プロファイルの設定 （22 ページ）

（注）

PSK 設定の場合は、事前共有鍵が強力であり、推奨されるセキュリティプラクティスに従っていることを確認してください。

オープン認証を使用した SSID プロファイルの設定

オープン認証により、デバイスはログイン情報を必要とせずにネットワークに接続できます。これは、ゲストネットワークやパブリックアクセスポイントなどの特定のシナリオに適しています。

手順

オープン認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication open** コマンドを使用します。

```
Device# configure ssid-profile Guest-WiFi ssid Guest authentication open
```

PSK 認証を使用した SSID プロファイルの設定

PSK認証では、ユーザーに共有鍵を提供することにより、ワイヤレスネットワークが保護されます。このタスクでは、さまざまな鍵管理プロトコルに合わせて調整された、PSK認証を使用して SSID プロファイルを設定する手順について説明します。

手順

WPA2、802.11r、または 802.11w のいずれかのオプションを使用して、PSK 認証で SSID を設定します。

オプション	説明
強化されたワイヤレスセキュリティ	**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** コマンドを使用します。 `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management wpa2`
モバイルデバイスの高速ローミング	**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** コマンド使用します。 `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management dot11r`

オプション	説明
管理フレーム保護	**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** コマンドを使用します。 `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management dot11w`

Dot1x 認証を使用した SSID プロファイルの設定

Dot1x認証は、アクセスを許可する前にユーザーのログイン情報を要求することでセキュリティを強化するネットワークアクセス制御方式です。このタスクでは、適切な鍵管理オプションを使用して SSID プロファイルを設定する手順を説明します。

Dot1x認証を使用してSSIDプロファイルをセットアップし、拡張可能認証プロトコル（EAP）を使用してセキュアなネットワークアクセスを確保するには、このタスクを実行します。

手順

configure ssid-profile *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}} コマンドを使用して、Dot1x 認証を使用して SSID プロファイルを設定します。

```
Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication eap profile EAP-Profile1
key-management wpa2
```

次の場合...	次の操作を実行します。
高速ローミングを有効にする場合	**dot11r** 鍵管理オプションを使用します。
WPA2 セキュリティが必要な場合	**wpa2** 鍵管理オプションを使用します。
管理フレーム保護が必要な場合	**dot11w** 鍵管理オプションを **optional** または **required** とともに使用します。

Dot1x EAP-PEAP 認証による SSID プロファイルの設定

始める前に

Dot1x EAP-PEAP 認証を使用してセキュアな SSID プロファイルをセットアップするには、このタスクを実行します。これにより、ワイヤレスネットワークのセキュリティが強化されます。

このタスクは、Dot1x EAP-PEAP 認証をサポートするデバイスでワイヤレスプロファイルを設定する場合に適用されます。これにより、確実に、指定されたユーザー名とパスワードを使用してデバイスを安全に認証できるようになります。

手順

ステップ 1 **configure dot1x credential** *credential_name* **username** *username* **password** *password* コマンドを使用して、Dot1x ログイン情報を作成します。

```
Device# configure dot1x credential Corp-Cred username corpuser password C!sc0Str0ng
```

ステップ 2 **configure eap-profile** *profile_name* **dot1x-credential** *credential_name* コマンドを使用して、EAP プロファイルを設定し、設定済みの Dot1x ログイン情報に関連付けます。

```
Device# configure eap-profile Corp-EAP dot1x-credential Corp-Cred
```

ステップ 3 **configure eap-profile** *profile_name* **method peap** コマンドを使用して、プロファイルの EAP 方式を PEAP として定義します。

```
Device# configure eap-profile Corp-EAP method peap
```

ステップ 4 **configure ssid-profile** *ssid-profile-name* **ssid** *ssid name* **authentication eap profile** *eap-profile-name* **key-management wpa2** コマンドを使用して、SSID プロファイルを作成し、EAP プロファイルを使用して認証をセットアップします。

```
Device# configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1 key-management
 wpa2
```

WGB の無線インターフェイスの設定

Before you begin

IW9165E デバイスは、2.4 GHz 無線機をサポートしていません。そのため、WGB モードで動作するアップリンクとして設定できるのは dot11radio 1 インターフェイスのみです。

WGB モードを有効にし、適切な SSID プロファイルへの接続を確立するように無線インターフェイスを設定します。

手順

ステップ 1 **configure dot11radio** *slot_id* **mode wgb ssid-profile** *ssid-profile-name* コマンドを使用して、無線インターフェイスを WGB SSID プロファイルに設定します。

```
Device# configure dot11radio 1 mode wgb ssid-profile Corp-WiFi
```

（注）
使用されている SSID プロファイルがすでに設定されており、デバイスからアクセスできることを確認してください。

ステップ 2 **configure dot11radio** *slot_id* **enable** コマンドを使用して、無線インターフェイスを有効にします。

```
Device# configure dot11radio 1 enable
```

ステップ 3 （オプション）**configure dot11radio** *slot_id* **disable** コマンドを使用して、無線インターフェイスを無効にします。

```
Device# configure dot11radio 1 disable
```

セキュリティパラメータの設定

WGB のセキュリティパラメータを設定して、ワイヤレス通信のセキュアな認証および暗号化を確保するには、このプロセスを使用します。

手順

ステップ 1 デバイスパラメータをセットアップします。

- デバイスのユーザー名とパスワードを設定します。
- 正確な時刻の同期を確保するために NTP サーバーを設定します。
- ホスト名を定義し、有効な IP アドレスを割り当てます。

ステップ 2 トラストポイントを作成し、インポートします。

トラストポイントを確立し、お好みの方法で必要な証明書をインポートします。

ステップ 3 （オプション）dot1x ログイン情報を設定します。

セットアップで必要な場合は、必要な dot1x のユーザー名とパスワードのログイン情報を入力します。

ステップ 4 EAP プロファイルを作成します。

EAP メソッド、トラストポイント名、および dot1x ログイン情報（オプション）を EAP プロファイルにマッピングします。

ステップ 5 EAP プロファイルを SSID プロファイルに結び付けます。

EAP プロファイルを目的の SSID プロファイルに関連付けて、セキュアなワイヤレス接続を有効にします。

ステップ 6 SSID プロファイルを無線機に結び付けます。

SSID プロファイルを優先無線機インターフェイスにつなぎ、設定をアクティブにします。

（注）

- 認証の失敗を避けるために、NTP サーバーが到達可能であり、証明書が有効であることを確認してください。
- システムの完全性を維持するために、セキュアな方法を使用して証明書をインポートしてください。

• 証明書のインポートが失敗した場合は、証明書の形式を確認し、有効な方法を使用してインポートしなおします。

次のタスク

（注） dot1x ログイン情報プロファイル、トラストポイントプロファイル、または EAP プロファイルに変更を加えても、変更はすぐには有効になりません。変更を適用するには、EAP プロファイルを SSID プロファイルに手動でもう一度アタッチする必要があります。

configure ssid-profile *ssid_prof_name* **ssid** *ssid***authentication eap profile** *eap_prof_name* **key-management** *key_type* コマンドを使用して、EAP プロファイルを SSID プロファイルに再アタッチします。

```
Device# configure ssid-profile Corp-SSID ssid CorpNet authentication eap profile Corp-EAP
 key-management wpa2
```

EAP プロファイルの設定

このタスクでは、拡張可能認証プロトコル（EAP）プロファイルを設定して、ネットワークのセキュアで効率的な認証を確保するために必要な手順を説明します。

始める前に

EAP プロファイルは、ワイヤレスクライアントのセキュア認証を確保する上で重要です。プロファイルを正しく設定することにより、Dot1x ログイン情報、 SSID プロファイル、および無線設定との円滑な統合を確実に実現できます。

EAP プロファイルの設定を開始する前に、次のことを確認します。

1. 有効な Dot1x ログイン情報プロファイルがすでに作成されている。
2. SSID プロファイルが設定されている。
3. SSID をアタッチする無線機が正しくセットアップされている。
4. デバイスの CLI への管理アクセスが可能である。

手順

ステップ 1 **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} コマンドを使用して、希望のメソッドで EAP プロファイルを設定します。

```
Device# configure eap-profile Corp-EAP method peap
```

次の場合...	次の操作を実行します。
EAP プロファイルに TLS メソッドが選択されている場合	手順 2 を使用して CA トラストポイントをアタッチします。
プロファイルが不要になった場合	手順 4 を使用して EAP プロファイルを削除します。

ステップ 2 **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} コマンドを使用して、TLS の CA トラストポイントをアタッチします。デフォルトでは、WGB は認証に内部 MIC 証明書を使用します。

```
Device#configure eap-profile Corp-EAP trustpoint default
```

ステップ 3 **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* コマンドを使用して、Dot1x ログイン情報プロファイルをアタッチします。

```
Device#configure eap-profile Corp-EAP dot1x-credential Corp-Cred
```

ステップ 4 （オプション）**configure eap-profile** *profile-name* **delete** コマンドを使用して、EAP プロファイルを削除します。

```
Device#configure eap-profile Corp-EAP delete
```

Dot1x ログイン情報の設定

このタスクでは、Dot1X ログイン情報を設定して、デバイスが 802.1X 認証用に正しくセットアップされていることを確認します。これにより、セキュアなアクセス制御とネットワーク保護が実現されます。

手順

ステップ 1 **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* コマンドを使用して、Dot1X ログイン情報を設定します。

```
Device# configure dot1x credential Corp-Cred username corpuser password C!sc0Str0ng
```

ステップ 2 （オプション）**show wgb eap dot1x credential profile** コマンドを使用して、WGB EAP Dot1x プロファイルのステータスを表示します。

```
Device# show wgb eap dot1x credential profile
```

端末のトラストポイントの手動登録設定

この手順では、端末ベースの登録のためにトラストポイントを手動で設定する方法について説明します。信頼できる証明書を使用できるようにすることで、デバイスと認証局（CA）サーバー間のセキュアな通信を確保します。

手順

ステップ 1 **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** コマンドを使用して、WGB でトラストポイントを作成します。

```
Device# configure crypto pki trustpoint Corp-CA enrollment terminal
```

ステップ 2 **configure crypto pki trustpoint** *ca-server-name* **authenticate** コマンドを使用して、トラストポイントを手動で認証します。

base-64 でエンコードされた CA 証明書を入力し、「quit」と入力して終了します。中間証明書を使用する場合は、必ず、証明書チェーン全体をトラストポイントにインポートしてください。

```
Device# configure crypto pki trustpoint demotp authenticate Enter the base 64 encoded CA certificate.
 ....And end with the word "quit" on a line by itself.... -----BEGIN CERTIFICATE----- [base64 encoded
 root CA certificate] -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- [base64 encoded
intermediate CA certificate] -----END CERTIFICATE----- quit
```

ステップ 3 **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* コマンドを使用して、秘密鍵長を設定します。

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

ステップ 4 **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] コマンドを使用して、トラストポイントのサブジェクト名を設定します。

```
Device# configure crypto pki trustpoint Corp-CA subject-name
CN=AP1.cisco.com,C=US,ST=California,L=SanJose,O=CorpNet,OU=IT,email=admin@cisco.com
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name* **enroll** コマンドを使用して、秘密鍵と CSR を生成します。

```
Device# configure crypto pki trustpoint Corp-CA enroll
```

（注）
CA サーバーで、CSR 出力を使用して、デジタル署名付き証明書を作成してください。

ステップ 6 **configure crypto pki trustpoint** *ca-server-name* **import certificate** コマンドを使用して、署名付き証明書をインポートします。

```
Device# configure crypto pki trustpoint Corp-CA import certificate
```

base64 でエンコードされた CA 証明書を入力し、「quit」と入力して証明書のインポートを完了します。

ステップ 7 （オプション）**configure crypto pki trustpoint** *trustpoint-name* **delete** コマンドを使用して、トラストポイントを削除します。

```
Device# configure crypto pki trustpoint Corp-CA delete
```

ステップ 8 （オプション）**show crypto pki trustpoint** コマンドを使用して、すべてのトラストポイントのサマリーを表示します。

```
Device# show crypto pki trustpoint
```

ステップ 9 （オプション）**show crypto pki trustpoint** *trustpoint-name* **certificate** コマンドを使用して、トラストポイント用に作成された証明書の内容を表示します。

```
Device# show crypto pki trustpoint Corp-CA certificate
```

トラストポイント自動登録の設定

WGB 上のトラストポイントの自動登録を設定し、セキュアな証明書管理と合理化された運用を確保するには、このタスクを実行します。

手順

ステップ 1 **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* コマンドを使用して、サーバー URL を使用して WGB でトラストポイントを登録します。

```
Device#configure crypto pki trustpoint Corp-CA enrollment url http://10.10.10.5:80
```

ステップ 2 **configure crypto pki trustpoint** *ca-server-name* **authenticate** コマンドを使用して、トラストポイントを認証します。

```
Device# configure crypto pki trustpoint Corp-CA authenticate
```

（注）
このコマンドにより、CA サーバーから認証局（CA）証明書が自動的に取得されます。

ステップ 3 **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* コマンドを使用して、秘密鍵長を設定します。

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

ステップ 4 **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] コマンドを使用して、サブジェクト名を設定します。

```
Device# configure crypto pki trustpoint Corp-CA subject-name
CN=AP1.cisco.com,C=US,ST=California,L=SanJose,O=CorpNet,OU=IT,email=admin@cisco.com
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name* **enroll** コマンドを使用して、トラストポイントを登録します。

```
Device#configure crypto pki trustpoint Corp-CA enroll
```

（注）
この手順では、CA サーバーのデジタル署名付き証明書を要求します。

ステップ 6 **configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* コマンドを使用して、自動登録を有効にします。

```
Device#configure crypto pki trustpoint Corp-CA auto-enroll enable renew-percentage
```

（注）
configure crypto pki trustpoint *ca-server-name* **auto-enroll disable** コマンドを使用して、自動登録を無効にします。

ステップ 7 （オプション）**configure crypto pki trustpoint** *trustpoint-name* **delete** コマンドを使用して、トラストポイントを削除します。

```
Device# configure crypto pki trustpoint Corp-CA delete
```

ステップ 8 （オプション）**show crypto pki trustpoint** コマンドを使用して、すべてのトラストポイントのサマリーを表示します。

```
Device# show crypto pki trustpoint
```

ステップ 9 （オプション）**show crypto pki trustpoint** *trustpoint-name* **certificate** コマンドを使用して、トラストポイント用に作成された証明書の内容を表示します。

```
Device# show crypto pki trustpoint trustpoint-name certificate
```

TFTP サーバーを使用した手動での証明書の登録設定

TFTP サーバーを使用して手動で証明書を登録するには、このタスクを実行します。これにより、トラストポイントの証明書を取得、認証、および管理することで、セキュアな通信を確保できます。

手順

ステップ 1 **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* コマンドを使用して、トラストポイントの CA およびクライアント証明書を取得します。

```
Device# configure crypto pki trustpoint Corp-CA enrollment tftp 192.168.1.100/certs/corp-ca-cert.pem
```

ステップ 2 **configure crypto pki trustpoint** *ca-server-name* **authenticate** コマンドを使用して、指定された TFTP サーバーから CA 証明書を取得および認証します。

```
Device# configure crypto pki trustpoint Corp-CA authenticate
```

（注）
このコマンドでは、指定された TFTP サーバーから CA 証明書を取得して認証します。ファイル指定が含まれている場合、WGB は指定されたファイル名に **.ca** という拡張子を付加します。

ステップ 3 **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* コマンドを使用して、秘密鍵長を設定します。

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

ステップ 4 **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] コマンドを使用して、サブジェクト名を設定します。

```
Device# configure crypto pki trustpoint Corp-CA subject-name
CN=AP1.cisco.com,C=US,ST=California,L=SanJose,O=CorpNet,OU=IT,email=admin@cisco.com
```

ステップ 5 秘密鍵と証明書署名要求（CSR）を生成します。

configure crypto pki trustpoint *ca-server-name* **enroll** コマンドを使用して、秘密鍵と CSR を生成し、この要求を TFTP サーバーに送信します。

```
Device#configure crypto pki trustpoint Corp-CA enroll
```

（注）
このコマンドでは、証明書要求が生成され、この要求が TFTP サーバーに送信されます。書き込まれるファイル名には **.req** という拡張子が付加されます。

ステップ 6 署名済み証明書をインポートします。

configure crypto pki trustpoint *ca-server-name* **import certificate** コマンドを使用して、署名済み証明書を WGB にインポートします。

```
Device#configure crypto pki trustpoint Corp-CA import certificate
```

コンソール端末は TFTP を使用して証明書をインポートし、WGB は TFTP から承認済み証明書の取得を試みます。書き込まれるファイル名には **.req** という拡張子が付加されます。

ステップ 7 （オプション）**show crypto pki trustpoint** コマンドを使用して、すべてのトラストポイントのサマリーを表示します。

```
Device# show crypto pki trustpoint
```

ステップ 8 （オプション）**show crypto pki trustpoint** *trustpoint-name* **certificate** コマンドを使用して、トラストポイント用に作成された証明書の内容を表示します。

```
Device# show crypto pki trustpoint Corp-CA certificate
```

TFTP サーバーを使用した PKCS12、PFX、または P12 証明書登録の設定

このタスクにより、EAP-TLS 認証および秘密鍵の設定のために、完全な PKCS12 証明書バンドルをインポートできます。これにより、WGB モードでのセキュアな通信およびデバイス認証を確保できます。

手順

ステップ 1 **configure crypto pki trustpoint** *trustpoint_name* **import pkcs12 tftp** *tftp://IP_ADDRESS/path_to_certificate* **password** *certificate_password* コマンドを使用して、EAP-TLS 認証および秘密鍵用の完全な PKCS12 証明書バンドルをインポートします。

```
Device# configure crypto pki trustpoint Corp-CA import pkcs12 tftp tftp://1.2.3.4/corp-ca.p12
```

ステップ 2 （オプション）**show crypto pki trustpoint** コマンドを使用して、ダウンロードした PKCS12 証明書を確認します。

```
Device# show crypto pki trustpoint Crypto PKI trustpoints are:-
============================================================== Trustpoint name : example Enrollment
 method : TFTP TFTP path : tftp://192.168.0.1/users/example/ca CA-Cert file :
/storage/wbridge_pki_cert/example/example_ca.pem Subject :
```

```
C=US,ST=Unknown,L=Unknown,O=Cisco,OU=Wnbu,CN=ap.cisco.com ,emailAddress=wgb@cisco.com Key size :
2048
```

PKI タイマー情報の確認

手順

Public Key Infrastructure（PKI）タイマー情報を表示するには、**show crypto pki timers** コマンドを使用します。

```
Device#show crypto pki timers
```

WGB または uWGB タイマーの設定

アソシエーション、認証、EAP、およびブリッジクライアントの応答に関する適切なタイムアウト設定を確保するには、WGB モードまたは uWGB モードのタイマーを設定します。タイマーを設定するための CLI コマンドは、WGB モードと uWGB モードの両方で同じです。

アソシエーション応答のタイムアウトの設定

手順

configure wgb association response timeout *response-millisecs* コマンドを使用して、WGB アソシエーション応答のタイムアウトを設定します。

```
Device#configure wgb association response timeout 400
```

- デフォルト値：100 ミリ秒
- 有効な範囲：100 ～ 5000 ミリ秒

認証応答のタイムアウトの設定

手順

configure wgb authentication response timeout *response-millisecs* コマンドを使用して、WGB 認証応答のタイムアウトを設定します。

```
Device#configure wgb authentication response timeout 400
```

- デフォルト値：100 ミリ秒
- 有効な範囲：1 ～ 5000 ミリ秒

EAP のタイムアウトの設定

手順

configure wgb eap timeout *timeout-secs* コマンドを使用して、WGB EAP のタイムアウトを設定します。

```
Device#configure wgb eap timeout 15
```

- デフォルト値：3 秒
- 有効な範囲：2 ～ 60 秒

ブリッジクライアント応答のタイムアウトの設定

手順

configure wgb bridge client timeout *timeout-secs* コマンドを使用して、WGB のブリッジクライアント応答のタイムアウトを設定します。

```
Device#configure wgb bridge client timeout 400
```

- デフォルト値：300 秒
- 有効な範囲：10 ～ 1,000,000 秒

WGB 有線クライアントの認証解除

clear wgb client {**all** | **single** *mac-addr*} コマンドを使用して、WGB 有線クライアントの認証を解除します。

```
Device#clear wgb client all
```

無線インターフェイスでの uWGB の設定

uWGB モードは、アップリンク無線 MAC アドレスを使用してサードパーティ AP と関連付けることができるため、uWGB ロールは 1 つの有線クライアントのみをサポートします。

手順

---

configure dot11 *slot_id* **mode uwgb** *uwgb_wired_client_mac_address* **ssid-profile** *ssid-profile* コマンドを使用して、有線クライアントの MAC アドレスを設定します。

```
Device# configure dot11 1 mode uwgb 00:11:22:33:44:55 ssid-profile IoT-SSID
```

（注）
WGB 設定のほとんどが uWGB にも適用されます。唯一の違いは、このコマンドを使用して有線クライアントの MAC アドレスを設定することです。

次のタスク

これらの設定は、uWGB セットアップに関する詳細情報の概要を示しています。設定は WGB と uWGB の両方に共通です。

- SSID プロファイルの作成 （20 ページ）
- dot1x ログイン情報の設定
- EAP-TLS セキュリティの設定
- EAP プロファイルの設定
- 端末のトラストポイントの手動登録設定
- WGB のトラストポイント自動登録の設定
- TFTP サーバーを使用した手動での証明書の登録設定
- TFTP サーバーを使用した PKCS12、PFX、または P12 証明書登録の設定
- WGB または uWGB タイマーの設定

WGB モードと uWGB モード間の変換

WGB モードから uWGB モードへの変換

デバイスを WGB モードから uWGB モードに変換するには、このタスクを実行します。この変換により、目的の SSID プロファイルを使用して、確実に、機能を拡張し、有線クライアントと統合できます。

手順

configure dot11radio *radio_slot_id* **mode uwgb** *wired_client_mac* **ssid-profile** *ssid_profile_name* コマンドを使用して、WGB モードから uWGB モードに変換します。

```
Device#configure dot11radio 1 mode uwgb 00:11:22:33:44:55 ssid-profile IoT_Profile
```

uWGB モードから WGB モードへの変換

AP を uWGB モードから WGB モードに変換して、WGB モードで機能できるようにするには、この手順を実行します。

手順

ステップ 1 **configure dot11radio** *radio_slot_id* **mode wgb ssid-profile** *ssid_profile_name* コマンドを使用して、uWGB モードから WGB モードに変換します。この変換を行うと、AP が再起動されます。

```
Device# configure dot11radio 1 mode wgb ssid-profile IoT_Profile This command will reboot with
downloaded configs. Are you sure you want continue? [confirm]
```

ステップ 2 コマンドを入力すると、アクションの確認を求めるプロンプトが表示されます。この手順は、AP が再起動して新しい設定を適用するために必要です。

プロンプトが表示されたら、「**confirm**」と入力して変換を続行します。

WGB 設定のインポートとエクスポート

WGB 設定のインポート

展開内のすべての WGB にサンプル設定ファイルをダウンロードするには、このタスクを実行します。これにより、確実に、適切な動作に必要な設定でデバイスが設定されます。

手順

copy configuration download {**tftp:**| **sftp:scp:**| | **http:**}*ip-address* [*directory*] [*file-name*] コマンドを使用して、展開内のすべての WGB にサンプル設定をダウンロードします。

```
copy configuration download tftp: 192.168.1.100 configs startup-config.cfg
```

（注）

- **copy configuration download** コマンドを実行すると、AP の再起動が開始されます。新しい設定は、再起動後にのみ有効になります。
- 指定された `sftp:` または `tftp:` サーバーから設定ファイルにアクセスできることと、ファイルパスが正しく指定されていることを確認してください。

WGB 設定のエクスポート

既存の WGB の設定をエクスポートして、その設定を新しく展開された WGB で再利用できるようにします。これにより、一貫性が確保され、展開が簡素化されます。

適切なプロトコルを使用して、WGB の現在の設定をサーバーにアップロードできます。この設定ファイルを後でダウンロードして追加の WGB を設定することができ、セットアッププロセスが合理化されます。

手順

サーバーへの WGB 設定のアップロード

copy configuration upload {**tftp:**| **sftp:**| **scp:**| **http:**}*ip-address* [*directory*] [*file-name*] コマンドを使用して、既存の WGB で使用されている設定をサーバーにアップロードします。

```
Device# copy configuration upload tftp: 192.168.1.100 configs running-config.cfg
```

uWGB イメージのアップグレード

uWGB ソフトウェアイメージをアップグレードするには、まず、デバイスを uWGB モードから WGB モードに変換します。これは、uWGB モードが、イメージのアップグレードのために TFTP または SFTP プロトコルをサポートしていないためです。次に、TFTP または SFTP プロトコルを使用してソフトウェアイメージをダウンロードします。ダウンロードしたら、ソフトウェアイメージをインストールしてアップグレードを完了します。最後に、デバイスを WGB モードから uWGB モードに戻します。

手順

ステップ 1 TFTP または SFTP サーバーを uWGB の有線 0 ポートに接続します。

ステップ 2 **configure Dot11Radio** *slot_id* **disable** コマンドを使用して、無線インターフェイスを無効にします。

```
Device#configure Dot11Radio 1 disable
```

ステップ 3 **configure Dot11Radio** *slot_id* **mode wgb ssid-profile** *ssid_profile_name* コマンドを使用して、既存の SSID プロファイルを使用してデバイスを WGB モードに設定します。

```
Device# configure Dot11Radio 1 mode wgb ssid-profile WGB-SSID

 This command will reboot with downloaded configs. Are you sure you want continue? <confirm>
```

（注）
このコマンドは、ダウンロードされた設定でデバイスを再起動します。

ステップ 4 **configure ap address ipv4 static** *IPv4_address netmask Gateway_IPv4_address* コマンド使用して、デバイスに静的 IP アドレスを割り当てます。

```
Device# configure ap address ipv4 static 192.168.1.101 255.255.255.0 192.168.1.1
```

ステップ 5 **ping** *server_IP* コマンドを使用して、サーバーへの ICMP 接続をテストします。

```
Device# ping 192.168.1.20 Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds PING
 192.168.1.20 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0.858/0.932/1.001
ms
```

ステップ 6 **archive download/reload** [**tftp | sftp | http**] ://*server_ip*/*file_path* コマンドを使用して、TFTP、SFTP、または HTTP を使用して uWGB イメージをダウンロードおよびアップグレードします。

```
archive download /reload tftp://192.168.1.100/xxxx_iosxe.17.13.01.SPA.bin
```

ステップ 7 **configure Dot11Radio** *slot_id* **mode uwgb** *wired_client_mac_addr* **ssid-profile** *ssid_profile_name* コマンドを使用して、デバイスを uWGB モードに戻します。

```
Device#configure Dot11Radio 1 mode uwgb 0011.2233.4455 ssid-profile uWGB-SSID
```

高度な機能と最適化

高スループットでの伝送レートの設定

移動体の展開で WGB の高スループット伝送レートを設定するには、このタスクを実行します。高スループット変調および符号化方式（MCS）を使用して、伝送レートを手動で制限できます。

手順

ステップ 1 **config dot11radio** *interface* **802.11ax disable** コマンドを使用して、指定した dot11radio インターフェイスで 802.11ax 標準規格を無効にします。

```
Device# config dot11radio 1 802.11ax disable
```

ステップ 2 **config dot11radio** *interface* **802.11ac disable** disable コマンドを使用して、選択した dot11radio インターフェイスで 802.11ax 標準規格を無効にします。

```
Device# config dot11radio 1 802.11ac disable
```

ステップ 3 **config dot11radio** *interface speed ht-mcs m4 m5* コマンドを使用して、指定した dot11radio インターフェイスに必要な HT MCS レートを設定します。このアクションは、必要な伝送レートを達成するために役立ちます。

```
Device# config dot11radio 1 speed ht-mcs m4 m5
```

ステップ 4 （オプション）**debug wgb dot11 rate** コマンドを使用して、WGB Tx MCS レートを確認します。このコマンドの出力例を示します。

```
JWGB1#debug wgb dot11 rate
[*10/14/2023 03:16:08.6175]
[*10/14/2023 03:16:08.6175]                MAC    Tx-Pkts    Rx-Pkts                Tx-Rate(Mbps)              Rx-Rate(Mbps)  RSSI Tx-Retries
[*10/14/2023 03:16:08.6175] 24:16:1B:F8:02:6E          0          0          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70          0
JWGB1#[*10/14/2023 03:16:09.6179] 24:16:1B:F8:02:6E        330          3          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         15
[*10/14/2023 03:16:10.6183] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         25
[*10/14/2023 03:16:11.6187] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:12.6190] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         13
[*10/14/2023 03:16:13.6194] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         21
[*10/14/2023 03:16:14.6198] 24:16:1B:F8:02:6E        331          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         16
[*10/14/2023 03:16:15.6202] 24:16:1B:F8:02:6E        328          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         24
[*10/14/2023 03:16:16.6206] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         21
[*10/14/2023 03:16:17.6210] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         22
[*10/14/2023 03:16:18.6214] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         22
[*10/14/2023 03:16:19.6218] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:20.6221] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -71         17
[*10/14/2023 03:16:21.6258] 24:16:1B:F8:02:6E        328          3          HT-20,1SS,MCS5,(52)        HT-20,1SS,MCS5,SGI(57)   -70         16
```

WGB のレガシーレートの設定

必要に応じて、WGB のレガシーレートを設定することもできます。

手順

config dot11radio *interface* **speed legacy-rate***legacy-rate* コマンドを使用して、dot11radio インターフェイスで特定のレガシーレートを設定します。

```
Device# config dot11radio 1 speed legacy-rate basic-6.0
```

- 802.11 管理フレームと制御フレームの両方でレガシーレートが使用されます。

- WGBのアソシエーションの失敗を回避するために、WGBのレガシーレートがアクセスポイント（AP）のレガシーレートと一致するか重複していることを確認してください。

802.11v 機能

802.11v は、ワイヤレスネットワーク管理の標準規格で、

- ネットワーク支援型ローミングを有効にしてクライアントの接続を最適化し、
- クライアントデバイスにガイダンスを提供することでクライアントの負荷分散を支援し、
- 管理フレームと手順の改善により、ワイヤレス性能を向上させます。

802.11v は、IEEE 802.11 ファミリの Wi-Fi 標準規格に含まれています。ネットワーク支援型ローミングなどの機能が含まれています。この機能により、ネットワーク インフラストラクチャ（ワイヤレスコントローラなど）がクライアントをより適切なアクセスポイント（AP）に誘導できるため、輻輳が軽減され、ネットワーク全体の効率が向上します。

802.11v のサポートによるローミングの機能拡張

ワークグループブリッジ（WGB）で802.11vのサポートが有効になっている場合、最新の近隣AP情報に基づいて最適なAPをWGBが能動的に選択できるようにすることで、ローミングが強化されます。

- WGB は、動的に更新されたリストから得た適切な AP へのローミングを積極的に開始できます。
- 定期的にチェックすることで、WGB がきわめて正確な近隣 AP データを保持し、ローミング中に最適な決定を行えるようになります。

基本サービスセット移行要求フレーム

基本サービスセット（BSS）移行要求フレームには、近隣APのチャンネル情報が含まれます。走査をこれらの指定されたチャンネルに制限すると、複数のチャンネルを使用する環境でのローミングの遅延が大幅に減少します。

WLC を使用して AP のクライアントとの関連付けを解除する

ワイヤレス LAN コントローラ（WLC）は、AP の負荷、受信信号強度表示（RSSI）、データレートなどの要因に基づいて、クライアントの関連付けを解除できます。重要なポイントは次のとおりです。

- WLC は、BSS 移行管理要求フレームを介して、差し迫った関連付け解除について 802.11v 対応クライアントに通知できます。
- 設定可能な時間内にクライアントと別の AP との再関連付けができなかった場合、関連付け解除が実行されます。

その他の参考情報

管理者は WLC で disassociation-imminent 設定を有効にできます。有効にすると、BSS 移行管理要求フレーム内のオプションフィールドがアクティブになります。

WLC での 802.11v 設定の詳細については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』を参照してください。

802.11v サポートの有効化または無効化

チャネル走査を、近隣 AP リストから学習したものに制限して、ローミング性能を最適化するには、WGB での 802.11v サポートを有効にします。

手順

WGB での 802.11v サポートを有効または無効にします。

オプション	説明
WGB での 802.11v サポートの有効化	**configure wgb mobile station interface dot11Radio** *radio_slot_id* **dot11v-bss-transition enable** コマンドを使用します。 `Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition enable` （注） • 802.11v サポートが有効になっている場合、WGB は、近隣 AP リストで提供されるチャネルのみを走査し、ローミング時の効率を向上させます。 • 円滑なチャネル移行を可能にするために、インフラストラクチャ側で近隣 AP リストが適切に設定されていることを確認してください。
WGB での 802.11v サポートの無効化	**configure wgb mobile station interface dot11Radio** *radio_slot_id* **dot11v-bss-transition disable** コマンドを使用します。 `Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition disable`

BSS 移行クエリ間隔の設定

WGB が親 AP に BSS 移行クエリメッセージを送信する時間の間隔を設定するには、このタスクを実行します。これにより、移行クエリの頻度を管理することで、最適なネットワーク性能を確保できます。

手順

configure wgb neighborlist-update-interval *interval* コマンドを使用して、WGB が親 AP に BSS 移行クエリメッセージを送信する時間の間隔を設定します。

```
Device# configure wgb neighborlist-update-interval 50
```

（注）
有効な範囲は 0 ～ 100 で、デフォルト値は 10 です。時間の間隔は秒形式で設定してください。

近隣 AP リストの確認

アソシエートされている AP から受信した近隣 AP リストが正確かつ最新であることを確認します。

手順

show wgb dot11v bss-transition neighbour コマンドを使用して、アソシエートされている AP から受信した近隣 AP リストを表示します。

```
Device#show wgb dot11v bss-transition neighbour
```

（注）
- このコマンドを使用すると、デバイスが 802.11v ワイヤレスネットワーク拡張の一環として移行できる近隣 AP に関する詳細が表示されます。
- 正確な近隣 AP リストにより、ワイヤレスクライアントのハンドオフおよびローミングの効率を向上させることができます。

チャネルリストの確認

チャネルリストを確認して、デバイスが dot11v 近隣 AP、補助無線機走査、および残存チャネル走査からチャネルを正しく識別していることを確認します。この手順は、ワイヤレスネットワークに関連する接続や性能の問題をトラブルシューティングするために重要です。

手順

show wgb dot11v bss-transition channel コマンドを使用して、dot11v 近隣 AP、走査済みの補助無線機、走査済みの残存チャネルからのチャネルリストを確認します。

```
Device#show wgb dot11v bss-transition channel
```

（注）
このコマンドは、通常、WGB によって識別されたチャネルを検証する必要があるシナリオで使用されます。

近隣 AP リストの消去

エラー状態から回復するために近隣 AP リストを消去するには、このタスクを実行します。これにより、近隣 AP 情報に関連する潜在的な接続の問題を解決することで、デバイスの最適な性能を確保できます。

手順

clear wgb dot11v bss-transition neighbor コマンドを使用して、近隣 AP リストを消去してエラー状態からの回復を実現します。

```
Device#clear wgb dot11v bss-transition neighbor
```

（注）
このコマンドは、特に、エラー状態を解決する必要があるシナリオで近隣 AP リストをリセットするために使用されます。

補助走査

ローミング性能を向上させるために、補助走査モードを WGB 無線機 2（5 GHz）で走査専用モードまたはハンドオフモードのいずれかに設定できます。

走査専用モード

走査専用モードは、ワイヤレス アクセス ポイントの動作モードの 1 つです。

- 走査専用の無線機運用を有効にし、
- ワイヤレス環境を継続的に監視して、ネットワーク性能、干渉、不正デバイスに関するデータを収集し、
- チャンネルリストや走査間隔などの走査パラメータの設定を可能にします。

スロット 2 の無線機が走査専用モードに設定されている場合、スロット 1（5G）の無線機は常にアップリンクとして選択されます。スロット 2（5G）の無線機は、チャンネルリストに基づいて設定された SSID を継続的に走査します。デフォルトでは、チャンネルリストには、（規制ドメインに基づき）サポートされているすべての 5G チャンネルが含まれます。走査リストは手動で設定することが可能で、802.11v から学習することもできます。

ローミングが開始されると、アルゴリズムによって走査テーブルで候補が検索され、テーブルが空でなければ走査段階はスキップされます。その後、WGB は選択された候補 AP に関連付けられます。

走査専用モードの設定

デバイスが走査専用モードで動作できるようにします。これにより、データ送信なしのネットワークの監視とアセスメントが可能になります。

手順

configure dot11Radio 2 mode scan only コマンドを使用して、走査専用モードを設定します。

```
Device# configure dot11Radio 2 mode scan only
```

走査テーブルタイマーの設定

走査テーブルタイマーを調整して、候補 AP の選択プロセスを最適化し、古い RSSI 値によるローミングの失敗を防止します。

始める前に

走査テーブルには、デバイスによって検出された候補 AP のリストが保持されます。デフォルトでは、このテーブルのエントリは、1200 ミリ秒後に期限切れになります。期限切れタイマーを変更すると、RSSI の更新により多くの時間をかけられるようになり、ローミングの効率が向上する可能性があります。

手順

タイマーを調整するには、**configure wgb scan timeout** *interval* コマンドを使用します。デフォルトでは、走査テーブルの候補 AP エントリは 1200 ミリ秒で自動的に削除されます。

```
Device#configure wgb scan timeout 1500
```

（注）

- 走査を実行する AP の有効期限は 1 ～ 5000 です。
- AP は、走査テーブルから RSSI 値が最も高い候補を選択します。ただし、RSSI 値が更新されないことがあり、結果としてローミングが失敗する場合があります。

チャンネルリストのチャンネルの手動追加または削除

チャネルリストのチャネルを手動で追加または削除して、ワイヤレスネットワークの性能を最適化したり、特定の設定要件に合わせるには、このタスクを実行します。

手順

いずれかのオプションを使用して、チャネルリストのチャネルを追加または削除します。

オプション	説明
チャネルリストへのチャネルの追加	**configure wgb mobile station interface dot11Radio** *interface* **scan** *channel* **add** コマンドを使用します。 `Device#configure wgb mobile station interface dot11Radio 1 scan 36 add`
チャネルリストからのチャネルの削除	**configure wgb mobile station interface dot11Radio** *interface* **scan** *channel* **delete** コマンドを使用します。 `Device# configure wgb mobile station interface dot11Radio 1 scan 36 delete`

走査テーブルの確認

現在の AP 走査の詳細を確認し、最適な接続のために最良の AP を特定するには、このタスクを実行します。

手順

show wgb scan コマンドを使用して、走査テーブルを確認します。

```
Device#show wgb scan Best AP expire time: 5000 ms ************[ AP List ]*************** BSSID RSSI
 CHANNEL Time FC:58:9A:15:E2:4F 84 136 1531 FC:58:9A:15:DE:4F 37 136 41 ***********[ Best AP
]**************** BSSID RSSI CHANNEL Time FC:58:9A:15:DE:4F 37 136 41
```

補助走査ハンドオフモード

補助走査ハンドオフモードは、ワイヤレス無線機設定であり、

- 両方の無線機（無線機 1 と無線機 2）がアップリンク接続として機能できるように、
- 各ローミングイベント後の無線機間でのロールとトラフィックの動的切り替えをサポートし、

- 無線機の走査によって利用可能な最良のアクセスポイントにアソシエートすることで効率的なローミングを実現します。

補助走査リストは、手動で設定することも、802.11v 標準規格を使用して自動的に学習することもできます。このハンドオフモードは、利用可能な最良のアクセスポイントと迅速にアソシエートすることで、ローミングの性能を向上させます。

無線機のロール

無線機 2 は無線機 1 と同じ MAC アドレスを共有し、走査、アソシエーション、およびデータ伝送をサポートします。どちらの無線機も、サービス提供ロールまたは走査ロールで動作できます。各ローミングイベントの後に、ロールとトラフィックが無線機 1 と無線機 2 の間で自動的に切り替わります。

AP のローミング

ローミングが開始されると、システムアルゴリズムは、接続を確立するために最良の AP を走査データベースでチェックします。WGB は、常に、走査ロールで動作している無線機を使用して、新しい AP へのローミングアソシエーションを完了します。この設定により、ローミング瞬断が 20 ～ 50 ミリ秒に短縮されます。

次の表に、IW9165E での補助走査ハンドオフ無線機モードの設定例を示します。

スロット 0（2.4G）	スロット 1（5G）	スロット 2（5G のみ）	スロット 3（走査用無線機）
該当なし	WGB	走査ハンドオフ	該当なし

次の表に、3 つの異なるモードを使用した場合の各方式で発生するローミング瞬断の時間を示します。

ローミング瞬断時間	通常のチャネル設定	補助走査のみ	補助走査ハンドオフ
走査	(40+20)*3=180 ミリ秒	0 ～ 40 ミリ秒	0 ミリ秒
アソシエーション	30 ～ 80 ミリ秒	30 ～ 80 ミリ秒	20 ～ 50 ミリ秒
合計	～ 210 ミリ秒	70 ～ 120 ミリ秒	20 ～ 50 ミリ秒

補助走査ハンドオフモードの無線機 2 の設定

補助走査ハンドオフモードの WGB スロット 2 無線機を設定し、円滑な接続性と最適化されたネットワーク性能を確保するには、このタスクを実行します。

始める前に

補助走査ハンドオフモードでは、無線機が、アクティブな接続を中断することなく、利用可能なアクセスポイントを走査できます。この機能は、特に、複数のアクセスポイントがある環境でハンドオフの信頼性を向上させるために役立ちます。

手順

ステップ 1 **configure dot11Radio** *radio-num* **mode scan handoff** コマンドを使用して、WGB スロット 2 無線機を補助走査モードに設定します。

```
Device# configure dot11Radio 2 mode scan handoff
```

ステップ 2 （オプション）**show running-config** コマンドを使用して、無線機の設定を表示します。

```
Device# show running-config ... Radio Id : 1 Admin state : ENABLED Mode : WGB Spatial Stream : 1
Guard Interval : 800 ns Dot11 type : 11n 11v BSS-Neighbor : Disabled A-MPDU priority : 0x3f A-MPDU
 subframe number : 12 RTS Protection : 2347(default) Rx-SOP Threshold : AUTO Radio profile : Default
 Encryption mode : AES128 Radio Id : 2 Admin state : ENABLED Mode : SCAN - Handoff Spatial Stream
: 1 Guard Interval : 800 ns Dot11 type : 11n 11v BSS-Neighbor : Disabled A-MPDU priority : 0x3f
A-MPDU subframe number : 12 RTS Protection : 2347(default) Rx-SOP Threshold : AUTO Radio profile :
 Default
```

WGB 走査の確認

各無線機の現在のロールを確認し、最良の AP の選択と評価指標を含む補助走査の結果を分析するには、このタスクを実行します。

WGB 走査は、各無線機の補助走査プロセスに関する詳細情報を提供します。このデータは、信号強度（RSSI）、チャネル、および走査時間に基づいた最良の AP の決定に役立ちます。

手順

show wgb scan コマンドを使用して、各無線機の現在のロールと補助走査の結果を表示します。

```
Device#show wgb scan Best AP expire time: 2500 ms Aux Scanning Radio Results (slot 2) ************[
 AP List ]*************** BSSID RSSI CHANNEL Time FC:58:9A:15:DE:4E 54 153 57 FC:58:9A:15:E2:4E 71
 153 64 ***********[ Best AP ]**************** BSSID RSSI CHANNEL Time FC:58:9A:15:DE:4E 54 153 57
 Aux Serving Radio Results ************[ AP List ]*************** BSSID RSSI CHANNEL Time
FC:58:9A:15:DE:4E 58 153 57 FC:58:9A:15:E2:4E 75 153 133 ***********[ Best AP ]****************
BSSID RSSI CHANNEL Time FC:58:9A:15:DE:4E 58 153 57
```

デュアル無線機 WGB によるローミングの最適化

デュアル無線機 WGB は、ワイヤレス ワークグループブリッジであり、

- 2 つの無線機を使用して、ローミングの効率を向上させ、
- 既存の走査テーブルでアクティブな走査フェーズをスキップしてサービスの中断を最小限に抑え、

- ビーコンフレームが失われた場合またはパケット再試行のしきい値に達した場合にローミングを開始します。

Cisco IOS-XE 17.15.1 リリース以降、デュアル無線機構成のデバイスのローミング効率が向上しました。これにより、サービスの停止時間が短縮されます。

ローミングの契機となる要因

ローミングが開始される要因には、次のものが含まれます。

- Low RSSI：AP などのワイヤレスデバイスが信号から受信する電力レベルを測定します。RSSI 値を使ってワイヤレス接続の品質を判断し、ワイヤレスネットワークのトラブルシュートと最適化を行います。
- Beacon miss-count：クライアントデバイスがワイヤレスネットワーク内の AP から連続で受信できなかったビーコンフレーム数を示します。
- Maximum packet retries：クライアントデバイスが確認応答を送信しない場合に、データパケットを再送信する回数の上限を指定します。

デュアル無線機の設定オプション

デュアル無線機構成において、IW9165E AP で可能な設定は次のとおりです。

デュアル無線機	AP
5 GHz 無線機 1 + 無線機 2（走査専用モード）	IW9165E
5 GHz 無線機 1 + 無線機 2（補助走査ハンドオフモード）	

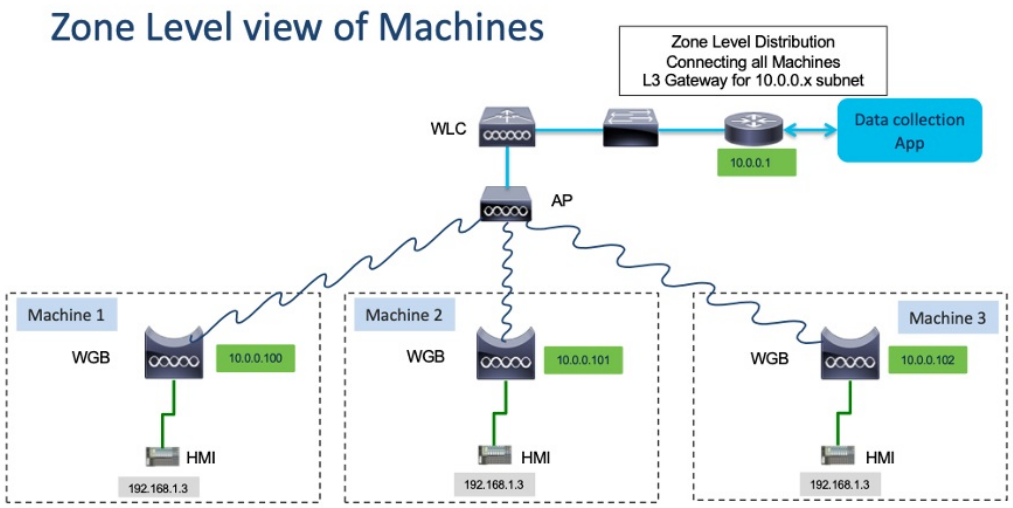
レイヤ 2 NAT

1 対 1（1:1）レイヤ 2 NAT により、固有のパブリック IP アドレスを既存のプライベート IP アドレス（エンドデバイス）に割り当てることができます。この操作により、エンドデバイスはパブリックネットワークと通信できるようになります。

レイヤ 2 NAT は、次の 2 つの変換表を維持します。

- プライベートからパブリックへのサブネット変換
- パブリックからプライベートへのサブネット変換

ヒューマンマシンインターフェイス（HMI）やロボットなどの産業用展開では、多くの場合、すべてのマシンに同じファームウェアがプログラムされます。その結果、複数のデバイスで重複する IP アドレスが発生します。レイヤ 2 NAT は、重複するプライベート IP アドレスを指定されたデバイスがパブリックネットワークと通信できるようにすることで、この問題を解決します。



レイヤ 2 NAT の設定

レイヤ 2 で VLAN 内の有線クライアントの IP アドレス変換を制御するには、レイヤ 2 NAT（ネットワークアドレス変換）設定コマンドを使用します。

これらのコマンドにより、管理者は次のことができます。

- デバイスでレイヤ 2 NAT をグローバルに有効または無効にします。
- NAT ルールを適用するデフォルト VLAN を定義します。
- 個々のホストアドレスをプライベートからパブリックに、またはパブリックからプライベートに変換します。
- サブネット全体をプライベートからパブリックに、またはパブリックからプライベートに変換します。

この設定により、VLAN ベースのトラフィック分離を維持しながら、IP アドレスを動的または静的にマッピングすることにより、プライベートネットワークと外部/パブリックネットワークの間の円滑な通信が確保されます。

手順

ステップ 1 **configure l2nat** {**enable** | **disable**} コマンドを使用して、レイヤ 2 NAT を有効または無効にします。

```
Device# configure l2nat enable
```

ステップ 2 **configure l2nat default-vlan** *vlan_id* コマンドを使用して、すべての NAT ルールを適用する VLAN を定義します。

```
Device# configure l2nat default-vlan 10
```

（注）

VLAN ID を指定しない場合、VLAN 0 が使用されます。

ステップ 3 **configure l2nat** {**add** | **delete**} **inside from host** *original_ip_addr* **to** *translated_ip_addr* コマンドを使用して、有線クライアントのプライベート IP アドレスをパブリック IP アドレスに変換します。

```
Device# configure l2nat add inside from host 192.168.1.10 to 203.0.113.10
```

ステップ 4 **configure l2nat** {**add** | **delete**} **outside from host** *original_ip_addr* **to** *translated_ip_addr* コマンドを使用して、パブリック IP アドレスをプライベート IP アドレスに変換します。

```
Device# configure l2nat add outside from host 203.0.113.20 to 192.168.1.20
```

ステップ 5 **configure l2nat** {**add** | **delete**} **inside from network** *original_nw_prefix* **to** *translated_nw_prefix subnet_mask* コマンドを使用して、プライベートサブネットをパブリックサブネットに変換します。

```
Device# configure l2nat add inside from network 192.168.1.0 to 203.0.113.0 255.255.255.0
```

ステップ 6 **configure l2nat** {**add** | **delete**} **outside from network** *original_nw_prefix* **to** *translated_nw_prefix subnet_mask* コマンドを使用して、パブリックサブネットをプライベートサブネットに変換します。

```
Device# configure l2nat add outside from network 203.0.113.0 to 192.168.1.0 255.255.255.0
```

レイヤ 2 NAT 設定の確認

トラブルシューティングのために、レイヤ 2 NAT 設定を確認し、変換統計を調べ、ルールまたはカウンタを消去するには、次のコマンドを使用します。

- **show l2nat entry**：レイヤ 2 NAT の実行中エントリを表示します。
- **show l2nat config**：レイヤ 2 NAT 設定の詳細を表示します。
- **show l2nat stats**：レイヤ 2 NAT パケット変換統計を表示します。
- **show l2nat rules**：設定からレイヤ 2 NAT ルールを表示します。
- **clear l2nat statistics**：パケット変換統計を消去します。
- **clear l2nat rule**：レイヤ 2 NAT ルールを消去します。
- **clear l2nat config**：レイヤ 2 NAT 設定を消去します。
- **debug l2nat**：パケット変換プロセスのデバッグを有効にします。
- **debug l2nat all**：パケット着信時に、NAT エントリに一致する結果を出力します。

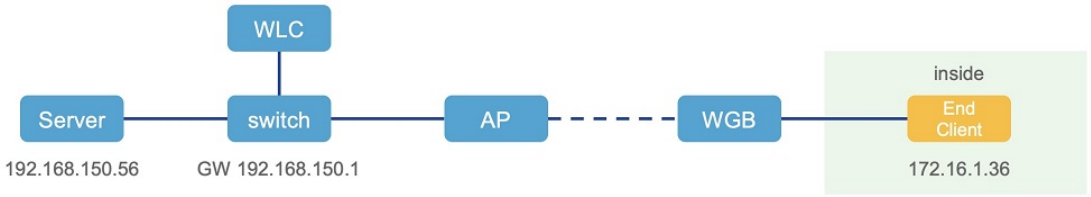
⚠

注意 このコマンドにより、コンソールに大量のログが出力される可能性があります。特に Syslog サービスがブロードキャストアドレスで有効になっている場合、このコマンドが原因でコンソールからの応答が失われる可能性があります。

- **undebug l2nat**：パケット変換プロセスのデバッグを無効にします。

ホスト IP アドレス変換の設定例

このシナリオでは、WGB に接続されたエンドクライアント（172.16.1.36）は、ゲートウェイに接続されたサーバー（192.168.150.56）と通信する必要があります。レイヤ 2 NAT は、外側ネットワーク（192.168.150.36）上のエンドクライアントのアドレスと内側ネットワーク（172.16.1.56）上のサーバーのアドレスを提供します。



レイヤ 2 NAT の設定例

レイヤ 2 NAT の詳細な設定例を以下に示します。出力の I2O は「内側から外側」を意味し、O2I は「外側から内側」を意味します。

```
Device# show l2nat config L2NAT Configuration are: ==================================
Status: enabled Default Vlan: 0 The Number of L2nat Rules: 4 Dir Inside Outside Vlan O2I
 172.16.1.56 192.168.150.56 0 I2O 172.16.1.36 192.168.150.36 0 I2O 172.16.1.255
192.168.150.255 0 I2O 172.16.1.1 192.168.150.1 0
```

レイヤ 2 NAT ルールの例

レイヤ 2 NAT ルールの例を以下に示します。

```
Device# show l2nat rule Dir Inside Outside Vlan O2I 172.16.1.56 192.168.150.56 0 I2O
172.16.1.36 192.168.150.36 0 I2O 172.16.1.255 192.168.150.255 0 I2O 172.16.1.1
192.168.150.1 0
```

レイヤ 2 NAT エントリの例

現在のレイヤ 2 NAT エントリの例を以下に示します。

```
Device# show l2nat entry Direction Original Substitute Age Reversed inside-to-outside
172.16.1.36@0 192.168.150. 36@0 -1 false inside-to-outside 172.16.1.56@0 192.168.150.
56@0 -1 true inside-to-outside 172.16.1.1@0 192.168.150. 1@0 -1 false inside-to-outside
 172.16.1.255@0 192.168.150. 255@0 -1 false outside-to-inside 192.168.150.36@0
172.16.1.36@0 -1 true outside-to-inside 192.168.150.56@0 172.16.1.56@0 -1 false
outside-to-inside 192.168.150.1@0 172.16.1.1@0 -1 true outside-to-inside 192.168.150.255@0
 172.16.1.255@0 -1 true
```

WGB 有線クライアントの例

ブリッジを介した WGB 有線クライアントの例を以下に示します。

レイヤ 2 NAT の有効化前：

```
Device# show wgb bridge ***Client ip table entries*** mac vap port vlan_id seen_ip
confirm_ago fast_brg B8:AE:ED:7E:46:EB 0 wired0 0 172.16.1.36 0.360000 true
24:16:1B:F8:05:0F 0 wbridge1 0 0.0.0.0 3420.560000 true
```

レイヤ 2 NAT の有効化後：

```
Device# show wgb bridge ***Client ip table entries*** mac vap port vlan_id seen_ip
confirm_ago fast_brg B8:AE:ED:7E:46:EB 0 wired0 0 192.168.150.36 0.440000 true
24:16:1B:F8:05:0F 0 wbridge1 0 0.0.0.0 3502.220000 true
```

（注） NAT の有線クライアントで E2E トラフィックの問題が発生した場合は、**clear wgb client single** コマンドを使用して、クライアント登録プロセスを再開できます。

レイヤ 2 NAT パケット変換統計の例

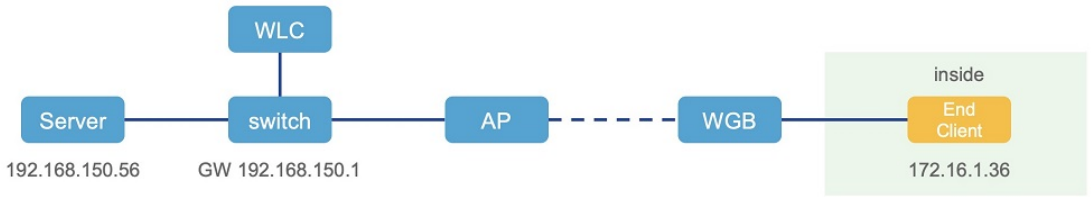
レイヤ 2 NAT パケット変換統計の例を以下に示します。

```
Device# show l2nat stats Direction Original Substitute ARP IP ICMP UDP TCP
inside-to-outside 172.16.1.1@2660 192.168.150.1@2660 1 4 4 0 0 inside-to-outside
172.16.1.36@2660 192.168.150.36@2660 3 129 32 90 1 inside-to-outside 172.16.1.56@2660
192.168.150.56@2660 2 114 28 85 1 inside-to-outside 172.16.1.255@2660 192.168.150.255@2660
 0 0 0 0 0 outside-to-inside 192.168.150.1@2660 172.16.1.1@2660 1 4 4 0 0 outside-to-inside
 192.168.150.36@2660 172.16.1.36@2660 3 39 38 0 1 outside-to-inside 192.168.150.56@2660
 172.16.1.56@2660 2 35 34 0 1 outside-to-inside 192.168.150.255@2660 172.16.1.255@2660
0 0 0 0 0
```

（注） 統計をリセットするには、**clear l2nat stats** コマンドを使用します。

ネットワークアドレス変換の設定例

このシナリオでは、レイヤ 2 NAT は、172.16.1.0/24 サブネット内の内側アドレスを 192.168.150.0/24 サブネット内のアドレスに変換し、変換中にネットワークプレフィックスのみを置き換えます。ホストビットは変更されません。



このシナリオで使用するコマンドは次のとおりです。

```
Device# configure l2nat add inside from network 172.16.1.0 to 192.168.150.0 255.255.255.0
```

イーサネットポートのネイティブ VLAN

一般的なワークグループブリッジ（WGB）展開では、単一の有線クライアントが WGB イーサネットポートに直接接続されます。そのため、有線クライアントトラフィックは、WGB 管理 VLAN と同じ VLAN 上に存在する必要があります。有線クライアントトラフィックを WGB 管理 VLAN 以外の VLAN に配置する必要がある場合は、イーサネットポートでネイティブ VLAN を設定します。

重要 イーサネットポートごとのネイティブ VLAN ID の設定はサポートされません。両方のイーサネットポートが同じネイティブ VLAN 設定を共有します。

注意 WGB ブロードキャストタギングが有効で、単一の有線パッシブクライアントが WGB イーサネットポートに直接接続している場合、インフラストラクチャの下流（DS）側のクライアントがパッシブクライアントの背後で WGB に ping を実行できないという問題が発生する可能性があります。回避策として、`configure wgb ethport native-vlan enable` コマンドと **configure wgb ethport native-vlan id X** コマンドを追加で設定します（X は WGB 管理 VLAN と同じ VLAN）。

設定を確認するには、**show wgb ethport config** または **show running-config** コマンドを使用します。

イーサネットポートでのネイティブ VLAN の設定

ワークグループブリッジ（WGB）イーサネットポートでタグなしトラフィックを処理する方法を管理するには、ネイティブ VLAN 設定コマンドを使用します。

これらのコマンドにより、管理者は次のことができます。

- WGB イーサネットポートでネイティブ VLAN 設定を有効または無効にします。
- ネイティブ VLAN ID を指定して、タグなしトラフィックが、確実に、目的の VLAN に正しく割り当てられるようにします。

手順

ステップ 1 **config wgb ethport** *ethport* **native-vlan** {**enable** | **disable**} コマンドを使用して、ネイティブ VLAN 設定を有効または無効にします。

```
Device# config wgb ethport 1 native-vlan enable
```

ステップ 2 **config wgb ethport** *ethport* **native-vlan** *vlan_id* コマンドを使用して、ネイティブ VLAN ID を指定します。

```
Device# config wgb ethport native-vlan id 2735
```

ステップ 3 （オプション）**show wgb ethport config** or **show running-config** コマンドを使用して、設定を確認します。

```
Device# show wgb ethport config
```

低遅延プロファイル

低遅延プロファイルは、IoT アプリケーションに不可欠な低遅延と Quality of Service（QoS）の要件を満たすように IEEE 802.11 ネットワークを最適化する設定です。IEEE 802.11 ネットワークは、遅延を減らし QoS を確保するメカニズムを提供することで、IoT アプリケーションの実現に不可欠な役割を果たします。これらの目標を達成するには、以下の機能が重要です。

- Enhanced Distributed Channel Access（EDCA）：EDCA パラメータは、音声およびビデオストリームなど、遅延の影響を受けやすいトラフィックのワイヤレスチャンネルアクセスに優先順位を付けて、一貫した QoS 性能を実現します。
- Aggregated MAC Protocol Data Unit（AMPDU）：このメカニズムは、複数のデータフレームを組み合わせて 1 つの伝送とし、オーバーヘッドを削減して効率を向上させます。
- パケット再試行（集約型または非集約型）：再試行メカニズムは、ネットワークの状況に応じて、集約パケットと個別パケットのいずれかを再送信することにより、正常なデータ配信を実現します。

これらの機能は、ワイヤレス環境での低遅延と高 QoS を必要とする IoT デバイスおよびアプリケーションの展開を集合的にサポートします。

音声最適化 EDCA プロファイルの有効化または無効化

遅延を減らし、QoS を向上させることでビデオの性能を改善するには、映像用途に最適化された低遅延プロファイルを設定します。

このタスクでは、WGB の特定の無線インターフェイスで、音声最適化 EDCA プロファイルを有効または無効にすることに焦点を当てています。音声最適化プロファイルは、ネットワーク内でビデオトラフィックを優先することにより、ビデオトラフィックの優れた処理を確保します。

手順

ステップ 1 いずれかのオプションを使用して、WGB の特定の無線インターフェイスで、音声最適化 EDCA プロファイルを有効または無効にします。

オプション	説明
音声最適化EDCAプロファイルの有効化	**configure dot11Radio** *radio_slot_id* **profile optimized-video enable** コマンドを使用します。 `Device# configure dot11Radio 1 profile optimized-video enable`
音声最適化EDCAプロファイルの無効化	**configure dot11Radio** *radio_slot_id* **profile optimized-video disable** コマンドを使用します。 `Device# configure dot11Radio 1 profile optimized-video disable`

ステップ 2 （オプション）**show controllers dot11Radio** *radio_slot_id* コマンドを使用して、設定を確認します。

```
Device# show controllers dot11Radio 1 EDCA profile: optimized-video EDCA in use ============= AC
Type CwMin CwMax Aifs Txop ACM AC_BE L 4 10 11 0 0 AC_BK L 6 10 11 0 0 AC_VI L 3 4 2 94 0 AC_VO L
2 3 1 47 0 Packet parameters in use ============= wbridge1 A-MPDU Priority 0: Enabled wbridge1 A-MPDU
 Priority 1: Enabled wbridge1 A-MPDU Priority 2: Enabled wbridge1 A-MPDU Priority 3: Enabled wbridge1
 A-MPDU Priority 4: Disabled wbridge1 A-MPDU Priority 5: Disabled wbridge1 A-MPDU Priority 6: Disabled
 wbridge1 A-MPDU Priority 7: Disabled wbridge1 A-MPDU subframe number: 3 wbridge1 Packet retries
drop threshold: 16
```

自動化最適化 EDCA プロファイルの有効化または無効化

自動化用途に最適化された低遅延プロファイルを有効にすることで、ワイヤレスネットワーク環境の性能と効率を向上させることができます。

手順

ステップ 1 いずれかのオプションを使用して、WGB の特定の無線インターフェイスで、音声最適化 EDCA プロファイルを有効または無効にします。

オプション	説明
自動化最適化EDCAプロファイルの有効化	**configure dot11Radio** *radio_slot_id* **profile optimized-automation enable** コマンドを使用します。 `Device# configure dot11Radio 1 profile optimized-automation enable`
自動化最適化EDCAプロファイルの無効化	**configure dot11Radio** *radio_slot_id* **profile optimized-automation disable** コマンドを使用します。 `Device# configure dot11Radio 1 profile optimized-automation disable`

ステップ 2 （オプション）**show controllers dot11Radio** *radio_slot_id* コマンドを使用して、設定を確認します。

```
Device# show controllers dot11Radio 1 EDCA profile: optimized-automation EDCA in use =============
 AC Type CwMin CwMax Aifs Txop ACM AC_BE L 7 10 12 0 0 AC_BK L 8 10 12 0 0 AC_VI L 7 7 3 0 0 AC_VO
 L 3 3 1 0 0 Packet parameters in use ============= wbridge1 A-MPDU Priority 0: Enabled wbridge1
A-MPDU Priority 1: Enabled wbridge1 A-MPDU Priority 2: Enabled wbridge1 A-MPDU Priority 3: Enabled
 wbridge1 A-MPDU Priority 4: Disabled wbridge1 A-MPDU Priority 5: Disabled wbridge1 A-MPDU Priority
 6: Disabled wbridge1 A-MPDU Priority 7: Disabled wbridge1 A-MPDU subframe number: 3 wbridge1 Packet
 retries drop threshold: 16
```

カスタマイズされた WMM EDCA プロファイルの設定

Wi-Fiマルチメディア（WMM）プロファイルをカスタマイズすることで、トラフィックキューを最適化し、特定タイプのネットワークトラフィックの QoS を向上させることができます。

WMM では、送信されるデータのタイプに基づいてトラフィックに優先順位を付けることで、Wi-Fi ネットワークの性能を向上させます。カスタマイズされた WMM EDCA（Enhanced

Distributed Channel Access）プロファイルを設定すると、音声、ビデオ、バックグラウンド、およびベストエフォートのトラフィックの性能パラメータを微調整できます。

手順

ステップ 1 **configure dot11Radio** *radio_slot_id* **profile customized-wmm enable** コマンドを使用して、カスタマイズされた WMM プロファイルを有効にします。

```
Device# configure dot11Radio 1 profile customized-wmm enable
```

ステップ 2 **configure dot11Radio** {**0**| **1**|**2**}**wmm** {**be**| **vi**| **vo**| **bk**} {**cwmin** *cwmin_num* |**cwmax** *cwmax_num* | **aifs** *aifs_num* |**txoplimit** *txoplimit_num*} コマンドを使用して、カスタマイズされた WMM プロファイルのパラメータを設定します。

```
configure dot11Radio 1 wmm vo cwmin 3
```

パラメータの説明：

- be：ベストエフォート型トラフィックキュー（CS0 および CS3）。
- bk：バックグラウンド トラフィック キュー（CS1 および CS2）。
- vi：ビデオトラフィックキュー（CS4 および CS5）。
- vo：音声トラフィックキュー（CS6 および CS7）。
- aifs：調停フレーム間スペース、<1 ～ 15>（単位：スロット時間）
- cwmin：コンテンションウィンドウ最小、<0 ～ 15> 2^n-1（単位：スロット時間）
- cwmax：コンテンションウィンドウ最大、<0 ～ 15> 2^n-1（単位：スロット時間）
- txoplimit：送信機会時間、<0 ～ 255> の整数（単位：32 マイクロ秒）

ステップ 3 （オプション）カスタマイズされた WMM プロファイルを無効にします。

configure dot11Radio *radio_slot_id* **profile customized-wmm disable** コマンドを使用して、カスタマイズされた WMM プロファイルを無効にします。

```
Device#configure dot11Radio 1 profile customized-wmm disable
```

コントローラ GUI を使用した EDCA パラメータの設定

Enhanced Distributed Channel Access（EDCA）パラメータを設定することにより、音声、ビデオ、およびその他の QoS トラフィックのワイヤレスチャネルアクセスを最適化できます。

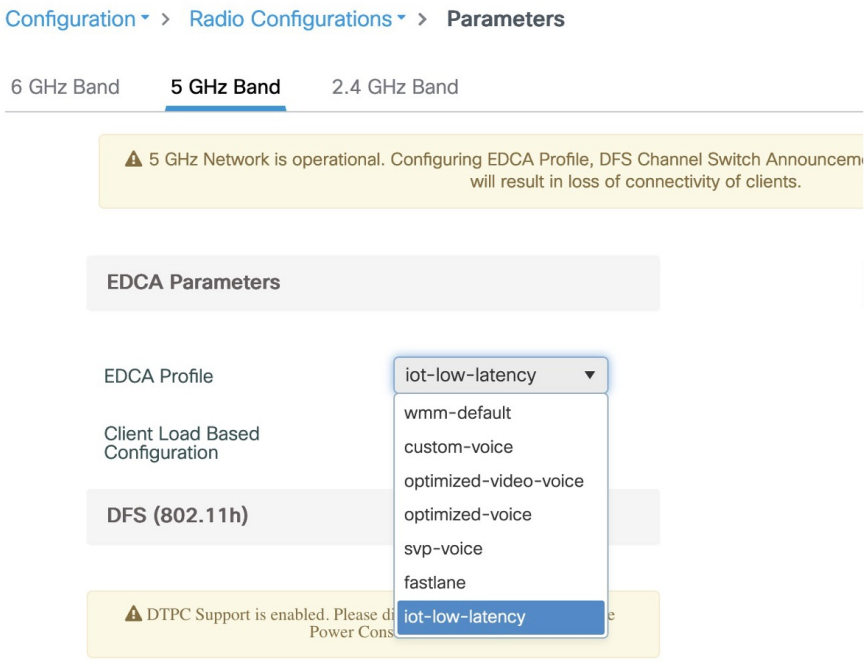
手順

ステップ 1 次の場所に移動します。 **[Configuration]** > **[Radio Configuration]** > **[Parameters]**を参照してください。

このページで、6 GHz、5 GHz、および 2.4 GHz 無線機のグローバルパラメータを設定できます。

（注）
無線ネットワークが有効になっている場合、パラメータを設定または変更することはできません。続行するには、[Configuration] > [Radio Configurations] > [Network] ページでネットワークステータスを無効にしてください。

ステップ 2 [EDCA Parameters] セクションで、[EDCA Profile] ドロップダウン リストから EDCA プロファイルを選択します。



EDCA パラメータで、音声、ビデオ、およびその他の QoS トラフィックに対して、優先的なワイヤレスチャネルアクセスを提供します。

ステップ 3 [Apply] をクリックします。

コントローラ CLI を使用した EDCA パラメータの設定

Enhanced Distributed Channel Access（EDCA）パラメータを調整することにより、IoT 低遅延アプリケーション向けにワイヤレスネットワークの性能を最適化できます。

シスコ ワイヤレス コントローラのコマンド ライン インターフェイス（CLI）で、次の手順を実行します。

手順

ステップ 1 グローバル コンフィギュレーション モードを開始するには、**configure terminal** コマンドを使用します。

```
Device# configure terminal
```

ステップ 2 **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **shutdown** コマンドを使用して、無線ネットワークを無効にします。

```
Device(config)# ap dot11 5ghz shutdown
```

ステップ 3 **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency** コマンドを使用して、5 GHz、2.4 GHz、または 6 GHzネットワークの iot-low-latency EDCA プロファイルを有効にします。

```
Device(config)# ap dot11 5ghz edca-parameters iot-low-latency
```

ステップ 4 **no ap dot11** {**5ghz** | **24ghz** | **6ghz**} **shutdown** コマンドを使用して、無線ネットワークを有効にします。

```
Device(config)# no ap dot11 5ghz shutdown
```

ステップ 5 **end** コマンドを使用して、特権 EXEC モードに戻ります。

```
Device(config)# end
```

ステップ 6 （オプション）**show ap dot11** {**5ghz** | **24ghz** | **6ghz**} **network** コマンドを使用して、現在の設定を表示します。

```
Device# show ap dot11 5ghz network EDCA profile type check : iot-low-latency
```

A-MPDU

集約は、複数のパケットデータフレームを個別に送信するのではなく、伝送用に単一のより大きなフレームにグループ化するプロセスです。この方法により、ワイヤレス通信の効率が向上し、オーバーヘッドが削減されます。一般的な集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU パラメータは、集約パケットのサイズと集約パケット間に必要な間隔を具体的に定義し、受信側 WLAN ステーションがデータを適切に復号化できるようにします。

A-MPDU の設定

始める前に

A-MPDUパラメータの設定により、パケットデータフレームの集約と送信を最適化し、WLAN ステーションによる効率的なデコードを確保することができます。

手順

ステップ 1 **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** *profile-name* コマンドを使用して、プロファイルベースの A-MPDU パラメータを設定します。

```
Device# ap dot11 5ghz rf-profile Video-Optimized
```

ステップ 2 **dot11n a-mpdu tx block-ack window-size** *window-size* コマンドを使用して、送信ブロック確認応答（block-ack）ウィンドウサイズを設定します。

```
Device(config-rf-profile)# dot11n a-mpdu tx block-ack window-size 64
```

（注）
RF プロファイルレベルで設定された値は、グローバルに設定された値に優先します。

ステップ 3 グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

```
Device(config-rf-profile)# exit
```

ステップ 4 **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** *window-size* コマンドを使用して、送信ブロック確認応答ウィンドウサイズをグローバルに設定します。

```
Device(config)# ap dot11 24ghz dot11n a-mpdu tx block-ack window-size 32
```

ステップ 5 **wireless tag rf** *rf-tag-name* コマンドを使用して、RF タグを作成します。

```
Device(config)# wireless tag rf Branch-RF-Tag
```

ステップ 6 **5ghz-rf-policy** *rf-profile-name* コマンドを使用して、RF タグを RF プロファイルに結び付け、それらを特定の無線機に適用します。

```
Device(config-wireless-rf-tag)# 5ghz-rf-policy Video-Optimized
```

ステップ 7 **end** コマンドを使用して、特権 EXEC モードに戻ります。

```
Device(config-wireless-rf-tag)# end
```

ステップ 8 （オプション）**show controllers dot11Radio** *radio_slot_id* コマンドを使用して、設定されている A-MPDU の長さの値を表示します。

```
Device# show controllers dot11Radio 1 Radio Aggregation Config: ========================== TX A-MPDU
 Priority: 0x3f TX A-MSDU Priority: 0x3f TX A-MPDU Window: 0x7f
```

SNMP 機能

WGB 上の Simple Network Management Protocol（SNMP）は、

- SNMP プロトコルを使用した WGB デバイスの監視と管理を容易にし、
- 情報交換のためのロール（マネージャ、エージェント、MIB）を内含し、
- ネットワークの正常性のアセスメントとパラメータ設定をサポートする機能要素です。

WGB の SNMP フレームワークには、以下が含まれます。

- SNMPマネージャ：SNMPを使用してネットワークデバイスのアクティビティを制御および監視します。通常はネットワーク管理システム（NMS）として導入されます。
- SNMPエージェント：デバイスのデータを維持し報告する、管理対象デバイス内のソフトウェアコンポーネント。
- SNMP MIB：SNMP マネージャによって照会または設定できる、管理対象オブジェクト（変数）の集合。

SNMP プロセス

次の図に、SNMPプロセスを示します。SNMPマネージャがデータを要求すると、エージェントはその要求を受信してサブエージェントに中継し、サブエージェントが応答します。その後、エージェントは SNMP 応答パケットをマネージャに送信します。

図 *2 : SNMP* プロセス

SNMP バージョン

Cisco IOS ソフトウェアでは、次のバージョンの SNMP がサポートされています。

- SNMPv2c：コミュニティストリングに基づく、SNMPv2 用の管理フレームワークです。SNMPv2c は、SNMPv2p（SNMPv2 クラシック）のプロトコル操作とデータ タイプが更新されたもので、SNMPv1 のコミュニティベースのセキュリティモデルを使用します。
- SNMPv3：SNMP バージョン 3。SNMPv3 は、次のセキュリティ機能によって、デバイスにセキュアなアクセスを提供します。
  - メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
  - 認証：有効な送信元からのメッセージであることを判別します。
  - 暗号化：パケットの内容をスクランブル化することにより、許可のないものに学習されないようにします。

サポートされる SNMP MIB ファイル

Management Information Base（MIB）は、デバイス上の管理可能なオブジェクトを含むデータベースです。変数とも呼ばれるこれらの管理対象オブジェクトを設定したり読み取ったりすることで、ネットワークデバイスやインターフェイスに関する情報を提供できます。オブジェクトは階層構造で編成され、オブジェクト識別子によって識別されるコレクションにグループ化されます。MIB へのアクセスは、SNMP などのネットワーク管理プロトコルを使用して提供されます。

MIB モジュールは、IEEE 802.11 ワイヤレスデバイスのアソシエーションの管理およびデータパケット転送の設定と統計に関するネットワーク管理情報を提供します。

オブジェクト識別子（OID）は、管理対象ネットワークデバイス上のMIBオブジェクトを一意に識別します。OID によって、MIB 階層内の MIB オブジェクトの位置が表示され、複数の管理対象デバイスのネットワーク内にあるMIBオブジェクトにアクセスする方法が示されます。

サポートされる OID

SNMP Management Information Base（MIB）でサポートされるオブジェクトのリスト。

- CISCO-DOT11-ASSOCIATION-MIB OID は次のとおりです。

表 *6 :* サポートされる *OID*

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11ParentAddress	1.3.6.1.4.1.9.9.273.1.1.1	文字列	親アクセスポイントの MAC アドレスです。
cDot11ActiveWirelessClients	1.3.6.1.4.1.9.9.273.1.1.2.1.1	ゲージ	このインターフェイス上のデバイスは、現在、この数のワイヤレスクライアントにアソシエートしています。
cDot11ActiveBridges	1.3.6.1.4.1.9.9.273.1.1.2.1.2	ゲージ	このインターフェイス上のデバイスは、現在、この数のブリッジにアソシエートしています。
cDot11ActiveRepeaters	1.3.6.1.4.1.9.9.273.1.1.2.1.3	ゲージ	このインターフェイス上のデバイスは、現在、この数のリピーターにアソシエートしています。

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11AssStatsAssociated	1.3.6.1.4.1.9.9.273.1.1.3.1.1	カウンタ	デバイスが再起動すると、このオブジェクトはインターフェイス上のデバイスがアソシエートされているステーションの数をカウントします。
cDot11AssStatsAuthenticated	1.3.6.1.4.1.9.9.273.1.1.3.1.2	カウンタ	デバイスが再起動すると、このオブジェクトは、インターフェイス上のデバイスで現在認証済みのステーションの数をカウントします。
cDot11AssStatsRoamedIn	1.3.6.1.4.1.9.9.273.1.1.3.1.3	カウンタ	デバイスが再起動すると、このオブジェクトは、別のデバイスからインターフェイス上のデバイスにローミングされたステーションの数をカウントします。
cDot11AssStatsRoamedAway	1.3.6.1.4.1.9.9.273.1.1.3.1.4	カウンタ	このオブジェクトは、デバイスの再起動以降、インターフェイス上のデバイスからローミングされたステーションの数をカウントします。

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11AssStatsDeauthenticated	1.3.6.1.4.1.9.9.273.1.1.3.1.5	カウンタ	このオブジェクトは、デバイスの再起動以降、インターフェイス上のこのデバイスから認証が解除されたステーションの数をカウントします。
cDot11AssStatsDisassociated	1.3.6.1.4.1.9.9.273.1.1.3.1.6	カウンタ	このオブジェクトは、デバイスの再起動以降、インターフェイス上のこのデバイスからアソシエーションが解除されたステーションの数をカウントします。
cd11IfCipherMicFailClientAddress	1.3.6.1.4.1.9.9.273.1.1.4.1.1	文字列	これは、直近の MIC 障害の原因となった無線インターフェイスに接続されているクライアントの MAC アドレスです。
cd11IfCipherTkipLocalMicFailures	1.3.6.1.4.1.9.9.273.1.1.4.1.2	カウンタ	デバイスが再起動すると、このオブジェクトは無線インターフェイスで発生した MIC 障害の数をカウントします。

OID オブジェクト名	OID	OID タイプ	OID の説明
cd11IfCipherTkipRemotMicFailures	1.3.6.1.4.1.9.9.273.1.1.4.1.3	カウンタ	デバイスが再起動すると、このオブジェクトは、無線インターフェイス上のクライアントによって報告された MIC 障害の数をカウントします。
cd11IfCipherTkipCounterMeasInvok	1.3.6.1.4.1.9.9.273.1.1.4.1.4	カウンタ	デバイスが再起動すると、このオブジェクトはインターフェイスで呼び出された TKIP カウンタ測定の回数をカウントします。
cd11IfCipherCcmpReplaysDiscarded	1.3.6.1.4.1.9.9.273.1.1.4.1.5	カウンタ	デバイスが再起動すると、このオブジェクトは、インターフェイスのリプレイメカニズムによって破棄された受信ユニキャストフラグメントの数をカウントします。
cd11IfCipherTkipReplaysDetected	1.3.6.1.4.1.9.9.273.1.1.4.1.6		デバイスが再起動すると、このオブジェクトはこのインターフェイスで検出された TKIP リプレイエラーの数をカウントします。
cDot11ClientRoleClassType	1.3.6.1.4.1.9.9.273.1.2.1.1.3	カウンタ	クライアントのロール分類。
cDot11ClientDevType	1.3.6.1.4.1.9.9.273.1.2.1.1.4	列挙値	クライアントのデバイスタイプ。

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11ClientRadioType	1.3.6.1.4.1.9.9.273.1.2.1.1.5	列挙値	クライアントの無線機の分類。
cDot11ClientWepEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.6	列挙値	クライアントのデータフレームの送信に WEP 鍵メカニズムを使用するかどうか。
cDot11ClientWepKeyMixEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.7	列挙値	このクライアントが WEP 鍵ミキシングを使用しているかどうか。
cDot11ClientMicEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.8	列挙値	クライアントの MIC が有効になっているかどうか。
cDot11ClientPowerSaveMode	1.3.6.1.4.1.9.9.273.1.2.1.1.9	列挙値	クライアントの電源管理モード。
cDot11ClientAid	1.3.6.1.4.1.9.9.273.1.2.1.1.10	ゲージ	これは、デバイスにアソシエートするクライアントまたはマルチキャストアドレスのアソシエーション識別子です。
cDot11ClientDataRateSet	1.3.6.1.4.1.9.9.273.1.2.1.1.11	文字列	このクライアントのデータ送受信におけるデータレートのセットです。
cDot11ClientSoftwareVersion	1.3.6.1.4.1.9.9.273.1.2.1.1.12	文字列	Cisco IOS ソフトウェアバージョン。
cDot11ClientName	1.3.6.1.4.1.9.9.273.1.2.1.1.13	文字列	Cisco IOS デバイスのホスト名。
cDot11ClientAssociationState	1.3.6.1.4.1.9.9.273.1.2.1.1.14	列挙値	このオブジェクトは、認証およびアソシエーションプロセスの状態を示します。

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11ClientVlanId	1.3.6.1.4.1.9.9.273.1.2.1.1.17	ゲージ	ワイヤレスクライアントがワイヤレスステーションに正常にアソシエートされたときに割り当てられる VLAN。
cDot11ClientSubIfIndex	1.3.6.1.4.1.9.9.273.1.2.1.1.18	整数	これは、このワイヤレスクライアントがワイヤレスステーションに正常にアソシエートされたときに割り当てられるサブインターフェイスの ifIndex です。
cDot11ClientAuthenAlgorithm	1.3.6.1.4.1.9.9.273.1.2.1.1.19	列挙値	アソシエーション中にワイヤレスステーションとこのクライアントの間で実行される IEEE 802.1x 認証方式。
cDot11ClientDot1xAuthenAlgorithm	1.3.6.1.4.1.9.9.273.1.2.1.1.21	オクテット文字列	ワイヤレスクライアントと認証サーバーの間で実行される IEEE 802.1x 認証方式。
cDot11ClientUpTime	1.3.6.1.4.1.9.9.273.1.3.1.1.2	ゲージ	このクライアントがこのデバイスにアソシエートされている時間（秒）。
cDot11ClientSignalStrength	1.3.6.1.4.1.9.9.273.1.3.1.1.3	整数	デバイス依存の測定単位で、クライアントから直近に受信したパケットの信号強度を測定します。

OID オブジェクト名	OID	OID タイプ	OID の説明
cDot11ClientSigQuality	1.3.6.1.4.1.9.9.273.1.3.1.1.4	ゲージ	デバイス依存の測定単位で、クライアントから直近に受信したパケットの信号品質を測定します。
cDot11ClientPacketsReceived	1.3.6.1.4.1.9.9.273.1.3.1.1.6	カウンタ	このクライアントから受信したパケット数。
cDot11ClientBytesReceived	1.3.6.1.4.1.9.9.273.1.3.1.1.7	カウンタ	クライアントから受信したバイト数。
cDot11ClientPacketsSent	1.3.6.1.4.1.9.9.273.1.3.1.1.8	カウンタ	クライアントに送信したパケット数。
cDot11ClientBytesSent	1.3.6.1.4.1.9.9.273.1.3.1.1.9	カウンタ	クライアントに送信したバイト数。
cDot11ClientMsduRetries	1.3.6.1.4.1.9.9.273.1.3.1.1.11	カウンタ	このカウンタは、1 回以上再送信した後に MSDU が正常に送信されるとカウントします。
cDot11ClientMsduFails	1.3.6.1.4.1.9.9.273.1.3.1.1.12	カウンタ	このカウンタは、送信試行回数が一定の上限を超えたためにクライアントが MSDU を正常に送信できないとカウントします。

SNMP パラメータの設定

このセクションでは、WGB で Simple Network Management Protocol（SNMP）を設定する方法を説明します。ネットワーク要件に応じて、SNMPv2c または SNMPv3 を有効にできます。手順には、コミュニティストリングまたはユーザー名の設定、認証方式と暗号化方式の定義、デバイスの SNMP 機能の有効化が含まれます。

- SNMP 機能を有効にする前に、CLI コマンド **configure snmp enabled** を使用して、すべての SNMP パラメータを設定します。
- SNMP 機能を無効にすると、すべての SNMP 設定が自動的に削除されます。

手順

ステップ 1 **configure snmp v2c community-id length** *length* コマンドを使用して、SNMP v2c コミュニティ ID を入力します（SNMP v2c のみ）。

```
Device#configure snmp v2c community-id 50
```

ステップ 2 **configure snmp version** {**v2c** | **v3**} コマンドを使用して、SNMP プロトコルのバージョンを指定します。

```
Device# configure snmp version v3
```

ステップ 3 **configure snmp auth-method** {**md5** | **sha**} コマンドを使用して、SNMP v3 認証プロトコルを指定します（SNMP v3 のみ）。

```
Device# configure snmp auth-method md5
```

ステップ 4 **configure snmp v3 username length** *length* コマンドを使用して、SNMP v3 ユーザー名を入力します（SNMP v3 のみ）。

```
Device# configure snmp v3 username length 32
```

ステップ 5 **configure snmp v3 password length** *length* コマンドを使用して、SNMP v3 ユーザーパスワードを入力します（SNMP v3 のみ）。

```
Device# configure snmp v3 password length 12
```

length の有効な範囲は 8 ～ 64 文字です。

ステップ 6 **configure snmp encryption** {**des** | **aes** | **none**} コマンドを使用して、SNMP v3 暗号化プロトコルを指定します（SNMP v3 のみ）。

```
Device#configure snmp encryption des
```

暗号化値は、**des** または **aes** です。v3 暗号化プロトコルが必要ない場合は、**none** を入力します。

ステップ 7 **configure snmp secret length** *length* コマンドを使用して、SNMP v3 暗号化パスフレーズを入力します（SNMP v3 のみ）。

```
Device#configure snmp secret length 12
```

length の有効な範囲は 8 ～ 64 文字です。

ステップ 8 **configure snmp enabled** コマンドを使用して、WGB で SNMP 機能を有効にします。

```
Device#configure snmp enabled
```

SNMP **v2c** を設定する場合は、ステップ 1、ステップ 2 およびステップ 8 を繰り返します。

SNMP **v3** を設定する場合は、ステップ 2 ～ 8 を繰り返します。

ステップ 9 （オプション）**configure snmp disabled** コマンドを使用して、SNMP 設定を無効にします。

```
Device# configure snmp disabled
```

SNMP の設定例

SNMP v2c の設定：

```
Device#configure snmp v2 community-id 25 Device#configure snmp version v2c Device#configure
 snmp enabled
```

SNMP v3 の設定（セキュリティレベル AuthPriv）：

```
Device#configure snmp auth-method md5 Device#configure snmp v3 username length 32
Device#configure snmp v3 password length 25 Device#configure snmp secret length 12
Device#configure snmp encryption aes Device#configure snmp version v3 Device#configure
snmp enabled
```

SNMP v3 の設定（セキュリティレベル AuthNoPriv）：

```
Device#configure snmp auth-method md5 Device#configure snmp v3 username length 32
Device#configure snmp v3 password length 32 Device#configure snmp encryption none
Device#configure snmp version v3 Device#configure snmp enabled
```

SNMP の確認

SNMP 設定を確認するには、**show snmp** コマンドを使用します。

SNMP version v3

```
Device# show snmp SNMP: enabled Version: v3 Community ID: test Username: username Password:
 password Authentication method: SHA Encryption: AES Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
```

SNMP version v2c

```
Device# show snmp SNMP: enabled Version: v2c Community ID: test Username: username
Password: password Authentication method: SHA Encryption: AES Encryption Passphrase:
passphrase Engine ID: 0x8000000903c0f87fe5f314
```

QoS ACL 分類およびマーキング

Quality of Service（QoS）ACL 分類およびマーキングは、アクセス制御リスト（ACL）ルールを使用してネットワークトラフィックを識別し、トラフィッククラスや優先順位値を割り当てます。

- 分類では、ACL を使用して、送信元または宛先 IP アドレス、プロトコルタイプ、ポート番号、その他のヘッダーフィールドなどのパラメータに基づいて、トラフィックフローを照合します。このステップでは、転送されるトラフィックのタイプ（音声、ビデオ、データなど）を特定します。
- マーキングは分類後に実行されます。パケットには、優先順位レベルを示す特定の QoS 値（DSCP、IP precedence、CoS など）がタグ付けされます。これらのマーキングは、ネットワーク全体のキューイング、ポリシング、シェーピングなどの QoS ポリシーを示します。

Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、2 つの有線ポートからの異なるパケットを分類し、それをユーザー設定に基づいて異なるアクセス制御ドライバキューに割り当てることができます。

WGB は、TCP または UDP に加えて、イーサネットタイプおよび DSCP に基づく分類もサポートします。ジッターおよび遅延の要件を満たすため、WGB はパケットを分類し、現場環境に応じてアクセス制御キューに割り当てます。

ルールベースのトラフィック分類

ルールベースのトラフィック分類は、次のようなネットワーク管理技術です。

- カスタムルールを使用して、802.1p、DSCP、プロトコルタイプなどの基準によって着信イーサネットパケットを分類し、
- 分類されたパケットを QoS を適用するためにワイヤレス側の優先順位キューに割り当てて、
- 重要なサービスがより高い優先順位になるようにし、遅延を減らしてネットワーク性能を最適化します。

ルール設定の基準

次のパラメータを使用して、マッピングルールを設定できます。

- イーサネットタイプ（Profinet など）
- トランスポート層のポート番号またはポート範囲
- DSCP 値
- 送信元 IP アドレスおよび宛先 IP アドレス
- プロトコルタイプ

パケットの分類と割り当て

着信パケットがイーサネットポートに到達すると、WGB は定義されたルールを次のように適用します。

- 重要なサービスまたはトラフィックフローの特定
- 事前定義された基準に基づくパケットの分類
- ワイヤレスネットワーク上の適切なアクセス制御キューへのパケットの割り当て

ルールベースのマッピングの利点

カスタマイズされたルールベースの分類とマッピングを使用して、以下を実行できます。

- QoS ポリシーの効果的な適用

- 重要なアプリケーションとサービスの優先順位付け
- 時間的制約のあるトラフィックの遅延を低減
- ネットワーク性能とユーザーエクスペリエンスの向上

QoS および ACL トラフィック分類方式

トラフィック分類は、パケットフィールドを調べて、特定のタイプのネットワークトラフィックを他のタイプから識別するプロセスです。QoS がアクティブな場合にのみ有効になります。分類時に、デバイスは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルによって、適用する QoS アクションが定義され、転送する出力キューが識別されます。

- 分類は複数のパケットレイヤのフィールドに依存しています。
- パケットは、Ethertype、DSCP、または TCP/UDP ポートに基づいてサービスクラスにグループ化され、各クラス内で一貫した扱いを受けます。
- データプレーンには分析のためにルールの的中数が記録され、コントロールプレーンではデータ転送が設定されます。

レイヤ 2 分類フィールド

レイヤ 2 イーサネットフレームでは、Ethertype フィールド（2 バイト）に分類情報が含まれます。このフィールドでは、通常、フレーム内のカプセル化されたデータのタイプが示されます。

レイヤ 3 分類フィールド

レイヤ 3 IP パケットでは、Type of Service（ToS）フィールド（8 ビット）に分類情報が含まれます。このフィールドには以下の値が含まれます。

- IP precedence 値（範囲 0 ～ 7）
- DSCP 値（範囲 0 ～ 63）

レイヤ 4 分類フィールド

レイヤ 4 TCP セグメントまたは UDP データグラムでは、source port フィールドまたは destination port フィールドが分類に使用されます。これらのポート番号を使用して、デバイスはアプリケーションまたはサービスに基づいてトラフィックを分類できます。

サービスクラスへのトラフィックの割り当て

システムにより、Ethertype、DSCP、または UDP/TCP ポート（またはポート範囲）に基づいて、トラフィックが特定のサービスクラスに割り当てられます。同一サービスクラス内のパケットは一貫した扱いを受けます。WGB は、有線ポートからのパケットを分類し、ユーザー設定に従って異なるドライバキューにマッピングします。

分類におけるデータプレーンの役割

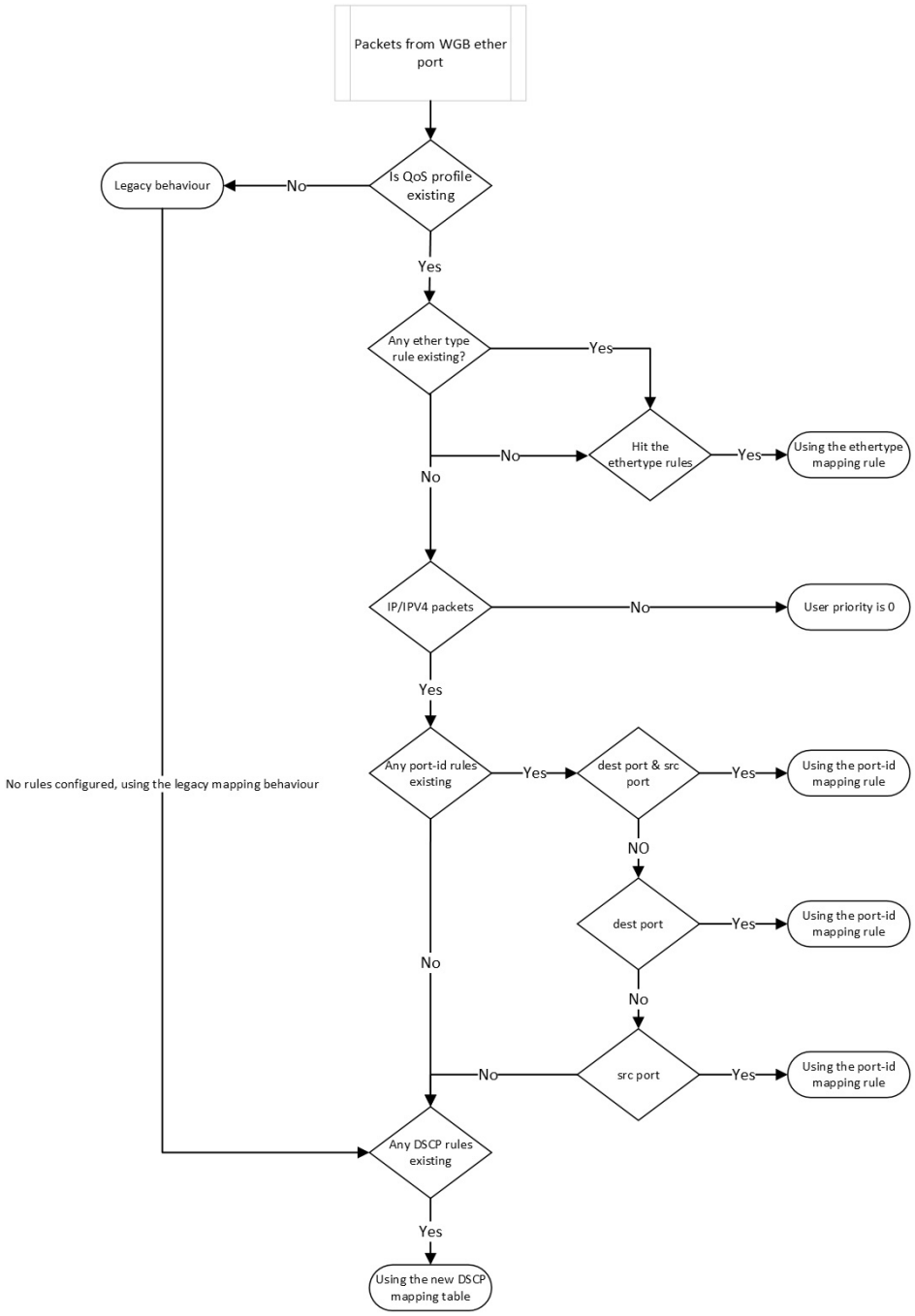
データプレーン統計には、トラフィックが各ルールと一致した回数を示すカウンタが表示されます。これらのカウンタは、管理者がルールの有効性を分析し、性能を最適化するのに役立ちます。

分類におけるコントロールプレーンの役割

コントロールプレーンは、ネットワークを介したデータの転送方法を管理および設定する役割を果たします。

次のフローチャートは、既存のプロファイル、Ethertype、ポート識別子、および DSCP 値に基づいて、WGB イーサネットポートからのパケットが分類され、QoS ルールにマッピングされる方法を示しています。

図 *3 : WGB* イーサネットポートからのトラフィックフローのフローチャート



レガシー QoS マッピング動作

process_summary

アクセスポイントは、VLAN ベースの TCI 値を取得し、Profinet に固定の優先順位 6 を適用し、IP および IPv6 トラフィックには DSCP から dot1p へのマッピングを使用して、トラフィックに優先順位を割り当てます。

process_workflow

アクセスポイントは、次のルールを使用して、トラフィックの優先順位を EtherType に基づいて決定します。

1. TCI の優先順位の取得：アクセスポイントは、指定された Ethertype 0x8100 の VLAN 要素からタグ制御情報（TCI）の優先順位を取得します。
2. Profinet の TCI 優先順位の割り当て：EtherType 0x8892（Profinet）の場合、アクセスポイントは、TCI の優先順位に 6 を割り当てます。
3. IP および IPv6 の DSCP 優先順位の設定：Ethertype 0x0800（IP）および 0x86DD（IPv6）の場合、アクセスポイントは、デフォルトの dscp2dot1p マッピングテーブルに従って DSCP の優先順位を設定します。

アクセスポイントによる QoS 優先順位の割り当て方法

process_summary

アクセスポイントは、プロトコルタイプと設定されたルールに基づいて QoS 優先順位を割り当てます。非 IP トラフィックの場合やルールが設定されていない場合は、デフォルトが適用されます。

process_workflow

アクセスポイントで QoS を有効にするプロセスの仕組みを以下に示します。

1. アクセスポイントが、設定に基づいて、Ethertype QoS マッピング 0x8892（Profinet）の優先順位を決定します。
2. Ethertype 0x0800（IP）および 0x86DD（IPv6）については、アクセスポイントが、ポートまたは DSCP のいずれかを考慮したマッピングルールに従って、優先順位を割り当てます。
   - アクセスポイントは、UDP/TCP ポート（またはポート範囲）ルールを確認します。
   - アクセスポイントは、DSCP ルールを確認します。
3. アクセスポイントが、IPv4/IPv6 以外のパケットにユーザー優先順位値 0 を割り当てます。
4. ルールが設定されていない場合、QoS プロファイルは、従来のマッピング動作にデフォルト設定されます。

（注） 802.1p の優先順位が存在する場合は、それがカスタマイズされたルールに優先します。

QoS マッピングプロファイルの設定

以下の手順により、WGB QoS マッピングを設定するための各種分類ルールを定義できます。

手順

ステップ 1 **config wgb qos-mapping** *profile-name* **enable** コマンドを使用して、指定された QoS マッピングプロファイルを有効にします。

```
Device# configure wgb qos-mapping demo-profile enable
```

ステップ 2 **config wgb qos-mapping** *profile-name* **add ethtype hex** *hex-number* **priority** *priority* コマンドを使用して、イーサネットタイプに基づくマッピングルールを追加します。

```
Device# configure wgb qos-mapping demo-profile add ethtype hex 8892 priority 5
```

（注）
指定されたプロファイルが存在しない場合、このコマンドによって新しい空のプロファイルが作成され、マッピングルールが追加されます。

config wgb qos-mapping *profile-name* **delete ethtype hex** *hex-number* を使用すると、イーサネットタイプに基づいてルールを削除できます。

（注）
指定されたプロファイルが存在しない場合、コマンドは警告を表示します。マッピングルールを削除するとプロファイルが空になる場合、そのプロファイルは自動的に削除されます。

ステップ 3 **config wgb qos-mapping** *profile-name* **add** [**srcport** *number* | **dstport** *number* | **range** *start-number ending-number*] **priority** *priority* コマンドを使用して、ポート ID または範囲に基づくマッピングルールを追加します。

```
Device# config wgb qos-mapping voice-profile add dstport 5004 priority 6
```

（注）
指定されたプロファイルが存在しない場合、このコマンドによって新しい空のプロファイルが作成され、マッピングルールが追加されます。

config wgb qos-mapping *profile-name* **delete** [**srcport** *number* | **range** *start-number ending-number* [**dstport** *number* | **range** *start-number ending-number*]] を使用すると、ポート ID/範囲に基づいてルールを削除できます。

（注）
指定されたプロファイルが存在しない場合、コマンドは警告を表示します。マッピングルールを削除するとプロファイルが空になる場合、そのプロファイルは自動的に削除されます。

ステップ 4 **config wgb qos-mapping** *profile-name* **add dscp** *number* **priority** *priority* コマンドを使用して、DSCP 値に基づくマッピングルールを追加します。

```
Device# configure wgb qos-mapping demo-profile add dscp 63 priority 4
```

（注）
指定されたプロファイルが存在しない場合、このコマンドによって新しい空のプロファイルが作成され、マッピングルールが追加されます。

config wgb qos-mapping *profile-name* **delete dscp** *number* **priority** *priority* コマンドを使用すると、DSCP 値に基づくマッピングルールを削除できます。

（注）
指定されたプロファイルが存在しない場合、コマンドは警告を表示します。マッピングルールを削除するとプロファイルが空になる場合、そのプロファイルは自動的に削除されます。

DSCP マッピングルールを削除すると、ルールは DSCP マッピングのデフォルト値にリセットされます。

ステップ 5 **config wgb qos-mapping** *profile-name* **disable** コマンドを使用して、指定された QoS マッピングプロファイルを無効にします。

```
Device# configure wgb qos-mapping demo-profile disable
```

無効にすると、プロファイルがデータパスから除去されますが、WGB 設定ファイルには残ります。プロファイルが存在しない場合、警告が表示され、新しいプロファイルは作成されません。

ステップ 6 （オプション）**config wgb qos-mapping** *profile-name* **delete** コマンドを使用して、指定された QoS マッピングプロファイルを削除します。

```
Device# configure wgb qos-mapping demo-profile delete
```

削除すると、プロファイルはデータパスと WGB 設定の両方から削除されます。

Quality of Service マップの確認

コントロールプレーンの QoS マッピング設定を確認するには、**show wgb qos-mapping** を実行します。

```
Device# show wgb qos-mapping Number of QoS Mapping Profiles: 2
==================================== Profile name : qos1 Profile status : active Number
 of Rules: 8 Rules: L4 srcport : 31000-31100, dstport : 6666-7777, priority : 7 L4 srcport
 : 23000, dstport : N/A, priority : 3 L4 srcport : N/A, dstport : 20000-20100, priority
 : 5 L4 srcport : N/A, dstport : 2222, priority : 2 L4 srcport : 12300-12500, dstport :
 N/A, priority : 6 IPv4/IPv6 dscp: 43, priority : 1 Ethernet type : 0x8892, priority :
0 L4 srcport : 8888, dstport : 9999, priority : 4

Profile name : qos2 Profile status : inactive Number of Rules: 8 Rules: L4 srcport :
31000-31100, dstport : 6666-7777, priority : 2 L4 srcport : 23000, dstport : N/A, priority
 : 6 L4 srcport : N/A, dstport : 20000-20100, priority : 4 L4 srcport : N/A, dstport :
2222, priority : 7 L4 srcport : 12300-12500, dstport : N/A, priority : 3 IPv4/IPv6 dscp:
 43, priority : 0 Ethernet type : 0x8892, priority : 1 L4 srcport : 8888, dstport : 9999,
 priority : 5
```

データプレーンの WGB QoS マッピング設定を確認するには、**show datapath qos-mapping rule** を実行します。

```
Device# show datapath qos-mapping rule Status: active QoS Mapping entries ======= dscp
mapping ======= Default dscp2dot1p Table Value: [0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0
 [6]->0 [7]->0 [8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1 [16]->2
```

```
[17]->2 [18]->2 [19]->2 [20]->2 [21]->2 [22]->2 [23]->2 [24]->3 [25]->3 [26]->3 [27]->3
 [28]->3 [29]->3 [30]->3 [31]->3 [32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4
 [39]->4 [40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5 [48]->6 [49]->6
 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6 [56]->7 [57]->7 [58]->7 [59]->7 [60]->7
 [61]->7 [62]->7 [63]->7

active dscp2dot1p Table Value: [0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1 [16]->7 [17]->2 [18]->2
[19]->2 [20]->2 [21]->2 [22]->2 [23]->2 [24]->3 [25]->3 [26]->3 [27]->3 [28]->3 [29]->3
 [30]->3 [31]->3 [32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4 [40]->5
 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5 [48]->6 [49]->6 [50]->6 [51]->6
 [52]->6 [53]->6 [54]->6 [55]->6 [56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7
 [63]->7
```

データプレーンの WGB QoS マッピング統計を確認するには、**show datapath qos-mapping statistics** コマンドを実行します。

```
Device# show datapath qos-mapping statistics ======= pkt stats per dscp-mapping rule
======= dscp up pkt_cnt 16 7 0
```

データプレーンの WGB QoS マッピング統計を消去するには、**clear datapath qos-mapping statistics** コマンドを実行します。

（注） このコマンドは、データプレーンのルールごとにパケットカウント統計を消去します。

パケットキャプチャ：TCP ダンプユーティリティ

TCP ダンプユーティリティは、ネットワーク パケット アナライザで、

- ネットワーク インターフェイスを介して送信されたパケットをキャプチャし、
- 監視および障害対応のためにパケットデータを表示および保存し、
- WGB での有線ネットワークトラフィックの詳細な分析を可能にします。

「WGB での TCP ダンプ」の章では、Catalyst IW9165E の WGB 有線インターフェイスを介して TCP ダンプを有効にする方法について説明します。

TCP ダンプユーティリティの目的

WGB の TCP ダンプは、ネットワーク通信を監視してトラブルシュートすることで、WGB により有線クライアントとワイヤレスネットワーク間でフレームが正しくリレーされるようにします。

TCP ダンプユーティリティは

- WGB 端末でキャプチャされたパケットをリアルタイムで表示し、
- ストレージにパケットをキャプチャする

（注） TCP ダンプユーティリティでは、パケットのストレージへのキャプチャと WGB 端末への表示を同時に行うことはできません。

パケットキャプチャモード

WGB パケット キャプチャ ユーティリティは、以下のモードと動作をサポートしています。

- Default：WGB 端末でキャプチャされたパケットをヘッダー付きでリアルタイムに表示します。
- Verbose：WGB 端末でリアルタイムパケットを解析して（ヘッダー付きで）出力し、各パケットのデータ（リンクレベルヘッダーを含む）を 16 進数フォーマットで出力します。

（注） text2pcap との互換性のためには Verbose 出力をフォーマットし直す必要があります。

デフォルトモードまたは冗長モードでは、WGB 端末は最大 1000 パケットのエントリを出力できます。

- Capture：パケットをリアルタイムで出力するのではなく、ファイルストレージにキャプチャします。キャプチャされた内部有線パケットを表示するには、**show pcap** コマンドを使用します。

（注） パケットキャプチャ（PCAP）を行うたびに、毎回既存の PCAP ファイルは消去されます。

新しい PCAP セッションを始める前に、現在の PCAP ファイルを外部サーバーに転送して、上書きされないようにします。

PCAP ファイルのサイズが 100 MB に達すると、PCAP は自動的に停止します。

プロトコル パケット キャプチャ機能

デフォルトフィルタまたはカスタムフィルタを使って、WGB 有線ポートを介して AP からパケットをキャプチャし、外部サーバーにアップロードできます。

デフォルトフィルタによるキャプチャでは、IP、TCP、UDP などの 3 つの主要なプロトコルパケットをキャプチャします。

カスタムフィルタによるキャプチャでは、特定の問題の障害対応または特定のタイプのネットワークアクティビティの監視に関連する特定のパケットをキャプチャします。

さまざまなプロトコルフィルタを使用して、デバッグのためのパケットをキャプチャできます。たとえば、フィルタ式に次のような特定のプロトコルを含めます。

- Transmission Control Protocol（TCP）、Internet Control Message Protocol（ICMP）、ICMPv6
- IP プロトコル 0x8892 を使用した Profinet
- アドレス解決プロトコル（ARP）
- インターネット グループ管理プロトコル（IGMP）
- User Datagram Protocol
- ポート 67 またはポート 68 を使用した Dynamic Host Configuration Protocol（DHCP）、およびポート 546 またはポート 547 を使用した DHCPv6
- TCP ポート 44818 を使用した Common Industrial Protocol（CIP）
- ポート 53 を使用したドメインネームシステム（DNS）
- ポート 161 またはポート 162 を使用した Simple Network Management Protocol

（注） こちらにリストされているプロトコルは、PCAP 機能の一部にすぎません。

パケットキャプチャのフィルタ式

PCAP のフィルタ式は、1 つ以上のプリミティブで構成されます。プリミティブは通常、修飾子とそれに続く識別子で構成されます。識別子には、名前または番号を指定できます。

修飾子は 3 種類あります。

- Type：識別子のタイプを指定します。タイプには、ポート、ホスト、ネットワーク、またはポートの範囲を指定できます。

  例：port 20

- Dir：特定の方向に転送されるパケットのみをキャプチャするよう指定します。

  例： src x.x.x.x and port ftp-data または dst x.x.x.x and port ftp

- Proto：特定のプロトコルに限定してキャプチャします。

  例： tcp port 21

論理演算子 AND、OR、および NOT を使用してフィルタ式を組み合わせることで、より具体的で複雑なフィルタを作成できます。

（注） フィルタ式を作成するときは、演算の順序を理解し、必要に応じてカッコを使って式をグループ化することで正しく解釈されるようにすることが重要です。

有線パケットキャプチャの有効化

この手順では、有線トラフィックを監視するために、WGB でパケットキャプチャ（PCAP）を有効にします。これにより、プロトコル（IP、TCP、UDP）ごとにパケットをキャプチャし、詳細な分析のために詳細出力を適用し、パケットデータを PCAP ファイルに保存し、カスタムフィルタ（VLAN を含む）を使用してネイティブ VLAN と非ネイティブ VLAN にわたる特定のトラフィックを分析することができます。

手順

ステップ 1 次のいずれかのオプションを選択して、PCAP を有効にします。

オプション	説明
デフォルトフィルタを使用して PCAP を実行する	**debug traffic wired** [**0**| **1**]{**ip**	**tcp**	**udp**}[**verbose**	**capture]** コマンドを使用します。 `Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition enable` [**0**| **1**] は、有線インターフェイス番号を指定します。選択されていない場合は、すべての有線インターフェイスからパケットをキャプチャします。 `Device# debug traffic wired 1 ip APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:35:50.529851 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 13721, seq 1, length 64 2 08:35:50.534813 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 13721, seq 1, length 64` このオプションはデフォルトであり、IP プロトコルヘッダーがあるパケットがキャプチャされます。 `Device# debug traffic wired 1 udp verbose APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:25:59.696990 IP6 fe80::322c:712c:5787:f246.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit 0x0000: 3333 0001 0002 fc58 9a16 e428 86dd 6001 0x0010: 7b92 006d 1101 fe80 0000 0000 0000 322c 0x0020: 712c 5787 f246 ff02 0000 0000 0000 0000 0x0030: 0000 0001 0002 0222 0223 006d 00a6 010c 0x0040: d064 0008 0002 ffff 0006 001e 0034 0011 0x0050: 0015 0016 0017 0018 001f 0038 0040 0043 0x0060: 0052 0053 005e 005f 0060 0001 000a 0003 0x0070: 0001 fc58 9a16 e428 0014 0000 0027 0013 0x0080: 0006 4150 4643 3538 0439 4131 3604 4534 0x0090: 3238 0000 0300 0c00 0000 0100 0000 0000 0x00a0: 0000 00` verbose オプションは、UDP プロトコルパケットから詳細情報をキャプチャします。 `Device# debug traffic wired 1 tcp capture % Writing packets to "/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)`
カスタムフィルタを使用して PCAP を実行する	**debug traffic wired** [**0**	**1**] **filter** *expression* [**verbose**	**capture]** コマンドを使用します。 有効にする PCAP プロセスは一度に 1 つとしてください。フィルタ式では、" ` $ ^ & | \ > < ? ; ~ などのサポートされていない文字を使用しないでください。 `Device# debug traffic wired 0 filter icmp APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 10:38:59.948729 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 16204, seq 1, length 64 2 10:38:59.954308 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 16204, seq 1, length 64`

オプション	説明
	このオプションはデフォルトであり、IP プロトコルヘッダーがあるパケットがキャプチャされます。 `Device# debug traffic wired 1 filter icmp verbose APXXXX.XXXX.XXXX##reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 17:13:30.706493 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 986, seq 1, length 64 0x0000: fc58 9a17 afd4 f8e4 3b9d 7322 0800 4500 0x0010: 0054 57a0 4000 4001 889e c0a8 6cc8 c0a8 0x0020: 6c51 0800 940c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637 17:13:30.710567 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 986, seq 1, length 64 0x0000: f8e4 3b9d 7322 fc58 9a17 afd4 0800 4500 0x0010: 0054 9102 0000 4001 8f3c c0a8 6c51 c0a8 0x0020: 6cc8 0000 9c0c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637` verbose オプションは、UDP プロトコルパケットから詳細情報をキャプチャします。 `Device# debug traffic wired 1 filter icmp capture % Writing packets to "/tmp/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)` capture オプションは、TCP パケット情報を PCAP ファイルに保存します。

カスタムフィルタを使用して複数 VLAN で PCAP を実行する	**debug traffic wired** [**0**| **1**][**filter** *expression* |**ip** } コマンドを使用します。
	（注）
	一部のカスタムフィルタでは、非ネイティブ VLAN のトラフィックをキャプチャできません。たとえば、カスタムフィルタコマンド **debug traffic wired 0 filter icmp** では、非ネイティブ VLAN のダウンリンク ICMP トラフィックをキャプチャできません。
	`Device#debug traffic wired 0 filter "icmp or (vlan and icmp)" 1 12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64 2 12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1, length 64`
	フィルタ式に VLAN を追加して、非ネイティブ VLAN の有線クライアントから双方向トラフィックをキャプチャします。
	`Device#debug traffic wired 0 ip 1 12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64 2 12`
	デフォルト IP フィルタを使用して、ネイティブ VLAN と非ネイティブ VLAN を含むすべての IP トラフィックをキャプチャします。

ステップ 2 パケットを外部サーバーにアップロードするために、次のコマンドを使用します。**copy pcap** *file-name.pcap0* {**tftp**| **sftp**}://*server-ip* [*directory*][*file-name*] コマンドを使用して、パケットを外部サーバーにアップロードします。

```
 Device# copy pcap APXXXX.XXXX.XXXX_capture.pcap0 scp://iot@209.165.200.213:/capture/wgb_sniffer.pcap
 copy ""/pcap/APXXXX.XXXX.XXXX_capture.pcap0"" to
"scp://iot@209.165.200.213:/capture/wgb_dhcp_sniffer_0_46_29.pcap" (Y/N)Y iot@209.165.200.213
password: APXXXX.XXXX.XXXX_capture.pcap0 0% 0 0.0KB/s --:-- ETA APXXXX.XXXX.XXXX_capture.pcap0 100%
 2530 916.5KB/s 00:00
```

（注）

アップロードする前に、PCAPプロセスを完了し、パケットをファイルに保存してください。TFTP、SFTP、または SCP サーバーを使用して、PCAP ファイルを外部サーバーに転送します。

有線パケットキャプチャの無効化

手順

ステップ 1 **no debug traffic wired** [*0-3*]{**ip** | **tcp** | **udp**}[**verbose** | **capture**] コマンドを使用して、デフォルトのフィルタで PCAP を無効にします。

```
Device# no debug traffic wired 1 ip verbose
```

ステップ 2 **no debug traffic wired** [*0-3*]**filter** *expression* [**verbose** | **capture**] コマンドを使用して、カスタムフィルタで PCAP を無効にします。

```
Device# no debug traffic wired 0 filter "icmp or (vlan and icmp)" capture
```

（注）
キャプチャプロセスを終了するために **no debug** コマンドまたは **undebug all** コマンドを使用することもできます。

有線パケットキャプチャの確認

- デバッグステータスを確認するには、**show debug** コマンドを使用します。

```
Device#show debug traffic: wired tcp debugging is enabled
```

- ファイルに保存されているキャプチャ済み内部有線パケットを表示するには、**show pcap** コマンドを使用します。

（注） パケットをファイルにキャプチャした後、**show pcap** コマンドを使用してパケットを表示します。

```
Device#show pcap reading from file /pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type
EN10MB (Ethernet) 1 00:00:00.000000 IP 0.0.0.0 > 224.0.0.1: igmp query v2 2
09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920, seq
 1, length 64 3 09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply,
 id 29920, seq 1, length 64 4 09:41:49.904914 IP 209.165.200.102 > 209.165.200.1:
ICMP echo request, id 29920, seq 2, length 64 5 09:41:49.909009 IP 209.165.200.1 >
209.165.200.102: ICMP echo reply, id 29920, seq 2, length 64
```

- キャプチャされたパケットの基本的な内容をフィルタ処理して順番に表示するには、**show pcap [filter** *expression***]** コマンドを実行します。

```
Device#show pcap filter "src 209.165.200.189" reading from file
/pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type EN10MB (Ethernet) 1 09:41:48.903670
```

```
 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920, seq 1, length 64
2 09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920, seq
 1, length 64
```

- 特定のパケットの詳細な内容をフィルタ処理して表示するには、**show pcap [filter** *expression***][detail** *no***]** コマンドを実行します。

```
Device#show pcap filter "src 209.165.200.189" detail 2 2024-04-25 09:41:49.904914
000000 18 59 f5 96 af 74 00 50 56 85 8a 0a 08 00 45 00 000010 00 54 14 6c 40 00 40
01 b7 9d 64 16 53 72 64 16 000020 53 01 08 00 70 81 74 e0 00 02 d4 3e 2b 66 00 00
000030 00 00 50 24 04 00 00 00 00 00 10 11 12 13 14 15 000040 16 17 18 19 1a 1b 1c
1d 1e 1f 20 21 22 23 24 25 000050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
000060 36 37
```

ポートアドレス変換

ポートアドレス変換（PAT）は、ネットワークアドレスポート変換（NAPT）とも呼ばれ、次のようなネットワークアドレス変換方式です。

- 複数の内部有線クライアントのプライベート IP アドレスとポート番号を
- 一意のパブリック IP アドレスとポート番号に変換し、
- 変換後にパケットが外部ネットワークに送信されます 。

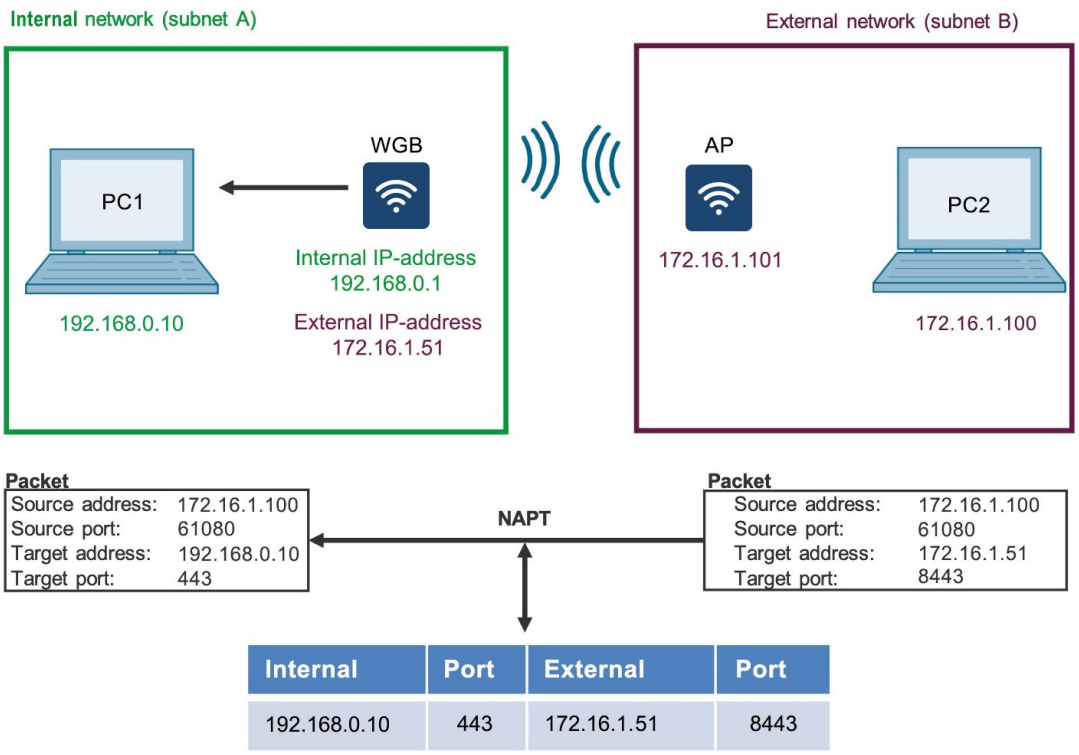
プライベート IP アドレスは、内部ネットワーク内のみで使用されます。パブリック IP アドレスは、グローバルに一意であり、インターネット上で使用されます。NAPTマッピングでは、IPアドレスとポート番号の両方が使用されます。両方を使用することにより、複数の内部ホストからのパケットを、異なるポート番号を使用して同じ外部 IP アドレスにマッピングできます。その結果、内部ローカルサブネット内のクライアントデバイスは、複数の無人搬送車（AGV）で同じ IP アドレスを再利用できるようになります。

UIW リリース 17.16.1 以降、PAT は、各 AGV の IW9165E ワークグループブリッジ（WGB）アクセスポイント（AP）でサポートされています。

（注） AGV 上の Profinet クライアントを、グローバルサブネットに属する一意の IP アドレスを使用して設定する必要があります。

次の画像は、ネットワークアドレスポート変換（NAPT）の概念を示しており、ワイヤレスゲートウェイ ブリッジ（WGB）が、外部 IP アドレスとポートを内部アドレスにマッピングすることにより、外部ネットワークから内部ホストへの着信パケットを変換する方法を図示しています。

図 *4*: 内部ネットワークと外部ネットワーク間の *NAPT* 変換



サポートされているプロトコル

NAPT は、内部ネットワークのデバイスと外部ネットワークのデバイス間の通信で TCP と UDP をサポートします。

WGB の制限事項

- NAT は、デバイスの背後からの 802.1Q VLAN タグ付き着信パケットに対してはサポートされません。
- マルチキャストトラフィックは、NAT の内側の有線クライアントに対してはサポートされません。
- FTP トラフィックは、アクティブモードでサポートされます。パッシブモードでは、FTP トラフィックは FTP サーバーが NAT の内側に配置されている場合にのみサポートされます。
- TFTP プロトコルは、TFTP サーバーが NAT の内側に存在する場合にのみサポートされます。
- アプリケーション レイヤ ゲートウェイ（ALG）はサポートされません。

uWGB の制限事項

- アクセス制御リスト（ACL）はサポートされません。
- NAPT は、1 つのプライベート LAN のみを NAPT の内側のネットワークとしてサポートします。

NAPT ルールとマッピングテーブル

NAPT ルールおよびマッピングテーブルは、以下のようなネットワーク変換メカニズムです。

- ワークグループブリッジ（WGB）が内部プライベートアドレスおよびポートを外部のルーティング可能なアドレスおよびポートに変換する方法を定義し、
- 内部デバイストラフィックを対応するグローバル IP/ポートペアにマッピングするテーブルを維持し、
- アドレスとポートの変換で TCP プロトコルと UDP プロトコルの両方をサポートします。

この設定は、WGB で最大 256 の IP NAT ルールをサポートします。

NAPT マッピングテーブル

このマッピングテーブルは、トラフィックルールと NAPT ルールに基づいて作成および管理されます。

NAPT は、送信元 IP アドレス、送信元ポート番号、プロトコルタイプ、宛先 IP アドレス、宛先ポート番号（TCP または UDP）を含むエントリを使用します。これらのエントリにより、システムはアドレスを変換し、パケットをフィルタリングし、NAPT マッピングテーブルをインデックス化できます。

（注） NAPT 変換テーブル内のマッピングエントリの最大数は 4096 です。

次の表に NAPT マッピングの例を示します。

表 *7: NAPT* マッピングテーブル

プロトコル	内部ローカル IP アドレスおよびポート	WGB グローバル IP アドレス	外部グローバル IP アドレスおよびポート
TCP	192.168.0.10: 80	172.16.100.11	172.16.100.11: 61080

上りと下りのデータ流

上りと下りのデータ流は、次のようなタイプのネットワークトラフィックの流れです。

- ネットワークアドレスおよびポート変換（NAPT）を使用して送信元アドレスまたは宛先アドレスを変換し、

- 内部ネットワークと外部ネットワークの間でデータを安全に転送できるようにし、
- IP アドレスのプライバシーと完全性を維持します。

NAPT を使用した下りのデータ流

下りのデータ流とは、外部ネットワークから AGV の内部ネットワークへのデータの流れを指します。ゲートウェイ（WGB または uWGB）は、外部ネットワークと内部ネットワーク間の通信を管理します。

パケットが外部 IP アドレスとポート番号を使用して到達すると、マッピングテーブルがチェックされ、対応する内部宛先が特定されます。

次にパケットが変換され、宛先 IP アドレスとポート番号に基づいて内部ネットワークに転送されます。

以下の図は、アドレスおよびポート変換によって、プライベート LAN クライアントと外部ネットワーク間の上り（内部から外部）と下り（外部から内部）両方のトラフィックの流れを管理する方法を示しています。

図 *5: WGB* での *NAPT* を使用した上りと下りのデータ流

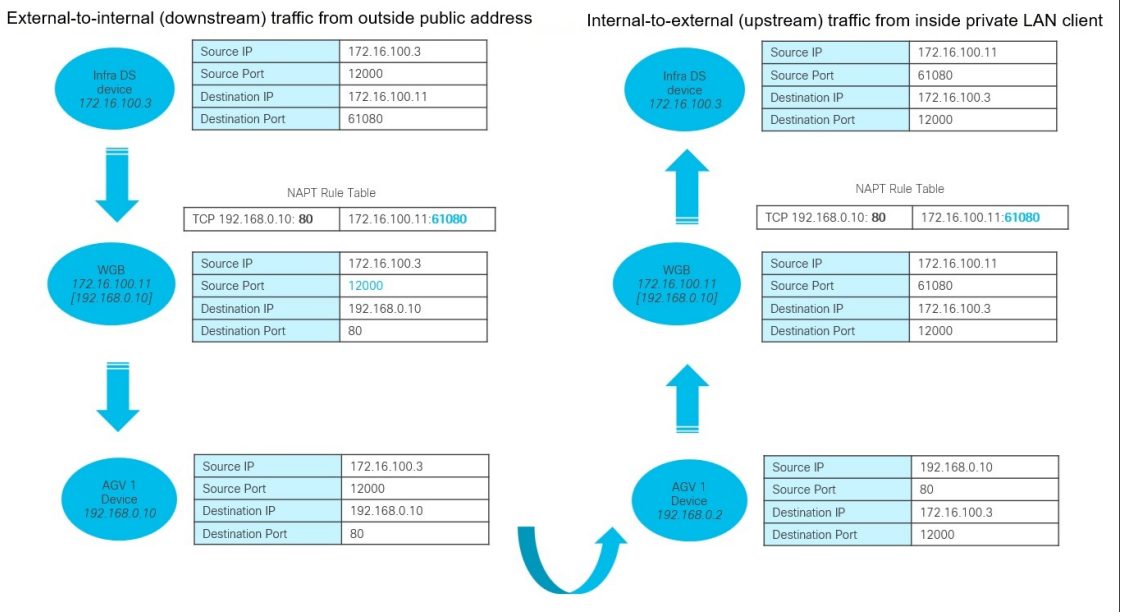
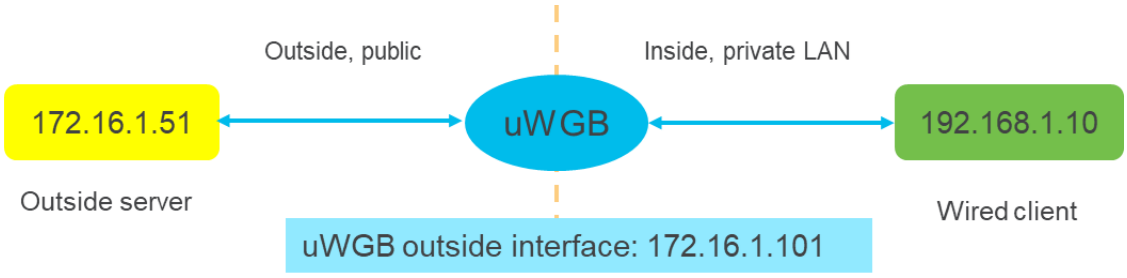


図 *6 : uWGB* での *NAPT* を使用した上りと下りのデータ流



SNAT を使用した上りのデータ流

上りのデータ流とは、内部ネットワークから外部ネットワークへのパケットの転送を指します。ゲートウェイにより、2 つのネットワーク間の通信が可能になります。

内部ネットワークからのすべての発信パケットは、送信元ネットワークアドレス変換（SNAT）を使用して外部ネットワークに対して変換されます。

上りのトラフィックの場合、SNAT は送信元 IP アドレスとポート番号をゲートウェイの IP アドレスに置き換え、内部 IP アドレスが外部ネットワークに公開されないようにします。

WGB での NAPT 変換

この手順では、上りのデータ流の送信元ネットワークアドレス変換（SNAT）と、下りのデータ流のネットワークアドレスポート変換（NAPT）を設定する方法について説明します。

SNAT を使用して上りのデータ流を設定するには、ステップ 1 ～ 3 を実行します。

NAPT を使用して下りのデータ流を設定するには、ステップ 4 および 5 を実行します。

手順

ステップ 1 **configure ip nat enable** コマンドを使用して、NAPT を有効にします。

```
Device#configure ip nat enable
```

NAPT を無効にするには、**configure ip nat disable** コマンドを使用します。

ステップ 2 **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* コマンドを使用して、内側の IPv4 アドレスとネットマスクを設定します。

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

ステップ 3 （オプション）**configure ip nat inside port range** *min-port-number max-port-number* コマンドを使用して、上りのデータ流の SNAT ポート範囲を設定します。

```
Device# configure ip nat inside port range 32000 33000
```

有効な値の範囲は 1 ～ 65535 です。デフォルトの範囲は 30000 ～ 59999 です。

（注）
SNAT ポート範囲と NAPT ポート範囲が重複しないようにしてください。

ステップ 4 **configure ip nat outside port range** *min-port-number max-port-number* コマンドを使用して、下りのデータ流の NAPT ポート範囲を設定します。

```
Device# configure ip nat outside port range 34000 62000
```

外側のポート番号の有効範囲は 1025 ～ 65535 です。予約済みのポート 1233、1234、20000 は使用しないでください。

（注）
NAPT ポート範囲と SNAT ポート範囲が重複しないようにしてください。

ステップ 5 **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} コマンドを使用して、下りのデータ流の NAPT マッピングルールを設定します。

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address は、内部有線クライアントネットワークの IP アドレスです。

inside-port-number は、内部有線クライアントネットワークの TCP ポート番号または UDP ポート番号です。

外側のポート番号は、設定された NAPT 範囲内である必要があります。

ステップ 6 （オプション）現在の NAPT 設定を表示するには、**show ip nat configuration** コマンドを使用します。

```
Device# show ip nat configuration IP NAT Configuration are: ====================================
Status: enabled inside interface ip/netmask: 192.168.0.1/255.255.255.0 SNAT port range: 10000 -
20000 NAPT port range: 61000 - 65535 The number of ip nat rules: 1 Id Outside_port Inside_ip
Inside_port Protocol 0 61080 192.168.0.10 80 tcp
```

ステップ 7 （オプション）NAPT ルールテーブルから現在の NAPT 変換エントリを表示するには、**show ip nat translations** コマンドを使用します。

```
Device# show ip nat translations UDP: src_ip port dst_ip port => src_ip port dst_ip port direction
 expiry_time (192.168.0.10, 41278, 172.16.1.51, 22000) => (172.16.1.101, 30004, 172.16.1.51, 22000)
 [forward] exp: 290 (172.16.1.51, 22000, 172.16.1.101, 61080) => (172.16.1.51, 22000, 192.168.0.10,
 41278) [reverse] exp: 290 ==================================== TCP: src_ip port dst_ip port =>
src_ip port dst_ip port direction expiry_time (192.168.0.10, 80, 172.16.100.3, 443) => (172.16.100.11,
 30000, 172.16.100.3, 443) [forward] exp: 138 (172.16.100.3, 443, 172.16.100.11, 30000) =>
(172.16.100.3, 443, 192.168.0.10, 80) [reverse] exp: 138
```

出力中の「forward」は、WGB によって処理されたデータパケットのログ詳細を指します。これには送信元、接続先、および変換情報が含まれます。

「Reverse」とは、戻りトラフィックのログ詳細を指し、トラフィックの方向を反転することによって、接続先からの応答が本来の送信元に確実に到達するようにします。この操作により、元のトラフィックの方向を逆にして、接続先からの応答が送信元に正常に到達するようになります。

NAPT 展開での uWGB の管理

NAPT 展開で uWGB を管理するには、次の手順に従います。

始める前に

すべての uWGB 有線クライアントがプライベート LAN 内にあることを確認します。

手順

ステップ 1 **configure dot11Radio 1 mode uwgb** *mac_address* **ssid-profile** *test_ssid* コマンドを使用して、無線モードを uWGB に設定します。

```
Device# configure dot11Radio 1 mode uwgb FC:58:9A:17:0D:52 ssid-profile testssid
```

一意の MAC アドレスを選択するか、次に示すオプションの方法を使用して一意の MAC アドレスを計算できます。

（注）
接続の問題を防ぐため、MAC アドレスがネットワーク上の既存のデバイスと競合しないようにしてください。

一意の MAC アドレスを計算するには、オフセット値 0x12 を基底 MAC アドレスに追加します。

基底 MAC アドレスを見つけるには、ステップ 2 に示すように、**show controllers dot11Radio** *interface* コマンドを使用します。

次の式を使用します。基底 MAC アドレス + オフセット = 一意の MAC アドレス

（注）
オフセット値が 0x12 以上であることを確認します。たとえば、FC:58:9A:17:0D:40 に 0x12 を追加すると、FC:58:9A:17:0D:52 になります。

ステップ 2 （オプション）**show controllers dot11Radio 1** コマンドを使用して基底 MAC アドレスを検索します。

```
Device#show controllers dot11Radio 1 wifi1 Link encap:Ethernet HWaddr FC:58:9A:17:0D:40 UP BROADCAST
 RUNNING MULTICAST MTU:1500 Metric:1 RX packets:9109 errors:70 dropped:59043 overruns:0 frame:0 TX
 packets:27920 errors:13 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:2699 RX bytes:913806
 (892.3 KiB) TX bytes:5399794 (5.1 MiB)
```

ステップ 3 （オプション）**show wgb dot11 associations** コマンドを使用して、uWGB が WGB 状態であることを確認します。

```
Device#show wgb dot11 associations Uplink Radio ID : 1 Uplink Radio MAC : FC:58:9A:17:0D:52 SSID
Name : SSID_NAME Connected Duration : 56 hours, 37 minutes, 11 seconds Parent AP MAC :
B0:B8:67:3D:5E:D6 Uplink State : CONNECTED Auth Type : PSK Key management Type : WPA2 Uclient mac
: FC:58:9A:17:0D:52 Current state : WGB Uclient timeout : 60 Sec Dot11 type : 11ac Channel : 157
Bandwidth : 20 MHz Current Datarate (Tx/Rx) : 156/144 Mbps Max Datarate : 156 Mbps RSSI : 35 IP :
172.16.1.101/24 Default Gateway : 172.16.1.1 IPV6 : ::/128 Assoc timeout : 100 Msec Auth timeout :
 100 Msec Dhcp timeout : 60 Sec'
```

ステップ 4 uWGB 有線クライアントのエンドツーエンド トラフィック フローを有効にするように NAPT を設定します。

uWGB での NAPT 設定

この手順では、上りのデータ流の送信元ネットワークアドレス変換（SNAT）と、下りのデータ流のネットワークアドレスポート変換（NAPT）を設定する方法について説明します。

SNAT を使用した上りのデータ流のサポートを設定するには、ステップ 1 ～ 4 の手順に従います。

NAPT を使用した下りのデータ流のサポートを設定するには、ステップ 5 とステップ 6 の手順に従います。

手順

ステップ 1 **configure ip nat enable** コマンドを使用して、NAPT を有効にします。

```
Device#configure ip nat enable
```

（注）
NAPT を無効にするには、**configure ip nat disable** コマンドを使用します。

ステップ 2 （オプション）**configure ip nat inside port range** *min-port-number max-port-number* コマンドを使用して、上りのデータ流の SNAT ポート範囲を設定します。

```
Device# configure ip nat inside port range 32000 33000
```

有効な範囲は 1025 ～ 65535 です。デフォルトの範囲は 30000 ～ 59999 です。

（注）
SNAT ポート範囲は、内部ネットワークから外部ネットワークにトラフィックを送信するときに uWGB が使用する送信元ポートです。

SNAT ポート範囲と NAPT ポート範囲が重複しないようにしてください。

ステップ 3 **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* コマンドを使用して、uWGB で内部有線クライアントのゲートウェイ IPv4 アドレスを設定します。

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

ステップ 4 **configure interface nat-outside address ipv4 static** *static-ip-address static-netmask gateway-ip-address* コマンドを使用して、uWGB で外部 IPv4 アドレスを設定します。

```
Device# configure interface nat-outside address ipv4 static 172.16.1.101 255.255.255.0 172.16.1.1
```

static-ip-address は、uWGB 自身のパブリックアドレスです。

gateway-ip-address は、uWGB の外部 IP アドレスです。

外側のポート番号は、上りのデータ流用に自動的に生成されます。

この設定は、内部から外部へのトラフィックフローをサポートします。

ステップ 5 **configure ip nat outside port range** *min-port-number max-port-number* コマンドを使用して、外部ネットワークから内部ネットワークへのトラフィックを受信するように uWGB で NAPT ポート範囲を設定します。

```
Device# configure ip nat outside port range 34000 62000
```

外側のポート番号の有効範囲は 1025 ～ 65535 です。予約済みのポート 1233、1234、20000 は使用しないでください。

（注）
NAPT ポート範囲と SNAT ポート範囲が重複しないようにしてください。

ステップ 6 **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} コマンドを使用して、下りのデータ流の NAPT マッピングルールを設定します。

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address は、内部有線クライアントネットワークの IP アドレスです。

inside-port-number は、内部有線クライアントネットワークの TCP ポート番号または UDP ポート番号です。

外側のポート番号は、設定された NAPT 範囲内である必要があります。

ステップ 7 （オプション）現在の NAPT 設定を表示するには、**show ip nat configuration** コマンドを使用します。

```
Device# show ip nat configuration IP NAT Configuration are: ===================================
Status: enabled inside interface ip/netmask: 192.168.1.1/255.255.255.0 SNAT port range: 30000 -
59999 NAPT port range: 60000 - 65000 outside proxy ip/netmask/gateway:
172.16.1.101/255.255.255.0/172.16.1.1 The number of ip nat rules: 2 Id Outside_port Inside_ip
Inside_port Protocol 0 61001 192.168.1.10 20001 udp 1 61002 192.168.1.10 20002 tcp
```

ステップ 8 （オプション）NAPT ルールテーブルから現在の NAPT 変換エントリを表示するには、**show ip nat translations** コマンドを使用します。

```
Device#show ip nat translations ICMP: src_ip dst_ip port => src_ip dst_ip port direction expiry_time
 (172.16.1.1, 172.16.1.101, 30257) => (172.16.1.1, 192.168.1.10, 267) [reverse] exp: 272 (192.168.1.10,
 172.16.1.1, 11) => (172.16.1.101, 172.16.1.1, 30001) [forward] exp: 272
=================================== UDP: src_ip port dst_ip port => src_ip port dst_ip port direction
 expiry_time (192.168.1.10, 20000, 172.16.1.51, 35200) => (172.16.1.101, 61001, 172.16.1.51, 35200)
 [reverse] exp: 214 (192.168.1.10, 51184, 172.16.1.51, 22000) => (172.16.1.101, 30001, 172.16.1.51,
 22000) [forward] exp: 161 (172.16.1.51, 35200, 172.16.1.101, 61001) => (172.16.1.51, 35200,
192.168.1.10, 20000) [forward] exp: 214 (172.16.1.51, 22000, 172.16.1.101, 30001) => (172.16.1.51,
 22000, 192.168.1.10, 51184) [reverse] exp: 161 ================================== TCP: src_ip
port dst_ip port => src_ip port dst_ip port direction expiry_time (192.168.1.10, 44155, 172.16.1.51,
 23000) => (172.16.1.101, 30002, 172.16.1.51, 23000) [forward] exp: 238 (172.16.1.51, 23000,
172.16.1.101, 30002) => (172.16.1.51, 23000, 192.168.1.10, 44155) [reverse] exp: 238
==================================
```

出力中の「forward」は、uWGB によって処理されたデータパケットのログ詳細を指します。これには送信元、接続先、および変換情報が含まれます。

「Reverse」とは、戻りトラフィックのログ詳細を指し、トラフィックの方向を反転することによって、接続先からの応答が本来の送信元に確実に到達するようにします。この操作により、元のトラフィックの方向を逆にして、接続先からの応答が送信元に正常に到達するようになります。

NAPT マッピングルールの削除

この手順では、NAPT 設定エントリを削除する方法について説明します。inside と outside パラメータを指定することで特定の NAPT マッピングルールを削除できます。ルール ID でルール

を削除したり、設定からすべてのNAPTルールを消去したりできます。特定のルールを削除するか、あるいはNAPT設定全体をリセットするかに基づいて、方法を選択します。

手順

以下のいずれかのオプションを使用して、NAPTマッピングルールを削除します。

オプション	説明
特定のNAPTマッピングルールの削除	**configure ip nat rule delete inside ip** *inside- ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} コマンドを使用します。 `Device#configure ip nat rule delete inside ip 192.168.1.10 port 80 outside port 61080 protocol tcp`
ルールIDを使用したNAPTマッピングルールの削除	**configure ip nat entry delete** *rule-id* コマンドを使用します。 `Device# configure ip nat entry del 0` （注） **show ip nat configuration** コマンドを使用してルールIDを表示できます。
すべてのNAPTマッピングルールの削除	**configure ip nat entry delete all** コマンドを使用します。 `Device# configure ip nat entry delete all`

NAPT IP アドレスの削除

この手順では、設定されているNAT IPアドレスの削除方法について説明します。内部有線クライアントに割り当てられたゲートウェイIPv4アドレスを削除できます。または、NATの外側のインターフェイスに設定されている外部IPv4アドレスを削除できます。

（注） NAPT設定をすべて削除するには、IPアドレスとインターフェイスも削除する必要があります。

手順

次のいずれかのオプションを使用して、NAPT IPアドレスを削除します。

オプション	説明
内部有線クライアントのゲートウェイIPv4アドレスの削除	**configure ip nat address delete** コマンドを使用します。 `Device#configure ip nat address delete`

オプション	説明
外部 IPv4 アドレスの削除	**configure interface nat-outside address delete** コマンドを使用します。 `Device#configure interface nat-outside address delete`

AAA ユーザー認証

AAA ユーザー認証は、以下を実行するネットワーク管理メカニズムです。

- ユーザー認証を介してネットワークリソースへのアクセスを制御し、
- 差別化された権限レベルをユーザーに割り当て、
- ユーザー名とパスワードを AAA サーバーで一元的に管理します。

リリース 17.15.1 以降、 IW9165E WGB では AAA ベースのユーザー管理および認証がサポートされます。

AAA サーバーは、Authorization-Reply メッセージを使用して、権限レベル（0 ～ 15）を割り当てます。レベル 1（表示ユーザー）と 15（管理ユーザー）のみがサポートされています。レベル 2 ～ 14 は予約済みで、割り当てることはできません。

権限レベルを指定しないでユーザーを追加した場合、そのユーザーには WGB によって最も低い権限レベルが割り当てられます。

AAA ベースのユーザー管理および認証の機能

AAA ベースのユーザー管理および認証には、以下の機能が含まれます。

- マルチユーザーをサポート
- AAA サーバーにユーザー名とパスワードを保存
- AAA を使用したユーザーの認証
- ユーザー毎に異なる権限をサポート
- ユーザーの権限に基づいた CLI アクセス制限

（注） Cisco ルータまたはスイッチと同様に、ワークグループブリッジ（WGB）も、ユーザー名とパスワードをローカルに作成して保存できます。

AAA サーバーの設定

始める前に

- プライマリ AAA サーバーを追加する前に、セカンダリ AAA サーバー（RADIUS または TACACS+）を追加できます。プライマリ AAA サーバーが追加されると、クライアントはプライマリ AAA サーバーに接続します。
- プライマリ RADIUS サーバーとセカンダリ RADIUS サーバーの両方が設定されている場合、WGB はプライマリ RADIUS サーバーとの接続を 3 回試行してから、セカンダリ RADIUS サーバーに切り替えます。
- TACACS+ サーバーの場合、プライマリ TACACS+ サーバーとの接続は 1 回のみ試行されます。プライマリ TACACS+ サーバーが応答しない場合は、セカンダリ TACACS+ サーバーが使用されます。

（注） WGB AAA RADIUS サーバー設定コマンドは、17.15.1 リリース以降で正式にサポートされます。

イメージを 17.15.1 以降から 17.14.1 以前のリリースにダウングレードした場合、または 17.14.1 以前から 17.15.1 以降にアップグレードした場合、もともと設定されていた RADIUS サーバーポートはゼロにリセットされます。そのため、RADIUS サーバーポートの再設定が必要になります。

手順

AAA サーバー（RADIUS または TACACS+）を追加または削除します。

オプション	説明
AAA サーバーの設定	**config** {**radius**	**tacplus**} **authentication** {**primary**	**secondary**} **add** {**ipv4**	**ipv6**} *ip-address* **port** *port-number* **secret** *secret-string* コマンドを使用します。 `Device# configure radius authentication primary add ipv4 10.10.10.5 port 100 secret radiusSecret123` （注） secret-string パラメータでサポートされていない文字を使用しないでください。サポートされていない文字には、縦棒（|）、セミコロン（;）、ドル記号（$）、小なり（<）、大なり（>）、アンパサンド（&）、キャレット記号（^）、抑音アクセント（`）、バックスラッシュ（\）、改行（\r）、および二重引用符（“”）が含まれます。

オプション	説明
AAA サーバーの削除	**config** {**radius**	**tacplus**} **authentication** {**primary**	**secondary**}**delete** コマンドを使用します。 `Device# configure radius authentication primary delete`

ログインユーザーの RADIUS 認証の有効化または無効化

手順

ステップ 1 以下のいずれかのオプションを使用して、ログインユーザーの AAA RADIUS 認証を有効または無効にします。

オプション	説明
ログインユーザーの AAA RADIUS 認証の有効化	**config ap management aaa radius enable** コマンドを使用します。 `Device# config ap management aaa radius enable`
ログインユーザーの AAA RADIUS 認証の無効化	**config ap management aaa radius disable** コマンドを使用します。 `Device# config ap management aaa radius disable`

ステップ 2 （オプション）**show running-config | include aaa** コマンドを使用して、AAA サーバー（RADIUS または TACACS+）の設定を確認します。

```
Device# show running-config | include aaa AAA server configuration:- ================================
 Status: Enabled AAA server type : radius Primary RADIUS IP address : 192.0.2.0 Primary RADIUS port
 : 1812 . . .
```

ログインユーザーの TACACS+ 認証の有効化または無効化

手順

ステップ 1 以下のいずれかのオプションを使用して、ログインユーザーの AAA RADIUS 認証を有効または無効にします。

オプション	説明
ログインユーザーの AAA TACACS+ 認証の有効化	**config ap management aaa tacplus enable** コマンドを使用します。 `Device# config ap management aaa tacplus enable`
ログインユーザーの AAA TACACS+ 認証の無効化	**config ap management aaa tacplus disable** コマンドを使用します。 `Device# config ap management aaa tacplus disable`

ステップ 2 （オプション）**show running-config | include aaa** コマンドを使用して、AAA サーバー（TACACS+）の設定を確認します。

```
Device# show running-config | include aaa AAA server configuration:- ================================
 Status: Enabled AAA server type : tacplus Primary TACPLUS IP address : 192.0.2.0 Primary TACPLUS
port : 49 . . .
```

AAA 認証の設定例

AAA RADIUS 認証が有効になっている場合に show running-config コマンドを使用すると、次の例のような出力が生成されます。

```
Device# show running-config AAA server configuration:- ================================
Status: Enabled AAA server type : radius Primary RADIUS IP address : 192.0.2.0 Primary
RADIUS port : 1812 . . .
```

AAA TACACS+ 認証が有効になっている場合に show running-config コマンドを使用すると、次の例のような出力が生成されます。

```
Device# show running-config AAA server configuration:- ================================
Status: Enabled AAA server type : tacplus Primary TACPLUS IP address : 192.0.2.0 Primary
 TACPLUS port : 49 . . .
```

検証と監視

WGB および uWGB の設定の確認

WGB および uWGB に関連する show 設定を確認するには、これらのタスクを実行します。

手順

ステップ 1 いずれかのオプションを使用して、AP が WGB モードか uWGB モードかを確認します。

オプション	説明
WGB	**show run** コマンドを使用します。 `Device#show run AP Name : APFC58.9A15.C808 AP Mode : WorkGroupBridge CDP State : Enabled Watchdog monitoring : Enabled SSH State : Disabled AP Username : admin Session Timeout : 300 Radio and WLAN-Profile mapping:- ========== Radio ID Radio Mode SSID-Profile SSID Authentication ---------- ---------- 1 WGB myssid demo OPEN Radio configurations:- ========== Radio Id : NA Admin state : NA Mode : NA Radio Id : 1 Admin state : DISABLED Mode : WGB Dot11 type : 11ax Radio Id : NA Admin state : NA Mode : NA`
uWGB	**show run** コマンドを使用します。 `Device#show run AP Name : APFC58.9A15.C808 AP Mode : WorkGroupBridge CDP State : Enabled Watchdog monitoring : Enabled SSH State : Disabled AP Username : admin Session Timeout : 300 Radio and WLAN-Profile mapping:- ========== Radio ID Radio Mode SSID-Profile SSID Authentication ---------- ---------- 1 UWGB myssid demo OPEN Radio configurations:- ========== Radio Id : NA Admin state : NA Mode : NA Radio Id : 1 Admin state : DISABLED Mode : UWGB Uclient mac : 0009.0001.0001 Current state : WGB UClient timeout : 0 Sec Dot11 type : 11ax Radio Id : NA Admin state : NA Mode : NA`

ステップ 2 いずれかのオプションを使用して、WGB または uWGB に関連付けられているワイヤレスクライアントに関する情報を確認します。

オプション	説明
WGB	**show wgb dot11 associations** コマンドを使用します。 `Device#show wgb dot11 associations Uplink Radio ID : 1 Uplink Radio MAC : 00:99:9A:15:B4:91 SSID Name : roam-m44-open Parent AP Name : APFC58.9A15.C964 Parent AP MAC : 00:99:9A:15:DE:4C Uplink State : CONNECTED Auth Type : OPEN Dot11 type : 11ax Channel : 100 Bandwidth : 20 MHz Current Datarate (Tx/Rx) : 86/86 Mbps Max Datarate : 143 Mbps RSSI : 53 IP : 192.168.1.101/24 Default Gateway : 192.168.1.1 IPV6 : ::/128 Assoc timeout : 100 Msec Auth timeout : 100 Msec Dhcp timeout : 60 Sec`
uWGB	**show wgb dot11 associations** コマンドを使用します。 `Device#show wgb dot11 associations Uplink Radio ID : 1 Uplink Radio MAC : 00:09:00:01:00:01 SSID Name : roam-m44-open Parent AP MAC : FC:58:9A:15:DE:4C Uplink State : CONNECTED Auth Type : OPEN Uclient mac : 00:09:00:01:00:01 Current state : UWGB Uclient timeout : 60 Sec Dot11 type : 11ax Channel : 36 Bandwidth : 20 MHz Current Datarate (Tx/Rx) : 77/0 Mbps Max Datarate : 143 Mbps RSSI : 60 IP : 0.0.0.0 IPV6 : ::/128 Assoc timeout : 100 Msec Auth timeout : 100 Msec Dhcp timeout : 60 Sec`

Syslog

Syslogは、保存および分析のためにイベントデータログを一元化された場所に送信するプロトコルのカテゴリです。Syslogは、イベントメッセージをキャプチャすることによるネットワークデバイスの監視と障害対応に広く使用されています。Syslogという用語は、このプロトコル自体を指す場合や、このプロトコルを導入するシステムを指す場合もあります。

- プロトコルタイプ：Syslogは、システムイベントのロギングに一般的に使用される標準化されたプロトコルです。
- トランスポートプロトコル：現在、Syslog はデータ伝送で UDP モードのみをサポートしています。
- デバッグログの収集：WGB で debug コマンドが有効になっている場合、デバッグログが収集されて Syslog サーバーに送信されます。
- ログ分類：WGB から Syslog サーバーに送信されるログは、「kernel facility」に分類され、「warning level」で記録されます。

WGB syslog の有効化または無効化

ワークグループブリッジ（WGB）で syslog 機能を設定するには、このタスクを実行します。これにより、特定のホストへのロギングを有効または無効にして、適切な監視およびデバッグを確保することができます。

手順

ステップ 1 以下のいずれかのオプションを使用して、ログインユーザーの AAA RADIUS 認証を有効または無効にします。

オプション	説明
WGB syslog の有効化	**logging host enable** *server_ip* **UDP** コマンド使用します。 `Device# logging host enable 192.168.1.200 udp`
WGB syslog の有効化	**logging host disable** *server_ip* **UDP** コマンドを使用します。 `Device# logging host disable 192.168.1.200 UDP`

ステップ 2 （オプション）**show running-config** コマンドを使用して、現在の syslog 設定を表示します。

```
Device# show running-config
```

無線機統計コマンド

debug wgb dot11 rate コマンドでは、ネゴシエートされたデータレートに関連したデバッグ情報が表示されます。アクセスポイントと通信するときに WGB がデータレートを選択して使用する方法を示すことにより、接続、性能、またはローミングの問題のトラブルシュートに役立ちます。

```
Device# debug wgb dot11 rate [*03/13/2023 18:00:08.7814] MAC Tx-Pkts Rx-Pkts Tx-Rate(Mbps)
 Rx-Rate(Mbps) RSSI SNR Tx-Retries [*03/13/2023 18:00:08.7814] FC:58:9A:17:C2:51 0 0
HE-20,2SS,MCS6,GI0.8 (154) HE-20,3SS,MCS4,GI0.8 (154) -30 62 0 [*03/13/2023 18:00:09.7818]
 FC:58:9A:17:C2:51 0 0 HE-20,2SS,MCS6,GI0.8 (154) HE-20,3SS,MCS4,GI0.8 (154) -30 62 0
```

この例では、FC:58:9A:17:C2:51 が親 AP の無線機 MAC です。

show interfaces dot11Radio *slot-id***statistics** コマンドでは、ワイヤレス無線インターフェイスの詳細な統計が表示されます。送受信パケット、エラー、再試行、信号品質、その他の性能指標などの情報が提供されます。この統計は、無線インターフェイスの状態の監視、接続の問題の特定、ワイヤレス性能の障害対応に役立ちます。

```
Device# show interfaces dot11Radio 1 statistics Dot11Radio Statistics: DOT11 Statistics
 (Cumulative Total/Last 5 Seconds): RECEIVER TRANSMITTER Host Rx K Bytes: 965570/0 Host
 Tx K Bytes: 1611903/0 Unicasts Rx: 379274/0 Unicasts Tx: 2688665/0 Broadcasts Rx:
3166311/0 Broadcasts Tx: 0/0 Beacons Rx: 722130099/1631 Beacons Tx: 367240960/784 Probes
 Rx: 588627347/2224 Probes Tx: 78934926/80 Multicasts Rx: 3231513/0 Multicasts Tx: 53355/0
 Mgmt Packets Rx: 764747086/1769 Mgmt Packets Tx: 446292853/864 Ctrl Frames Rx: 7316214/5
 Ctrl Frames Tx: 0/0 RTS received: 0/0 RTS transmitted: 0/0 Duplicate frames: 0/0 CTS
not received: 0/0 MIC errors: 0/0 WEP errors: 2279546/0 FCS errors: 0/0 Retries: 896973/0
 Key Index errors: 0/0 Tx Failures: 8871/0 Tx Drops: 0/0 Rate Statistics for Radio::
[Legacy]: 6 Mbps: Rx Packets: 159053/0 Tx Packets: 88650/0 Tx Retries: 2382/0 9 Mbps:
Rx Packets: 43/0 Tx Packets: 23/0 Tx Retries: 71/0 12 Mbps: Rx Packets: 1/0 Tx Packets:
 119/0 Tx Retries: 185/0 18 Mbps: Rx Packets: 0/0 Tx Packets: 5/0 Tx Retries: 134/0 24
Mbps: Rx Packets: 235/0 Tx Packets: 20993/0 Tx Retries: 5048/0 36 Mbps: Rx Packets: 0/0
 Tx Packets: 781/0 Tx Retries: 227/0 54 Mbps: Rx Packets: 133/0 Tx Packets: 9347/0 Tx
Retries: 1792/0 [SU]: M0: Rx Packets: 7/0 Tx Packets: 0/0 Tx Retries: 6/0 M1: Rx Packets:
 1615/0 Tx Packets: 35035/0 Tx Retries: 3751/0 M2: Rx Packets: 15277/0 Tx Packets:
133738/0 Tx Retries: 22654/0 M3: Rx Packets: 10232/0 Tx Packets: 1580/0 Tx Retries:
21271/0 M4: Rx Packets: 218143/0 Tx Packets: 190408/0 Tx Retries: 36444/0 M5: Rx Packets:
 399283/0 Tx Packets: 542491/0 Tx Retries: 164048/0 M6: Rx Packets: 3136519/0 Tx Packets:
 821537/0 Tx Retries: 329003/0 M7: Rx Packets: 1171128/0 Tx Packets: 303414/0 Tx Retries:
 154014/0 Beacons missed: 0-30s 31-60s 61-90s 90s+ 2 0 0 0
```

show wgb dot11 uplink latency コマンドでは、アクセスポイント（AP）へのワークグループブリッジ（WGB）アップリンク接続の遅延統計が表示されます。フレームが WGB から AP に通過するのにかかる時間を測定し、ワイヤレスリンクの性能と潜在的な遅延の問題についての状況を把握するのに役立ちます。

```
AP# show wgb dot11 uplink latency Latency Group Total Packets Total Latency Excellent(0-8)
 Very Good(8-16) Good (16-32 ms) Medium (32-64ms) Poor (64-256 ms) Very Poor (256+ ms)
AC_BK 0 0 0 0 0 0 0 0 AC_BE 1840 4243793 1809 10 14 7 0 0 AC_VI 0 0 0 0 0 0 0 0 AC_VO
24 54134 24 0 0 0 0 0
```

show wgb dot11 uplink コマンドでは、アクセスポイント（AP）へのワークグループブリッジ（WGB）アップリンクに関する情報が表示されます。関連する SSID、BSSID、チャンネル、信号強度、データレート、認証タイプ、およびアップリンク接続の全体的なステータスなどの詳細が表示されます。この情報は、接続の確認と、AP への WGB のワイヤレスリンクの監視に役立ちます。

```
AP# show wgb dot11 uplink HE Rates: 1SS:M0-11 2SS:M0-11 Additional info for client
8C:84:42:92:FF:CF RSSI: -24 PS : Legacy (Awake) Tx Rate: 278730 Kbps Rx Rate: 410220
Kbps VHT_TXMAP: 65530 CCX Ver: 5 Rx Key-Index Errs: 0 mac intf TxData TxUC TxBytes TxFail
 TxDcrd TxCumRetries MultiRetries MaxRetriesFail RxData RxBytes RxErr TxRt(Mbps) RxRt(Mbps)
 LER PER stats_ago 8C:84:42:92:FF:CF wbridge1 1341 1341 184032 0 0 543 96 0 317 33523 0
 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8 (458) 27272 0 1.370000 Per TID packet
statistics for client 8C:84:42:92:FF:CF Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last
5 s) 0 35 1314 0 8 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 182 24 1 0 7 3 3
 0 0 Rate Statistics: Rate-Index Rx-Pkts Tx-Pkts Tx-Retries 0 99 3 0 4 1 1 9 5 21 39 35
 6 31 185 64 7 26 124 68 8 28 293 82 9 77 401 151 10 32 140 97 11 2 156 37
```

イベントロギングの設定

WGB フィールド展開の場合、イベントロギングは、WGB の状態変化や送受信されたパケットなどの有用な情報を収集します。この情報により、特にローミング中の問題の分析に役立つログ履歴が提供されます。

probe、auth、assoc、EAP、dhcp、icmp、arp などのパケットタイプに対して WGB トレースフィルタを設定できます。

製品は、次の 4 種類のイベントをサポートしています。

- Basic event：WGB の基本レベルの情報メッセージのほとんどをカバーします。
- Detail event：基本イベントと追加のデバッグレベルメッセージをカバーします。
- Trace event：有効になっている場合、WGB トレースイベントを記録します。
- All event：トレースイベントと詳細イベントをバンドルします。

ログのフォーマットは次のとおりです。[*timestamp* | *module* | *level* | *event log string*]

（注） UIW リリース 17.17.1 以降では、「リモートサーバーの設定」手順で説明されているコマンドを使用して、より包括的な診断情報を取得することを推奨します。

手順

ステップ 1 **config wgb event trace** {**enable** | **disable**}コマンドを使用して、WGB トレースを有効または無効にします。

```
Device# config wgb event trace enable
```

ステップ 2 （オプション）**show wgb event** [**basic** | **detail** | **trace** | **all**] コマンドを使用して、イベントログメッセージをメモリに手動でダンプし、WGB ロギングを表示します。

```
Device# show wgb event all [*08/16/2023 08:18:25.167578] UP_EVT:4 R1 IFC:58:9A:17:B3:E7] parent_rssi:
 -42 threshold: -70 [*08/16/2023 08:18:25.329223] UP_EVT:4 R1 State CONNECTED to SCAN_START
[*08/16/2023 08:18:25.329539] UP_EVT:4 R1 State SCAN_START to STOPPED [*08/16/2023 08:18:25.330002]
 UP_DRV:1 R1 WGB UPLINK mode stopped [*08/16/2023 08:18:25.629405] UP_DRV:1 R1 Delete client
FC:58:9A:17:B3:E7 [*08/16/2023 08:18:25.736718] UP_CFG:8 R1 configured for standard: 7 [*08/16/2023
 08:18:25.989936] UP_CFG:4 R1 band 1 current power level: 1 [*08/16/2023 08:18:25.996692] UP_CFG:4
 R1 band 1 set tx power level: 1 [*08/16/2023 08:18:26.003904] UP_DRV:1 R1 WGB uplink mode started
 [*08/16/2023 08:18:26.872086] UP_EVT:4 Reset aux scan [*08/16/2023 08:18:26.872096] UP_EVT:4 Pause
 aux scan on slot 2 [*08/16/2023 08:18:26.872100] SC_MST:4 R2 reset uplink scan state to idle
[*08/16/2023 08:18:26.872104] UP_EVT:4 Aux bring down vap - scan [*08/16/2023 08:18:26.872123]
UP_EVT:4 Aux bring up vap - serv [*08/16/2023 08:18:26.872514] UP_EVT:4 R1 State STOPPED to SCAN_START
 [*08/16/2023 08:18:26.8727091 SC_MST:4 R1 Uplink Scan Started. [*08/16/2023 08:18:26.884054] UP_EVT:8
 R1 CH event 149
```

show wgb event コマンドは、コンソールに出力が表示されるまでに時間がかかる場合があります。Ctrl+C を使用して出力を中断しても、メモリへのログダンプには影響しません。

ステップ 3 （オプション）**clear wgb event** [**basic** | **detail** | **trace** | **all**] コマンドを使用して、メモリ内の WGB イベントを消去します。

```
Device# clear wgb event all
```

ステップ 4 （オプション）**copy event-logging flash** コマンドを使用して、すべてのイベントログを WGB フラッシュに保存します。

```
Device# copy event-logging flash
```

パッケージファイルには、4つの個別のログファイル（異なるログレベルごとのファイル）が含まれます。

ステップ 5 （オプション）**copy event-logging upload**[**tftp** | **sftp** | **scp**] ://*ip-address* [*dir*][*/filename.tar.gz*] コマンドを使用して、イベントログをリモートサーバーに保存します。

```
Device# copy event-logging upload tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz
 Starting upload of WGB config tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz
... It may take a few seconds. If longer, please cancel command, check network and try again.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! 100.0% Config upload
completed.
```

リモートサーバーの設定

このタスクでは、デバイスでのログ転送設定を指定します。ログ転送設定は、転送プロトコル（TFTP または SFTP）、認証ログイン情報（SFTP の場合）、リモートサーバーの IP アドレス、およびオプションのサーバーパスを定義します。このセットアップにより、保管、監視、またはトラブルシューティングのために、確実に、イベントログとシステムログがリモートサーバーにセキュアにアップロードされます。

手順

ステップ 1 **transfer upload mode** {**delete** | **sftp** | **tftp**} コマンドを使用して、ログ転送のプロトコルを選択します。

```
Device# transfer upload mode tftp
```

ステップ 2 **transfer upload credential add** *username* **password** *password* コマンドを使用して、ユーザー名とパスワードを設定します。

```
Device# transfer upload credential add Cisco password Cisco123
```

ステップ 3 **transfer upload server-ip add** *remote-server-ip* コマンドを使用して、リモートサーバーの IP アドレスを設定します。

```
Device# transfer upload server-ip add 192.168.71.11
```

ステップ 4 （オプション）**transfer upload server-ip add** *remote-server-ip* **path** *remote-server-path* コマンドを使用して、リモートサーバーのパスを設定します。

```
Device# transfer upload server-ip add 192.168.71.11 path /upload/wgb
```

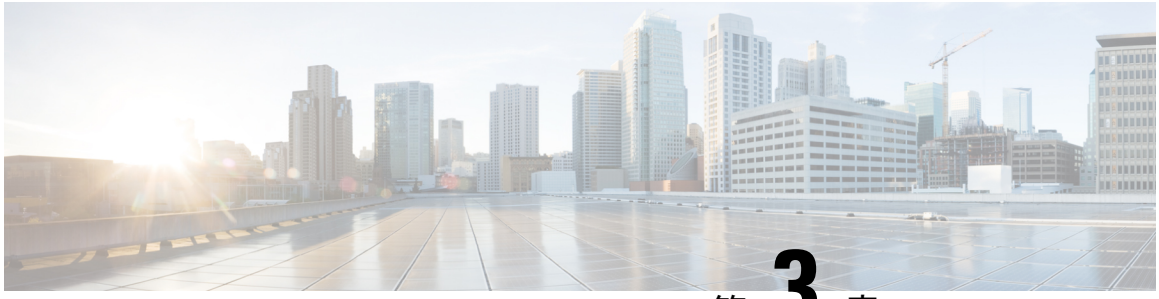
これらの静的設定は持続的で、デバイスのリロード後も引き続き有効です。

ステップ 5 **transfer upload start** コマンドを使用して、イベントログを収集し、リモートサーバーに転送します。

```
Device# transfer upload start
```

リモートサーバーが設定されると、デバイスは次のタイプのデータを収集および転送します。

- トラブルシューティングを支援するためのコアファイル。
- システムのイベントとアクティビティを監視するための syslog ファイル。
- 設定をバックアップするための WGB または uWGB 実行設定。
- 潜在的な接続の問題を特定するための無線機のリセット履歴。
- システム性能とインシデントを追跡するためのイベントロギングデータ。



第 3 章

Control And Provisioning of Wireless Access Points（CAPWAP）

概要

CAPWAP は、ワイヤレス LAN コントローラが複数の AP とワイヤレス LAN コントローラ（WLC）を管理し、セキュア通信トンネルを介してコントロールプレーンとデータプレーン情報を交換できるようにする IEEE 標準規格プロトコルです。

CAPWAP はレイヤ 3 でのみ動作し、AP と WLC の両方で IP アドレスの提示を必要とします。CAPWAP は、UDP ポート 5246 および 5247 で、それぞれ IPv4 および IPv6 用のトンネルを確立します。Datagram Transport Layer Security（DTLS）暗号化により、一層セキュリティが強化されます。

DTLS は、AP と WLC 間のセキュリティを担保するプロトコルとして機能し、通信の暗号化を促進することで中間者攻撃による盗聴や改ざんを防ぎます。

デフォルトでは、DTLS は CAPWAP の制御チャンネルを保護し、AP と WLC 間のすべての CAPWAP 管理トラフィックおよび制御トラフィックを暗号化します。

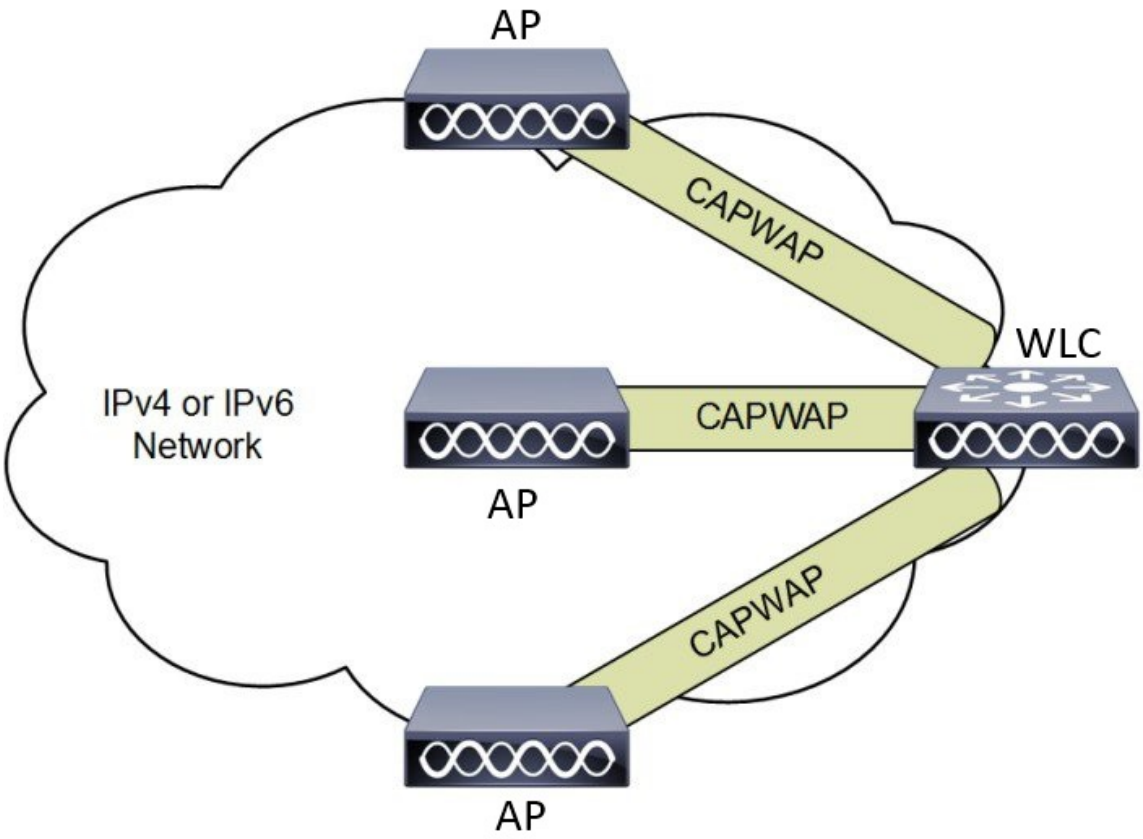
データチャンネルはデフォルトでは無効であり、AP と WLC 間を移動するクライアントデータは暗号化されません。CAPWAP データ暗号化を有効にするかどうかは任意であり、AP でアクティブ化する前に WLC に DTLS ライセンスをインストールする必要があります。

AP が DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンのみ有効となり、データプレーンの DTLS セッションは確立されません。

AP がデータ DTLS をサポートしている場合は、コントローラから新しい設定を受信した後にデータ DTLS を有効にします。AP は、ポート 5247 で DTLS ハンドシェイクを実行し、ハンドシェイクが成功すると DTLS セッションを確立します。すべてのデータトラフィック（AP からコントローラ、およびコントローラから AP）が暗号化されます。

CAPWAP によって、管理者はワイヤレスネットワーク全体を中央で一元的に管理できます。IW9165E は、コントローラとネットワーク上の他の AP 間の通信に Internet Engineering Task Force（IETF）標準規格の CAPWAP を使用します。

図 *7: WLC* に接続された *CAPWAP AP*



Lightweight アクセスポイントでの証明書のプロビジョニング

次の段階では、Lightweightアクセスポイント（LAP）での証明書のプロビジョニングについて説明します。

1. **証明書要求**：LAP は、署名された X.509 証明書を取得するためにコントローラに証明書要求を送信します。
2. **CA プロキシ**：コントローラは、CA プロキシとして機能して、CA による証明書要求の署名を容易にします。

3. **証明書のインストールと再起動**：LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動的に再起動します。
4. **参加要求**：再起動後、LAP は、参加要求の一部として LSC デバイス証明書をコントローラに送信します。
5. **参加応答と検証**：参加応答の一部として、コントローラは、新しいデバイス証明書を送信し、新しい CA ルート証明書を使用して受信 LAP 証明書を検証します。

whats_next

次の実施手順

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニング機能を使用します。

AP の CAPWAP 接続について

CAPWAP を有効にすると、最初の機能として、ディスカバリフェーズが開始されます。ワイヤレス AP は、ディスカバリ要求メッセージを送信してコントローラを検索します。ディスカバリ要求を受信すると、コントローラはディスカバリ応答を返します。この時点で、この2台のデバイスの間に、CAPWAP 制御メッセージとデータメッセージを交換するための Datagram Transport Layer Security（DTLS）プロトコルを使ったセキュアな接続が確立されます。

AP は CAPWAP ディスカバリメカニズムを使用して、コントローラに CAPWAP 接続要求を送信します。コントローラは AP に CAPWAP 接続応答を送信し、AP がコントローラに接続できるようにします。APがワイヤレスコントローラに接続すると、ワイヤレスコントローラによって AP の設定、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

CAPWAP には、制御とデータの 2 つのチャンネルがあります。AP は制御チャンネルを使用して、設定メッセージの送信、イメージとクライアント鍵のダウンロード、またはコンテキストの受信を行います。現在の実装では、制御チャンネルには単一のウィンドウが設けられます。AP は、コントローラから送信されたすべてのメッセージを単一のウィンドウ内で確認する必要があります。AP は、前の制御パケットの確認応答が終わるまで、次の制御パケットを送信しません。

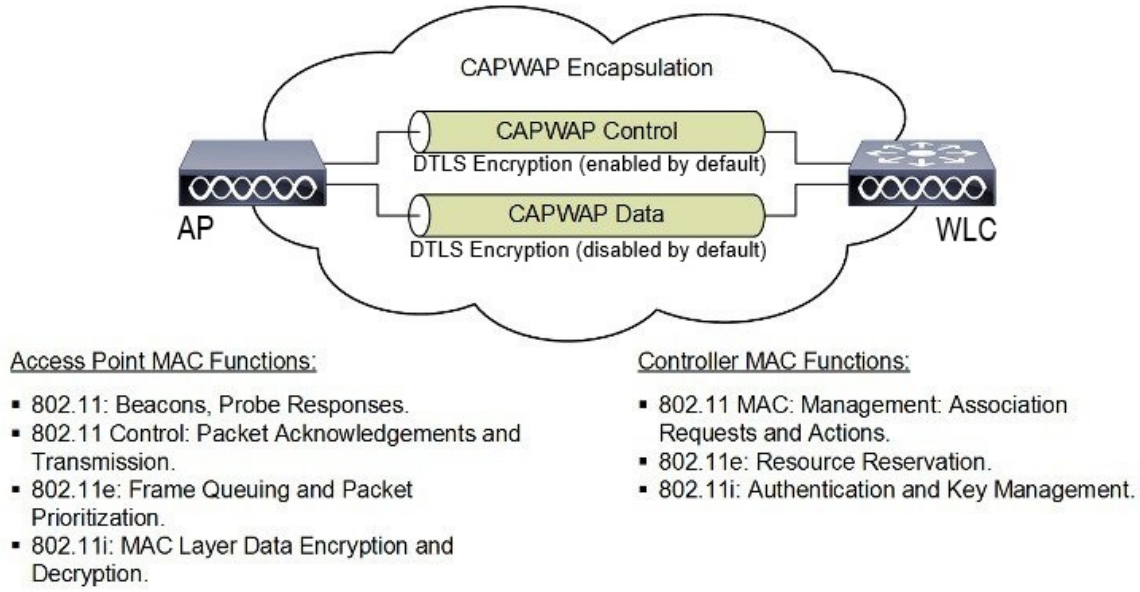
CAPWAP データチャンネルは、AP と WLC 間のユーザーデータトラフィックのカプセル化とトンネリングを担います。これにより、ユーザーデータフローの中央管理が可能になり、WLC はポリシーを適用し、Quality of Service（QoS）を適用し、ワイヤレスネットワーク全体で一貫したセキュリティ対策を確保できます。ユーザーデータは CAPWAP フレーム内でカプセル化され、AP と WLC 間で転送できるようになります。

IETF に従い、CAPWAP は 2 つの動作モードをサポートしています。

- **Split Media Access Control（MAC）**：CAPWAP の主要なコンポーネントの 1 つに、スプリットMAC という概念があります。これは、802.11 プロトコルでの動作の一部を CAPWAP AP が管理し、残りの部分を WLC が管理するというものです。

スプリット MAC モードでは、CAPWAP プロトコルがすべてのレイヤ 2 ワイヤレスデータおよび管理フレームをカプセル化し、これらのデータやフレームが WLC と AP 間で交換されます。

図 *8 :* スプリット *MAC* アーキテクチャ



- **Local MAC**：ローカル MAC モードでは、データフレームをイーサネットフレームとしてローカルにブリッジまたはトンネリングできます。

  ローカル MAC では、すべてのワイヤレス MAC 機能が AP で実行されます。管理フレームおよび制御フレームの処理を含む完全な 802.11 MAC 機能が AP に常駐します。

どちらのモードでも、AP はレイヤ 2 ワイヤレス管理フレームをローカルで処理してから、コントローラに転送します。

リセットボタンの設定

IW9165E では、（ブートローダがリセット信号を受信した後に）LED が赤色の点滅に変わると、次のリセットアクションが実行されます。デバイスの電源を入れる前に、必ずデバイスのリセットボタンを押します。

- 完全にリセットするには、ボタンを長押し（20 秒未満）します。
- 工場出荷時の状態まで完全にリセットする（FIPS フラグを解除する）には、ボタンを長押し（20 秒以上 60 秒未満）します。

CAPWAP モードでのイーサネットポートの使用状況

Catalyst IW9165E では、2 つの 2x2 Multiple Input and Multiple Output（MIMO）と 2 つのイーサネットポート（2.5G mGig および 1G）により、最大 3.6 Gbps の物理データレートがサポートされています。

Catalyst IW9165E には、以下の内部ポートマッピングルールがあります。

- Wired0：802.3af、802.3at、802.3bt PoE をサポートする 1 つの mGig（2.5 Gbps）イーサネットポート。

（注） AP のローカルモードや FlexConnect モードでは、wired0 ポートは CAPWAP アップリンクポートとして使用されます。

- Wired1：1Gig イーサネット LAN ポート。

（注） 17.14.1 リリース以降、RLAN 機能は wired1 ポートではサポートされません。

屋内展開の設定

IW9165E は、規制ドメイン -B（米国）、-E（EU）、-A（カナダ）、-Z（オーストラリア、ニュージーランド）の屋内および屋外展開をサポートします。

デフォルトでは、AP の展開モードは屋内です。

-B ドメインでは屋外と屋内の周波数は同じです。

表 *8*：無線機の *6G* 出力モードの対応表

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	はい

（注） 屋外モードは屋内で使用できますが、5150 ～ 5350 MHz のチャンネルは -E の国々では屋内のみであるため、屋内モードを屋外で使用することはできません。

ワイヤレスコントローラでの AP 展開モードの設定方法については、『Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア コンフィギュレーション ガイド』を参照してください。

このコマンドは、AP の再起動を開始します。再起動後に AP がワイヤレスコントローラに登録されたら、対応する国番号を AP に割り当てる必要があります。

屋内展開の確認

WLC で屋内展開が有効になっているかどうかを確認します。

#show ap name <AP_Name> config general | inc Indoor コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor AP Indoor Mode : Enabled
```

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor AP Indoor Mode : Disabled
```

AP の屋内展開のステータスを確認するには、**show controllers Dot11Radio [1|2]** コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します：

```
Device#show controllers Dot11Radio [1|2] … Radio Info Summary: ======================
 Radio: 5.0GHz Carrier Set: (-Ei) ( GB ) Base radio MAC: FC:58:9A:15:B7:C0 Supported
 Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

（注） コマンド出力の「-Ei」は、屋内モードが有効になっていることを示します。

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します：

```
Device#show controllers Dot11Radio [1|2] … Radio Info Summary: ======================
Radio: 5.0GHz Carrier Set: (-E) ( GB ) Base radio MAC: FC:58:9A:15:B7:C0 Supported
Channels: 100 104 108 112 116 120 124 128 132 136 140
```

（注） コマンド出力の「-E」は、屋内モードが無効になっていることを示します。

CLI 出力には、サポートされるチャンネルも表示されます。

AP 無線スロット

Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、Cisco Catalyst IW9165E では、2x2 5GHz Wi-Fi 専用無線機と 5 GHz および 6 GHz のデュアルバンド（XOR）2x2 無線機が使用できます。

Catalyst IW9165E には、5G バンドと 6G バンドを切り替えるオプションがあります。5G バンドと 6G バンドを切り替えるには、次の CLI コマンドを使用します。

```
ap name <ap-name> dot11 dual-band band 6ghz/5ghz
```

（注） デフォルトでは、管理状態は無効です。

スロット 2 の XOR 無線機は 5G に固定されています。

表 *9 : AP Wi-Fi* 無線機アーキテクチャモード

モード	**5 GHz** **スロット 1**	**5/6 GHz** **スロット 2**
5G + 5G	5GHz 2x2:2SS（20/40/80 MHz）	5G 2x2:2SS（20/40/80/160 MHz）
5G + 6G	5GHz 2x2:2SS（20/40/80 MHz）	6G 2x2:2SS（20/40/80/160 MHz）

固定ドメインと国コードのサポート

ROW 規制ドメインにより、特定のドメインがマッピングされていないすべての国コードの製造プロセスのドメイン管理が簡素化されます。この項では、Catalyst IW9165E アクセスポイントの固定ドメインと国コードのサポートについて説明します。

サポートされている固定ドメイン

ドメイン	国番号
A	CA（カナダ）
B	US（米国）

ドメイン	国番号
E	

ドメイン	国番号
	• AT（オーストラリア） • AT（オーストラリア） • BE（ベルギー） • BG（ブルガリア） • HR（クロアチア） • CY（キプロス） • CZ（チェコ共和国） • DK（デンマーク） • EE（エストニア） • FI（フィンランド） • FR（フランス） • DE（ドイツ） • GR（ギリシャ） • HU（ハンガリー） • IS（アイスランド） • IE（アイルランド） • IT（イタリア） • LV（ラトビア） • LI（リヒテンシュタイン） • LT（リトアニア） • LU（ルクセンブルク） • MT（マルタ） • NL（オランダ） • NO（ノルウェー） • PL（ポーランド） • PT（ポルトガル） • RO（ルーマニア） • SK（スロバキア共和国）

ドメイン	国番号
	• SI（スロベニア） • ES（スペイン） • SE（スウェーデン） • CH（スイス）
F	ID（インドネシア）
Q	JP（日本）
Z	• AU（オーストラリア） • NZ（ニュージーランド）

Catalyst IW9165 でサポートされている国コード（ROW）

ドメイン	国番号
ROW	• CL（チリ） • KR（韓国） • GB（英国） • VN（ベトナム）

使用している AP の各国における認可状況については、お客様にご確認いただく必要があります。認可状況および特定の国に関連する規制ドメインの確認方法。詳細については、「Cisco Product Approval Status」[英語] を参照してください。

無線アンテナ配置の設定

Catalyst IW9165E は、RP-SMA（f）コネクタで 4 つの外部アンテナをサポートしています。無線機 1 はアンテナポート 1 および 2 に接続します。無線機 2 はアンテナポート 3 および 4 に接続します。

IW9165E は、6G バンドの Self Identifiable Antenna（SIA）アンテナとの互換性があります。アンテナポート 1 および 3 では、SIA アンテナをサポートできます。アンテナの詳細については、『Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント ハードウェア設置ガイド』を参照してください。

（注） 初めて SIA アンテナを取り付けた後は、電源を一度切って入れ直す必要があります。

SIA は、アンテナ IW-ANT-OMV-2567-N および IW-ANT-OMH-2567-N のみをサポートします。

表 *10* : アンテナ利得（*dBm*）

5 GHz スロット 1	5 GHz スロット 2	6 GHz スロット 2
3 4 7 8 10 13 15	3 4 7 8 10 13 15	7

以下の項で、SIA テストを確認するための CLI コマンドについて説明します。

コントローラの SIA ステータスを確認するには、**show ap config slots <AP>** コマンドを実行します。

```
Device#show ap config slot ap_name

show ap config slots AP2CF8.9B1C.CE78 Cisco AP Name : AP4C42.1E51.A144 Attributes for
Slot 2 SIA Status : Present(RPTNC) SIA Product ID : IW-ANT-OMV-2567-N
```

6G 標準出力モードの AFC サポート

Cisco Catalyst IW9165E は、自動周波数調整（AFC）6 GHz 標準出力モードをサポートします。標準出力 AP がシステムに接続されます。標準出力を有効にする前に、AP は AFC システムから使用可能な周波数と各周波数範囲の出力を取得する必要があります。

AFC システムは、規制機関（米国の場合は FCC）から提供される情報に基づいて、使用可能な周波数と最大許容出力を計算します。応答がコントローラに返送され、AFC システムから返された許可チャンネルリストに基づいて標準出力チャンネルが AP に割り当てられます。

標準出力 AP は、AFC サービスを通じて調整を行います。AFC は情報にアクセスし、AP の地理位置情報とアンテナの特性に加え、AP の干渉半径をモデル化したトポグラフィック伝達マップを作成します。このマップを使用することで、最大送信電力を割り当て、チャンネル設定を調整または設定して干渉を回避できます。

表 *11* : 無線機の *6 GHz* 出力モードの対応

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	はい

送信電力の実効等方放射電力（EIRP）は最大 36 dB に制限され、 AFC サービスを通じて AP を調整する必要があります。これらの AP は、-B（米国）ドメインでは、UNII-5（5.925 ～ 6.425 GHz）および UNII-7（6.525 ～ 7.125 GHz）での運用が許可されます。

表 *12* : *6 GHz* 目標出力

経路ごとの最大伝導出力（SP/AFC）		アンテナ利得	Tx x Rx チェーン	最大 EIRP（SP/AFC）
20 ～ 80Mhz	160Mhz			
17 dBm	17 dBm	7 dBi	2 X 2	27 dBm

AP の AFC ステータスの確認

AP の AFC 要求および応答データを確認するには、**show rrm afc** コマンドを実行します。

```
Device#show rrm afc Location Type: 1 Deployment Type: 2 Height: 129 Uncertainty: 5 Height
 Type: 0 Request Status: 5 Request Status Timestamp: 2023-08-31T06:20:17Z Request Id
Sent: 5546388983266789933 Ellipse 1: longitude: -121.935066 latitude: 37.512830 major
axis: 43 minor axis: 9 orientation: 36.818100 AFC Response Request ID: 5546388983266789933
 AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

現在稼働中の出力モードを確認するには、**show controllers dot11Radio 2 | i Radio** コマンドを実行します。

```
Device#show controllers dot11Radio 2 | i Radio Dot11Radio2 Link encap:Ethernet HWaddr
24:16:1B:F8:06:C0 Radio Info Summary: Radio: 6.0GHz (SP)
```

GNSS のサポート

IW9165E では、全地球航法衛星システム（GNSS）がサポートされます。AP は、屋外環境に展開されたデバイスの GPS 情報を追跡し、ワイヤレスコントローラに GNSS 情報を送信します。

AP の GNSS 情報を表示するには、次のコマンドを使用します。

```
ap# show gnss info
```

AP の GPS 位置情報を表示するには、次のコマンドを使用します。

```
controller# show ap geolocation summary
controller# show ap name <Cisco AP> geolocation detail
```

アンテナ切断検知について

アクセスポイント（AP）の送信機と受信機に複数のアンテナがあると、性能と信頼性が向上します。複数のアンテナによって、受信機側でより強い信号を選択するか、個々の信号を組み合わせることで受信状態が改善します。したがって、障害のあるアンテナやアンテナの物理的な破損を検出することは、AP の信頼性を確保する上で重要です。

アンテナの切断検知機能は、受信機のアンテナ間における信号強度の差分に基づきます。この差分が一定期間に定義された制限を超えると、そのアンテナは問題があると見なされます。

設定した検知期間ごとに、AP はアンテナの状態を伝える Inter-Access Point Protocol（IAPP）メッセージを送信します。このメッセージは、問題が検知された場合に一度だけ送信され、コントローラ トラップ メッセージ、SNMP トラップ、およびコントローラデバッグログに表示されます。

設定ワークフロー

1. AP を設定します。
2. AP プロファイルを設定します。

3. AP プロファイルで機能を有効にします。
4. 機能のパラメータを設定します。
5. 設定を確認します。

ワイヤレスコントローラでのアンテナ切断検知の設定方法について詳しくは、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』を参照してください。

アンテナ切断検知の確認

AP のアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Conroller#sh ap name AP4C42.1E51.A144 config general Cisco AP Name : AP4C42.1E51.A144
 ================================================= Cisco AP Identifier : 8c84.4292.f840
 Country Code : Multiple Countries : US,CN,GB,HK,DE,IN,CZ,NZ Regulatory Domain Allowed
by Country : 802.11bg:-ACE^ 802.11a:-ABCDEHNSZ^ 802.11 6GHz:-BEZ^ Radio Authority IDs :
 None AP Country Code : CZ - Czech Republic AP Regulatory Domain 802.11bg : -E 802.11a
: -E MAC Address : 8c84.4292.f840 IP Address Configuration : DHCP IP Address : 9.9.33.3
 IP Netmask : 255.255.255.0 Gateway IP Address : 9.9.33.1 Fallback IP Address Being Used
 : Domain : Name Server : CAPWAP Path MTU : 1485 Capwap Active Window Size : 1
```

APプロファイルのアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Controller#show ap profile name ap-profile detailed AP Profile Name: ap-profile .
. . AP broken antenna detection: Status : ENABLED RSSI threshold : 40 Weak RSSI : -80
Detection Time : 120
```

トラブルシューティング

このドキュメントでは、アクセスポイント（AP）とワイヤレスコントローラ間の Control And Provisioning of Wireless Access Points（CAPWAP）/Lightweight Access Point Protocol（LWAPP）トンネルが切断される理由を理解するための用例を紹介します。詳細については、「コントローラからのアクセスポイントの関連付け解除のトラブルシューティング」を参照してください。

（注） ソフトウェアまたはハードウェアの変更により、コマンドが動作しなくなったり、構文が変更されたり、リリースによって GUI や CLI の見た目が異なったりする場合があります。

フィードバックのリクエスト

ユーザー入力が役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。

- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。