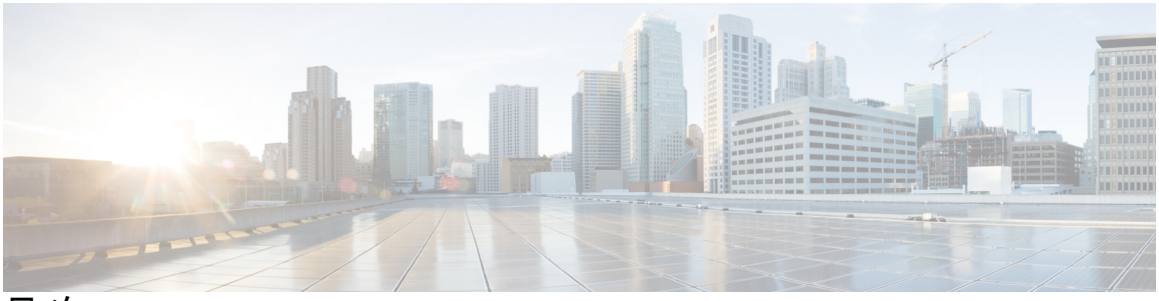
Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.16.x

最終更新：2025 年 12 月 16 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

はじめに

ここでは、このガイドについて説明し、Cisco Catalyst 産業用ワイヤレスアクセスポイントでの URWB の設定に関する情報と、関連資料を提供します。

内容は次のとおりです。

このマニュアルについて

このガイドでは、Cisco Catalyst IW9167E、IW9165E、および IW9165D アクセスポイントの URWB 動作モードの設定について詳しく説明します。UWRB は、Unified Industrial Wireless （UIW）ソフトウェアの一部としてサポートされています。UIW リリース 17.16.1 では、次の新機能が導入されます。

- ライセンスの適用による米国およびカナダでの 4,900 ～ 4,990 MHz 周波数のサポート
- サポートされる国コードの追加
- ネットワーク アドレス変換

関連資料

Catalyst IW9167 および IW9165 アクセスポイントの Control And Provisioning of Wireless Access Points（CAPWAP）およびワークグループブリッジ（WGB）動作モードに関するドキュメントは、次の URL で入手できます。

- Catalyst IW9167 Heavy Duty アクセスポイント
- Catalyst IW9165E 高耐久性アクセスポイント
- Catalyst IW9165D Heavy Duty アクセスポイント

通信、サービス、およびその他の情報

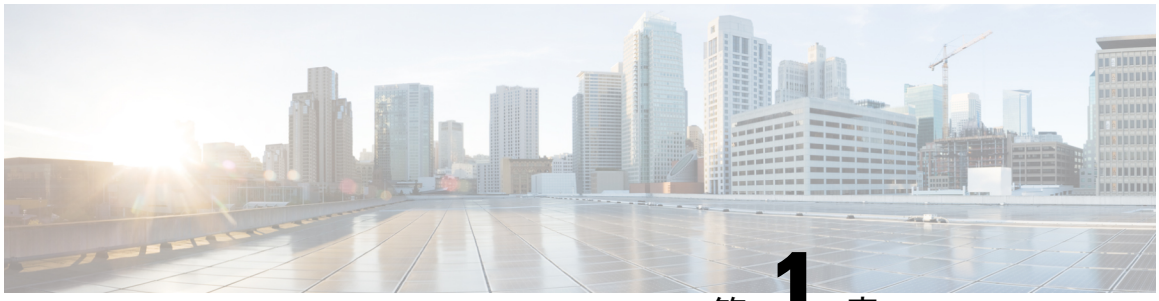
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

シスコのバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

Cisco Catalyst IW9167E および IW9165 アクセスポイントの概要

Cisco Catalyst IW9167E および IW9165 アクセスポイントの概要

Cisco Catalyst IW9167E の概要

Catalyst IW9167E アクセスポイントは、最先端のプラットフォームでミッションクリティカルなアプリケーションに信頼性の高いワイヤレス接続を提供し、スループットが高く、容量が大きく、デバイス干渉が少ない、信頼性と安全性の高いネットワークを実現します。Catalyst IW9167E は、トライ無線機およびトライバンド（2.4/5/6 GHz 帯域）をサポートしている、シスコ初の屋外 Wi-Fi 6E 対応アクセスポイントです。Catalyst IW9167E は、Wi-Fi（Control And Provisioning of Wireless Access Points（CAPWAP））モードまたは Ultra-Reliable Wireless Backhaul（URWB）モード、およびシスコスタイルのパーサーをサポートするように設計された Catalyst IW9167E に関連する URWB ソフトウェアで動作できます。

Cisco Catalyst IW9165 の概要

Catalyst IW9165 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（2.5 mGig および 1G）により、最大 3.6 Gbps の PHY データレートがサポートされています。Catalyst IW9165 は、シームレスなハンドオフ、低遅延、高可用性を実現する、URWB を使用します。Catalyst IW9165 は、6 GHz 帯域への拡張を活かしてより信頼性と安全性の高いネットワークを構築し、スループットと容量を増大しつつもデバイスへの干渉を軽減するよう設計されています。Catalyst IW9165 には、ハードウェアを変更することなく、ワークグループブリッジ（WGB）または URWB モードで Catalyst IW9165 を動作させるためにソフトウェアを更新するだけで、イメージを切り替えるオプションがあります。

Catalyst IW9165 シリーズには、次の 2 つのモデルがあります。

- 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

Cisco Catalyst IW9167E および IW9165 アクセスポイントの概要

- Catalyst IW9165D アクセスポイント

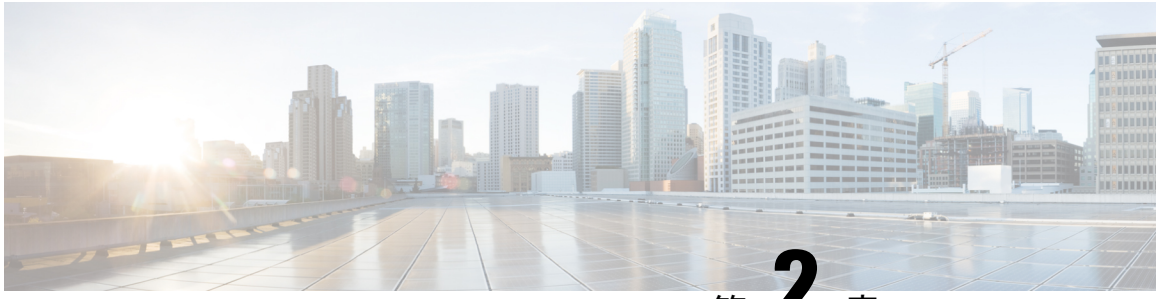
Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント

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て、移動する車両やマシン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、小型フォームファクタにより、Catalyst IW9165E は産業資産に非常に簡単に統合できます。

UIW リリース 17.14.1 以降、Catalyst IW9165E は Dying Gasp 機能をサポートします。DC 入力電源が停止すると、Dying Gasp 機能により、デバイスは少なくとも 100 ミリ秒間電力を維持できます。この間、デバイスはネットワーク内の他のデバイスに、まもなくシャットダウンすることを示すメッセージを送信します。これにより、急にパケット送信に障害が発生する事態を回避できます。Catalyst IW9165E は Dying Gasp メッセージを生成し、Catalyst IW9165D、IW9165E、および IW9167E デバイスはこれらのメッセージを処理します。

Cisco Catalyst IW9165D アクセスポイント

Catalyst IW9165D は、内部アンテナと外部アンテナを備えた 2x2 Wi-Fi 6E 設計をサポートしていて、ワイヤレスバックホールの展開を簡素化するように設計されています。Catalyst IW9165D は、耐久性の高い IP67 と内蔵の指向性アンテナを使用して設計されていて、光ファイバを使用できない場所での長距離、高スループットの接続が可能になるため、固定ワイヤレスインフラストラクチャ（ポイントツーポイント、ポイントツーマルチポイント、メッシュ）の構築だけでなく、沿道や沿線でのモバイルデバイスからのトラフィックをバックホールすることもできます。外部アンテナポートを使用すると、必要に応じてネットワークを新しい場所にすばやく拡張し、ユースケースと導入アーキテクチャに基づいて適切なアンテナを選択できます。



第 2 章

プロビジョニングモードでのデバイスの初期設定

プロビジョニングモード

UIW リリース 17.16.1 以降 IoT OD IW は変更され、IW サービスと呼ばれるようになりました。URWB モードで動作する Catalyst IW アクセスポイント（AP）は、次のいずれかの方法による設定をサポートしています。

- オンラインクラウド管理：産業用ワイヤレス（IW）サービスを使用してデバイスを設定します。または、
- オフライン：ローカル管理インターフェイス（GUI または CLI）を使用してデバイスを設定します。

デフォルトでは、設定のない AP はプロビジョニングモードで起動します。このモードでは、IW サービスによって初期設定が提供されます。

プロビジョニングモードの仕組み

プロビジョニングモードでは、AP は、DHCP を使用したネットワーク設定の要求を試み、その後、IW サービスに接続します。

- ネットワーク接続がある場合、AP は IW サービスに接続します。
  - IW サービスを使用した AP の設定：AP は、ネットワーク接続を取得すると、IW サービスへの接続を試みます。IW サービスは、DNS の位置情報を使用して、AP を適切なクラスタ（米国または EU）に転送します。IW サービスの組織が正しいクラスタに設定されていることを確認します。
- ネットワーク接続がない場合は、AP をローカルに設定できます。ローカル管理には、コンソールポートまたは SSH を使用してアクセスできます。
  - ローカル設定を使用した AP の設定：ネットワーク接続を使用できない場合は、コンソールポートまたは SSH を介してアクセスできる GUI または CLI を使用して、AP をローカルに設定できます。

これらのデフォルトログイン情報を使用して、GUI または CLI のいずれかにログインします。

- ユーザー名：Cisco
- パスワード：Cisco

プロビジョニングモードでの DHCP と IP アドレスの処理

デバイスは、プロビジョニングモードの場合、DHCP サーバーからの IP アドレスの取得を試みます。このプロセスが失敗した場合、または DHCP が使用できない場合は、次のオプションが適用されます。

- DHCP を介して IP アドレスを受信できない場合、デバイスはフォールバック IP アドレス（192.168.0.10/24）に切り替わります。
- DHCP が使用できず、IW サービスを介した設定が必要な場合は、IP アドレス、サブネット、デフォルトゲートウェイ、および DNS を手動で設定できます。

（注） DHCP はプロビジョニングモードのときにのみ使用されます。通常のタスクの場合は、静的 IP アドレスを使用してください。

GUI を使用したフォールバック IP アドレスの設定

デバイスが DHCP サーバーから IP アドレスを取得できない場合に使用するフォールバック IP アドレスを設定するには、このタスクを実行します。これにより、動的 IP 割り当てがない場合でもデバイスが継続的に動作できます。

始める前に

フォールバック IP アドレスは、DHCP による IP アドレスの割り当てに失敗した場合にデバイスがデフォルトで使用する静的 IP アドレスとして機能します。この機能は、DHCP サーバーを使用できないシナリオで接続を維持するために重要です。

手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力して URWB コンフィギュレータのログインページを開きます。

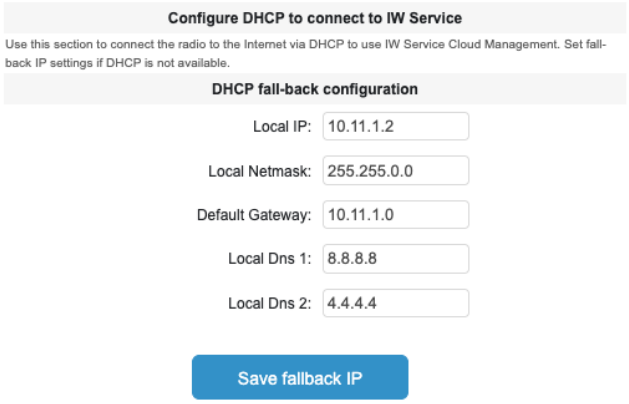
ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI に正常にログインすると、URWB コンフィギュレータページが表示されます。

ステップ 4 URWB コンフィギュレータページで [IW Service] をクリックし、[Configure DHCP to connect to IW Service] セクションに移動します。

ステップ 5 それぞれのフィールドに適切な IP アドレスを入力します。

- フォールバックのローカル IP
- ローカルネットマスク
- デフォルト ゲートウェイ
- ローカルプライマリ DNS
- ローカルセカンダリ DNS



ステップ 6 [Save fallback IP] をクリックして設定を完了します。

CLI を使用したフォールバック IP アドレスの設定

始める前に

AP は、DHCP サーバーから IP アドレスを取得できない場合、事前設定されたフォールバック IP アドレスに戻ります。

手順

AP でフォールバック IP アドレスを設定するには、このタスクを実行します。

デバイスで `configure ap address ipv4 static` *`IP address`*`static netmask` *`IP address`* `of gatewaydns1 ip` *`IP address`*`dns2 ip` *`IP address`* コマンド使用してフォールバック IP アドレスを設定します。

```
Device#configure ap address ipv4 [ static IP address [ static netmask [ IP address of default gateway
 [ dns1 ip [ dns2 ip ] ] ] ] ]
```

例：

```
Device#configure ap address ipv4 static 192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200
192.168.10.201
```

GUI を使用した AP の設定（オフライン）

手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力して URWB コンフィギュレータのログインページを開きます。

ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI に正常にログインすると、URWB コンフィギュレータページが表示されます。

ステップ 4 [IW Service] をクリックします。
[IW Service Configuration Mode] ページが表示されます。

ステップ 5 [Offline] を選択します。
デバイスは、プロビジョニングモードを終了し、フォールバック IP アドレスに切り替わります。

IW サービスを使用した AP の設定（オンラインクラウド管理）

このタスクでは、IW サービスを介してオンラインクラウド管理モードでアクセスポイントを設定する方法について説明します。このモードでは、インターネットに接続されている場合、IW サービスクラウドサーバーからデバイスを管理できます。

手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力して URWB コンフィギュレータのログインページを開きます。

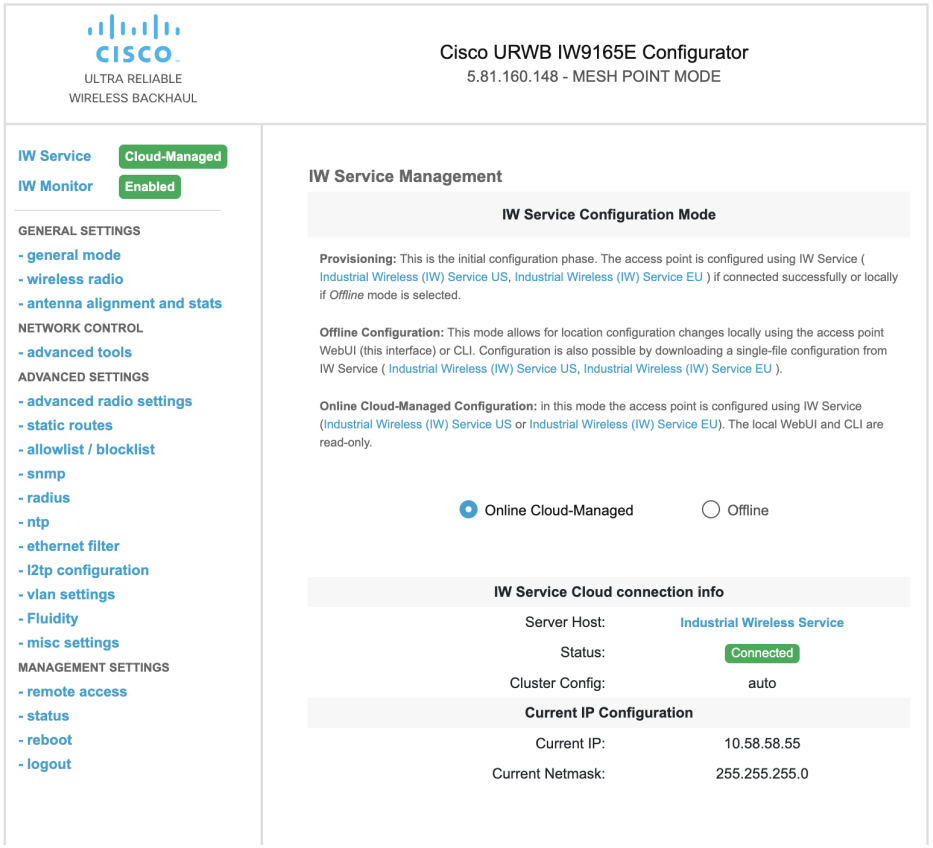
ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI に正常にログインすると、URWB コンフィギュレータページが表示されます。

ステップ 4 [IW Service] をクリックします。
[IW Service Configuration Mode] ページが表示されます。

ステップ 5 デフォルトでは、デバイスは [Online Cloud-Managed] として表示されます。

IW サービスクラウドサーバーからデバイスを管理できます（インターネットに接続されている場合）。デバイスは、ユーザーが IW サービスから設定をプッシュした場合またはオフラインモードに切り替えた場合にのみ、プロビジョニングモードを終了します。



デバイスは、設定が IW サービスからプッシュされた場合またはモードがオフラインに切り替えられた場合にのみ、プロビジョニングモードを終了します。

GUI を使用した AP ステータスの確認

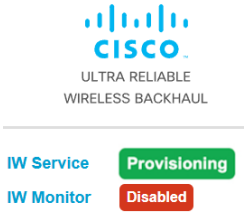
手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力して URWB コンフィギュレータのログインページを開きます。

ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

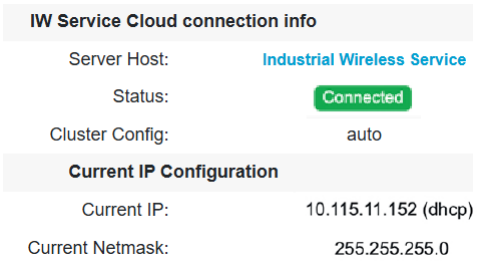
ステップ 3 [ログイン（Login）] をクリックします。
GUI に正常にログインすると、URWB コンフィギュレータページが表示されます。

- プロビジョニングモード



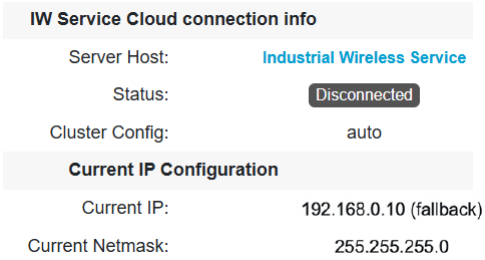
- ステータスが「接続中」のデバイスコンフィギュレータ

  IW サービスへの接続が成功すると、ステータスが [Connected] と表示されます。

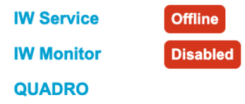


- ステータスが「切断中」のデバイスコンフィギュレータ

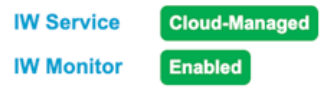
  IW サービスへの接続が失敗すると、ステータスが [Disconnected] と表示されます。



- オフライン モード



- オンラインクラウド管理



CLI を使用した AP ステータスの確認

URWB コンフィギュレータ内で AP の現在の動作ステータスを確認するには、このタスクを使用します。

手順

`show iw-service status` コマンドを使用して、デバイスのステータスを確認します。

```
Device#show iw-service status
```

例：

- プロビジョニングモードのデバイス

```
Device#show iw-service status

IW Service mode: Provisioning

Status: Connected
```

- オフラインモードのデバイス

```
Device#show iw-service status

IW Service mode: Offline
```

- オンラインクラウド管理モードのデバイス

```
Device#show iw-service status

IW Service mode: Online Cloud-Managed

Status: Connected
```

CLI を使用した DHCP 接続ステータスの確認

手順

ステップ 1 次の CLI の例は、デバイスがプロビジョニングモードであり、DHCP サーバーから IP アドレスを取得していることを示しています。

DHCP のステータスを表示するには、`show ip` を使用します。

- 例：DHCP の成功

```
Device#show ip


IP: 192.168.0.10

Network: 255.255.255.0

Gateway:
```

```
Nameservers:

DHCP Address (PROVISIONING Mode):

IP: 10.0.0.2

Network: 255.255.255.0

Gateway: 10.0.0.1

Nameservers: 8.8.8.8

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

ステップ 2 次の CLI の例は、デバイスが、プロビジョニングモードであり、DHCP サーバーから IP アドレスを取得できず、デフォルトのフォールバック IP アドレスの 192.168.0.10 を使用することを示しています。

DHCP のステータスを表示するには、`show ip` を使用します。

- 例：DHCP の失敗（デフォルトのフォールバック IP を使用）

```
Device#show ip

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers:

DHCP Address (PROVISIONING Mode):

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers: 127.0.0.1

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

LED の動作

デバイスのステータス LED は、そのデバイスがフォールバック状態、オンラインクラウド管理モード、またはオフラインモードになるまで、一定のサイクルで連続的に点滅します。具体

的な LED のパターンについては、「Catalyst IW9165 の LED パターン」または「Catalyst IW9167 の LED パターン」を参照してください。

プロビジョニングモードでの IW サービス接続のトラブルシューティング

デバイスが IW サービスに接続できない場合は、次の手順を試してください。

手順

ステップ 1 物理的な接続：イーサネットケーブルが正しく接続されていることを確認します。

ステップ 2 DNS 解決：次を確認します。

- device.ciscoiot.com
- us.ciscoiot.com
- eu.ciscoiot.com

ステップ 3 アウトバウンド HTTPS：アクセスポイントが、手順 2 でリストされたドメインに対して tcp/443 でのアウトバウンド HTTPS 接続を許可することを確認します。

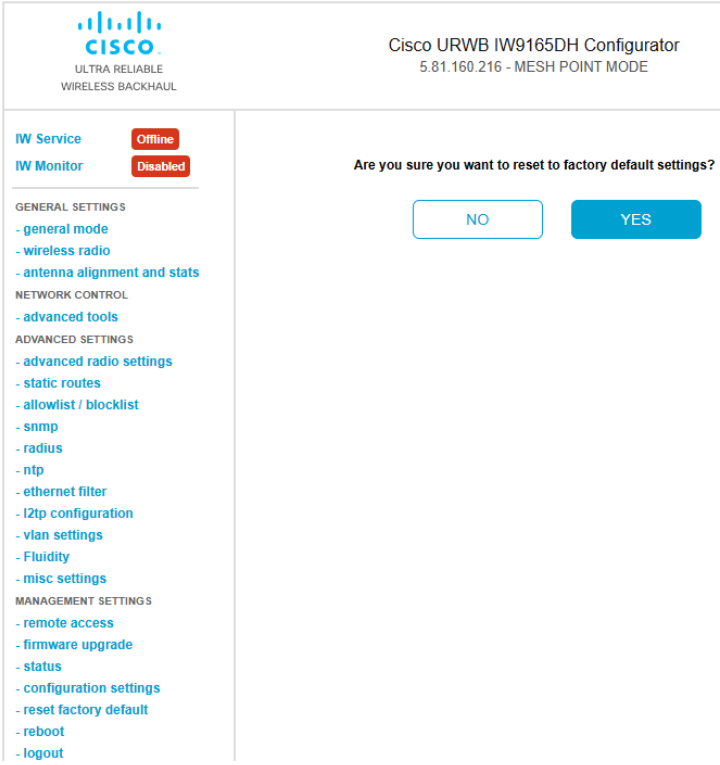
ステップ 4 ローカル設定：IW サービスがオフラインのままである場合、デバイスのコンフィギュレータインターフェイスを使用してローカル（オフライン）設定を行います。

GUI を使用したデバイスの工場出荷時のデフォルトへのリセット

アクセスポイントに電力が供給されているときにリセットボタンを 30 秒間押すか、コンフィギュレータインターフェイスを使用して、デバイスを工場出荷時のデフォルトにリセットすることができます。リセットボタンの詳細については、「Using the Reset Button」を参照してください。

（注） ハードリセットにより、デバイスの IP アドレスや管理者パスワードを含む、すべてのデバイス設定が工場出荷時のデフォルトに戻ります。ハードリセットではなく、デバイスをリブートする場合は、GUI を使用したデバイスのリブート （14 ページ）を参照してください。

1. [MANAGEMENT SETTINGS] で、[reset factory default] をクリックします。



2. 確認ポップアップウィンドウで [YES] をクリックします。工場出荷時の状態へのリセットを中止するには、[NO] をクリックします。
3. 以前にデバイスの設定ファイルを保存している場合は、保存した設定をデバイスに復元できます。デバイス設定の保存と復元 （15 ページ）を参照してください。

（注） 開始点として工場出荷時の設定を使用してデバイスを再設定する必要がある場合を除き、ハードリセットを実行しないでください。ハードリセットでは、デバイスの IP アドレスと管理者パスワードがリセットされ、ネットワークからデバイスが切断されます。

CLI を使用したデバイスの工場出荷時のデフォルトへのリセット

デバイスの設定をリセットするには、次の CLI コマンドを使用します。

```
device#configure factory reset config
WARNING: "configure factory reset config" will clear config and reboot.
Do you want to proceed? (y/n)
```

CLI コマンドで `y` を入力してデバイスのリセットプロセスを開始するか、`n` を入力してプロセスを中止します。

デバイス設定のリセットとデータワイプを実行するには、次の CLI コマンドを使用します。

```
Device#configure factory reset default
WARNING: "configure factory reset default" will take minutes to perform DATA WIPE.
```

このプロセスの一環として、次のファイルがクリアされます。

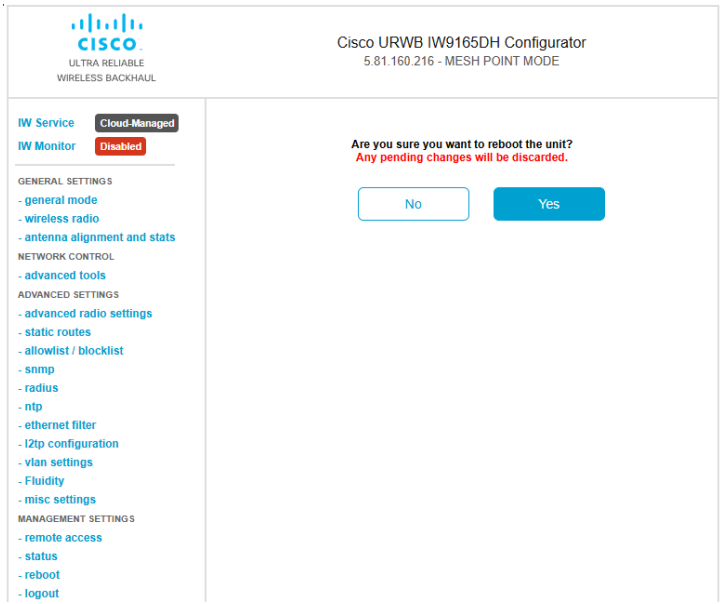
```
1) Config, Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
5) Pktlogs
6) Manually created files
Do you want to proceed? (y/n)
```

CLI コマンドで `y` を入力して設定のデバイスリセットとデータワイプを開始するか、`n` を入力してプロセスを中止します。

GUI を使用したデバイスのリブート

デバイスのオペレーティングシステムをリブートするには、次の手順を実行します。

1. [MANAGEMENT SETTINGS] で、[reboot] をクリックします。



2. 確認ポップアップウィンドウで [Yes] をクリックします。リブートを中止するには、[No] をクリックします。

CLI を使用したデバイスのリブート

リブートを実行するには、次の CLI コマンドを使用します。

```
Device#reload
Proceed with reload command (cold)? [confirm]
```

CLI コマンドで `confirm` と入力して、デバイスのリブートプロセスを開始します。

デバイス設定の保存と復元

[LOAD OR RESTORE SETTINGS] ウィンドウでは、次のタスクを実行できます。

- デバイスの既存のソフトウェア設定を設定（*.conf）ファイルとして保存する。
- 保存した設定ファイルを現在のデバイスにアップロードして適用する。

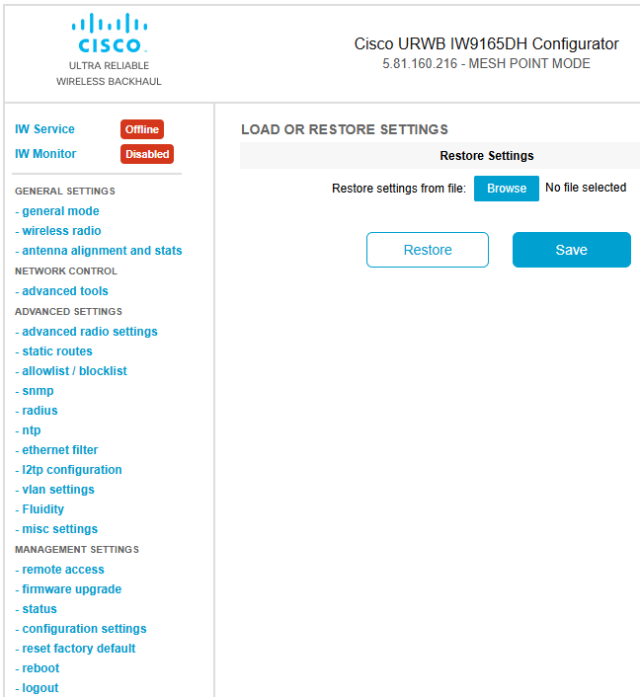
（注） デバイスソフトウェア設定（*.conf）ファイルは、IW Service 設定セットアップ（*.iwconf）ファイルと交換できません。

ヒント 保存済みの設定ファイルは、同じタイプのすべてのデバイスで再利用されます。これらの保存済みの設定ファイルは設定のバックアップファイルとして機能し、破損したデバイスを同じタイプのデバイスと交換する必要がある場合に、短時間で再展開できます。

デバイスの既存の設定をコンピュータにダウンロードするには、次の手順を実行します。

1. [MANAGEMENT SETTINGS] で、[configuration settings] をクリックします。

   [LOAD OR RESTORE SETTINGS] ウィンドウが表示されます。



2. [Save] をクリックしてデバイス設定（*.conf）をダウンロードします。

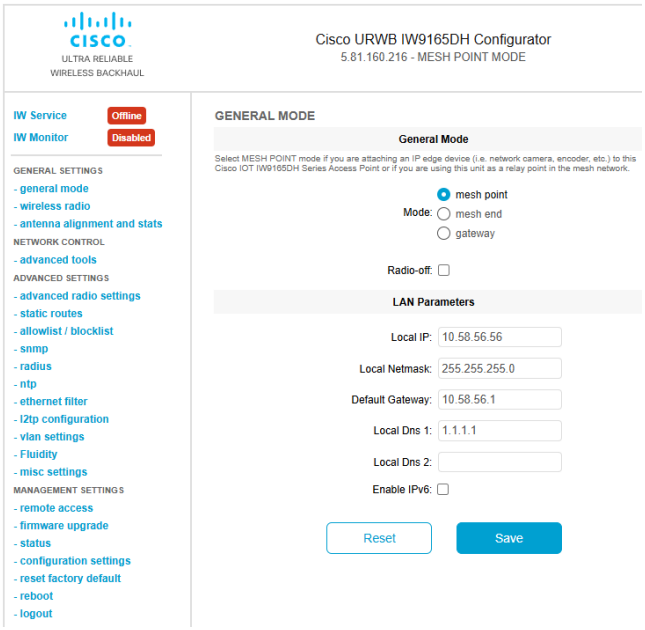
保存した設定ファイルをデバイスにアップロードするには、次の手順を実行します。

1. [Browse] をクリックして、デバイスにアップロードする設定（*.conf）ファイルを見つけます。
2. [Restore] をクリックして、設定をデバイスに適用します。

一般設定の設定

[General Mode] 設定を変更するには、次の手順を実行します。

1. [GENERAL SETTINGS] で、[general mode] をクリックします。



[General Mode] には、動作モードのコントロールがあります。メッシュ無線ネットワークで動作可能なデバイスは、[mesh point] モードで出荷されます。

（注） 必要なネットワークレイアウトを設計する場合は、少なくとも1つのメッシュエンドデバイスが必要です。このデバイスは、ライセンス管理などの制御および管理機能を実行します。これは、ネットワークが2つのデバイスのみで構成されている場合でも、ネットワークを正しく動作させるために必要です。

デバイスの動作モードを変更するには、次のいずれかのモードを選択します。

- **Gateway**：このモードは高度なレイヤ 3 モビリティ展開に適用され、ほとんどのネットワークでは使用されません。

- **Mesh Point**：このモードは、ネットワーク内の残りのアクセスポイントに適用されます。これらのアクセスポイントは、ワイヤレスリンクまたは有線リンクを使用して、メッシュエンドまたはメッシュポイントとして設定された同じネットワークパスフレーズを持つ他のアクセスポイントへのリンクを確立します。このシナリオでは、アクセスポイントに他のアクセスポイントがレイヤ 2 で可視化されます。
- **Mesh End**：このモードは、制御および管理のネットワーク機能を実行するようにアクセスポイントを設定します。各ネットワークには少なくとも 1 つのメッシュエンドが必要です。このアクセスポイントは、通常、ワイヤレスネットワークと有線ネットワークが収束する最も中心的なポイントに設置されます。

CLI を使用した一般設定の設定

一般設定を設定するには、次の CLI コマンドを使用します。

```
Device#configure modeconfig mode
  gateway    layer 3 global gateway mode
  meshend    mesh end mode
  meshpoint  mesh point mode

Device#configure modeconfig mode meshend
  mpls       MPLS support
  radio-off  disable radio interfaces
```

LAN パラメータの変更

LAN パラメータには、ローカルアドレス設定のエントリ制御があります。LAN パラメータを変更するには、次の手順を実行します。

1. [General Mode] ウィンドウを初めて開くと、[Local IP] および [Local Netmask] の LAN パラメータには工場出荷時のデフォルト値が表示されます。
2. 必要に応じて、[Dns 1] フィールドにローカルプライマリ DNS アドレスを入力し、[Dns 2] フィールドにローカルセカンダリ DNS アドレスを入力します。
3. [Save] をクリックして、LAN 設定を保存します。設定をクリアするには、[Reset] をクリックします。

CLI を使用した LAN パラメータの設定

LAN パラメータを設定するには、次の CLI コマンドを使用します。

例：

```
device#configure ip address ipv4 static
192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200 192.168.10.201
```

アクセスポイントのコンソールポイントへの接続

アクセスポイントを（有線 LAN に接続せずに）ローカルに設定するには、DB-9 to RJ-45 シリアルケーブルを使用してコンピュータをアクセスポイントのコンソールポートに接続します。アクセスポイントのコンソールポートに接続して CLI を開くには、次の手順を実行します。

1. 9 ピンのメスの DB-9 to RJ-45 シリアルケーブルを、アクセスポイントの RJ-45 シリアルポートと、コンピュータの COM ポートに接続します。
2. アクセスポイントと通信できるようにターミナルエミュレータを設定します。ターミナルエミュレータには、次の設定値を使用します。

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

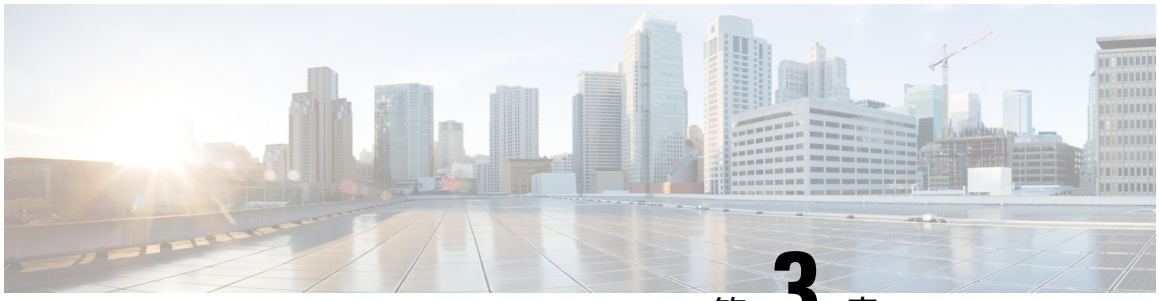
3. 使用可能なコマンドプロンプトモードには、標準コマンドプロンプト（>）と特権コマンドプロンプト（#）の 2 つがあります。ログインしてすぐは、特権のないコマンドを実行するための標準コマンドプロンプト（>）モードになります。

   特権コマンドプロンプト（#）モードにアクセスするには、enable コマンド（省略形は en）を入力し、イネーブルパスワードを入力します（特権モードのログインパスワードは、標準のログインパスワードとは異なります）。

   次のデフォルト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、アクセスポイントからシリアルケーブルを取り外します。



第 3 章

GUIを使用したデバイスのアップグレード

GUI を使用したデバイスのアップグレード

手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力して URWB コンフィギュレータのログインページを開きます。

ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI に正常にログインすると、URWB コンフィギュレータページが表示されます。

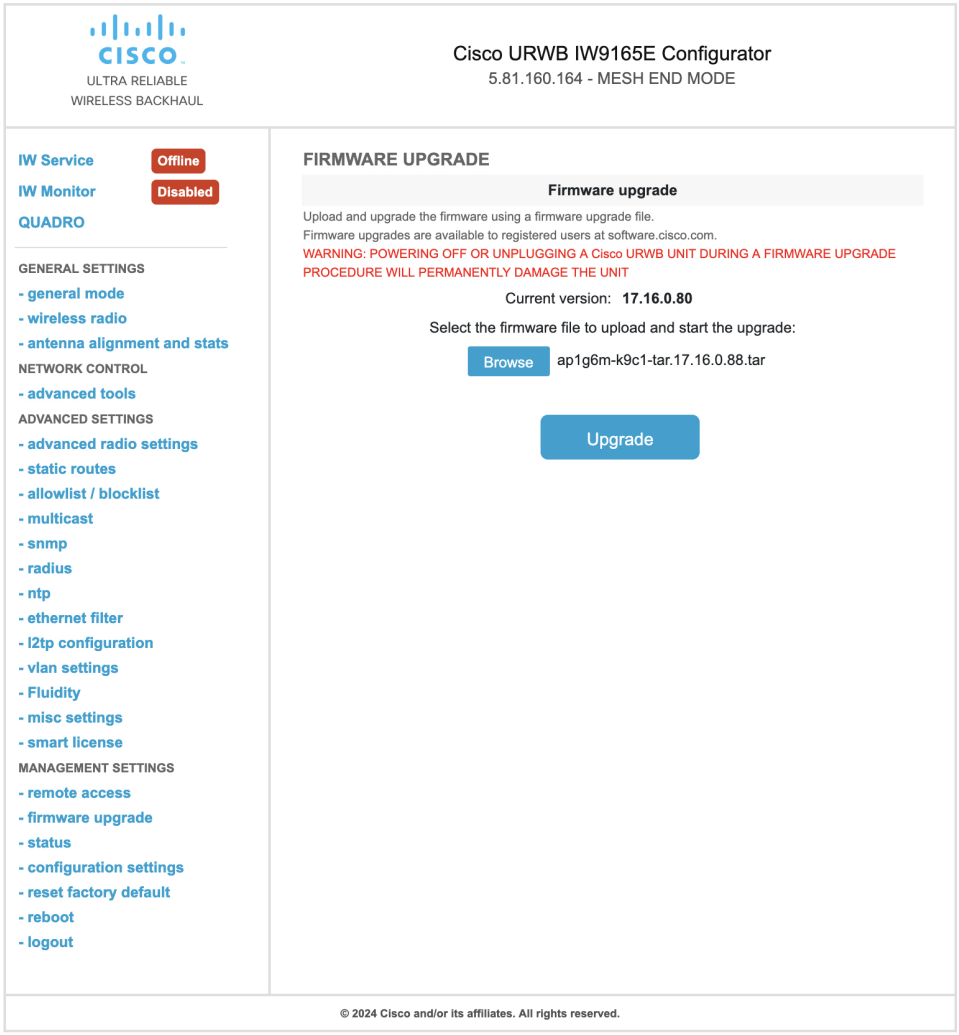
ステップ 4 [MANAGEMENT SETTINGS] で、[firmware upgrade] リンクをクリックして [FIRMWARE UPGRADE] ウィンドウを開きます。

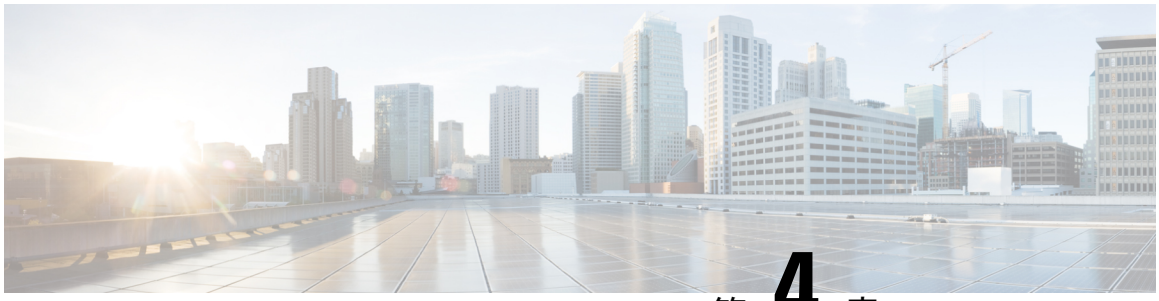
ステップ 5 [Browse] ボタンをクリックして、ファームウェア アップグレード ファイルを探して選択します。

ステップ 6 [Upgrade] ボタンをクリックして、アップグレードプロセスを開始します。

ステップ 7 [OK] をクリックして、デバイスへのファームウェアファイルのアップロードを確認します。
ファームウェアがデバイスに正常にアップロードされると、AP でイメージが確認されてから、AP がリブートします。

GUI を使用したデバイスのアップグレード





第 4 章

TFTP を使用したデバイスのアップグレード

トリビアルファイル転送プロトコル（TFTP）を使用してデバイスをアップグレードするには、次の条件を満たす必要があります。

- デバイスがネットワークに接続されていること。
- デバイスがローカル TFTP サーバーと通信するように設定されていること。
- ターゲットデバイスイメージがローカル TFTP サーバーのルートディレクトリにアップロードされていること。

TFTP を使用したデバイスのアップグレード

TFTP デバイスアップグレード機能を使用すると、デバイスの自動アップグレードまたはデバイスの直接アップグレードを実行できます。デバイスの自動アップグレードでは、デバイスはマニフェストファイルを使用して新しいデバイスが利用可能かどうかを定期的にチェックし、アップグレードプロセスを開始します。デバイスの直接アップグレードでは、デバイスは指定されたデバイスイメージを TFTP サーバーから取得し、アップグレードプロセスを開始します。次のいずれかの方法を選択できます。

- TFTP を使用したデバイスの自動アップグレード
- TFTP を使用したデバイスの直接アップグレード

TFTP を使用したデバイスの自動アップグレード

始める前に

この方法を使用すると、デバイスはユーザーが指定した間隔でローカル TFTP サーバーに接続して、新しいデバイスイメージが利用可能かどうかを確認できます。デバイスはデバイスイメージファイルを検出し、アップグレードを実行します。

手順

ステップ 1 *device.manifest* ファイルを作成し、デバイスイメージが保存されているのと同じ TFTP サーバーのルートディレクトリにアップロードします。

ステップ 2 TFTP 自動アップグレードを有効にする前に、TFTP サーバーと時間間隔を設定します。

（注）
時間間隔は、時間単位で指定する必要があります。

注意
デバイスのダウンロードが完了するまでは、デバイスを切り離したり、再起動したりしないでください。イメージファイルのサイズによっては、デバイスのアップグレードに時間がかかる場合があります。

TFTP サーバー上のマニフェストファイルの設定

最初に、デバイスは TFTP サーバーからマニフェストファイルを取得します。マニフェストファイルの情報に基づいて、デバイスは TFTP サーバーからデバイスイメージを取得します。条件が満たされると、デバイスはデバイスのアップグレードプロセスを開始します。

マニフェストファイルの形式

マニフェストファイルは、TFTP サーバーでホストされている必要があります。このファイルには、デバイスアップグレード用のデバイスイメージに関連する情報が含まれます。マニフェストファイルに含まれる情報は次のとおりです。

- デバイスイメージのファイル名
- デバイスイメージファイルの MD5 チェックサム
- デバイスイメージのバージョン

マニフェストファイル名は、IW デバイスモデルに応じて指定する必要があります。

デバイスタイプ	マニフェストファイル名
IW9167EH	IW9167EH.manifest
IW9165E	IW9165E.manifest
IW9165DH	IW9165DH.manifest

マニフェストファイルの形式の例：
`image_name=ap1g6m-k9c1-tar.202307110910`
`image_md5=376e15acd4e82a49a81d42add904f5b0`
`image_version=8.8.1.101`

TFTP を使用したデバイスの直接アップグレード

デバイスは、指定されたデバイスイメージを TFTP サーバーから取得します。デバイスの直接アップグレードプロセスを開始するには、次の CLI コマンドを使用します。

目的	コマンドまたはアクション
IP アドレスを使用して TFTP サーバーを設定する	`Device#configure tftp server A.B.C.D` A.B.C.D：TFTP サーバーの IP アドレス
TFTP アップグレードイメージを設定する	`Device#configure tftp upgrade <image file>` Configure TFTP upgrade image <image file bin>

デバイスはすぐにアップグレードプロセスを開始します。

⚠

注意 デバイスのダウンロードが完了するまでは、デバイスを切り離したり、再起動したりしないでください。イメージファイルのサイズによっては、デバイスのアップグレードに時間がかかる場合があります。

CLI を使用した TFTP デバイスのアップグレード

目的	コマンドまたはアクション
TFTP サーバーを使用してデバイスのアップグレードを実行する	`Device#configure tftp server A.B.C.D` A.B.C.D：TFTP サーバーの IP アドレス
TFTP デバイスの自動アップグレードを無効にする	`Device#configure tftp upgrade automatic disable`

目的	コマンドまたはアクション
TFTPデバイスの自動アップグレードを有効にする	`Device#configure tftp upgrade automatic enable`
チェック期間を待たずに即座にマニフェストファイルを確認する	`Device#configure tftp upgrade check now`
TFTPデバイスのアップグレードを定期的に確認する	`Device#configure tftp upgrade check period 3` （注） チェック期間は、時間単位で指定する必要があります。
TFTP 設定を確認する	`Device#show tftp config`

TFTP 設定の表示の例：

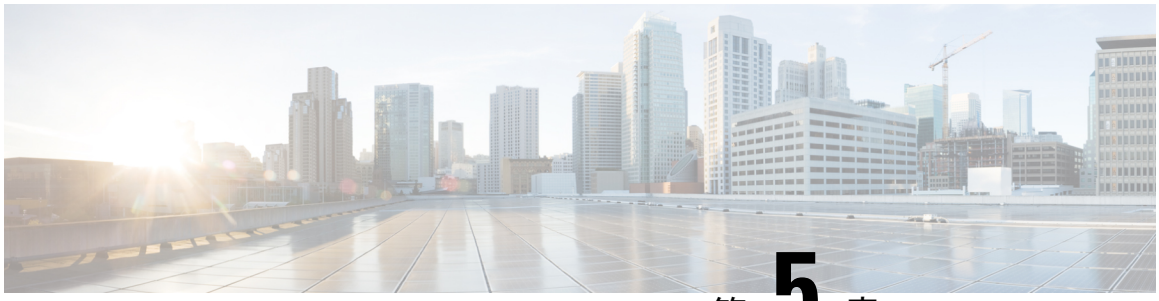
```
Device#show tftp config
Automatic TFTP Upgrade settings:
Status: enabled
Server: A.B.C.D
Check period (hours): 3
```

自動 TFTP アップグレードの例：

```
Device#configure tftp server A.B.C.D
Device#configure tftp upgrade check period 3
Device#write
Device#configure tftp upgrade automatic enable
Device#write
Device#reload
```

次の場合には、デバイスのアップグレード手順を開始できません。

- マニフェストファイルで報告された MD5 チェックサムサムが、デバイスイメージファイル（*image_name*）で計算された MD5 チェックサムと一致しない場合。
- マニフェストファイルで報告されたデバイスイメージのバージョンが、デバイスで実行されている現在のデバイスバージョンと一致する場合。



第 5 章

IPv6 のサポート

概要

UIW リリース 17.15.1 以降、AP は IPv6 アドレスをサポートします。デフォルトでは、AP の IPv6 サービスは無効になっています。CLI または GUI を使用して、AP の IPv6 アドレスの有効化と設定ができます。

IPv6 アドレス タイプ

AP に次の IPv6 アドレスタイプを設定できます。

- リンクローカル
- ユニークローカル
- グローバルユニキャスト

リンクローカル

リンクローカルアドレスは、単一リンクの範囲内で使用され、ルーティングできません。これらのアドレスは、明確に特定の物理リンクを参照し、自動アドレス設定、近隣探索プロトコルなどを目的とした単一のリンクのアドレッシングに使用されます。リンクローカルアドレスは、同じリンクに接続された近隣ノードに到達するために使用できます。

ユニークローカル

ユニークローカルアドレスは、プライベートな組織内ではルーティングできますが、パブリックインターネットを介してルーティングすることはできません。グローバルインターネット上でルーティングされることは想定されていません。ただし、サイトなどの限られたエリア内のルーティングは可能であり、限られたサイト間のルーティングも可能な場合があります。

グローバルユニキャスト

グローバル ユニキャスト アドレスは、パブリック IPv4 アドレス空間と同様に、IPv6 インターネットでルーティング可能なアドレスです。

AP における IPv6 の制約事項

- IPv6 のサポートは、ホスト機能に限定されます。
- Fluidity レイヤ 3 ネットワークは IPv6 をサポートしません。

CLI を使用した IPv6 の有効化または無効化

デフォルトでは、AP の IPv6 サポートは無効になっています。IPv6 を有効にすると、AP に自動的にリンクローカルアドレスが割り当てられます。

このコマンドを使用して、AP の IPv6 アドレスを有効または無効にします。

```
Device#configure ipv6 {enable | disable}
```

CLI を使用した IPv6 RA 自動設定の有効化または無効化

このコマンドを使用して、AP の IPv6 RA 自動設定を有効または無効にします。

```
Device#configure ipv6 enable autoconfig-ra {enable | disable}
```

（注）
- enable：ルータアドバタイズメントからの自動設定を有効にします。
- disable：ルータアドバタイズメントからの自動設定を無効にします。

EUI-64 による静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスの設定

このコマンドを使用して、AP の EUI-64 による静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスを設定します。

```
Device#configure ap address ipv6 static fc00::4236:5aff:xxxx:168/64 eui-64 fc00::1
2001:4860:4860::xxxx 2001:4860:4860::xxxx
```

EUI-64 による静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスの確認

AP の EUI-64 による静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスを確認するには、次の **show** コマンドを使用します。

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::4236:5aff:xxxx:168/64
Gateway: fc00::1
DNS1: 2001:4860:4860::xxxx
DNS2: 2001:4860:4860::xxxx
Currently assigned addresses:
fc00::4236:5aff:xxxx:168/64 global
fe80::4236:5aff:xxxx:168/64 link
```

EUI-64 によらない静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスの設定

このコマンドを使用して、AP の EUI-64 によらない静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスを設定します。

```
Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def/64 fc00::1
2001:4860:4860::xxxx 2001:4860:4860::xxxx
```

EUI-64 によらない静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスの確認

AP の EUI-64 によらない静的 IPv6 アドレス、ゲートウェイ、および DNS サーバーアドレスを確認するには、次の **show** コマンドを使用します。

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/64
Gateway: fc00::1
DNS1: 2001:4860:4860::xxxx
DNS2: 2001:4860:4860::xxxx
Currently assigned addresses:
fc00::1234:5678:xxxx:def/64 global
fe80::4236:5aff:xxxx:168/64 link
```

EUI-64 による静的 IPv6 アドレスの設定

このコマンドを使用して、AP の EUI-64 による静的 IPv6 アドレスを設定します。

```
Device#configure ap address ipv6 static fc00::4236:5aff:xxxx:168/64 eui-64
```

EUI-64 による静的 IPv6 アドレスの確認

AP の EUI-64 による静的 IPv6 アドレスを確認するには、次の **show** コマンドを使用します。

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::4236:5aff:xxxx:168/64
Currently assigned addresses:
fc00::4236:5aff:xxxx:168/64 global
fe80::4236:5aff:xxxx:168/64 link
```

EUI-64 によらない静的 IPv6 アドレスの設定

このコマンドを使用して、AP の EUI-64 によらない静的 IPv6 アドレスを設定します。

```
Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def
```

EUI-64 によらない静的 IPv6 アドレスの確認

AP の EUI-64 によらない静的 IPv6 アドレスを確認するには、次の **show** コマンドを使用します。

```
Device#show ipv6
IPv6: Enabled
Router Advertisement auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/128
Currently assigned addresses:
fc00::1234:5678:xxxx:def/128 global
fe80::4236:5aff:xxxx:168/64 link
```

IPv6 ゲートウェイおよび DNS サーバー設定のクリア

このコマンドを使って、AP の IPv6 ゲートウェイとドメインネームシステム（DNS）サーバーのアドレス設定をクリアします。

```
Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def/64 :: :: ::
```

クリアされた IPv6 ゲートウェイと DNS サーバーの設定の確認

AP のクリア済み IPv6 ゲートウェイおよび DNS サーバーのアドレス設定を確認するには、次の **show** コマンドを使用します。

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/64
Currently assigned addresses:
fc00::1234:5678:xxxx:def/64 global
fe80::4236:5aff:xxxx:168/64 link
```

（注） TFTP などのサービスを IPv6 で機能するよう適応させる場合には、リンクローカル IP アドレスにはネットワークインターフェイスの指定が求められる場合がある事を考慮する必要があります。

GUI を使用した静的 IPv6 の有効化と設定

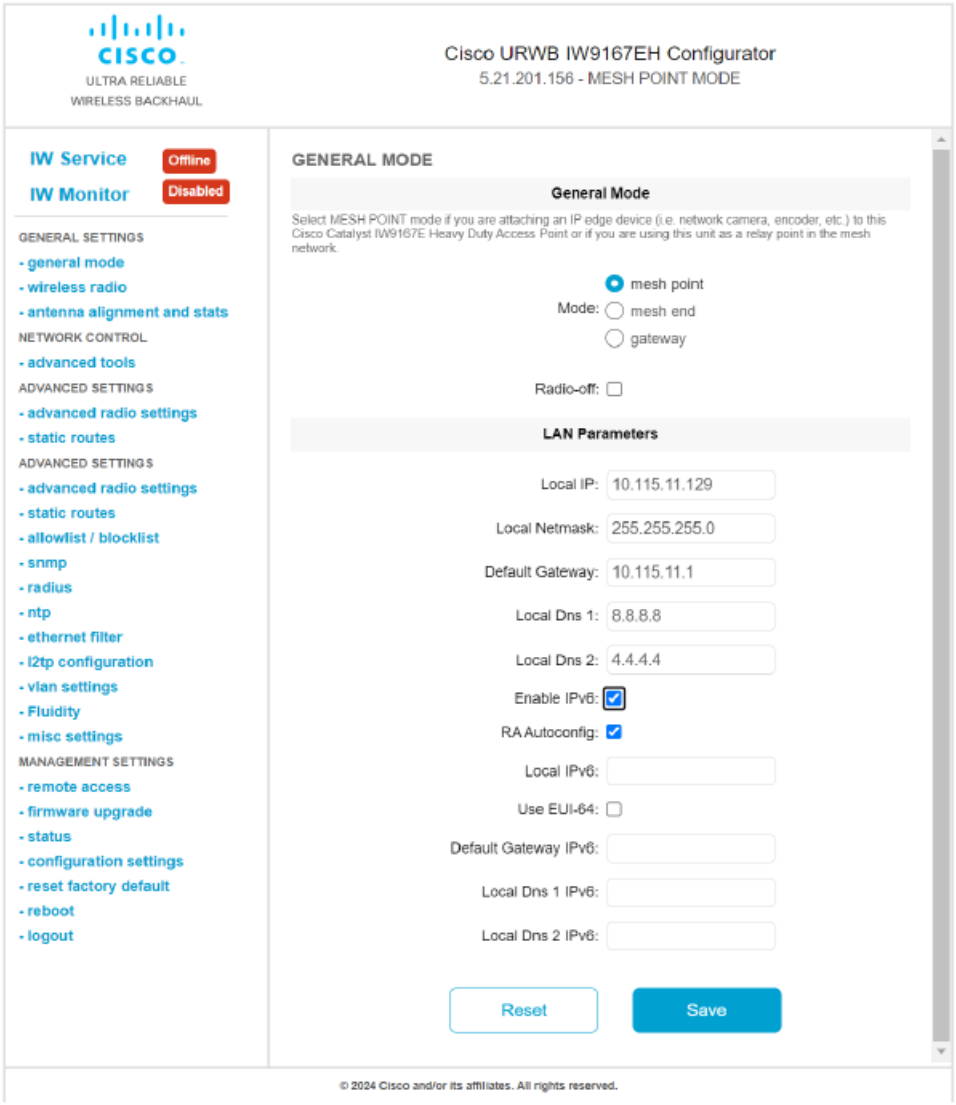
手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力してコンフィギュレータのログインページを開きます。

ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI にログインすると、URWB コンフィギュレータが表示されます。

ステップ 4 [GENERAL SETTINGS] で、[general mode] をクリックして [General Mode] ウィンドウを開きます。



（注）
GUI では、「ローカル」という用語は、静的に設定された IPv4 または IPv6 アドレスを指します。具体的には、[Local IPv6] にはすべてのタイプの IPv6 アドレスを使用できるため、デバイスの IPv6 アドレスを静的に設定できます。

ステップ 5 [Enable IPv6] チェックボックスをオンにします。[RA Autoconfig] がシステムによって自動的に有効になります。

ステップ 6 [Local IPv6] フィールドに IPv6 アドレスを入力します。

ステップ 7 （オプション）[Use EUI-64] チェックボックスをオンにします。

（注）
IPv6 アドレスは、EUI-64 オプションを使用するかどうかで異なります。

ステップ 8 （オプション）[Default Gateway IPv6] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 9 （オプション）[Local Dns 1 IPv6] フィールドに DNS サーバー 1 の IP アドレスを入力します。

ステップ 10 （オプション）[Local Dns 2 IPv6] フィールドに DNS サーバー 2 の IP アドレスを入力します。

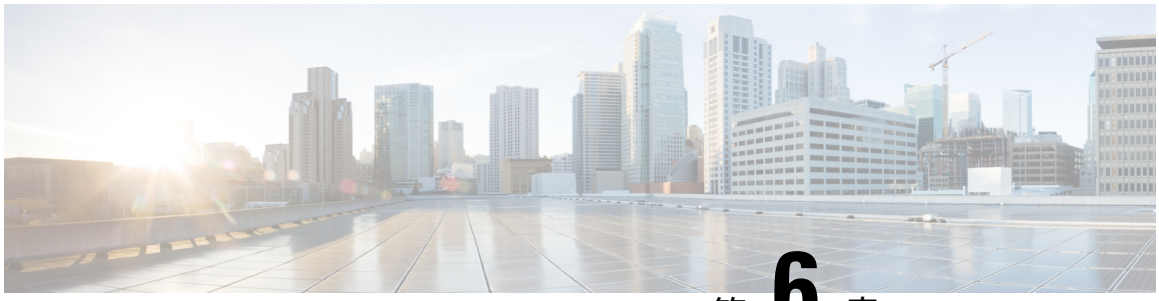
ステップ 11 [Save] をクリックします。

GUI を使用した静的 IPv6 の確認

手順

ステップ 1 [MANAGEMENT SETTINGS] で、[status] をクリックします。

ステップ 2 [STATUS] ページの [DEVICE SETTINGS] セクションで、IPv6 の詳細を確認できます。



第 6 章

URWB 動作モードの設定

URWB 動作モードの設定

Catalyst 産業用ワイヤレスアクセスポイントは、Catalyst Wi-Fi（AP）、Cisco Ultra-Reliable Wireless Backhaul（URWB）、ワークグループブリッジ（WGB）などの複数のワイヤレステクノロジーをサポートしています。サポートされるモードは、具体的なアクセスポイントによって異なります。

アクセスポイントの OS は、Catalyst Wi-Fi（AP）と Unified Industrial Wireless（UIW）の 2 つの異なるソフトウェアイメージをサポートしています。URWB と WGB は、どちらも UIW ソフトウェアの一部です。アクセスポイントのモードは、アクセスポイントが動作するように設定されているモードに基づいてブート時に決定されます。

CLI による判別

アクセスポイントの OS は、Catalyst Wi-Fi（AP）と UIW の 2 つの異なるソフトウェアイメージをサポートしています。次の show コマンドを使用して、実行されているソフトウェアを判別し、指定されたプラットフォームコードを探します。

```
Device# show version
Cisco AP Software, (ap1g6j), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu Aug 18 01:01:29 PDT 2022
ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100
APFC58. 9A16.E464 uptime is 1 days, 3 hours, 58 minutes
Last reload time : Wed Sep 7 11:17:00 UTC 2022
Last reload reason: reload command
```

show version で ap1g6a または ap1g6b と表示された場合は、アクセスポイント OS が実行されていることを意味します。show version で ap1g6j または ap1g6m と表示された場合は、UIW ソフトウェアが実行されていることを意味します。

アクセスポイントが URWB モードで動作しているかどうかを確認するには、次の CLI コマンドを実行します。

```
Device#show iw-service status
```

このコマンドが存在する場合、アクセスポイントは URWB モードで動作しています。存在しない場合、アクセスポイントは WGB モードで動作しています。

リセットボタンの設定

URWB モードでは、（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。

- リセットボタンを 20 秒より短く押すと、既存の設定がクリアされます。
- リセットボタンを 20 秒より長く 60 秒より短く押すと、工場出荷時設定へのリセットがトリガーされます。
- リセットボタンを 60 秒より長く押しても、設定はクリアされません。

イメージ変換の設定

Catalyst IW9167E アクセスポイントを Wi-Fi モード（CAPWAP AP）から URWB モードに、または URWB モードから Wi-Fi モード（CAPWAP AP）に変換するには、次の手順を実行します。

1. CAPWAP から URWB モードに、または WGB/uWGB から URWB モードに変換するには、次の CLI コマンドを使用します。続いてアクセスポイントが再起動され、URWB モードで起動します。

   configure boot mode urwb

2. URWB から CAPWAP モードに、または WGB/uWGB から CAPWAP モードに変換するには、次の CLI コマンドを使用します。続いてアクセスポイントが再起動され、CAPWAP モードで起動します。

```
configure boot mode capwap
```

3. CAPWAP から WGB/uWGB モードに、または URWB から WGB/uWGB モードに変換するには、次の CLI コマンドを使用します。

```
configure boot mode wgb
```

（注） 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、設定とデータが完全に削除されます。

GUI へのアクセス手順

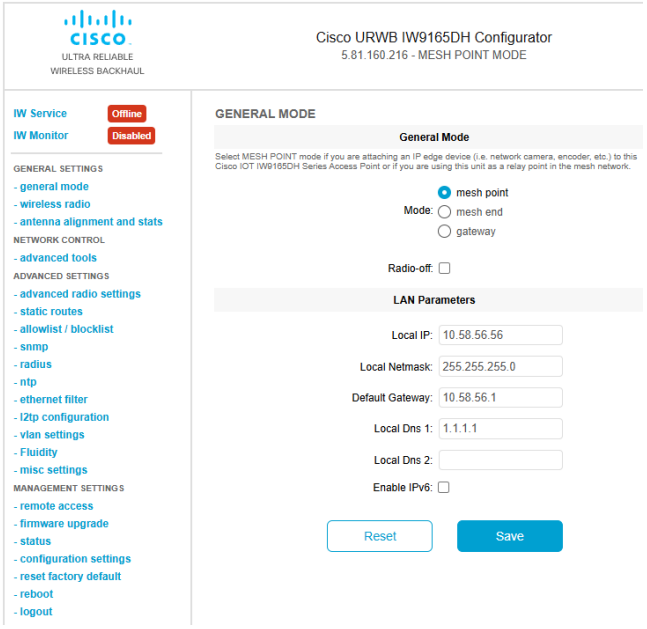
Web UI（Web ユーザーインターフェイス）にアクセスするには、次の手順を使用します。

1. Web UI にアクセスするには、Web ブラウザを開き、次の URL を入力します：https://<IP address of unit>/

   [IW9167E Configurator] または [IW9165 Configurator] ウィンドウが表示されます。

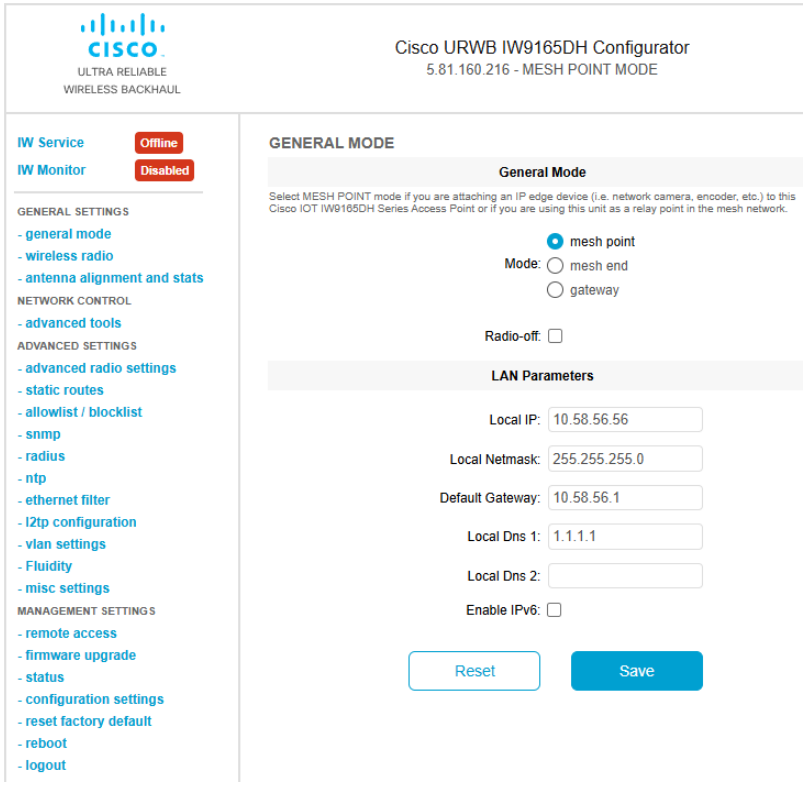
2. 設定ページにアクセスするには、[Username] と [Enable password] のログイン情報を使用します。

3. GUI にログインすると、URWB コンフィギュレータが表示されます。



GUI を使用した URWB Catalyst IW9167E の設定

次の画像に、Catalyst IW9167E コンフィギュレータの設定を示します。



CLI 設定のコミット

現在の設定または実行中の設定をローカルストレージまたはメモリに保存するには、`write`CLI コマンドを入力します。変更された値はキャッシュ設定ファイルにあるため、`write` コマンドを入力した後に、デバイスを再起動して現在の設定を有効にします。設定を有効にするには、次の CLI コマンドを使用します。

```
Device# write
```

または

```
Device# wr
```

write または wr：現在の設定をメモリにコミットします。

```
Device# reload
```

reload：デバイスをリロードします。

例：

```
Device# write
```

```
!!! Please reboot to take effect
Device# reload
```

Proceed with reload? [confirm]

（確認のために入力します）

CLI を使用した IW Service のクラウド管理モードおよびオフラインモードの設定

IW Service はクラウド管理ポータルであり、デバイスはネットワークを介してクラウド管理に接続されます。オフラインモードでは、デバイスは CLI と GUI によってローカルモードで設定され、クラウドには接続されません。

デバイスがオフラインモードに設定されている場合は、次のオプションを選択します。

- CLI と GUI を使用して、デバイスを手動で設定します。
- IW Service クラウドサービスでデバイスを設定して、IW Service からエクスポートされた設定ファイルを選択し、IW Service 管理ページの最後にある設定のアップロードボタンを使用して設定ファイルをアップロードします。

IW Service 設定機能をアクティブまたは非アクティブにするには、次の CLI コマンドを使用します。

```
Device#configure iw-service {offline | cloud-managed}
```

cloud-managed：IW Service モードをクラウド管理にします。IW Service クラウドサーバーからデバイスを管理できます（ネットワークに接続されている場合）。

offline：IW Service モードをオフラインに設定します。デバイスは IW Service から切断され、CLI またはオフライン コンフィギュレータ インターフェイスを使用して手動で設定する必要があります。

CLI を使用したパスワードの設定（初回ログイン後）

デバイスがオフラインモードに切り替わると（初回ログイン後）、新しいログイン情報を設定する必要があります。GUI または CLI を使用してログイン情報を設定する場合、ログイン情報は次の条件を満たす必要があります。

- ユーザー名の長さは 3 ～ 32 文字にする必要があります。
- パスワードの長さは 8 ～ 32 文字にする必要があります。
- パスワードには、次が含まれている必要があります。
  - 少なくとも 1 つの大文字
  - 少なくとも 1 つの小文字

- 少なくとも 1 つの数字
- 少なくとも 1 つの特殊文字

- パスワードには英数字と特殊文字（33 ～ 126 の ASCII 10 進コード）を含めることができますが、次の特殊文字は使用できません。

  " [二重引用符]

  ' [一重引用符]

  ? [疑問符]

- パスワードに次の要素を含むことはできません。
  - 連続する 3 つの文字または数字（ABC/CBA）
  - 3 つ連続して同じ文字または数字（AAA）または（666）
  - 現在のパスワードまたは既存のパスワードと同じもの
  - 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

例：

デフォルトログイン情報：

```
username: Cisco
password: Cisco
enable password: Cisco
```

ログイン情報をリセットするには、次のサンプルログイン情報を使用します。

```
username: demouser
password: DemoP@ssw0rd
enable password: DemoE^aP@ssw0rd
```

CLI を使ったパスワードの設定例：

```
Device#configure iw-service {offline}
Switching to IW Service  Offline mode...
Will switch from Provisioning Mode to IW Service  offline Mode, device need to reboot:Y/N?
Y
User access verification.
[Device rebooting...]

User Access Verification:
Username: Cisco
Password: Cisco
```

初回ログイン後に、ログイン情報をリセットします。

```
Current Password:Cisco
Current Enable Password:Cisco
New User Name:demouser
New Password:DemoP@ssw0rd
Confirm New Password:DemoP@ssw0rd
New Enable Password:DemoE^aP@ssw0rd
Confirm New Enable Password:DemoE^aP@ssw0rd
```

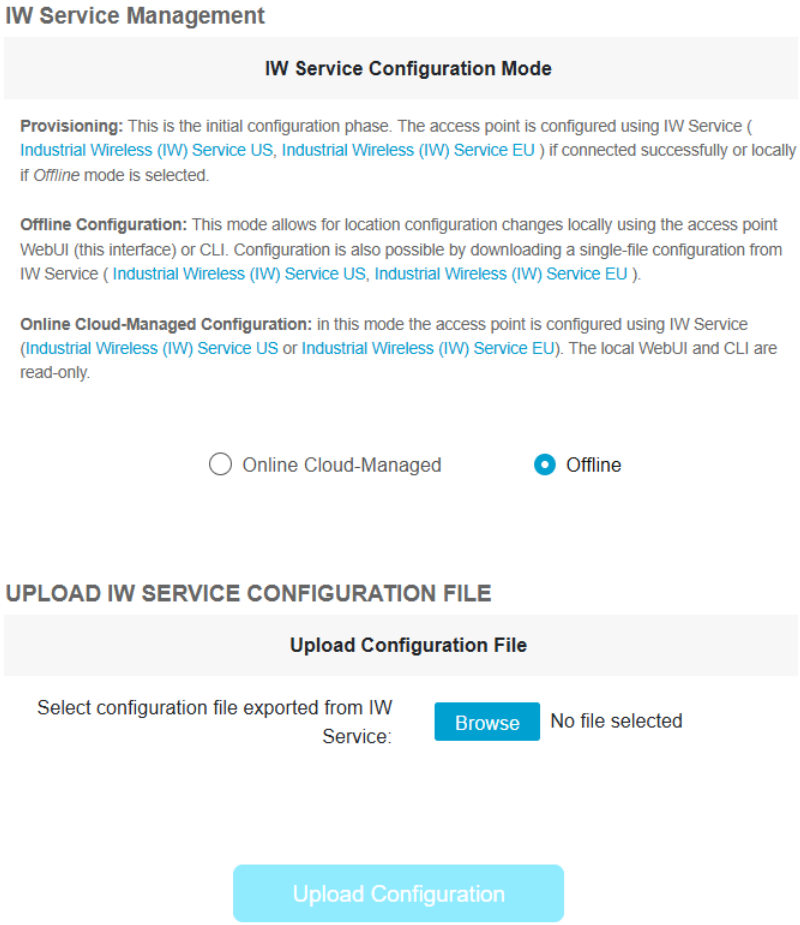
ログイン情報を変更したら、再度ログインします。

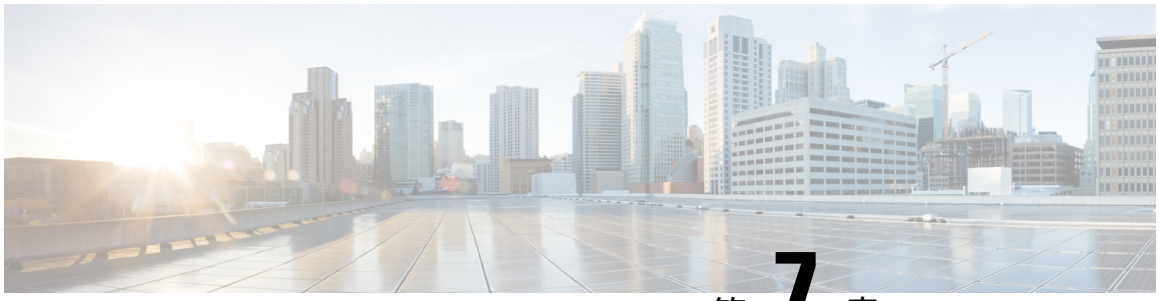
```
User access verification
Username: demouser
Password: DemoP@ssw0rd
Device> enable
Password:DemoE^aP@ssw0rd
Device#
```

（注） 上記の例では、すべてのパスワードがプレーンテキストです。これはデモ用（サンプルログイン情報）です。実際には、パスワードはアスタリスク（*）で表示されます。

GUI を使用した IW Service の設定

次の画像は、IW Service の設定を示しています。


IW Service Management
IW Service Configuration Mode
Provisioning: This is the initial configuration phase. The access point is configured using IW Service (Industrial Wireless (IW) Service US, Industrial Wireless (IW) Service EU) if connected successfully or locally if Offline mode is selected.
Offline Configuration: This mode allows for location configuration changes locally using the access point WebUI (this interface) or CLI. Configuration is also possible by downloading a single-file configuration from IW Service (Industrial Wireless (IW) Service US, Industrial Wireless (IW) Service EU).
Online Cloud-Managed Configuration: in this mode the access point is configured using IW Service (Industrial Wireless (IW) Service US or Industrial Wireless (IW) Service EU). The local WebUI and CLI are read-only.
Online Cloud-Managed
Offline
UPLOAD IW SERVICE CONFIGURATION FILE
Upload Configuration File
Select configuration file exported from IW Service:
Browse
No file selected
Upload Configuration



第 7 章

URWB 無線機モードの設定

URWB 無線機モードの設定

ワイヤレスインターフェイスは、特定のモードで動作するように設定するか、無効にできます。無線機モードを設定すると、デバイスは Fluidity または固定インフラストラクチャとして動作を開始します。

次の表に、デバイスでの無線機モードの設定を示します。

URWB 無線機モードの設定

表 *1:* 無線機モードの設定

無線機のロール	無線機モード	説明
固定インフラストラクチャ	Fixed Fluidmax プライマリ Fluidmax セカンダリ	P2P モード（ポイントツーポイント） P2MP（ポイントツーマルチポイント）モード（Fluidmax）および P2MP P2MP モード（Fluidmax）および P2MP
モビリティ AP	Fluidity	モビリティモード
モビリティクライアント	Fluidity	モビリティモード

次の表に、有効な無線インターフェイスの動作モードから導出される Fluidity ステータスを示します。

表 *2:* 無線インターフェイスの動作モード

無線機 1/無線機 2	固定インフラストラクチャ	Fluidity
固定インフラストラクチャ	Fluidity が無効	Fluidity が有効
Fluidity	Fluidity が有効	Fluidity が有効

次の表に基づき、複数およびデュアルの無線インターフェイスを設定できます。

表 *3:* 複数の無線インターフェイスの設定

無線機 1/無線機 2	固定インフラストラクチャ/メッシュ	モビリティ AP	モビリティクライアント
固定インフラストラクチャ/メッシュ	ME/MP リレー、P2MP（メッシュ）	あり、トレーラの使用例（採掘トレーラ）	サポートされていますが、具体的な使用例はありません
モビリティ AP	あり、トレーラの使用例（採掘トレーラ）	標準の Fluidity（各無線機に複数のクライアント）	サポートされていません。V2V または Fixed + AP を使用してください
モビリティクライアント	サポートされていますが、具体的な使用例はありません	サポートされていません。V2V または Fixed + AP を使用してください	標準の Fluidity（各無線機に複数のクライアント）

CLI による無線機オフモードの設定

両方の無線機（Fluidity と fixed）が無効になっている場合に無線機オフモードを設定するには、次の CLI コマンドと手順を使用します。

（注） [radio-off] を指定すると、デバイスはすべてのワイヤレスインターフェイスを無効にします。

1. デバイスの現在の動作モードを設定します。モードは、メッシュエンド、メッシュポイント、またはグローバルゲートウェイ（L3）に設定できます。

```
Device# configure modeconfig mode {meshpoint | meshend | gateway}
```

2. デバイスのマルチプロトコル ラベル スイッチング（MPLS）OSI レイヤを選択して設定します。[layer] に指定できる値は 2（OSI レイヤ 2）または 3（OSI レイヤ 3）です。

```
Device# configure modeconfig mode {meshpoint | meshend | gateway}[layer {2|3}]
```

3. [radio-off] モードを設定します。

```
Device# configure modeconfig mode { meshpoint | meshend | gateway } [layer {2|3}] [
 radio-off {fluidity | fixed}]
```

4. 現在の設定を終了するには、次の CLI コマンドを使用します。

```
Device# (configure modeconfig mode { meshpoint | meshend | gateway } [layer {2|3}]
[ radio-off {fluidity | fixed}])# end
```

```
Device# wr
```

例：

```
Configure modeconfig mode meshend radio-off fluidity
```

```
Configure modeconfig mode meshend radio-off fixed
```

CLI による URWB の無線機モードの設定

URWB の無線機モードを設定するには、次の CLI コマンドを使用します。

ワイヤレスインターフェイスの動作機能を選択するには、次の CLI コマンドを使用します。デバイスでは、さまざまなインターフェイスに対して Fluidity と固定インフラストラクチャを組み合わせることができます。

1. 無線インターフェイス番号 <1 または 2> でワイヤレスを設定します。

```
Device# configure dot11Radio <interface>
```

2. 指定したインターフェイスの動作モードを設定します。

```
Device# configure dot11Radio <interface> mode {fixed|fluidity|fluidmax}
```

fluidity：このインターフェイスでは、デバイスは Fluidity のモビリティ インフラストラクチャまたは車両モードのいずれかで動作します。

fixed：このインターフェイスは、固定インフラストラクチャモード（Fluidity なし）で動作します。

fluidmax：このインターフェイスは、Fluidmax P2MP モードで動作します。その他のパラメータを指定して、Fluidmax の動作機能（プライマリ/セカンダリロール、クラスタ ID など）を設定できます。

3. Fluidmax インターフェイスモードの fluidmax ロールを設定します。

```
Device# configure dot11Radio <interface>mode {fixed|fluidity|fluidmax} {primary | secondary}
```

primary：Fluidmax ロールをプライマリに設定します

secondary：Fluidmax ロールをセカンダリに設定します

4. 現在の設定を終了するには、次の CLI コマンドを使用します。

```
Device (configure dot11Radio <interface>mode{fixed|fluidity|fluidmax}) # end
Device# wr
```

（注） 少なくとも 1 つのインターフェイスが Fluidity モードに設定されている場合、デバイス全体が Fluidity モードで動作します。すべてのインターフェイスが fixed に設定されている場合、Fluidity は無効になります。

CLI を使用した AMPDU の設定

Aggregated MAC Protocol Data Unit（AMPDU）の長さと優先順位を設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> ampdu length <length>
```

length：<0 ～ 255> の整数（マイクロ秒）

```
Device# configure dot11radio <interface> ampdu priority {enable | disable}
```

enable：ampdu tx 優先順位を有効にする

disable：ampdu tx 優先順位を無効にする

```
Device# configure dot11radio <interface> ampdu priority [enable]
```

0：インデックス 0 の ampdu tx 優先順位

1：インデックス 1 の ampdu tx 優先順位

2：インデックス 2 の ampdu tx 優先順位

3：インデックス 3 の ampdu tx 優先順位

4：インデックス 4 の ampdu tx 優先順位

5：インデックス 5 の ampdu tx 優先順位

6：インデックス 6 の ampdu tx 優先順位

7：インデックス 7 の ampdu tx 優先順位

all：すべてのインデックスの ampdu tx 優先順位（インデックス 0 ～ 7）

CLI による周波数の設定

動作周波数を設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> frequency <frequency>
```

frequency：<0 ～ 7125> MHz 単位の動作周波数。

CLI による最大変調符号化方式インデックスの設定

最大変調符号化方式（MCS）インデックスを設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> mcs <maxmcs>
```

最大 MCS インデックスを整数または文字列 AUTO で設定します。AUTO の場合、バックグラウンドプロセスにより自動的に maxmcs が設定されます。

maxmcs の値：

< 0 ～ 11 > 0 ～ 11 の最大 mcs インデックス。

AUTO という単語

（注） [High Efficiency] モードが無効になっている場合は、MCS 指数値を 0 ～ 9 の範囲で設定します。[High Efficiency] モードが有効になっている場合は、MCS 指数値を 10 または 11 に設定します。

CLI による空間ストリームインデックスの最大数の設定

空間ストリーム（NSS）インデックスの最大数を設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> spatial-stream <maxnss>
```

最大空間ストリーム番号を整数または文字列 AUTO で設定します。AUTO の場合、バックグラウンドプロセスにより自動的に maxnss が設定されます。

maxnss の値：

< 1 ～ 4 > 最大 nss インデックス 1 ～ 4。

AUTO という単語

（注） Catalyst IW9165 は最大 2 つの空間ストリームをサポートし、Catalyst IW9167 は最大 4 つの空間ストリームをサポートします。設定された空間ストリームの最大数は、有効になっているアンテナの数以下である必要があります。

CLI による Rx-SOP しきい値の設定

Receiver Start of Packet（Rx-SOP）しきい値を設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> rx-sop-threshold
```

<0 ～ 91> rx-sop- threshold を入力します（0：自動、値：-値 dBi）。

CLI による RTS モードの設定

Ready to Send（RTS）モードを無効にするには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> rts <disable>
```

disable：RTS 保護を無効にします。

しきい値を使用した RTS を有効にするには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> rts enable <threshold>
```

threshold：しきい値の範囲 <0 ～ 2346>。

CLI による WMM モードの設定

ワイヤレスマルチメディア（WMM）モードを設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11radio <interface> wmm [bk|be|vi|vo]
```

[bk|be|vi|vo]：サービスクラス（CoS）パラメータを表します。

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）。

ワイヤレス統計カウンタをクリアするには、次の CLI コマンドを使用します。

```
Device# configure dot11Radio <interface> wifistats <clear>
```

clear：ワイヤレス統計カウンタをクリアします。

CLI による NTP の設定

NTP サーバーアドレスを設定するには、次の CLI コマンドを使用します。

```
Device# configure ntp server <string>
```

string：IP アドレスまたはドメイン名。

例：

```
Device# configure ntp server 192.168.216.201
```

NTP 認証を設定するには、次の CLI コマンドを使用します。

```
Device# configure ntp authentication none
Device# configure ntp authentication md5 <password> <keyid>
Device# configure ntp authentication sha1 <password> <keyid>
```

none：NTP 認証 md5|sha1（認証方式）を無効にします。

例：

```
Device# configure ntp authentication md5 test1234 65535
```

（注） オプションで、md5 のパスワードとキー ID は、NTP サーバーの md5 のパスワードとキー ID と一致する必要があります。

GUI または CLI を使用して新しいパスワードを設定する場合、パスワードは次の条件を満たす必要があります。

- パスワードの長さの範囲は 8 ～ 20 文字です。
- 次の特殊文字は使用できません。
  - ' [一重引用符]
  - " [二重引用符]
  - ` [逆引用符]
  - $ [ドル記号]
  - = [等号]
  - \ [バックスラッシュ]
  - # [シャープ記号]
  - 空白

NTP サービスを有効または無効にするには、次の CLI コマンドを使用します。

```
Device# configure ntp { enable|disable }
```

NTP タイムゾーンを設定するには、次の CLI コマンドを使用します。

```
Device# configure ntp timezone <string>
```

例：

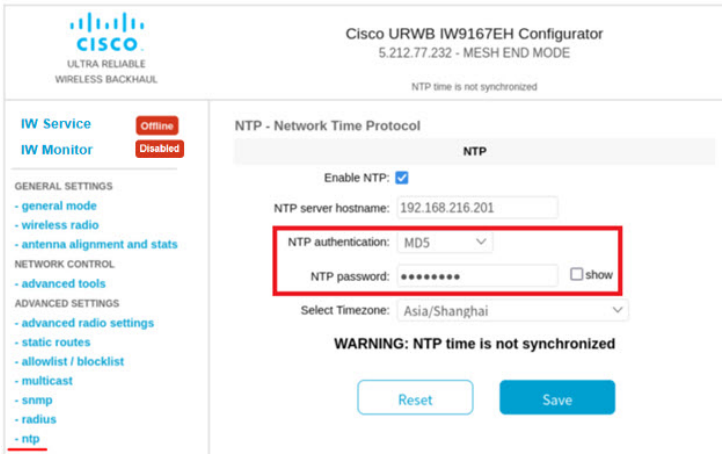
```
Device# configure ntp timezone Asia/Shanghai
```

NTP の設定とステータスを検証するには、次の show コマンドを使用します。

```
Device# show ntp config
NTP status: enabled
NTP server: 192.168.216.201
authentication: MD5
password: test123
keyid: 5
timezone: Asia/Shanghai

Device# #show ntp (Using this command to check if device can sync up time with NTP server)
Stratum Version Last Received  Delay    Offset  Jitter    NTP server
1           4      9sec ago    1.840ms -0.845ms 0.124ms 192.168.216.201
```

GUI を使用した NTP の設定

次の画像は、NTP の GUI を示しています。



URWB の無線機モードの検証

無線機モードを検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio <interface> config
```

例：

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
Channel : 157
Channel width : 40 MHz
```

```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
```

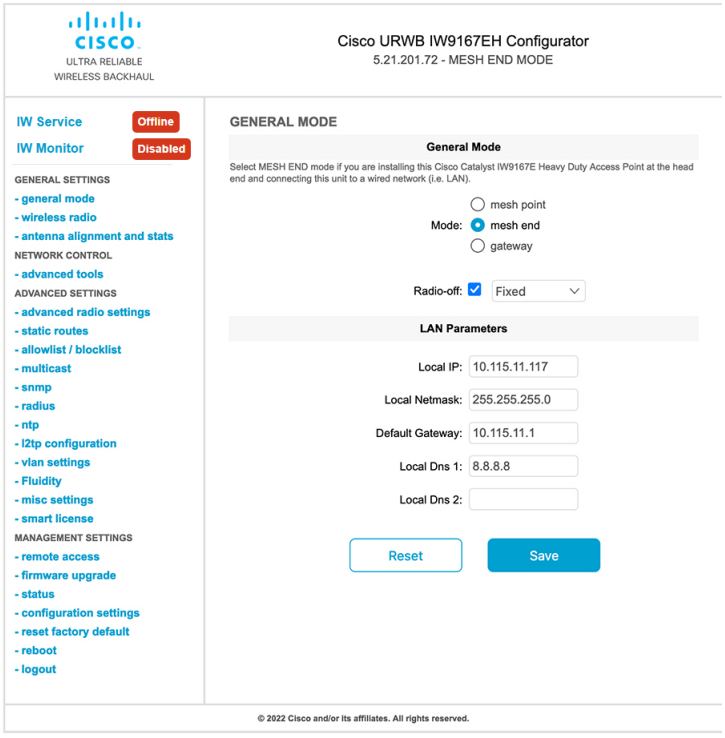
車両アクセスポイント（モビリティクライアント）の無線機モードを Fixed または Fluidmax に変更するには、CLI を使って、Fluidity ロールをインフラストラクチャに設定します。

```
Device# configure fluidity id infrastructure
```

。

GUI を使用した無線機オフモードの設定

[Radio-off] モードを設定するには、図のように [Fixed] モードまたは [Fluidity] モードを選択します。ヘッドエンドに Catalyst IW9167E アクセスポイントを設置し、このデバイスを LAN などの有線ネットワークに接続する場合は、[mesh end] モードを選択します。

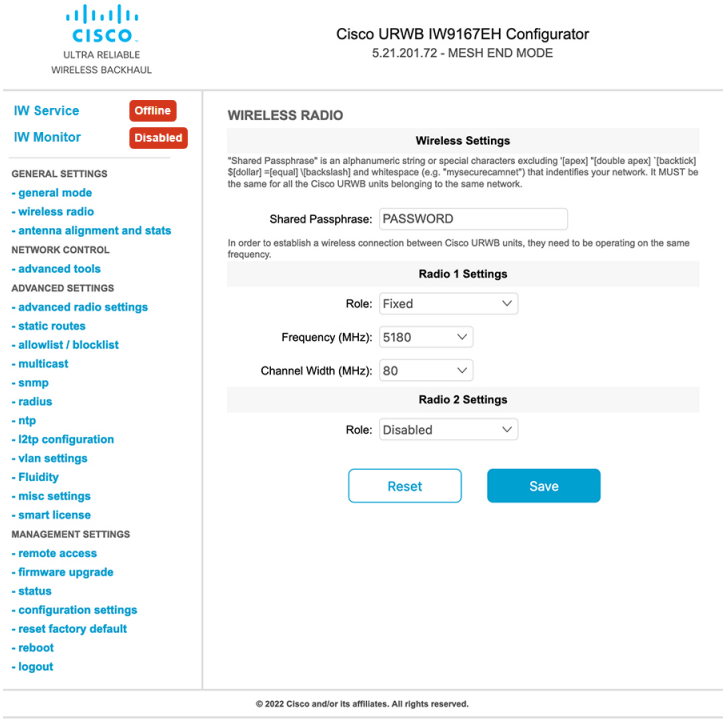


GUI を使用した無線機モードの設定

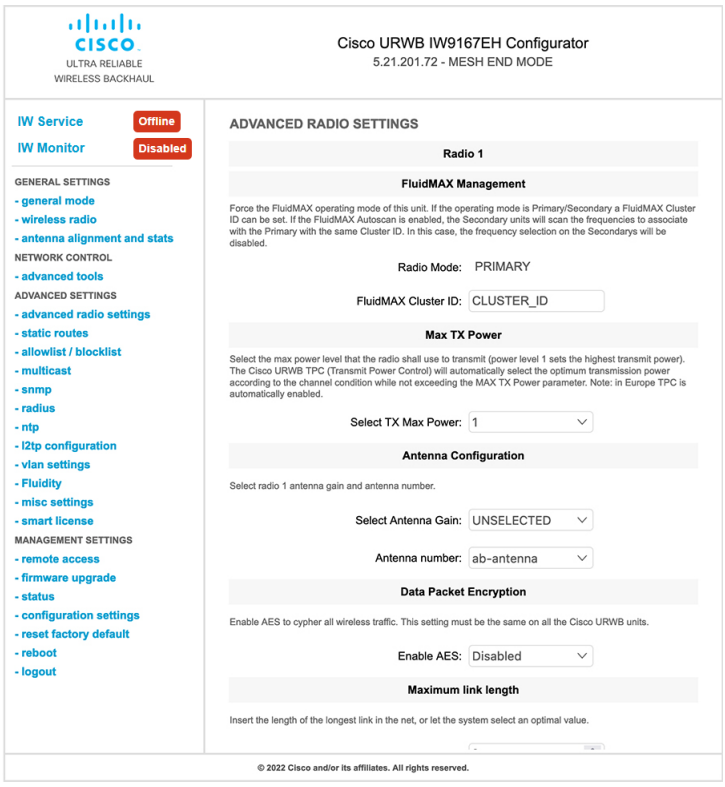
ワイヤレス接続を確立するには、デバイス間で動作周波数が同じである必要があります。

GUI を使用して無線機モードを設定するには、次の手順を実行します。

1. 指定した無線機（無線機 1 および無線機 2）インターフェイスの動作モードを設定します。

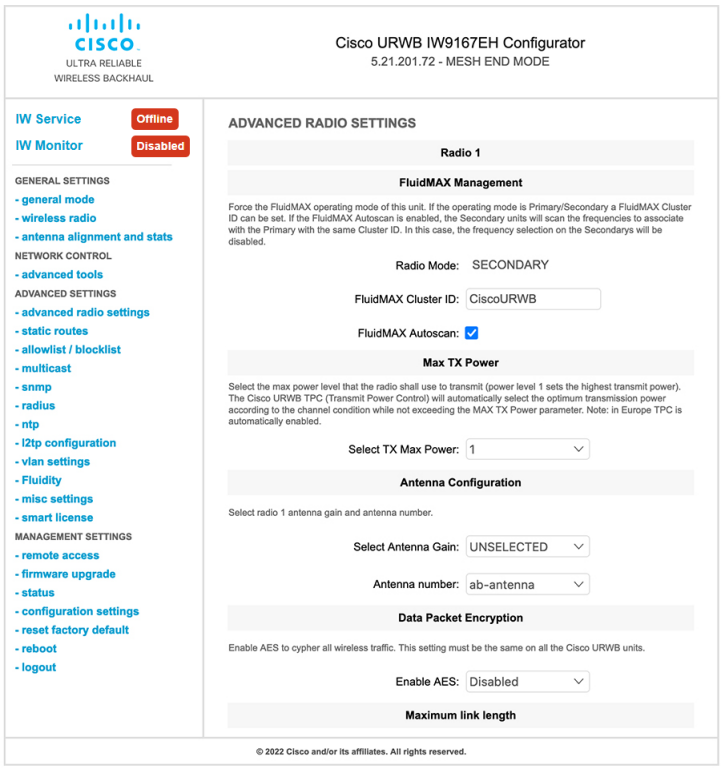


2. [WIRELESS RADIO] セクションで、[Radio 1] の [Role] で FluidMAX クラスタ ID を持つ [Fluidmax Primary] を選択します。このシナリオでは、プライマリの周波数選択が有効になり、セカンダリが無効になります。[ADVANCED RADIO SETTINGS] ウィンドウの [Max TX Power] セクションに移動し、[Select TX Max Power] ドロップダウンリストから電力レベル 1 を選択すると、URWB の送信電力制御（TPC）により自動的に最適な送信電力が選択されます。



（注） ヨーロッパでは、TPC は自動的に有効になります。

3. [WIRELESS RADIO] セクションで、[Radio 1] の [Role] で FluidMAX クラスタ ID を持つ [Fluidmax Secondary] を選択します。[ADVANCED RADIO SETTINGS] で、[FluidMAX Autoscan] チェックボックスをオンにすると、セカンダリデバイスは周波数を走査して、同じクラスタ ID を持つプライマリに関連付けます。この場合、セカンダリでの周波数選択は無効モードになります。[Max TX Power] セクションで、[Select TX Max Power] ドロップダウンリストから電力レベル 1 を選択すると、URWB の TPC により自動的に最適な送信電力が選択されます。



（注） ヨーロッパでは、TPC は自動的に有効になります。

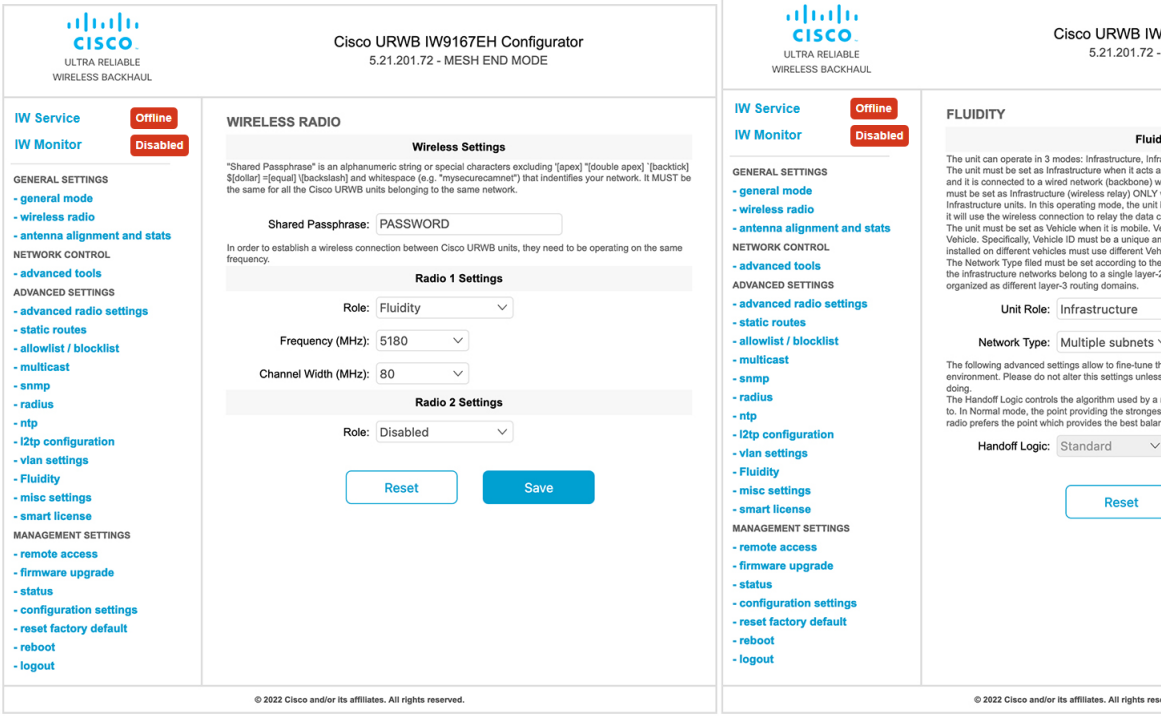
4. デバイスがモバイル車両のインフラストラクチャのエントリポイントとして機能する場合は、[Fluidity Settings] で、[Unit Role] ドロップダウンリストから [Infrastructure] を選択します。デバイスが他のインフラストラクチャ ユニットへのワイヤレス リレー エージェントとして使用される場合にのみ、ユニットロールに [Infrastructure (wireless relay)] を選択します。また、デバイスがモバイルである場合は、ユニットロールに [Vehicle] を選択します。

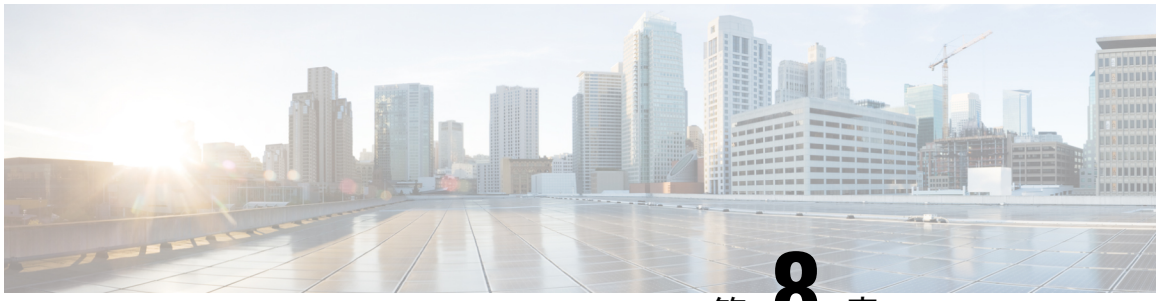
5. 一般的なネットワークアーキテクチャに基づいてネットワークタイプを選択します。

   1. ネットワークが単一のレイヤ2ブロードキャストドメインに属している場合は、[Network Type] ドロップダウンリストから [Flat] モードを選択します。

      または

   2. ネットワークが単一のレイヤ3ブロードキャストドメインに属している場合は、[Multiple subnets] を選択します。


CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
WIRELESS RADIO
Wireless Settings
"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
Shared Passphrase: PASSWORD
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.
Radio 1 Settings
Role: Fluidity
Frequency (MHz): 5180
Channel Width (MHz): 80
Radio 2 Settings
Role: Disabled
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.
FLUIDITY
Unit Role: Infrastructure
Network Type: Multiple subnets
Handoff Logic: Standard
Reset



第 8 章

IW Service Cluster

概要

IW Service Cluster

Cisco Industrial Wireless は、IoT デバイスやネットワークを監視および管理するために設計されたクラウドベースの IoT サービスプラットフォームです。IW Serviceの詳細については、「Introduction to Industrial Wireless」を参照してください。

リリース 17.15.1 より前の IW Service クラスタ

Cisco UIW リリース 17.15.1 より前は、IW Service クラスタを選択してアクセスするオプションはありませんでした。デフォルト設定は [auto] で、ユーザーは地理位置情報に基づいて米国または EU クラスタのいずれかにリダイレクトされます。たとえば、米国内のデバイスは US クラスタにリダイレクトされ、米国外のデバイスは EU クラスタにリダイレクトされます。

リリース 17.15.1 の IW Service クラスタ

Cisco UIW リリース 17.15.1 から、IW Service クラスタ URL を [Auto]、[EU]、または [US] オプションに設定できます。

CLI による IW Service クラスタの設定

手順

AP で IW Service クラスタを設定するには、次のコマンドを実行します。

Device#**iw-cluster** {**auto** | **us** | **eu**}

（注）
デフォルトでは、[auto] オプションが有効になっています。

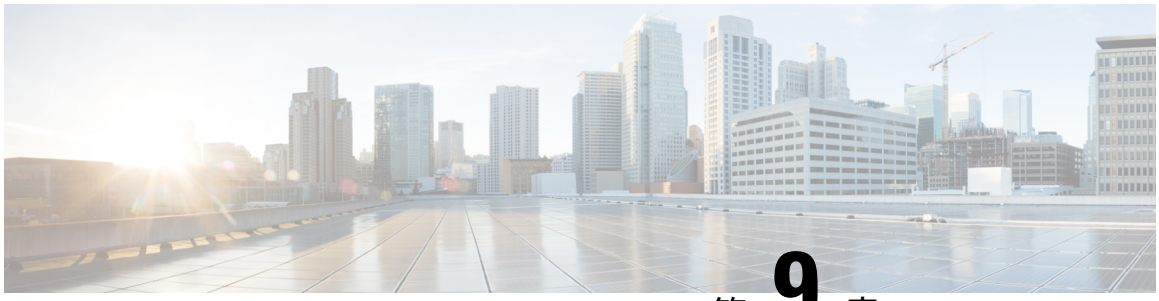
AP に必要なクラスタを設定したら、次の URL を使用して IW Service にアクセスします。

- [auto] の場合、device.ciscoiot.com を使用します。
- [us] の場合、us.ciscoiot.com を使用します。
- [eu] の場合、eu.ciscoiot.com を使用します。

IW Service クラスタの確認

IW Service クラスタの設定を確認するには、次のコマンドを実行します。

```
Device#show iw-service cluster configuration IW Service EU Cluster
```



第 9 章

無線アンテナ配置の設定

無線アンテナ配置の設定

Catalyst IW9167E は、複数のアンテナオプションをサポートするために、8 つの N 型メスコネクタを備えた 8 つの外部アンテナをサポートしています。アンテナポート 1、4、および 5 で、Self-Identifying Antenna（SIA）をサポートできます。無線機 1 はポート 1 ～ 4 に接続し、無線機 2 はポート 5 ～ 8 に接続します。アンテナの詳細については、「Antennas and Radios」を参照してください。

Catalyst IW9165E は、逆極性 SMA（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 と 2 に接続し、無線機 2 はアンテナポート 3 と 4 に接続します。アンテナポート 1 と 3 は SIA アンテナをサポートできます。

Catalyst IW9165D には指向性アンテナが内蔵されていて、N 型（f）コネクタで 2 つの外部アンテナをサポートしています。無線機 1 は内部アンテナに接続します。無線機 2 はアンテナポート 1 および 3 に接続します。アンテナポート 3 では、SIA アンテナをサポートできます。

以下の項では、さまざまな無線機モードの各アンテナのアンテナポートと利得を管理する CLI コマンドについて説明します。

アンテナ利得の設定

アンテナ利得を設定するには、次の CLI コマンドを使用します。

最大アンテナ利得値を、整数または文字列 UNSELECTED で設定します。

UNSELECTED の場合、バックグラウンドプロセスによって、サポートされている最小アンテナ利得が自動的に設定されます。

（注） SIA が接続されると、入力なしで利得が自動的に設定されます。

```
Device# configure dot11radio <interface> antenna gain <gain>
gain:
<1-19> antenna gain in dBi
WORD UNSELECTED
Device# write
```

送受信アンテナの設定

送信チェーンを設定するには、次の CLI コマンドを使用します。

（注） Catalyst IW9165 は abcd-antenna モードをサポートしていません。

```
Device# configure dot11radio <interface> antenna < A >
configure antenna chains (A) in use as follows
a-antenna - configure dot11 antenna a
ab-antenna - configure dot11 antenna ab
abcd-antenna - configure dot11 antenna abcd
Device# write
```

送信電力の設定

送信電力を設定するには、次の CLI コマンドを使用します。

最大送信電力レベルを設定します。AUTO の場合、バックグラウンドプロセスにより自動的に最大許容電力であるレベル 1 が設定されます。

（注） 8 が最も低い電力レベルで、1 が最も高い電力レベルです。

```
Device# configure dot11radio <interface> txpower-level <level>
txpower level:
<1-8> tx power level value
WORD AUTO
Device# write
```

URWB アンテナ別 RSSI 値の検証

Cisco UIW リリース 17.15.1 では、Catalyst IW9167E、IW9165E、および IW9165D アクセスポイントを対象とした、URWB アンテナ別の受信信号強度表示（RSSI）が導入されます。この機能を使用すると、アンテナごとに測定された RSSI 値を個別に表示できます。複数の RSSI 値によって、無線インターフェイス上の各アンテナが受信した信号強度を個別に監視できます。

たとえば、Catalyst IW9167E の各無線機に 4 つずつアンテナがある場合、4 つのアンテナそれぞれの RSSI を個別に確認できるようになりました。この詳しい情報は、障害対応のための貴重な情報であり、個々のアンテナまたはケーブルで発生する可能性のある問題を特定するのに役立ちます。各無線機チェーンの RSSI を調べることで、特定のアンテナの異常の有無、または他のアンテナと比較した特定のアンテナの性能の差異を判別できます。

表 *4 :* 無線機チェーンとアンテナポートのマッピング

アクセス ポイント（**Access Point**）	無線インターフェイス	無線機チェーン	アンテナ ポート
IW9167EH	1	[A、B、C、D]	[4、3、2、1]
	2	[A、B、C、D]	[5、6、7、8]
IW9165E	1	[A、B]	[1、2]
	2	[A、B]	[3、4]
IW9165D	2	[A、B]	[1、3]

手順

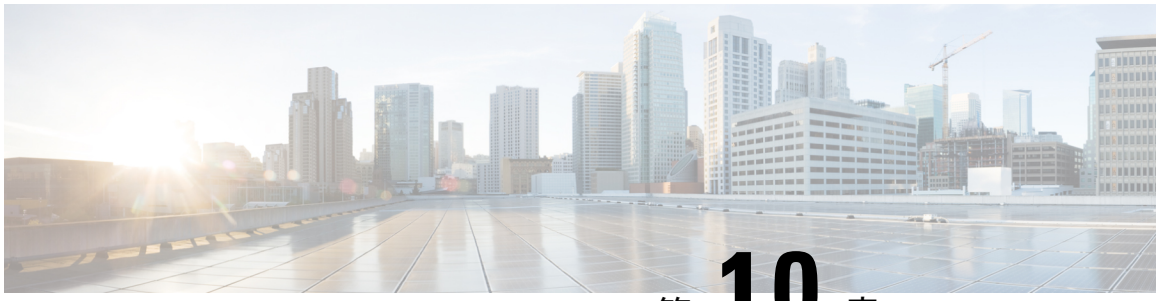
AP の個々のアンテナの RSSI を検証するには、次のコマンドを使用します。

```
Device#show dot11Radio <n> wifistats rssi
```

<n> を適切な無線機番号に置き換えます。

例：

```
Device#show dot11Radio 1 wifistats rssi
FC:58:9A:15:E4:D2
       MeshID 5.21.201.204 via R1
       rssi [-70, -69, -70, -71]
FC:58:9A:15:B9:12
       MeshID 5.21.200.80 via R1
       rssi [-70, -69, -70, -71]
```



第 10 章

有線インターフェイスの設定

有線インターフェイスの有効化と無効化

有線インターフェイスの設定はUIWリリース17.12.1から導入され、この機能により有線インターフェイスを無効にできます。両方の有線インターフェイスを同時に無効にすることはできません。CLIを使用して有線インターフェイスを有効にできます。

CLIを使用した有線インターフェイスの有効化または無効化

特定の有線インターフェイスを有効または無効にするには、次のCLIコマンドを使用します。

```
Device# configure wired <0-1>
                disabled disable wired interface
                enabled enable wired interface
```

例：

```
Device# configure wired 0 disabled
         Device# configure wired 1 enabled
         Device# write
         Device# reload
```

エラー処理設定

次のCLIコマンドは、両方のインターフェイスが無効モードとして設定されている場合にエラーを表示します。

```
Device # configure wired 0 disabled
         Device# configure wired 1 disabled
         ERROR: Interface wired0 is disabled, cannot disable both interfaces
```

CLIを使用した有線インターフェイスの有効化と無効化の確認

有線インターフェイスの有効状態または無効状態を確認するには、次のshowコマンドを使用します。

```
Device# #show wired <0-1> config
```

例：

```
Device# show wired 0 config
         WIRED0 status: enabled
Device# show wired 1 config
         WIRED1 status: disabled
```

最大伝送単位設定の設定

URWB ネットワークを介して転送できる最大フレームサイズを設定できます。この設定は、URWB ネットワーク内のすべてのアクセスポイントで設定する必要があります。

CLI を使用した MTU 設定の設定

有線インターフェイスの MTU 値を変更するには、次の CLI コマンドを使用します。

```
Device# configure wired mtu
         <1530-1600> Unsigned integer set wired mtu
```

例：

```
Device# configure wired mtu 1600
```

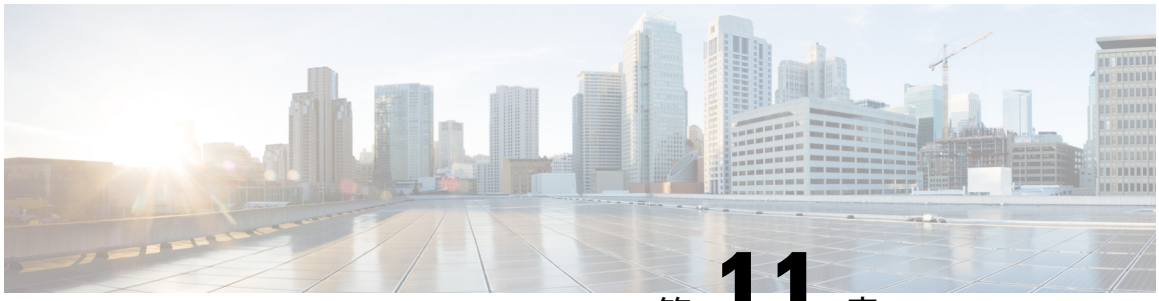
CLI を使用した MTU 設定の確認

有線インターフェイスの MTU 値を確認するには、次の show コマンドを使用します。

```
Device# show wired mtu
```

例：

```
Device# show wired mtu
         Configured MTU: 1600
```



第 11 章

SSH アクセスと Web UI アクセスの有効化または無効化

SSH アクセスの有効化

手順

ステップ 1 SSH へのアクセスを有効にするには、次のコマンドを使用します。

```
Device# configure ssh enable
```

ステップ 2 SSH が有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show ssh

SSH: enabled
```

SSH アクセスの無効化

手順

ステップ 1 SSH へのアクセスを無効にするには、次のコマンドを使用します。

```
Device# configure ssh disable
```

ステップ 2 SSH が無効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show ssh

SSH: disabled
```

Web UI アクセスの有効化

手順

ステップ 1 Web UI アクセスを有効にするには、次のコマンドを使用します。

```
Device# configure webui enable
```

ステップ 2 Web UI アクセスが有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show webui config

Web-UI: enabled
```

Web UI アクセスの無効化

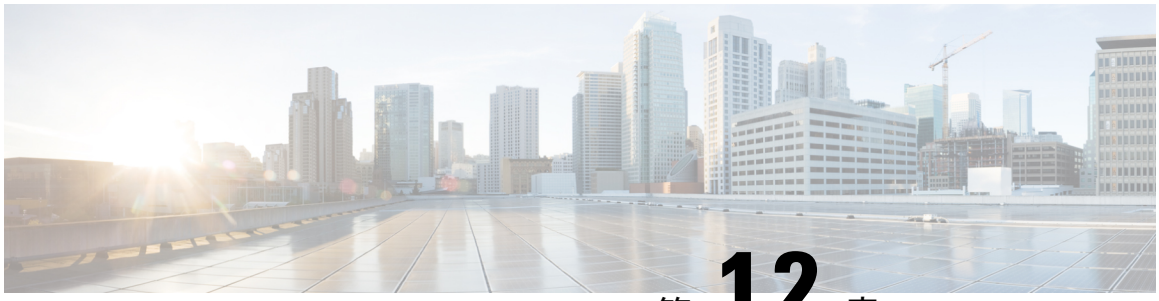
手順

ステップ 1 Web UI アクセスを無効にするには、次のコマンドを使用します。

```
Device# configure webui disable
```

ステップ 2 Web UI アクセスが無効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show webui config

Web-UI: disabled
```



第 12 章

無線チャネルと帯域幅の設定と検証

ライセンスの適用による米国およびカナダでの 4,900 ～ 4,990 MHz 周波数のサポート

UIW リリース 17.16.1 以降、Cisco Catalyst IW9167E、IW9165D、および IW9165E AP には、カナダ（-A）および米国（-B）のドメイン向けに、URWB モードでの 4.9 GHz 周波数帯域の追加サポートが導入されています。

-A および -B ドメインの 4.9 GHz 周波数帯域で動作する場合、デバイスは 5 MHz のチャネル間隔で 10 MHz および 20 MHz のチャネル帯域幅を使用します。

4.9 GHz の周波数帯域は無線スロット 1 とスロット 2 の両方で使用できますが、デフォルトでは無効になっています。

（注） -A および -B ドメインは、4.9 GHz での動作時に IEEE 802.11ax のレートをサポートしません。

表 *5 : 10 MHz* および *20 MHz* チャネル帯域幅でサポートされる *4.9 GHz* 周波数帯域

チャネル	チャネル帯域幅（10 MHz）	チャネル帯域幅（20 MHz）
11	4,945	該当なし
19	4,985	該当なし
20	4,950	4,950
21	4,955	4,955
22	4960	4960
23	4965	4965
24	4,970	4,970
25	4,975	4,975
26	4980	4980

4,900 ～ 4,990 MHz 周波数帯域の有効化

IW Service は、4.9 GHz 周波数帯域の有効化設定を AP に送信します。

AP で 4.9 GHz 周波数帯域を有効にするには、次の作業を実行します。

手順

ステップ 1 IW Service のクラウド管理またはオフラインの展開モードを使用して、4.9 GHz 周波数帯域の有効化を設定します。

IW Service から 4.9 GHz 帯域を有効にする設定方法の詳細については、「Introduction to Industrial Wireless」を参照してください。

ステップ 2 4,900 MHz 周波数帯域を有効または無効にします。

4,900 MHz 周波数帯域の有効または無効にするには、`configure dot11Radio <radio> 4.9G high-throughput` コマンドを使用します。

```
Device#configure dot11Radio <radio> 4.9G high-throughput

  disable  disable high-throughput and use 802.11a
  enable   enable hight-throughput (802.11ac/n) in low mode
```

例：

- `Device#configure dot11Radio 1 4.9G high-throughput enable`
- `Device#configure dot11Radio 1 4.9G high-throughput disable`

（注）

- 無効にすると、無線インターフェイスは 802.11a レートでのみ動作し、高出力プロファイルのロックが解除されます。
- 有効にすると、無線機がより高いレートで動作できるようになり、出力プロファイルは制限されます。

CLI を使用した動作チャネルの設定

（注） UIW リリース 17.15.1 以降、Cisco Catalyst IW9167E、IW9165D、および IW9165E AP は、-Q ドメイン（日本）の URWB モードで 4.9 Ghz 周波数帯域をサポートします。

4.9 Ghz 周波数帯域で動作する場合、デバイスは 20 MHz のチャンネル帯域幅のみをサポートします。

-Q ドメインは、4.9 GHz での動作時に 802.11ax のレートをサポートします。

表 *6 : 4.9 GHz* バンドでサポートされるチャンネルと周波数

チャネル番号	周波数（MHz）
184	4920
188	4940
192	4960
196	4980

動作チャンネルを設定するには、次に示すコマンドを使用します。

手順

ステップ 1 ワイヤレスデバイスの無線インターフェイス番号 <1 または 2> を設定します。

```
Device# configure dot11Radio <interface>
```

ステップ 2 動作チャンネル ID を設定します。

```
Device# configure dot11Radio [1|2] channel <1 to 256>
```

ステップ 3 特権 EXEC モードに戻ります。

```
Device(configure dot11Radio [1|2] channel <1 to 256>)# end
```

CLI によるチャネル帯域幅の設定

1. 無線インターフェイス番号 <1 または 2> でワイヤレスデバイスを設定します。

   ```
   Device#configure dot11Radio <interface>
   ```

2. チャンネル帯域幅を MHz で設定します。

   - 無線機 1 は、20、40、80 MHz の帯域幅をサポートします。
   - 無線機 2 は、20、40、80、160 MHz の帯域幅をサポートします。

   ```
   Device#configure dot11Radio [1|2] band-width [20|40|80|160]
   ```

3. 特権 EXEC モードに戻ります。

   ```
   Device (configure dot11Radio [1|2] band-width [20|40|80|160])#end
   ```

CLI による動作チャネルと帯域幅の検証

無線チャネルと帯域幅を検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio <interface> config
```

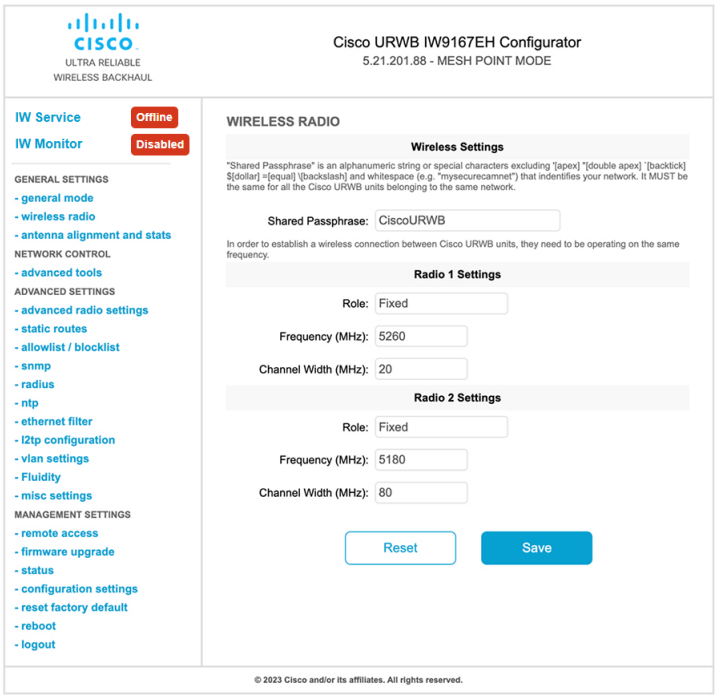
例：

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz

Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
Channel : 157
Channel width : 40 MHz
```

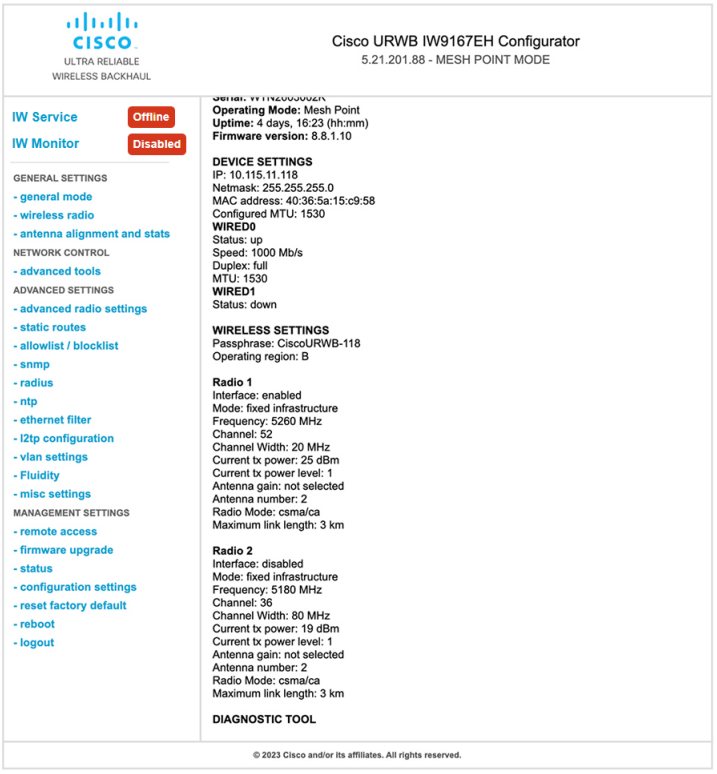
GUI による無線チャネルと帯域幅の設定

GUI を使って無線チャンネルと帯域幅を設定するには、動作チャンネル ID、無線機モード（Fluidity または固定インフラストラクチャ）、無線周波数の範囲と帯域幅を設定します。

次の画像は、無線チャンネルと帯域幅の設定を示しています。



次の画像は、無線チャンネルと帯域幅の設定のステータスと、各ワイヤレスインターフェイスに固有の情報を示しています。



VLAN 設定の設定

アクセスポイントのデフォルトの VLAN 設定パラメータは次のとおりです。

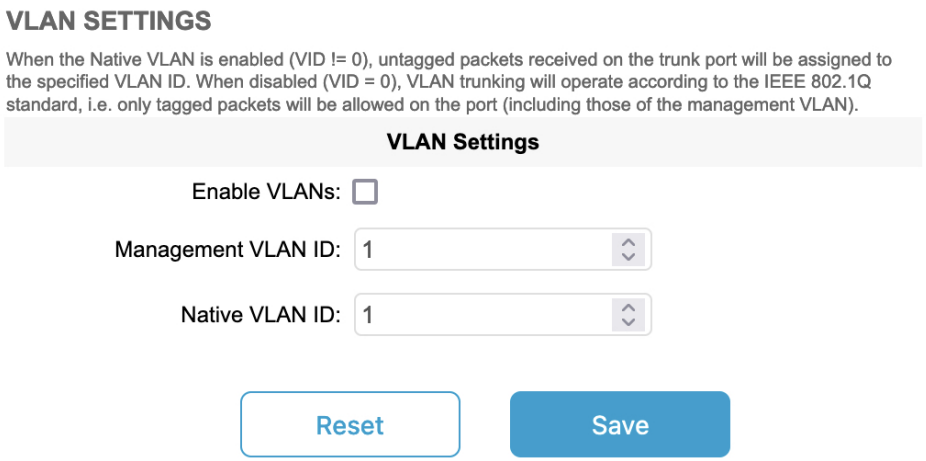
パラメータ	デフォルト値
Management VLAN ID（MVID）	1
Native VLAN ID（NVID）	1

アクセスポイントをローカル ワイヤレス ネットワークの一部である VLAN に接続するには、次の手順を実行します。

手順

ステップ 1 [ADVANCED SETTINGS] で、[vlan settings] をクリックします。

[VLAN SETTINGS] ウィンドウが表示されます。



ステップ 2 [Enable VLANs] チェックボックスをオンにして、アクセスポイントをローカル ワイヤレス ネットワークの一部である VLAN に接続します。

ステップ 3 [Management VLAN ID] フィールドに、管理 VLAN の識別番号を入力します。VLAN 設定とパケット管理の詳細については、「パケット管理の規則」を参照してください。

（注）
同じメッシュネットワークの一部であるすべてのアクセスポイントで、同じ [Management VLAN ID] を使用する必要があります。

ステップ 4 [Native VLAN ID] フィールドに、ネイティブ VLAN の識別番号を入力します。

ステップ 5 [Save] をクリックします。

パケット管理の規則

トラフィック管理

着信データパケットは、次のパラメータ値に基づいて分類されます。

スマートモードのアクセスポイントにおける着信パケットのアクセスポートルール管理	
タグなしパケット	ネイティブ VLAN がオンの場合、パケットは許可される（NVID でタグ付け） ネイティブ VLAN がオフの場合、パケットは破棄される
タグ付きパケット（すべての VID、チェックなし）	パケットは元のタグ付きで許可される

スマートモードのアクセスポイントにおける発信パケットのアクセスポートルール管理	
アクセスポイントからのパケット（例：IW Service インターフェイス）	MVID でタグ付けされたパケット
シグナリング トラフィック	MVID でタグ付けされたパケット
有効な VID（1 ～ 4094）でタグ付けされているが、NVID のタグなし	パケットは許可される（タグ付き）
null VID（0）または NVID のタグ付き	パケットは許可される（タグなし）

（注） Cisco VIC SFP+インターフェイスを介して送信されるパケットは、常に VLAN ヘッダーでタグ付けされます。このインターフェイスが送信する発信パケットは、VLAN ID タグが 0 の IEEE 802.1p ヘッダー付きのタグなしに分類されます。

GUI を使用した Fluidity の設定

GUI を使って Fluidity モードを設定するには、以下のシナリオに従います。

1. [GENERAL SETTINGS] で、[wireless radio] をクリックします。

   [WIRELESS RADIO] ウィンドウが表示されます。

2. 無線機モードには、[Role] ドロップダウンリストから [Fluidity] を選択します。

無線機のロールで [Fluidity] を選択したら、[Fluidity] 設定に移動します。Fluidity に移動するには、次の手順を実行します。

1. [ADVACED SETTINGS] で、[Fluidity] をクリックします。

   [FLUIDITY] ウィンドウが表示されます。

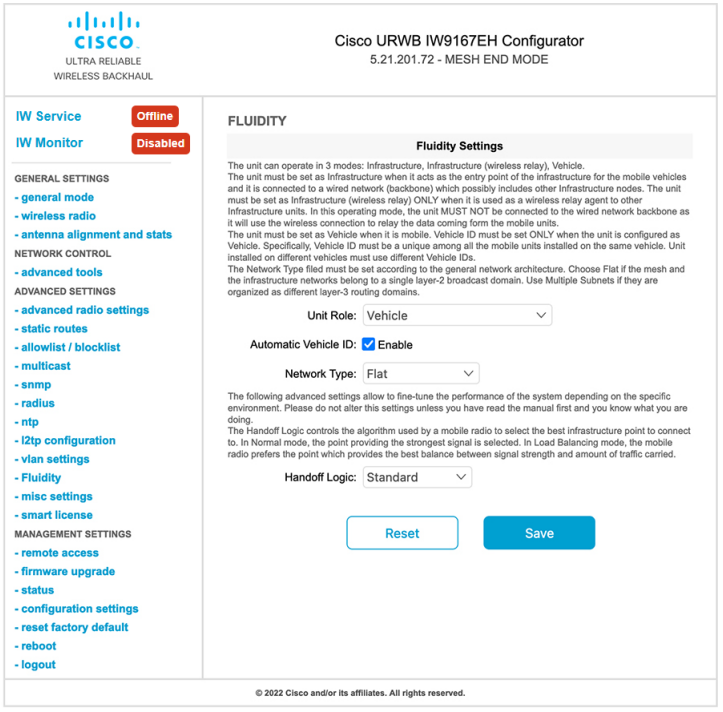
2. [Fluidity Settings] で、ドロップダウンリストから [Unit Role] を選択します。デバイスロールを次のいずれかのモードにします。

   - Infrastructure
   - Infrastructure (wireless relay)
   - Vehicle

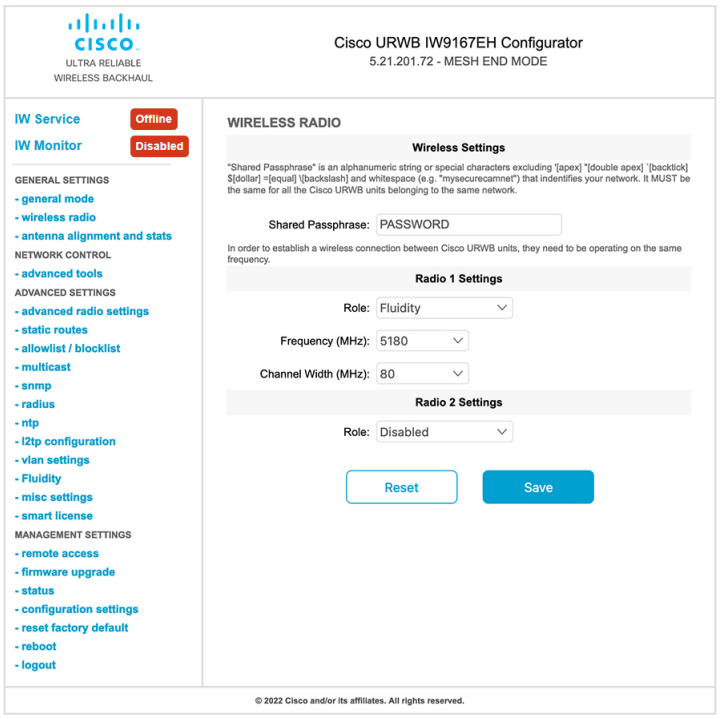
（注）

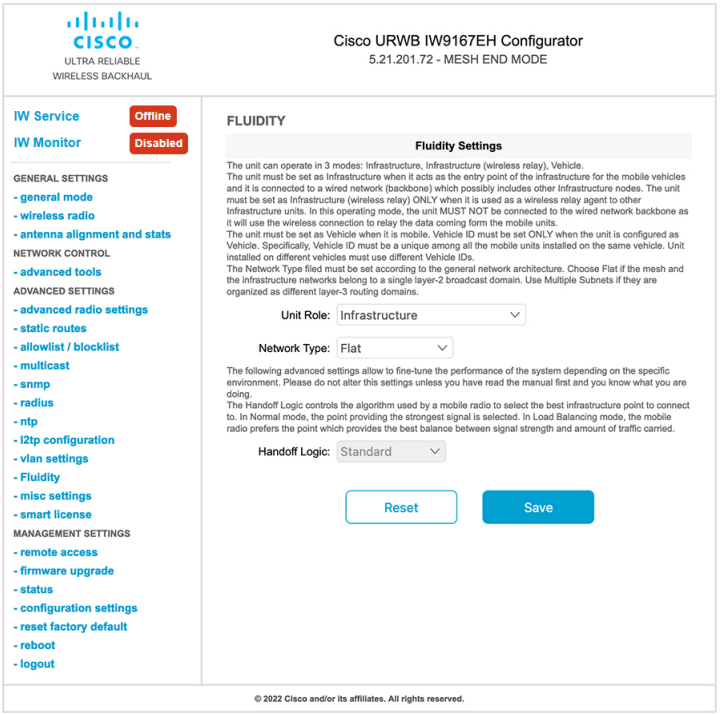
- 車両 ID は、同じ車両にインストールされているすべてのモバイルデバイス間で一意である必要があります。
- 異なる車両にインストールされているデバイスが異なる車両 ID を使用する必要がある場合。

3. モバイルユニットの車両 ID を自動設定するには、[Automatic Vehicle ID] チェックボックスをオンにします。

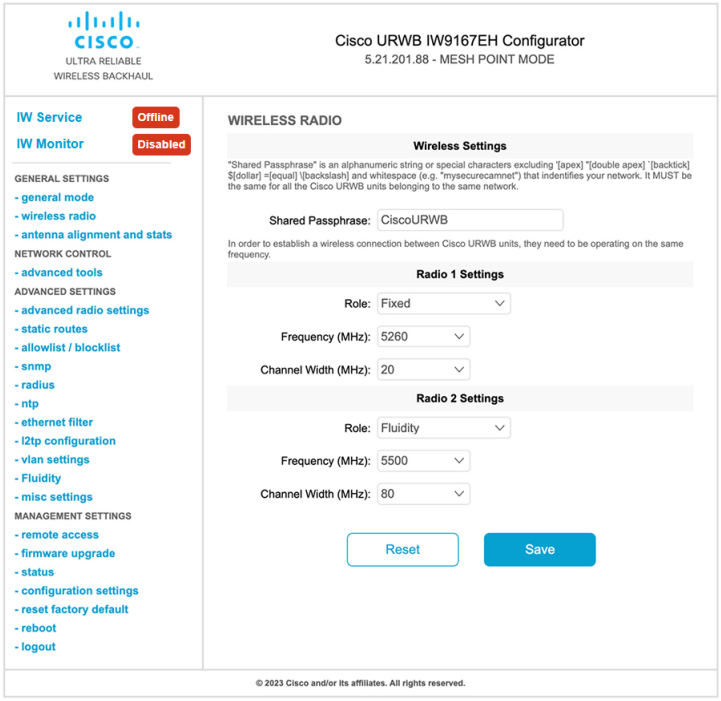


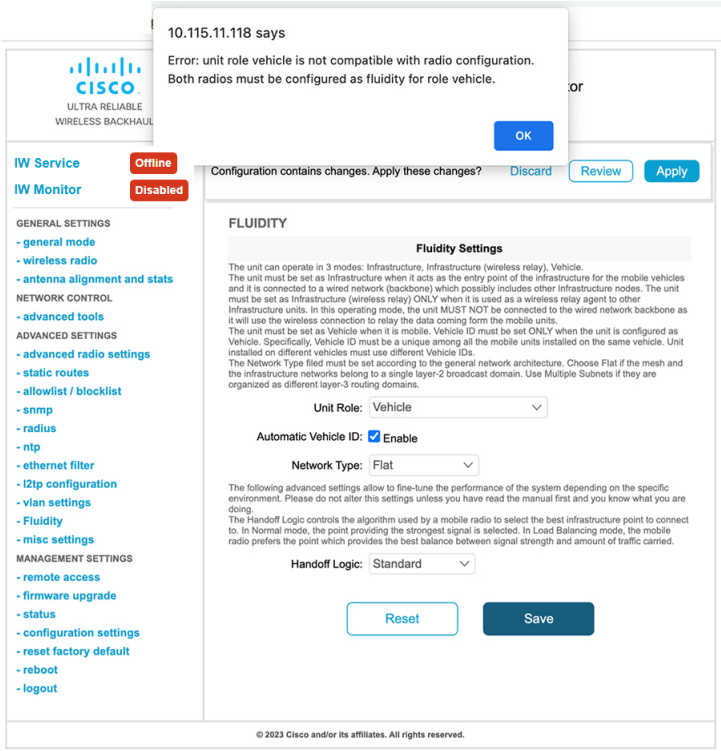
次のFluidity設定では、ワイヤレスインターフェイスのデバイスロールがインフラストラクチャモードに設定されています。





次の画像は、ロールが [Vehicle] の場合、両方の無線を [Fluidity] に設定する必要があることを示しています。一方のワイヤレスインターフェイスが固定モードに設定され、もう一方が [Fluidity] モードに設定されている場合、ユニットロールに [Vehicle] は選択できません。


Cisco URWB IW9167EH Configurator
5.21.201.88 - MESH POINT MODE
ULTRA RELIABLE
WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
WIRELESS RADIO
Wireless Settings
"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] ${[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
Shared Passphrase: CiscoURWB
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.
Radio 1 Settings
Role: Fixed
Frequency (MHz): 5260
Channel Width (MHz): 20
Radio 2 Settings
Role: Fluidity
Frequency (MHz): 5500
Channel Width (MHz): 80
Reset
Save
© 2023 Cisco and/or its affiliates. All rights reserved.


10.115.11.118 says
Error: unit role vehicle is not compatible with radio configuration.
Both radios must be configured as fluidity for role vehicle.
OK
Configuration contains changes. Apply these changes?
Discard
Review
Apply
FLUIDITY
Fluidity Settings
The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.
Unit Role: Vehicle
Automatic Vehicle ID: Enable
Network Type: Flat
The following advanced settings allow to fine-tune the performance of the system depending on the specific environment. Please do not alter this settings unless you have read the manual first and you know what you are doing.
The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to connect to. In Normal mode, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.
Handoff Logic: Standard
Reset
Save
© 2023 Cisco and/or its affiliates. All rights reserved.

CLI を使用した Fluidity の設定

Fluidity を有効にするには、次の CLI コマンドを使用します。

（注） 少なくとも 1 つの無線インターフェイスを Fluidity モードにする必要があります。

```
Device# configure dot11Radio <interface> mode fluidity
```

無線機 1 の Fluidity を有効にする場合の例：

```
configure dot11Radio 1 mode fluidity
```

目的の Fluidity ロールが車両の場合、両方の無線機を Fluidity モードにする必要があります。

```
configure dot11Radio 1 mode fluidity
configure dot11Radio 2 mode fluidity
```

CLI を使用した Fluidity ロールの設定

Fluidity ロール（インフラストラクチャまたはクライアント）を設定するには、次の CLI コマンドを使用します。

1. Fluidity ロール（インフラストラクチャまたはモバイル）の設定

   ```
   Device# configure fluidity id
   ```

2. Fluidity ID モードを設定します。

   ```
   Device# configure fluidity id {mode}
   Mode is one of the following values
   vehicle-auto - vehicle mode with automatic vehicle ID selection
   vehicle ID - (alphanumeric) vehicle mode with manual ID.
   infrastructure - infrastructure mode
   wireless-relay - wireless infrastructure with no ethernet connection to the backhaul
   ```

3. この設定を終了するには、次の CLI コマンドを使用します。

   ```
   Device (configure fluidity id {mode}) # end
   ```

   ```
   Device# wr
   ```

   例：

   ```
   Device# configure fluidity id [vehicle-auto | infrastructure | vehicle-id |
   wireless-relay]
   ```

Fluidity の色分けの設定

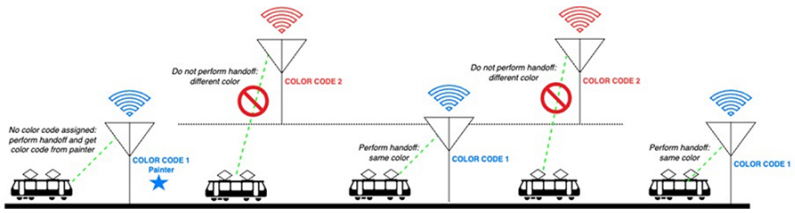
Fluidity の色分けは、UIW リリース 17.12.1 から導入されました。Fluidity の色分けを使用すると、沿線または外部のデバイス（Fluidityインフラストラクチャデバイス）に特定のカラーコー

ドを指定して、ハンドオフプロセスを向上または促進できます。標準設定では、受信信号強度表示（RSSI）に基づいてハンドオフの決定が行われます。

一般的な使用例：列車が線路の片側を一方向に移動していて（単一のトンネルを線路の両方向に使用する地下鉄路線）、トンネルの反対側にあるアクセスポイントに接続する必要がない場合は、反対側の線路にあるインフラストラクチャデバイスにごく稀にハンドオーバーされないようにするために、各側のアクセスポイントを異なる色でマーク付けします。

Fluidity の色分けロジック

次の図は、Fluidity の色分けロジックを説明しています。ペインタは、沿線または外部デバイス（Fluidity インフラストラクチャ デバイス）の重要なロールです。



Fluidity の色分けのプロセスは次のとおりです。

- ペインタが、カラーコードに基づいて、どの Fluidity インフラストラクチャ デバイスがハンドオフに適しているかを Fluidity 車両デバイスに通知します。
- Fluidity 車両デバイスは、ペインタを検出するまで、色の設定を無視し（RSSI レベルに基づく）標準のハンドオフメカニズムを使用し続けます。
- Fluidity 車両デバイスがペインタ設定を持つ Fluidity インフラストラクチャ デバイスでのハンドオフを完了すると、同じカラーコードを持つ Fluidity インフラストラクチャ デバイスまたは他のペインタを持つ Fluidity インフラストラクチャ デバイスのみが考慮されるようになります。
- 複数の Fluidity インフラストラクチャ デバイスをペインタとして機能させることができます。

次の表では、Fluidity の色のロールと対応するオプションについて説明します。

表 *7 : Fluidity* の色分けロール

Fluidity の色分けロール	オプション
沿線ペインタ（Fluidity インフラストラクチャ デバイス）	ペインタとして設定された Fluidity インフラストラクチャ デバイスには、1 つのカラーコードのみを割り当てることができます
沿線標準（Fluidity インフラストラクチャ デバイス）	ペインタ以外の Fluidity インフラストラクチャ デバイスには、複数のカラーコードを設定できます

Fluidity の色分けロール	オプション
Fluidity 車両	Fluidity 車両デバイスには、1 つの色のみを割り当てることができます

CLI を使用した Fluidity の色分けの設定

Fluidity カラーモードを設定するには、次の CLI コマンドを使用します。

```
Device# configure fluidity color mode
                Disabled: disable coloring
                Enabled: enable coloring

Device# configure fluidity color value
WORD quoted list of colors from 1 to 7 or "p X" for painter (for example: "1 2 6","4",
"p 1"). "clear" to reset
```

例（ペインタ）：

```
Device# configure fluidity color mode enabled
Device# configure fluidity color value "p 1"
Device# write
Device# reload
```

例（ペインタ以外）：

```
Device# configure fluidity color mode enabled
Device# configure fluidity color value "3 4 5"
Device# write
Devie# reload
```

例（クリア）：

```
Device# configure fluidity color value clear
```

CLI を使用した Fluidity の色分けの確認

Fluidity カラーモードを確認するには、次の show コマンドを使用します。

```
Device# #show fluidity config
```

例（ペインタ）：

```
Device# show fluidity config
                ...
                Color: enabled, current: p 1
                ...
```

例（ペインタ以外）：

```
Device# show fluidity config
                ...
                Color: enabled, current: 3 4 5
                ...
```

例（クリア）：

```
Device# show fluidity config
                ...
                Color: enabled, current: 0
                ...
```

Fluidity の色分けの RSSI しきい値の設定

カバレッジホールがあり、現在の RSSI が設定された RSSI しきい値よりも小さい場合、Fluidity 車両デバイスは Fluidity の色分け設定を一時的に無視します。この場合、Fluidity 車両デバイスは、現在のカラーコードを持つ Fluidity インフラストラクチャ デバイスからハンドオフを受信するまで、Fluidity の色分け設定を維持し、色分け設定を無視します。Fluidity 車両デバイスは、現在の値とは異なるカラーコードを持つ Fluidity インフラストラクチャ デバイスで 4 回連続してハンドオフした後に、Fluidity の色分け設定をデフォルト値（色なし）にリセットします。

CLI を使用した Fluidity の色分けの RSSI しきい値の設定

```
Device# configure fluidity color rssi-threshold
         <0-96> COLOR_RSSI_THRESHOLD
```

例：

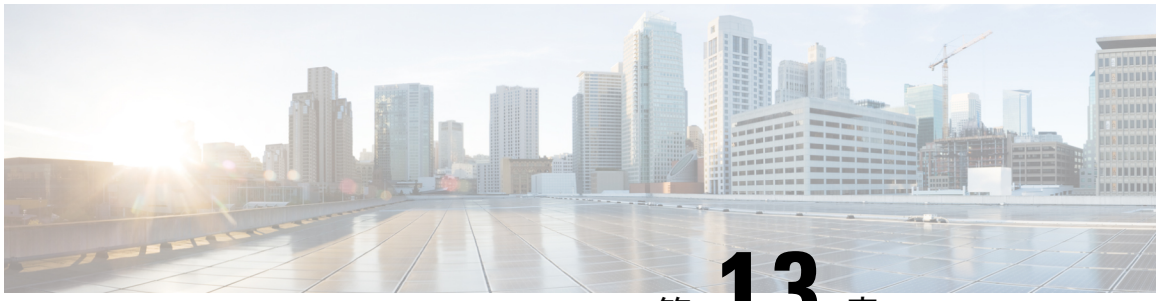
```
Device# configure fluidity color rssi-threshold 55
```

CLI を使用した Fluidity の色分けの RSSI しきい値の確認

```
Device# show fluidity config
```

例：

```
Device# show fluidity config
                 ...
                 Color: enabled, current: 0
                 Color min RSSI threshold: 55
```



第 13 章

High Efficiency の設定と検証（802.11 ax）

High Efficiency の設定と検証

High Efficiency（HE）が有効になっている場合、802.11ac との後方互換性があります。802.11ax HE を有効または無効にするために、次のリストがサポートされています。

- URWB HE は、スロット 1 で 20、40、80 MHz の帯域幅をサポートします。
- URWB HE は、スロット 2 で 20、40、80、160 MHz の帯域幅をサポートします。
- URWB HE はデフォルト設定では無効になっています。
- HE ネゴシエーションは、HE が有効になっているデバイス間でのみサポートされます。

HE モードを有効にするには、次の CLI コマンドを使用します。

```
Device# configure dot11Radio [1|2] high-efficiency enable
```

maxmcs を 11 に設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11Radio [1|2] mcs maxmcs 11 <mcs index in integer or string>
```

（注） デフォルトの maxmcs は 9 です。

HE モードを無効にするには、次の CLI コマンドを使用します。

```
Device# configure dot11Radio [1|2] high-efficiency disable
default maxmcs is 9.
```

HE モードを検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio 1 config
Maximum tx mcs : 9
High-Efficiency : Enabled
Maximum tx nss : 2
RTS Protection : disabled
guard-interval : 800ns
```

```
Device# show dot11Radio 2 config
Maximum tx mcs : 9
High-Efficiency : Enabled
Maximum tx nss : 2
RTS Protection : disabled
guard-interval : 800ns
```

```
Device# show eng-stats
```

WLAN1 Rx：

```
FC:58:9A:16F8:52 rate 1201 MCS 11/2 HE80/G1(800ns) ssn 48 rssi-48 received
```

WLAN1 Tx：

```
FC:58:9A:16F8:52 rate 1201 MCS 11/2 HE80/G1(800ns) sent 195612 failed 0
```

WLAN2 Rx：

```
FC:58:9A:16F8:13 rate 1201 MCS 11/2 HE80/G1(800ns) ssn 50 rssi-46 received
```

WLAN2 Tx：

```
FC:58:9A:16F8:13 rate 864 MCS 11/2 HE80/G1(800ns) sent 390797 failed 1
```

GUI を使用したグローバルゲートウェイの設定

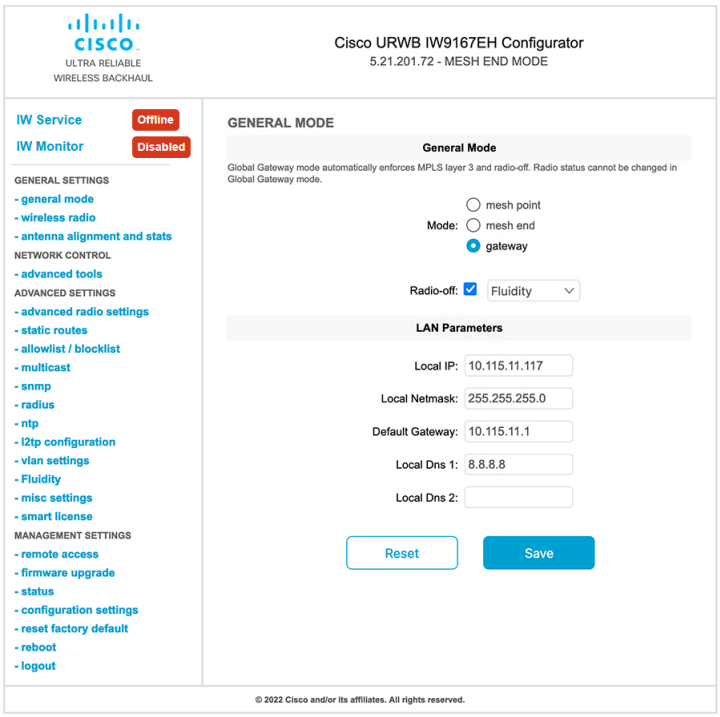
グローバル ゲートウェイ モードでは、MPLS レイヤ 3 が自動的に適用されます。このモードでは、無線機オフと無線機ステータスは変更できません。

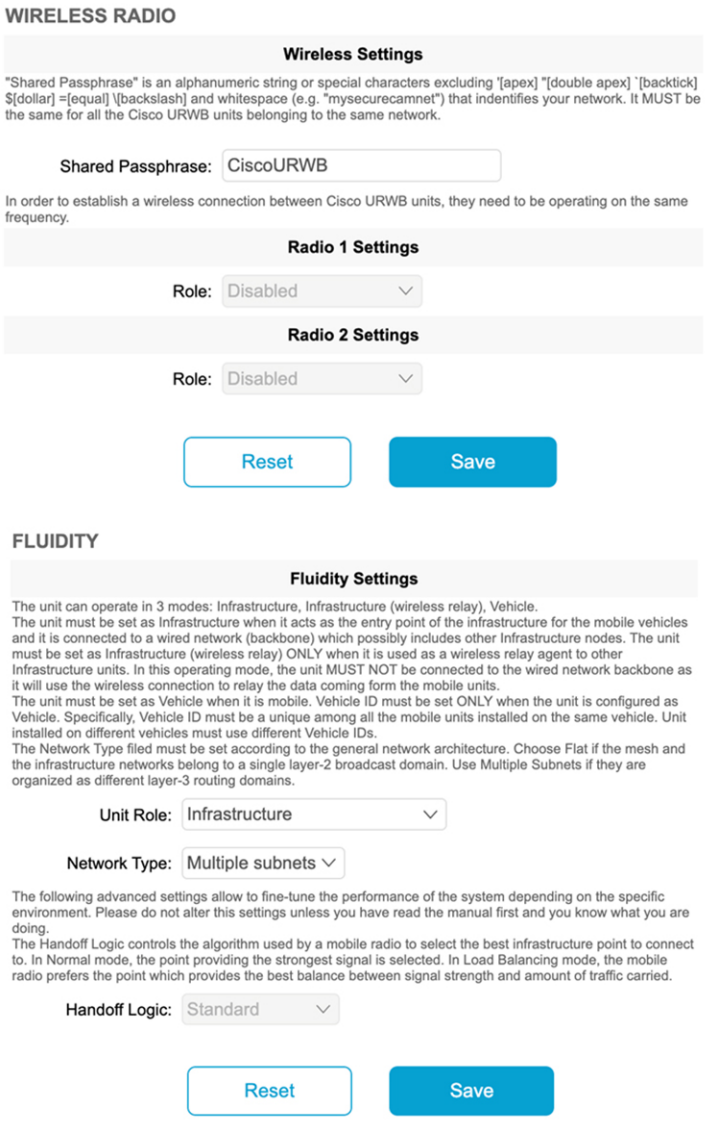
1. [GENERAL SETTINGS] で、[general mode] をクリックします。

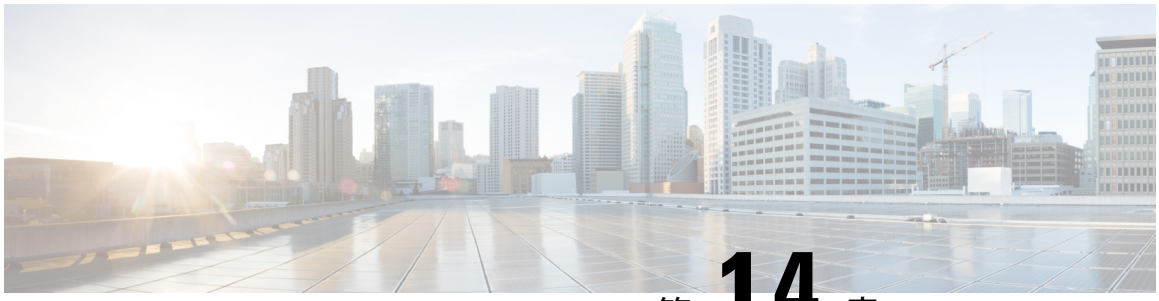
   [GENERAL MODE] ウィンドウが表示されます。

2. [Mode] で [gateway] をクリックします。

次の画像は、グローバル ゲートウェイ モードの GUI 設定を示しています。


CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
GENERAL MODE
General Mode
Global Gateway mode automatically enforces MPLS layer 3 and radio-off. Radio status cannot be changed in Global Gateway mode.
Mode:
mesh point
mesh end
gateway
Radio-off:
Fluidity
LAN Parameters
Local IP:
10.115.11.117
Local Netmask:
255.255.255.0
Default Gateway:
10.115.11.1
Local Dns 1:
8.8.8.8
Local Dns 2:
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.


WIRELESS RADIO
Wireless Settings
"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
Shared Passphrase: CiscoURWB
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.
Radio 1 Settings
Role: Disabled
Radio 2 Settings
Role: Disabled
Reset
Save
FLUIDITY
Fluidity Settings
The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.
Unit Role: Infrastructure
Network Type: Multiple subnets
The following advanced settings allow to fine-tune the performance of the system depending on the specific environment. Please do not alter this settings unless you have read the manual first and you know what you are doing.
The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to connect to. In Normal mode, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.
Handoff Logic: Standard
Reset
Save



第 14 章

HE（High Efficiency）のガード間隔の設定

HE（High Efficiency）のガード間隔の設定

ガード間隔を長くすると、長距離の屋外展開でリンクの信頼性が向上します。ガード間隔などの機能は、URWB スタックをサポートしています。

ガード間隔を設定するには、次の CLI コマンドを使用します。

```
Device# configure dot11Radio [interface] guard-interval [gi]
```

gi：ガード間隔の値は次のとおりです。

1600：1600 ns のガード間隔を設定します（HE モードでのみサポートされる）

3200：3200 ns のガード間隔を設定します（HE モードでのみサポートされる）

400：400 ns のガード間隔を設定します（HT および VHT モードでサポートされる）

800：800 ns のガード間隔を設定します（デフォルトガード間隔モードと HT、VHT、HE での無効モード）

例：

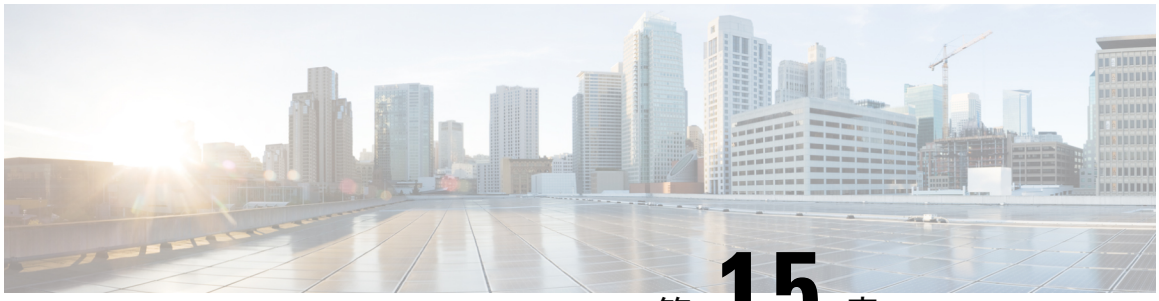
```
Device# configure dot11Radio 1 high-efficiency enable

Device# configure dot11Radio 1 guard-interval 1600

Device# configure dot11Radio 1 guard-interval 3200

Device# wr
```

ガード間隔を検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio 1 config
Maximum tx mcs: 9
High-efficiency : enabled
Maximum tx nss : 2
RTS protection : disabled
guard-interval : 1600 ns

Device# show dot11Radio 2 config
Maximum tx mcs: 9
High-efficiency : enabled
Maximum tx nss : 2
```

HE（High Efficiency）のガード間隔の設定

```
RTS protection : disabled
guard-interval : 3200 ns
```



第 15 章

SNMP の設定と検証

SNMP の設定と検証

Simple Network Monitoring Protocol（SNMP）アプリケーションは URWB ソフトウェアで使用され、ネットワーク管理機能を実現します。

SNMP クライアントは、SNMP エージェントに要求を送信します。SNMP エージェントは、この要求をサブエージェントに渡します。サブエージェントは SNMP エージェントに応答します。SNMP エージェントは SNMP 応答パケットを作成し、それを要求の発信元であるリモートネットワーク管理ステーションに送信します。

図 *1 : SNMP* プロセス

CLI による SNMP の設定

SNMP を設定するには、次の CLI コマンドを使用します。

（注）
- SNMP 設定用に変更された SNMP CLI ロジックでは、CLI を使用して SNMP 機能を有効にする前に、すべての SNMP パラメータを設定する必要があります。
- SNMP 機能を無効にすると、関連するすべての設定が自動的に削除されます。

SNMP 機能を無効にするには、次の CLI コマンドを使用します。

```
Device#configure snmp [enable | disable]
```

SNMP のプロトコルバージョンを指定するには、次の CLI コマンドを使用します。

```
Device#configure snmp version {v2c | v3}
```

SNMP v2c コミュニティ ID の番号を指定するには（SNMP v2c のみ）、次の CLI コマンドを使用します。

```
Device#configure snmp v2c community-id <length 1-64>
```

SNMP v3 ユーザー名を指定するには（SNMP v3 のみ）、次の CLI コマンドを使用します。

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

SNMP v3 ユーザーパスワードを指定するには（SNMP v3 のみ）、次の CLI コマンドを使用します。

```
Device#configure snmp v3 password <length 8-64>
```

SNMP v3 認証プロトコルを指定するには（SNMP v3 のみ）、次の CLI コマンドを使用します。

```
Device#configure snmp auth-method <md5|sha>
```

SNMP v3 暗号化プロトコルを指定するには（SNMP v3 のみ）、次の CLI コマンドを使用します。

```
Device#configure snmp encryption {des | aes | none}
```

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

SNMP v3 暗号化パスフレーズを指定するには（SNMP v3 のみ）、次の CLI コマンドを使用します。

```
Device#configure snmp secret <length 8-64>
```

SNMP 定期トラップ設定を指定するには、次の CLI コマンドを使用します。

```
Device#configure snmp periodic-trap {enable | disable}
```

定期 SNMP トラップの通知トラップ期間を指定するには、次の CLI コマンドを使用します。

```
Device#configure snmp trap-period <1-2147483647>
```

通知値トラップ期間は分単位です。

SNMP イベントトラップを有効または無効にするには、次の CLI コマンドを使用します。

```
Device#configure snmp event-trap {enable | disable}
```

SNMP NMS ホスト名または IP アドレスを指定するには、次の CLI コマンドを使用します。

```
Device#configure snmp nms-hostname {hostname |Ip Address}
```

SNMP 設定を無効にするには、次の CLI コマンドを使用します。

```
Device#configure snmp disabled
```

SNMP を無効にすると、ログイン情報を含むすべての機密情報がクリアされます。SNMP を有効にするには、有効な値をすべて再度指定する必要があります。

SNMP の設定例：

SNMP v2 の CLI：

```
Device#configure snmp v2 community-id <length 1-64>
Device#configure snmp nms-hostname hostname/Ip Address
Device#configure snmp trap-period <1-2147483647>
Device#configure snmp periodic-trap enable/disable
Device#configure snmp event-trap enable/disable
```

```
Device#configure snmp version v2c
Device#configure snmp enabled
```

SNMP v3 の CLI：

```
Device #configure snmp nms-hostname hostname/Ip Address
Device#configure snmp trap-period <1-2147483647>
Device#configure snmp v3 username <length 32>
Device#configure snmp v3 password <length 8-64>
Device#configure snmp auth-method <md5|sha>
Device#configure snmp encryption <aes|des|none>
Device#configure snmp secret <length 8-64>
Device#configure snmp periodic-trap enable/disable
Device#configure snmp event-trap enable/disable
Device#configure snmp version v3
Device#configure snmp enabled
```

CLI による SNMP の検証

SNMP を検証するには、次の show コマンドを使用します。

```
Device# show snmp
SNMP: enabled
Version: v3
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show snmp
SNMP: enabled
Version: v2c
Community ID: test
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show system status snmpd
Service Status
Service Name : snmpd
Loaded : loaded
Active : active (running)
Main ProcessID : 6437
Running Since : Mon 2022-09-19 14:45:27 UTC; 3h 34min ago
Service Restart : 0
```

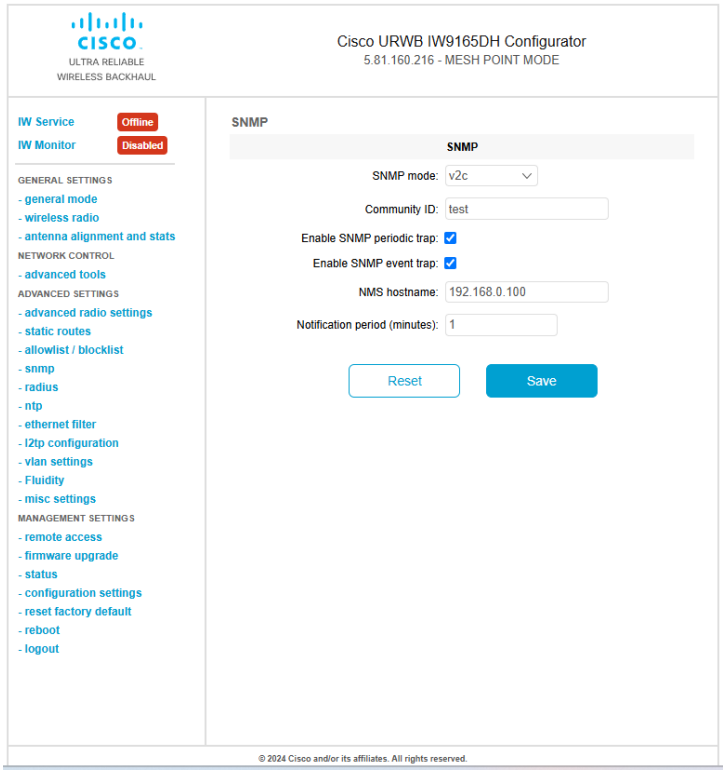
GUI を使用した SNMP バージョン v2c の設定

デフォルトでは、工場出荷時のアクセスポイントの SNMP モードは無効になっています。

アクセスポイントの SNMP モードをバージョン **v2c** に変更し、アクセスアクセスポイントを設定するには、次の手順を実行します。

手順

ステップ 1 [SNMP mode] ドロップダウンリストから [v2c] を選択します。
[SNMP] ウィンドウが表示されます。



ステップ 2 [Community ID] フィールドにコミュニティ識別子の値を入力します。

重要
ネットワーク内のすべてのアクセスポイントに、同じコミュニティ識別子の値を設定する必要があります。

ステップ 3 [Enable SNMP event trap] チェックボックスをオンにして、重要なシステム関連イベントの SNMP イベントトラップを有効にし、[NMS hostname] フィールドにネットワーク管理ステーション（NMS）のホスト名を入力します。

重要
トラップの送信先となる NMS ホストには、SNMP v2c トラップを収集するように設定された SNMP エージェントが必要です。

ステップ 4 [Enable SNMP periodic trap] チェックボックスをオンにして、定期的な SNMP トラップを有効にし（定義された一定の間隔で SNMP トラップが送信されます）、[NMS hostname] フィールドに NMS のホスト名を入力します。[Notification period] に通知期間（分単位）を入力します。

ステップ 5 [Save] をクリックします。

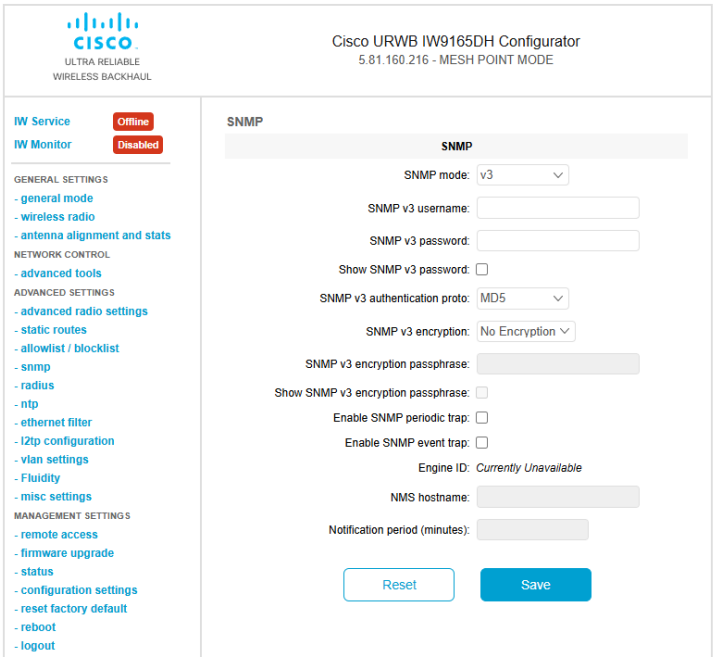
GUI を使用した SNMP バージョン v3 の設定

デフォルトでは、工場出荷時のアクセスポイントの SNMP モードは無効になっています。

アクセスポイントの SNMP モードをバージョン **v3** に変更し、アクセスアクセスポイントを設定するには、次の手順を実行します。

手順

ステップ 1 [SNMP mode] ドロップダウンリストから [v3] を選択します。
[SNMP] ウィンドウが表示されます。



ステップ 2 [SNMP v3 username] フィールドに SNMP v3 ユーザー名を入力します。

（注）
ネットワーク内のすべてのアクセスポイントに、同じ SNMP v3 ユーザー名を設定する必要があります。

ステップ 3 現在の SNMP v3 パスワードを変更するには、[SNMP v3 password] フィールドに新しいパスワードを入力します。

ステップ 4 [SNMP v3 authentication proto] ドロップダウンリストから認証タイプを選択します。次のオプションを使用できます。

- **[MD5]**

- **SHA**

重要
ネットワーク内のすべてのアクセスポイントに、同じ SNMP 認証プロトコルを設定する必要があります。

ステップ 5 [SNMP v3 encryption] ドロップダウンリストから適切な暗号化プロトコルを選択します。次のオプションを使用できます。

- **暗号化なし**
- **DES**（データ暗号規格）
- **AES**（Advanced Encryption Standard）

（注）
ネットワーク内のすべてのアクセスポイントに、同じ暗号化プロトコルを設定する必要があります。

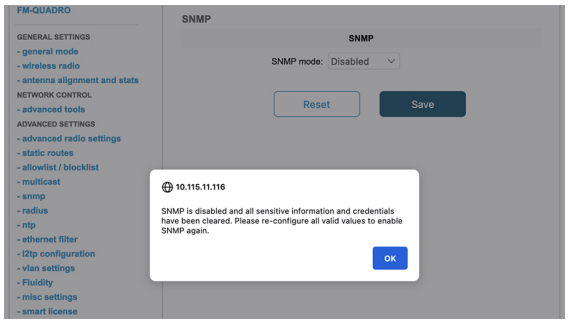
ステップ 6 暗号化パスフレーズを変更するには、[SNMP v3 encryption passphrase] フィールドに新しいパスフレーズを入力します。

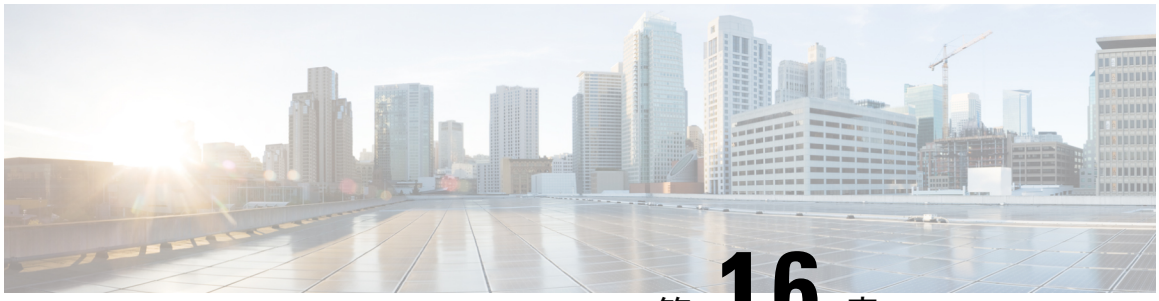
ステップ 7 [Enable SNMP periodic trap] チェックボックスをオンにして、定期 SNMP トラップにより定義された一定の間隔で SNMP トラップが送信されるようにし、[NMS hostname] フィールドに NMS のホスト名を入力します。[Notification period] に通知期間（分単位）を入力します。

ステップ 8 [Enable SNMP event trap] チェックボックスをオンにして、重要なシステム関連イベントの SNMP イベントトラップを有効にし、[NMS hostname] フィールドに NMS のホスト名を入力します。

（注）
トラップの送信先となる NMS ホストには、v3 トラップを収集するように設定された SNMP エージェントが必要です。

ステップ 9 [Save] をクリックします。
SNMP を無効にすると、次のポップアップが表示されます。





第 16 章

マルチキャスト

マルチキャストの概要

AP は、レイヤ 2 ネットワークおよびレイヤ 3 ネットワークのマルチキャスト転送をサポートしています。マルチキャストは、GUI または CLI のいずれかを使用して設定できます。マルチキャストは、データを 1 つの送信元から複数の宛先に同時に送信する通信方式です。マルチキャスト伝送は、ポイントツーマルチポイントまたはマルチポイント ツー マルチポイントにすることができます。

（注）

- デフォルトでは、以下で指定されたマルチキャスト IP アドレスのみが URWB ネットワークを介して転送されます。
- マルチキャスト設定は、メッシュエンドデバイスでのみ必要です。
- マルチキャスト予約 IP アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 です。

マルチキャストプロトコル用に予約済みの IP アドレスの範囲

デフォルトでは、指定された IP アドレスの範囲内にある次のプロトコルに対してマルチキャストが有効です。

プロトコル	予約済みのマルチキャスト IP アドレスの範囲
ユニバーサル プラグ アンド プレイ（UPnP）	239.255.255.250
Open Shortest Path First（OSPF）	224.0.0.5 および 224.0.0.6

プロトコル	予約済みのマルチキャスト IP アドレスの範囲
インターネット グループ管理プロトコル（IGMP）	該当なし

マルチキャスト設定の利点

- 1 つの送信元から複数の宛先に単一のデータのストリームを送信するため、使用される帯域幅の量が削減されます。
- ネットワークの負荷を大幅に増加させることなく、多くのデバイスがサポートされます。
- リアルタイムのデータ配信を必要とするアプリケーションのネットワーク性能が最適化されます。
- 重複するストリームの数を減らすことで一貫した品質が維持され、すべての受信側 AP で一貫した Quality of Service（QoS）を維持するために役立ちます。

GUI を使用したマルチキャストの設定

始める前に

- マルチキャストは、メッシュエンドデバイスでのみ設定できます。
- 有効なマルチキャストグループ、ネットマスク、および宛先 IP アドレスがあることを確認します。
- マルチキャストを設定するためのサポートされているメッシュエンドデバイスがあることを確認します。

手順

ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力してコンフィギュレータのログインページを開きます。

ステップ 2 [Username] および [Enable Password] フィールドに、ユーザー名とパスワードをそれぞれ入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI にログインすると、URWB コンフィギュレータが表示されます。

ステップ 4 [ADVANCED SETTINGS] で、[multicast] をクリックして [MULTICAST] ウィンドウを開きます。

ステップ 5 [Add a new multicast route] セクションで、次の詳細を入力します。

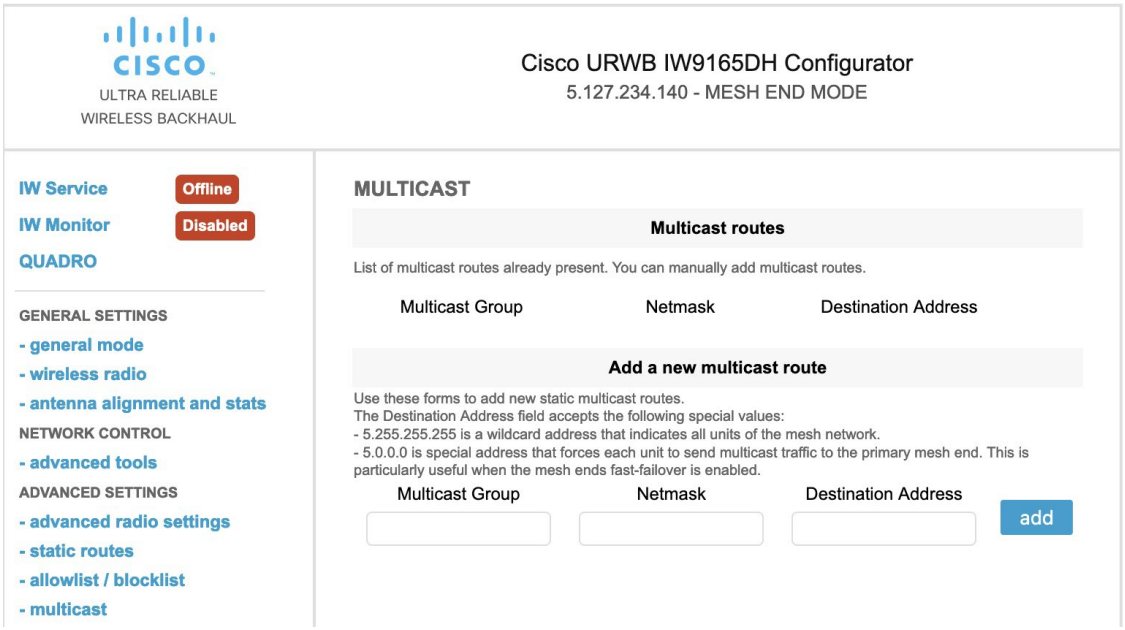
- [Multicast Group] フィールドのマルチキャスト IP アドレス。
- [Netmask] フィールドのネットマスク IP アドレス。
- [Destination Address] フィールドの宛先 IP アドレス。

（注）
[Destination Address] フィールドには、次の特殊な値を使用できます。

- [Destination Address] フィールドの 5.255.255.255 という IP アドレス：メッシュネットワーク経由ですべてのメッシュポイントデバイスにデータを送信します。これは、ダウンストリームデータ フローにのみ適用できます。
- [Destination Address] フィールドの 5.0.0.0 という IP アドレス：現在のプライマリ メッシュ エンド デバイスにデータを送信します。これは、特にメッシュエンドの高速フェールオーバーが有効になっている場合に役立ちます。これは、アップストリーム データ フローにのみ適用できます。

ヒント
ネットマスクのフィールドでは、マルチキャストアドレスのブロックを指定できます。複数のマルチキャストグループを指定する場合は、マルチキャスト IP アドレスがそのグループのネットワークアドレスを反映している必要があります。

ステップ 6 [add] をクリックします。
規則を正常に追加すると、新しいマルチキャストルートが [Multicast routes] セクションに表示されます。



ステップ 7 [Apply] をクリックして、設定を更新します。
AP がリブートし、変更が適用されます。

CLI を使用したマルチキャストの設定

宛先 IP アドレスを追加するには、**configure multicast group add** *multicast-IP-address Netmask destination-IP-address* コマンドを使用します。

例：

```
Device#configure multicast group add 224.5.5.5 255.255.255.255 5.255.255.255
```

（注） この設定は、リブート後にのみ有効になります。

レイヤ3モードで、すべてのメッシュエンドデバイスとグローバルゲートウェイでマルチキャスト規則を設定します。アップストリーム トラフィックとダウンストリーム トラフィックに、次の異なるマルチキャスト IP アドレスを使用します。

- 224.5.5.5/5.0.0.0：現在のプライマリ メッシュ エンド デバイスにデータを送信します。これは、特にメッシュエンドの高速フェールオーバーが有効になっている場合に役立ちます。これは、アップストリーム データ フローにのみ適用できます。
- 224.5.5.6/5.255.255.255：メッシュネットワーク経由ですべてのメッシュポイントデバイスにデータを送信します。これは、ダウンストリーム データ フローにのみ適用できます。

CLI を使用したマルチキャストの削除

マルチキャストグループから meshID IP アドレスを削除するには、**configure multicast group delete** *multicast IP-address Netmask meshID IP-address* コマンドを使用します。

例：

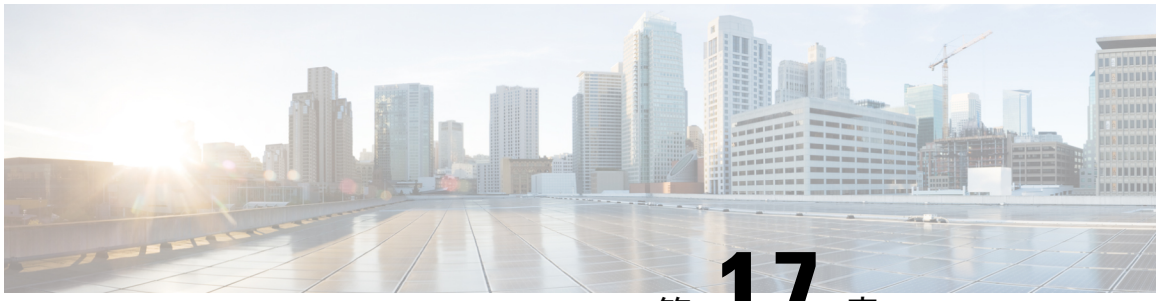
```
Device#configure multicast group delete 224.5.5.5 255.255.255.255 5.255.255.255
```

（注） この設定は、リブート後にのみ有効になります。

CLI を使用したマルチキャスト設定の確認

マルチキャスト設定のステータスを表示するには、**show multicast configuration** コマンドを使用します。

```
Device#show multicast configuration
Multicast Group 224.5.5.5/255.255.255.255
Destination Address 5.255.255.255
```



第 17 章

QoS

Quality of Service の概要

Quality of Service（QoS）は、特定のタイプのネットワークトラフィックを他よりも優先するために役立ちます。これにより、重要なアプリケーションや安全プロトコルの品質と性能が維持されます（遅延とパケット損失の影響を受けやすい音声やビデオなど）。さまざまなレベルのサービス品質を提供するために、データパケットの分類、マーキング、および管理が行われます。

QoS に基づくトラフィック分類

トラフィック分類は、パケットフィールドを調べてトラフィックのさまざまなタイプを識別するプロセスです。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。このラベルによって、パケットに対して実行されるすべての QoS アクションが示され、パケットの送信元キューが識別されます。QoS が有効になっている場合、デバイスはパケットの優先順位を分類できます。URWB デバイスは、URWB ネットワークの着信または発信データトラフィックに QoS ラベルを適用しません。代わりに、トラフィックの送信元、またはネットワーク内の他のポイントで割り当てられた既存の QoS マーキングを認識します。URWB デバイスは、レイヤ 2（PCP/VLAN）またはレイヤ 3（DSCP）で適用されるマーキングを受け入れます。

QoS の利点

- 優先順位付け：パケット IP ヘッダーでマークされた QoS 優先順位に従ってトラフィックを管理します。
- 帯域幅管理：優先順位の高いアプリケーションに十分な帯域幅を確保するためにネットワークリソースを割り当てます。
- 遅延管理：パケット到着時間の遅延を最小限に抑えて、時間的制約のあるアプリケーションの品質を維持します。

QoS マーキング

QoS マーキングにより、ネットワークデバイスは、割り当てられた優先順位に従ってパケットを識別および処理できます。このプロセスにより、優先順位の高いトラフィックが迅速かつ効率的に送信されるようになります。QoS マーキングでは、IP ヘッダーの DiffServ コードポイント（DSCP）またはタイプオブサービス（ToS）のフィールド、またはイーサネットパケットの VLAN ヘッダーの優先順位コードポイント（PCP）のフィールドがよく使用されます。これらのフィールドにより、さまざまな優先順位レベルが提供されます。IW デバイスは 8 つの優先順位レベルをサポートしていて、0 が最も低く、7 が最も高くなります。この 0 ～ 7 の範囲は、ToS 値のビット B5 ～ B7 から抽出されます。ToS は、IP パケットにある完全な 8 ビット値の名前です。

B7	B6	B5	B4	B3	B2	B1	B0
Priority			X	X	X	X	X

802.1p

802.1p は、より広範な 802.1Q 仕様の一部として IEEE によって開発された標準規格です。イーサネットネットワークでのネットワークトラフィックの優先順位付けと QoS に対応しています。この標準規格では、802.1Q VLAN ヘッダーで 3 ビットの優先順位コードポイント（PCP）を使用して、トラフィックを優先順位付けします。

QoS シェーピング

QoS シェーピング（トラフィックシェーピングとも呼ばれる）は、ネットワーク上のデータフローを制御するために使用されるネットワーク管理技術です。これには、さまざまなタイプのネットワークトラフィックで使用できる帯域幅の規制が含まれます。これにより、重要なアプリケーションが必要なリソースを受け取ることができるようになり、ネットワークの輻輳が防止されます。

CLI を使用した QoS 設定

デフォルトでは、デバイスの QoS 機能は無効になっています。

CLI を使用した QoS の有効化または無効化

デバイスの QoS 処理を有効にするには、**configure qos status enabled** コマンドを使用します。

```
Device#configure qos status enabled
```

（注） デバイスの QoS 設定を無効にするには、**configure qos status disabled** コマンドを使用します。

CLI を使用した QoS 設定の確認

デバイスの QoS 設定を確認するには、**show qos** コマンドを使用します。

有効：

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p disabled
```

無効：

```
Device#show qos
QoS: disabled
```

CLI を使用した 802.1p VLAN 優先度の優先

CLI を使用した 802.1p VLAN 優先度の優先の有効化または無効化

IP パケットの DSCP よりも 802.1p VLAN 優先度を優先するには、**configure qos 8021p enabled** コマンドを使用します。

```
Device#configure qos 8021p enabled
```

（注） デバイスの 802.1p を無効にするには、**configure qos 8021p disabled** コマンドを使用します。

- QoS 802.1p オプションが無効になっている場合、URWB デバイスは最初に L3 ヘッダー内の QoS マーキングを調べます。マーキングが見つからない場合は、L2-VLAN ヘッダーをチェックします。
- QoS 802.1p オプションが有効になっている場合、URWB デバイスは VLAN タグの PCP フィールド内の CoS 値のみを考慮します。

CLI を使用した 802.1p VLAN 優先度の優先の確認

デバイスの QoS 802.1p 設定を確認するには、**show qos** コマンドを使用します。

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p enabled
```

CLI を使用した CoS の再マッピングの設定

URWB システムでは、ネットワーク管理者の設計に基づいて QoS 優先順位マークを再マッピングできます。この設定では、1 つ以上の CoS 値の優先順位を変更できます。

着信パケットの CoS 値を異なる CoS 値にマッピングするには、**configure qos cos-map** *values* コマンドを使用します。

```
Device#configure qos cos-map 0 1 2 3 4 4 4 4
```

この CLI コマンドの例では、CoS の再マッピングは次のように行われます。

- CoS 0 は 0 のまま
- CoS 1 は 1 のまま
- CoS 2 は 2 のまま
- CoS 3 は 3 のまま
- CoS 4 は 4 のまま
- CoS 5、6、7 は 4 に再マッピング

この例では、CoS 値が 5、6、および 7 のパケットが 4 に再マッピングされ、最初から CoS 4 でマークされていたパケットと同じ優先順位が実質的に与えられます。

このコマンドを使用すると、ネットワークに入るパケットの CoS 値を変更して、ネットワークトラフィックの優先順位を調整することができます。これは、帯域幅の管理や、優先順位の高いトラフィックのより効率的な配信のために役立ちます。

重要 URWB システムは、元のマーキングを変更せずに再マッピングプロセスを管理します。再マッピングされた QoS 優先順位は、URWB ネットワーク内でのみ意味があり、有効です。

CLI を使用した CoS の再マッピングの確認

デバイスの CoS の再マッピング設定を確認するには、**show qos** コマンドを使用します。

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 4 4 4 ]
qos-shaping disabled
qos-8021p disabled
```

CLI を使用した QoS シェーピングの設定

CoS ごとのレートの設定

ネットワークデバイスで異なる CoS に帯域幅を割り当てて制御するには、**configure qos shaper-rates** *bandwidths* コマンドを使用します。

```
Device#configure qos shaper-rates <eigth traffic rates, one for each CoS>
```

（注） 8 つすべての帯域幅をゼロにすることはできません。

例：

```
Device#configure qos shaper-rates 30000 50000 50000 50000 0 0 0 0
```

この例では、各 CoS 値の帯域幅を設定します。

- CoS 0 には 30,000 kbps のレートが割り当てられています。
- CoS 1 ～ 3 には 50,000 kbps のレートが割り当てられています。
- CoS 4 ～ 7 は 0 kbps に設定されています。0 は無制限のレート（帯域幅の制限なし）を意味します。

QoS シェーピングの有効化または無効化

デバイスの QoS シェーピングを有効にするには、**configure qos shaping enabled** コマンドを使用します。

```
Device#configure qos shaping enabled
```

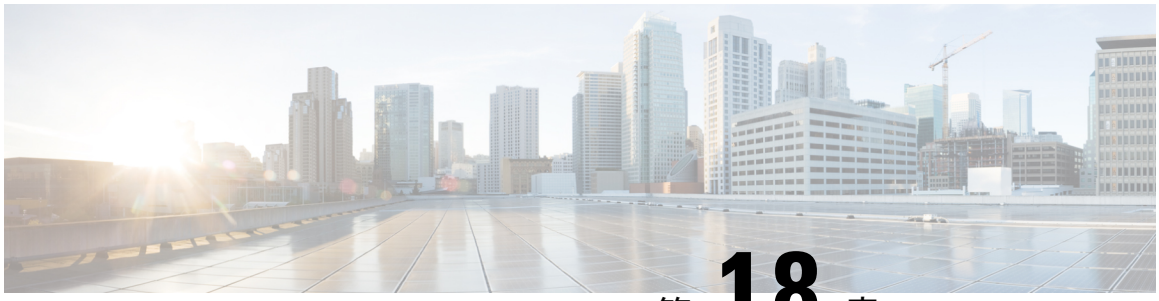
（注）

- デバイスの QoS シェーピングを無効にするには、**configure qos shaping disabled** コマンドを使用します。
- ネットワークでスループットが制限されたライセンスが実行されている場合は、すべてのクラスの帯域幅の合計が、ライセンスされたスループット制限を超えないようにする必要があります。

CLI を使用した QoS シェーピングの確認

デバイスの QoS シェーピング設定を確認するには、**show qos** コマンドを使用します。

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping enabled
Shaper rates (Kbps): 30000 50000 50000 50000 0 0 0 0
qos-8021p disabled
```



第 18 章

周波数スキャン

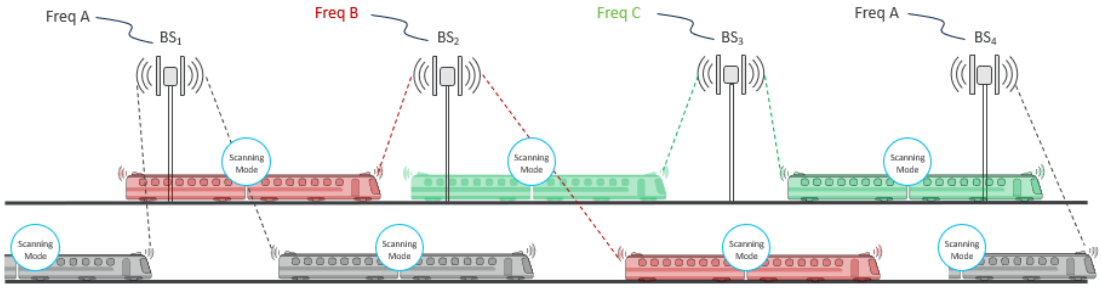
周波数スキャン

URWB デバイスは、次の 2 種類の周波数スキャンをサポートしています。

1. Fluidity 周波数スキャン
2. Fluidmax 周波数スキャン

Fluidity 周波数スキャンの概要

Fluidity 周波数スキャンは、インフラストラクチャ側で複数の周波数を使用して、自己干渉を減らし、無線チャネルの容量と性能を向上させる、高密度モビリティ環境関連のシナリオ向けに設計されています。この機能は、それらのデバイスが異なるネットワーク領域を移動する際に継続的で途切れのない接続を確保するために役立ち、AP 間のスムーズな移行を容易にします。現在の信号強度が弱い場合、デバイスは、安定した接続を維持するために、より良好な信号を持つ周波数を探し始めます。この機能は、路車間通信、鉱山、港湾ターミナルといったあらゆる高密度モビリティ環境に適用可能ます。



効果的な周波数スキャンには、通常、モバイルデバイスに少なくとも 2 つの無線機が必要です。

- 無線機 1：ネットワークとの現在の接続を維持します。
- 無線機 2：無線機 1 の既存の接続を妨げることなく、より良好な利用可能周波数をスキャンします。

スキャンは、次の 2 つのモードで実行できます。

- 定期スキャン：最良の利用可能チャネル周波数を見つけるために、デバイスが定期的に自動実行します。
- 信号トリガー（しきい値）スキャン：現在のデバイスの信号強度が、指定された最小信号対雑音比（SNR）しきい値を下回ると、モバイルデバイスは、より強い信号を持つ別のデバイスの検索を開始します。

このデュアル無線機構成により、接続品質を最適化しながら継続的な接続を実現します。

（注）
- 周波数スキャンは、Fluidity 車両デバイスにのみ適用され、インフラストラクチャ デバイスには適用されません。
- scan-periodic パラメータと scan-isolation パラメータがゼロに設定されている場合、周波数スキャン機能は無効になります。

CLI を使用した Fluidity 周波数スキャンの設定

デバイスでFluidity周波数スキャンを設定および管理するには、以下のコマンドを使用します。

CLI を使用した Fluidity 周波数スキャンリストのクリア

デバイスで Fluidity 周波数スキャンリストをクリアするには、**configure fluidity scan list clear** コマンドを使用します。

```
Device#configure fluidity scan list clear
```

CLI を使用した Fluidity 周波数スキャンリストのチャネルの設定

チャネルのリストとその帯域幅を設定するには、**configure fluidity scan list** *pairs of channel numbers, bandwidths* コマンドを使用します。

```
Device#configure fluidity scan list 100 20 108 20
```

（注） 有効なチャネル番号とその帯域幅については、「CLIによる動作チャネルの設定」および「CLIによるチャネル帯域幅の設定」を参照してください。

CLI を使用した Fluidity 周波数スキャンの分離時間の設定

Fluidity 周波数スキャンの分離時間を設定するには、**configure fluidity scan isolation** *time* コマンドを使用します。

```
Device#configure fluidity scan isolation 3000
```

（注）
- 分離時間の有効な範囲は 0 ～ 65535 です。
- 信号強度が、3000 ミリ秒間にわたり連続して特定の SNR しきい値を下回ると、デバイスにより、より良好な接続オプションのスキャンが開始されます。
- デバイスで Fluidity 周波数スキャン分離モードを無効にするには、**configure fluidity scan isolation disabled** コマンドを使用します。

CLI を使用した Fluidity 周波数スキャンの SNR しきい値の設定

Fluidity 周波数スキャン分離モードの SNR しきい値を設定するには、**configure fluidity scan rssi-threshold** *value* コマンドを使用します。

```
Device#configure fluidity scan rssi-threshold 50
```

（注）
- デバイスは、指定された最小信号強度を満たすインフラストラクチャデバイスにのみ接続します。
- SNR しきい値の有効な範囲は 0 ～ 100 です。
- SNR しきい値を無効にするには、**configure fluidity scan rssi-threshold disabled** コマンドを使用します。

CLI を使用した Fluidity 周波数定期スキャン時間の設定

デバイスで定期スキャン時間を設定するには、**configure fluidity scan periodic** *scan interval time* コマンドを使用します。

```
Device#configure fluidity scan periodic 5000
```

（注）
- 指定される時間間隔はミリ秒単位です。
- 定期スキャン時間の有効な範囲は 0 ～ 65535 です。最良の結果を得るための最小推奨値は 1500 です。この値については、設定するチャネル数を考慮する必要があります。
- 周波数の定期スキャンを無効にするには、**configure fluidity scan periodic disabled** コマンドを使用します。

CLI を使用したオンボード無線機の Fluidity 周波数割り当て

同じチャネルの場合

同じチャネルで動作するようにオンボードデバイスの無線インターフェイスをロックするには、**configure fluidity scan vehicle-frequency locked** コマンドを使用します。

```
Device#configure frequency scan vehicle-frequency locked
```

個別のチャネルの場合

オンボードデバイスの無線インターフェイスが個別のチャネルで動作できるようにするには、**configure fluidity scan vehicle-frequency open** コマンドを使用します。

```
Device#configure fluidity scan vehicle-frequency open
```

CLI を使用した Fluidity 周波数スキャン設定の確認

デバイスでの Fluidity 周波数スキャンを確認するには、**show fluidity config command** を使用します。

```
Device#show fluidity config
Fluidity enabled
Fluidity interface: 1
Vehicle ID: automatic, current ID: 89235672 current role: mobile primary unit
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
Rssi low/high zones threshold: 35
Color: enabled, current: 0
Color min RSSI threshold: 20
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan list: 5200@20 5240@20
Scan isolation time: 300 ms
Current Frequency: 5180 MHz
Current Channel Width: 20 MHz
Critical RSSI threshold for autoscan: disabled
Periodic autoscan interval: disabled
Vehicle frequency: open
Large network optimization: enabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
```

```
DoP settings: limit 0, client 10, bias 0
Quadro telemetry: enabled
```

Fluidmax 周波数スキャンの概要

Fluidmax 周波数スキャンは、通常、静的または半静的なネットワーク環境のデバイスに使用されます。これらは多くの場合、固定の場所やネットワーク環境が頻繁に変化しないエリアにおける安定した信頼性の高い接続を必要とします。このような環境には、産業施設、リモートモニタリングステーション、または干渉のない一貫した接続を維持することが重要な設定が含まれます。

GUI を使用した Fluidmax 周波数スキャンステータスの確認

始める前に

（注） 無線機設定で、無線機 1 または無線機 2 のいずれかについて、無線機ロールを Fluidmax セカンダリとして選択できます。

手順

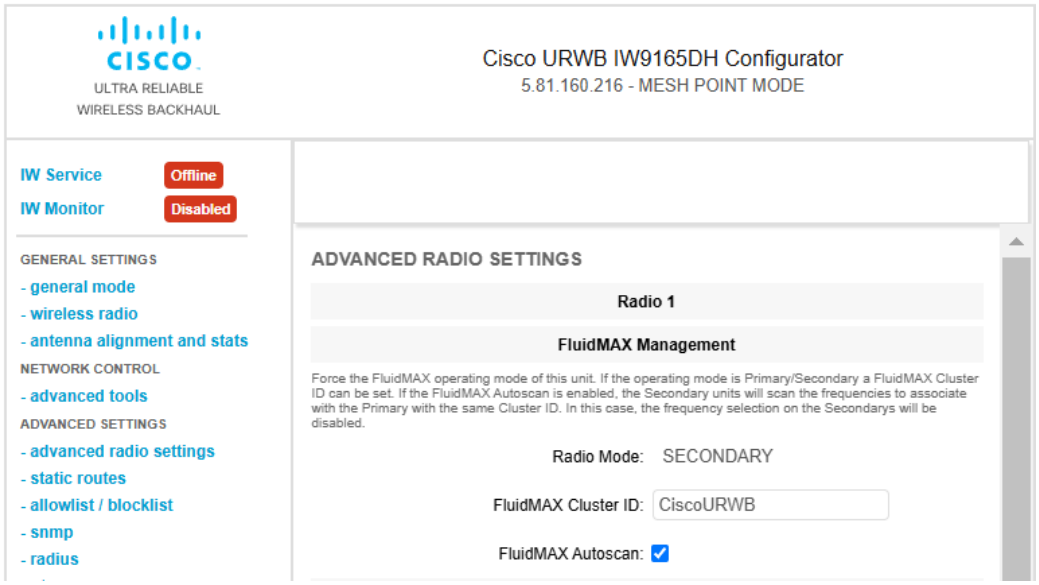
ステップ 1 コンピュータの Web ブラウザを起動し、URL を入力してコンフィギュレータのログインページを開きます。

ステップ 2 ユーザー名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [ログイン（Login）] をクリックします。
GUI にログインすると、URWB コンフィギュレータが表示されます。

ステップ 4 [ADVANCED SETTINGS] で、[advanced radio settings] をクリックして [ADVANCED RADIO SETTINGS] ウィンドウを開きます。

（注）
[FluidMAX Autoscan] チェックボックスがオンになっている場合、ステータスは有効になっています。オフになっている場合、ステータスは無効になっています。



CLI を使用した Fluidmax 周波数スキャンの設定

デバイスで Fluidmax 周波数スキャンを設定するには、以下のコマンドを使用します。

CLI を使用した Fluidmax 周波数スキャンの有効化または無効化

無線機で Fluidmax 周波数を有効にするには、**configure dot11Radio** *slot number* **mode fluidmax automatic-scan enable** コマンドを使用します。

```
Device#configure dot11Radio 1 mode fluidmax automatic-scan enable
```

（注） 無線機で Fluidmax 周波数を無効にするには、**configure dot11Radio** *slot number* **mode fluidmax automatic-scan disable** コマンドを使用します。

CLI を使用した Fluidmax 周波数スキャンのしきい値の設定

無線機で Fluidmax しきい値を設定するには、**configure dot11Radio** *slot number* **mode fluidmax** *threshold value* コマンドを使用します。

```
Device#configure dot11Radio 1 mode fluidmax threshold 90
```

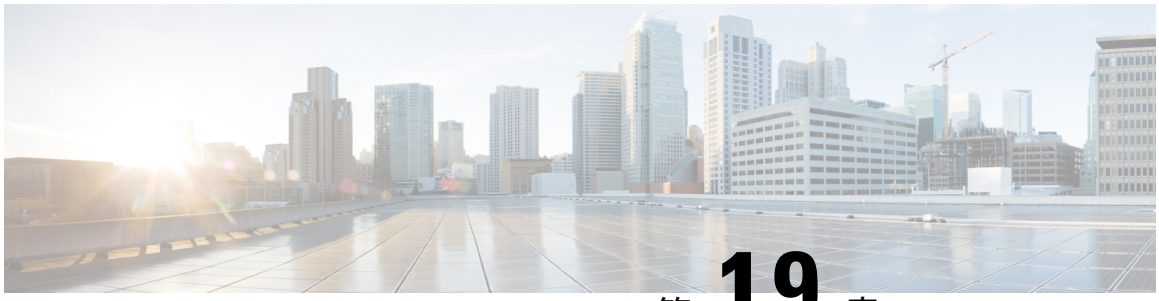
（注）
- Fluidmax しきい値の有効な範囲は 0 ～ 100 です。
- 自動スキャンが有効になっている場合、マスターからの信号が指定されたしきい値を下回るとトリガーされます。

CLI を使用した Fluidmax 周波数スキャン設定の確認

デバイスでの Fluidmax スキャンを確認するには、**show dot11Radio 1 config** コマンドを使用します。

```
Device #show dot11Radio 1 config

Interface: enabled

Mode: fluidmax secondary

Frequency: 5200 MHz
Channel: 40
Channel width: 20 MHz
Antenna number: 2
TX power level: 2
TX power: 14 dBm
Antenna gain: 15 dBi
Maximum tx mcs: 9
High-efficiency: disabled
Maximum tx nss: 2
RTS protection: 512
guard-interval: 800 ns
ampdu max length: 255
distance: 3000 m

The ampdu Tx
priority 0: enabled
priority 1: enabled
priority 2: enabled
priority 3: enabled
priority 4: enabled
priority 5: enabled
priority 6: disabled
priority 7: disabled

Fluidmax configuration
Tower ID: disabled
Cluster ID: CiscoURWB
Automatic scan: enabled
Automatic scan threshold: disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase: 58ac1e597fda4e37bc0c2472d8c8c69f
AES encryption: disabled
AES key-control: disabled
```

```
Key rotation: disabled
Key rotation timeout: 0(second)

DFS region: B
DFS radar role: auto
Radar detected: 0
Indoor deployment: disable
Rx-SOP Threshold: 0 dBm(AUTO)
Max packet retries: 32
High throughput 4.9Ghz: disabled
```



第 19 章

キーコントローラの設定と検証（ワイヤレスセキュリティ）

キーコントローラの設定と検証（ワイヤレスセキュリティ）

標準の Wi-Fi Protected Access（WPA）プロトコルに対するワイヤレスセキュリティをサポートするために、Catalyst IW9167E にはキーローテーション戦略が導入されています。キーコントローラプロトコルは、2 つのデバイス間のパケット交換であり、プロセスの各段階が各デバイスの状態にそれぞれ対応します。アルゴリズムフローは、パケット暗号化用の新しい Pairwise Transient Key/Group Transient Key を生成するために定期的にスケジュールされた一連のタイマーによって制御されます。キーが頻繁に更新されるほど、攻撃時に漏洩する情報量が少なくなります。

CLI によるキーコントローラの設定

キーコントローラを設定するには、次の CLI コマンドを使用します。

1. 無線機で Advanced Encryption Standard（AES）を有効にするには、次の CLI コマンドを使用します。

   ```
   Device# configure dot11Radio <interface> crypto aes enable
   ```

2. キーコントローラを有効にするには、次の CLI コマンドを使用します。

   ```
   Device #configure dot11Radio <interface> crypto key-control enable
   ```

3. キーローテーションを有効にするには、次の CLI コマンドを使用します。

   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation enable
   ```

4. キーローテーションタイマーを設定するには、次の CLI コマンドを使用します。

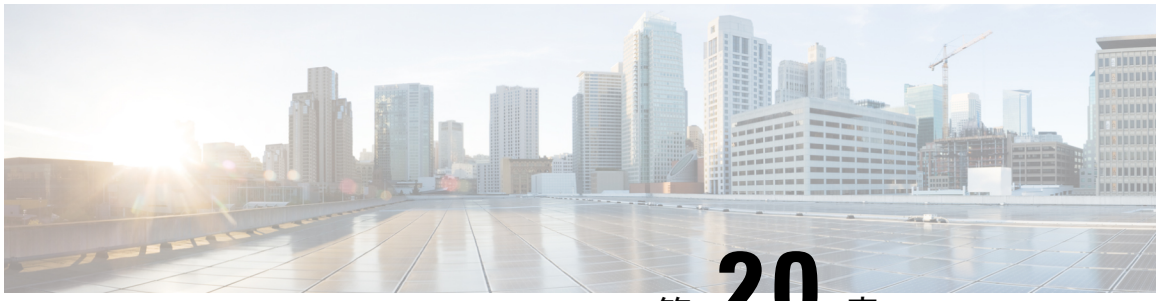
   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation 3600
   ```

（注） デフォルトでは、AES モードは無効です。設定はすべてのデバイスで同じである必要があります。

CLI によるキーコントローラの検証

キーコントローラを検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio X crypto
AES encryption: enabled
AES key-control: enabled
Key rotation: enabled
Key rotation timeout: 3600(second)
```



第 20 章

FIPS 認定

FIPS 認定

連邦情報処理標準（FIPS）モードは、SSH および GUI 機能によって NIST の FIPS140-3 セキュリティ標準が確実に順守されるようにします。FIPS が有効になっている場合、AP は設定が FIPS 要件に準拠していることを確認します。

（注） FIPS 認定では SNMP はサポートされません。

CLI を使用した FIPS モードの有効化または無効化

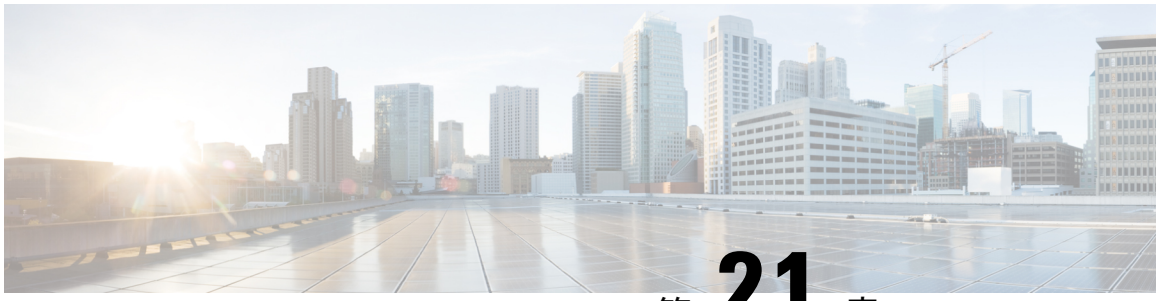
AP で FIPS モードを有効または無効にするには、このコマンドを使用します。

```
Device#configure fips {enable|disable}
```

CLI を使用した FIPS モードの確認

AP の FIPS モードを確認するには、このコマンドを使用します。

```
Device#show fips
FIPS: enabled
```



第 21 章

固定ドメインと国コード（ROW）

CLI を使用した国コードの設定と確認

その他の地域（ROW）ドメインの国コードを設定するには、次の CLI コマンドを使用します。

```
Device# configure countrycode [countrycode]
```

例：

```
Configure countrycode GB
```

上記の CLI は、設定された国コードが ROW に含まれていない場合にエラーを報告します。国コードが設定されていない場合、ワイヤレスインターフェイスは正常に機能しません。

（注） 周波数、チャネル幅などの他のワイヤレスパラメータを設定する前に、国コードを設定してからデバイスをリブートします。国コードの設定は、IW9167EH-ROW などの、ROW ドメインを持つアクセスポイントにのみ適用されます。

国コードのステータスを確認するには、次の show コマンドを使用します。

```
Device# show version | in Product
Product/Model Number: IW9167EH-ROW
```

ROW の国コードのステータスを確認するには、次の show コマンドを使用します。

```
Device# show dot11Radio <interface> config
```

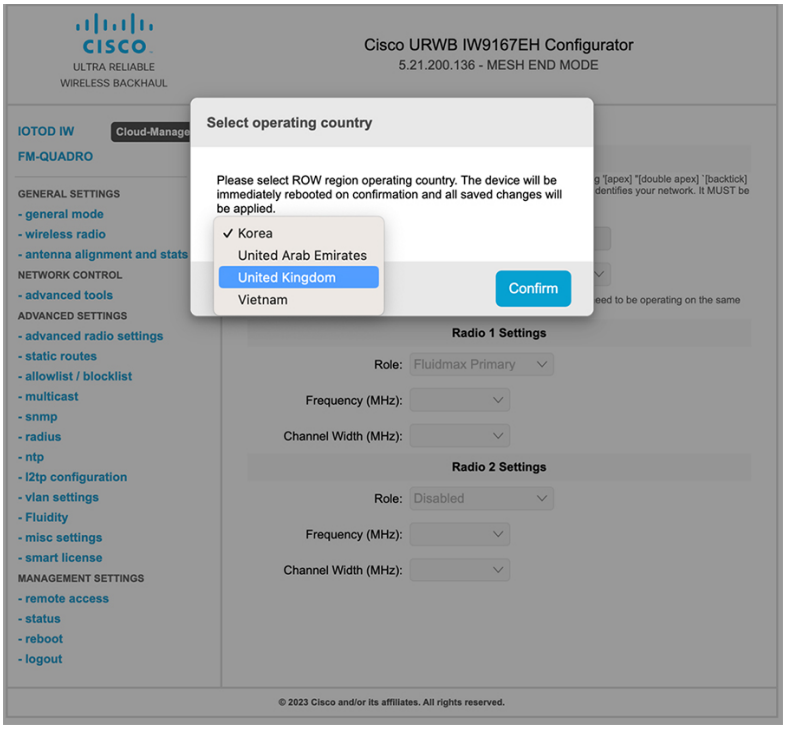
例：

```
Device# show dot11Radio 1 config
…….
DFS region : GB
DFS radar role : auto
Radar Detected : 0
Indoor deployment: disable
```

GUI を使用した国コードの設定

国コードが設定されていない場合、ワイヤレスインターフェイスは機能しません。国コードの設定方法は、次のとおりです。

1. [GENERAL SETTINGS] で、[wireless radio] をクリックします。
2. ROW ドメインでは、国コードが選択されていない場合、次のポップアップが表示されます。



3. 国コードを選択するには、上記の画像のポップアップをクリックすると、[Wireless Settings] セクションにリダイレクトされます。[Wireless Settings] セクションで、ドロップダウンリストから国を選択します。

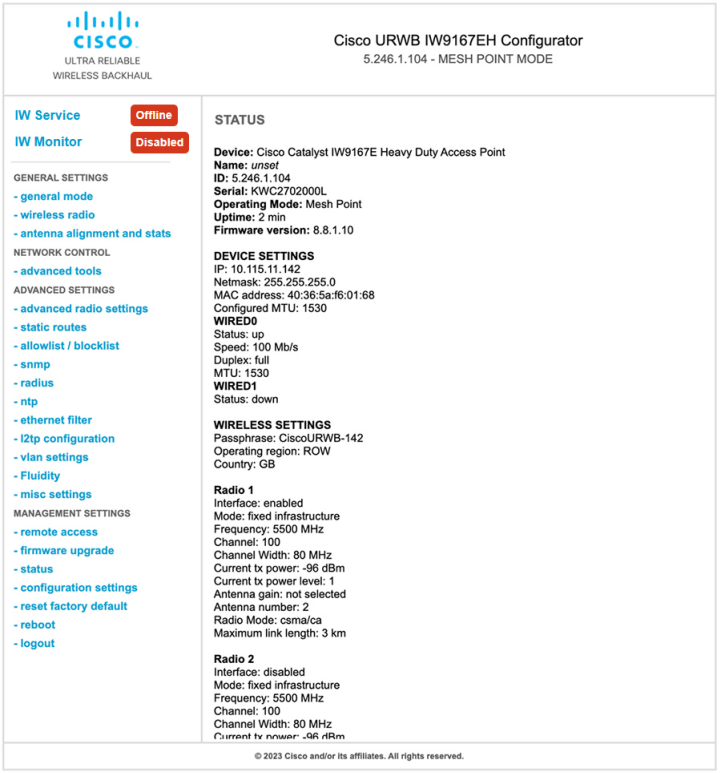
   確認ポップアップが表示されます。

4. [Confirm] をクリックします。

   リブートの確認画面が表示されます。

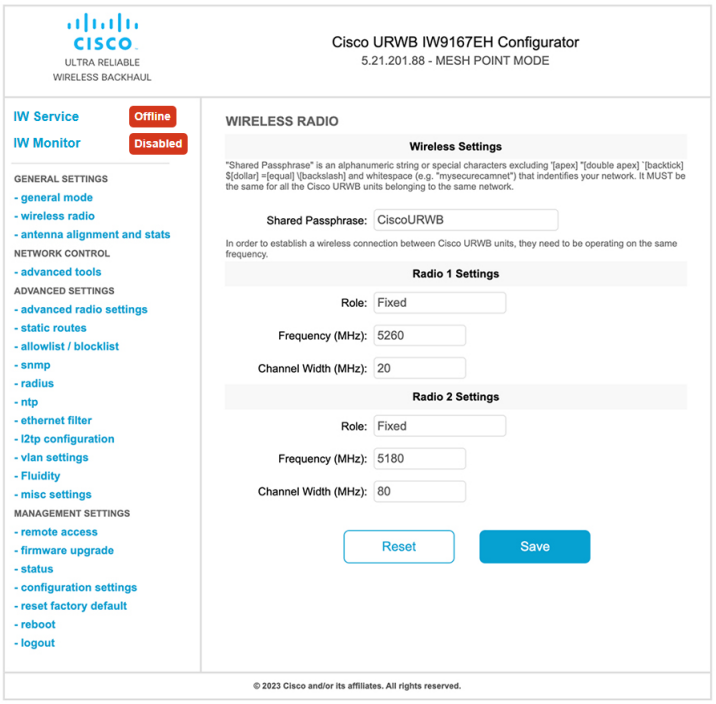
5. [Yes] をクリックします。
6. [MANAGEMENT SETTINGS] で、[status] をクリックします。

   [STATUS] ページで、運用する地域と国の詳細を確認します。

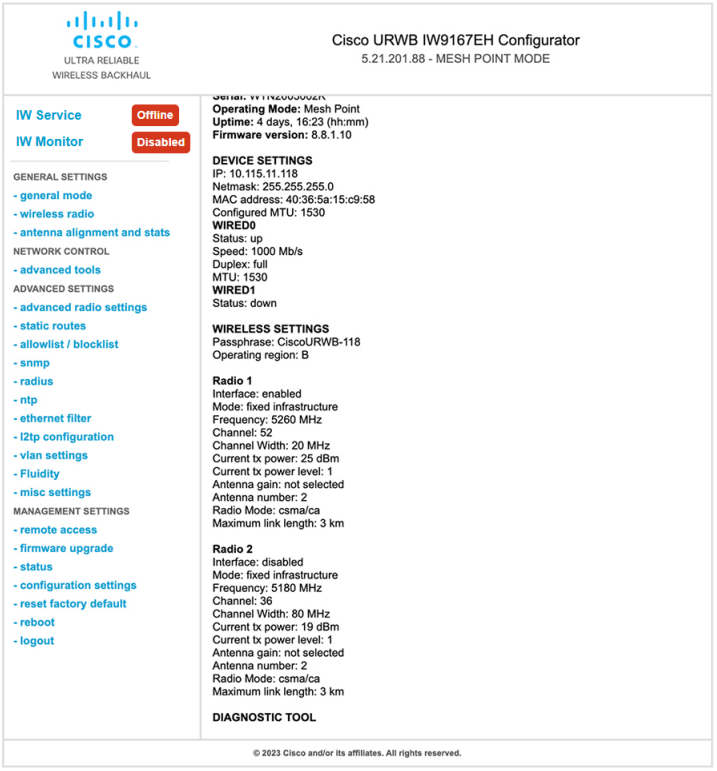


7. デバイス間のワイヤレス接続を確立するには、無線デバイスで同じ動作周波数を設定します。

（注） [Shared Passphrase] は、同じネットワークに属するすべてのデバイスで同じである必要があります。



次の画像は、GUI を使用した国コードの設定を示しています。



Catalyst AP の固定ドメインと国コード（ROW）

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地域の国コードの管理が簡素化されます。ここでは、Catalyst IW9167E、IW9165E、および IW9165D AP 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。

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については、「Cisco Product Approval Status」を参照してください。

Catalyst IW9167E でサポートされている固定ドメイン

ドメイン	屋内展開のサポート
A	非対応
B[1]	該当なし
E	対応
F	非対応
Q	非対応
Z	非対応

[1] ドメインでは屋外と屋内の周波数は同じです。

Catalyst IW9167E でサポートされている国コード

国コード	屋内展開のサポート	初期サポート
アルジェリア（DZ）	非対応	17.16.1
アルゼンチン（AR）	非対応	17.13.1
バハマ（BS）	非対応	17.16.1
ブラジル（BR）	非対応	17.13.1
ブルネイ（BN）	非対応	17.16.1
カメルーン（CM）	非対応	17.16.1
チリ（CL）	非対応	17.13.1
中国（CN）	非対応	17.13.1

国コード	屋内展開のサポート	初期サポート
コロンビア（CO）	非対応	17.13.1
コスタリカ（CR）	非対応	17.16.1
エクアドル（EC）	非対応	17.13.1
エジプト（EG）	非対応	17.15.1
エルサルバドル（SV）	非対応	17.16.1
ガーナ（GH）	非対応	17.16.1
英国（GB）	対応	17.11.1
香港（HK）	非対応	17.13.1
アイスランド（IS）[2]	対応	—
インド（IN）	非対応	17.12.1
イラク（IQ）	非対応	17.13.1
ケニア（KE）	非対応	17.16.1
韓国（KR）	非対応	17.12.1
クウェート（KW）	非対応	17.16.1
マカオ（MO）	非対応	17.16.1
マレーシア（MY）	非対応	17.15.1
メキシコ（MX）	非対応	17.13.1
モナコ（MC）[3]	対応	—
モンゴル（MN）	非対応	17.15.1
ナイジェリア（NG）	非対応	17.16.1
パキスタン（PK）	非対応	17.13.1
パナマ（PA）	非対応	17.16.1
パラグアイ（PY）	非対応	17.16.1
ペルー（PE）	非対応	17.12.1
フィリピン（PH）	非対応	17.12.1
プエルトリコ（PR）[4]	非対応	17.15.1

国コード	屋内展開のサポート	初期サポート
カタール（QA）	非対応	17.13.1
サウジアラビア（SA）	非対応	17.13.1
シンガポール（SG）	非対応	17.13.1
南アフリカ（ZA）	非対応	17.13.1
台湾、中華民国（TW）	非対応	17.13.1
タイ（TH）	非対応	17.13.1
アラブ首長国連邦（AE）	非対応	17.13.1
ウルグアイ（UY）	非対応	17.13.1
ベトナム（VN）	該当なし	17.11.1

[2] -E ドメインを使用してサポートされます。
[3] -E ドメインを使用してサポートされます。
[4] -B ドメインを使用してサポートされます。

（注） CLI または GUI を使用して選択できるのは、リストされている国コードです。ROW ドメインでは、デバイスが稼働する国のコードを選択します。このタスクは、IW9167E、IW9165E、および IW9165DH の 3 つの Catalyst AP すべてに共通です。

Catalyst IW9165E でサポートされている固定ドメイン

ドメイン	屋内展開のサポート
A	対応
B[5]	該当なし
E	対応
F	対応
Q	対応
Z	はい

[5] ドメインでは屋外と屋内の周波数は同じです。

Catalyst IW9165E でサポートされている国コード

国コード	屋内展開のサポート	初期サポート
アルジェリア（DZ）	はい	17.16.1
アルゼンチン（AR）	対応	17.15.1
バーレーン（BH）	はい	17.16.1
ボリビア（BO）	はい	17.16.1
ブラジル（BR）	対応	17.13.1
チリ（CL）	対応	17.13.1
中国（CN）	対応	17.15.1
コロンビア（CO）	対応	17.15.1
コスタリカ（CR）	はい	17.16.1
ドミニカ共和国（DO）	はい	17.16.1
エクアドル（EC）	対応	17.15.1
エジプト（EG）	対応	17.15.1
英国（GB）	対応	17.12.1
香港（HK）	対応	17.15.1
インド（IN）	対応	17.13.1
イラク（IQ）	対応	17.15.1
カザフスタン（KZ）	はい	17.16.1
ケニア（KE）	はい	17.16.1
韓国（KR）	対応	17.13.1
マレーシア（MY）	対応	17.15.1
メキシコ（MX）	対応	17.13.1
モンゴル（MN）	対応	17.15.1
パキスタン（PK）	対応	17.15.1
パナマ（PA）	はい	17.16.1

国コード	屋内展開のサポート	初期サポート
パラグアイ（PY）	はい	17.16.1
ペルー（PE）	対応	17.13.1
フィリピン（PH）	対応	17.13.1
カタール（QA）	対応	17.13.1
サウジアラビア（SA）	対応	17.13.1
シンガポール（SG）	対応	17.13.1
南アフリカ（ZA）	対応	17.13.1
スリランカ（LK）	対応	17.13.1
台湾、中華民国（TW）	対応	17.14.1
タイ（TH）	対応	17.13.1
アラブ首長国連邦（AE）	対応	17.13.1
ベトナム（VN）	対応	17.13.1

Catalyst IW9165DH でサポートされている固定ドメイン

ドメイン	屋内展開のサポート
A	非対応
B[6]	該当なし
E	対応
F	非対応
Q	非対応
Z	非対応

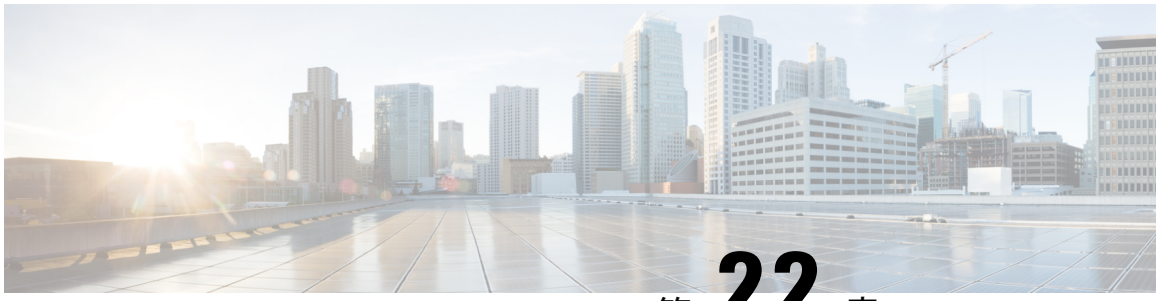
[6] ドメインでは屋外と屋内の周波数は同じです。

Catalyst IW9165DH でサポートされている国コード

国コード	屋内展開のサポート	初期サポート
アルジェリア（DZ）	非対応	17.16.1

国コード	屋内展開のサポート	初期サポート
アルゼンチン（AR）	非対応	17.15.1
ボリビア（BO）	非対応	17.16.1
ブラジル（BR）	非対応	17.13.1
カメルーン（CM）	非対応	17.16.1
チリ（CL）	非対応	17.13.1
中国（CN）	非対応	17.15.1
コロンビア（CO）	非対応	17.15.1
コスタリカ（CR）	非対応	17.16.1
コスタリカ（CR）	非対応	17.16.1
ドミニカ共和国（DO）	非対応	17.16.1
エクアドル（EC）	非対応	17.15.1
エジプト（EG）	非対応	17.15.1
ガーナ（GH）	非対応	17.16.1
英国（GB）	対応	17.12.1
香港（HK）	非対応	17.15.1
インド（IN）	非対応	17.13.1
イラク（IQ）	非対応	17.15.1
カザフスタン（KZ）	非対応	17.16.1
ケニア（KE）	非対応	17.16.1
韓国（KR）	非対応	17.13.1
クウェート（KW）	非対応	17.16.1
マレーシア（MY）	非対応	17.15.1
メキシコ（MX）	非対応	17.13.1
モンゴル（MN）	非対応	17.15.1
パキスタン（PK）	非対応	17.15.1
パナマ（PA）	非対応	17.16.1

国コード	屋内展開のサポート	初期サポート
パラグアイ（PY）	非対応	17.16.1
ペルー（PE）	非対応	17.13.1
フィリピン（PH）	非対応	17.13.1
カタール（QA）	非対応	17.13.1
サウジアラビア（SA）	非対応	17.13.1
シンガポール（SG）	非対応	17.13.1
南アフリカ（ZA）	非対応	17.13.1
スリランカ（LK）	非対応	17.13.1
台湾、中華民国（TW）	非対応	17.14.1
タイ（TH）	非対応	17.13.1
アラブ首長国連邦（AE）	非対応	17.13.1
ベトナム（VN）	非対応	17.13.1

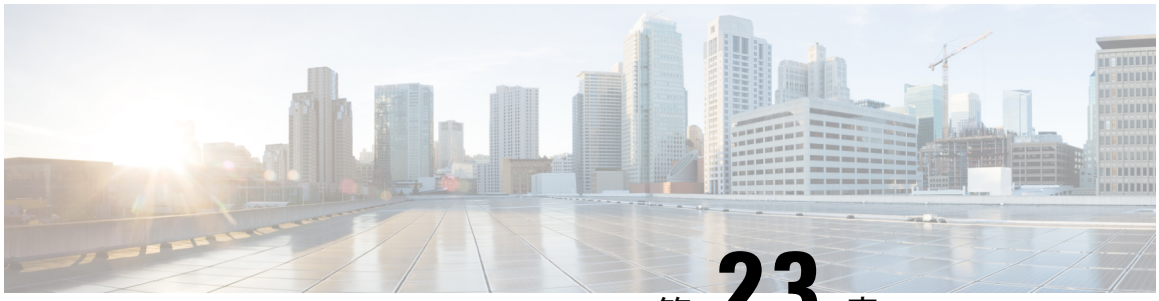


第 22 章

スマートライセンス

スマートライセンスのサポート

「スマートライセンス」の章は 、『Smart Licensing on the Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points』という新しい独立したガイドに置き換えられました。このガイドには、URWB モードで実行されているアクセスポイントのスマートライセンスに関連する最新の情報が含まれています。



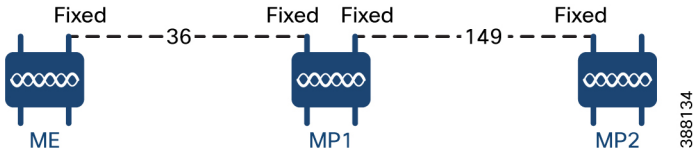
第 23 章

ポイントツーポイント リレー トポロジの設定と検証

ポイントツーポイント リレー トポロジの設定と検証

次の図には、ポイントツーポイントリレートポロジを導入するための単一のデバイス（MP1）上に 2 つの無線インターフェイスが示されています。

図 *2*:ポイントツーポイント リレー トポロジ



ポイントツーポイント リレー トポロジを設定するには、以下のシナリオに従います。

1. メッシュエンド（ME）、チャンネル 36 に MP1、デフォルトチャンネル 149 に MP2 を設定します。
2. ステップ 1 の設定から続行します。
3. メッシュポイント（MP2）の 2 番目のスロットインターフェイスを再度有効にして 30 秒待つと、単一のデバイス上の 2 つの無線インターフェイスによるポイントツーポイント リレー トポロジが導入されます。

CLI によるポイントツーポイント リレー トポロジの設定

ポイントツーポイント リレー トポロジを設定するには、次の CLI コマンドを使用します。

1. 無線インターフェイス番号 <1 または 2> でワイヤレスデバイスを設定します。

```
Device# configure dot11Radio <interface>
```

2. ワイヤレスインターフェイスの管理状態を有効モードまたは無効モードに設定します。

```
Device# configure dot11Radio <interface> > {enable | disable}
```

3. 指定したインターフェイスの動作モードを設定します（fixed、Fluidity、またはFluidmax）

```
Device# configure dot11Radio <interface> > [enable | disable] mode { fluidity | fixed
 | fluidmax }
```

4. 指定したインターフェイスの動作チャンネルと、有効な範囲（1 ～ 256）の動作チャンネル ID を設定します

```
Device# configure dot11Radio <interface> > [enable | disable] mode [fluidity | fixed
 | fluidmax] channel <channel id>
```

5. この設定を終了するには、次の CLI コマンドを使用します。

```
Device (configure dot11Radio <interface> > {enable | disable} mode {fluidity | fixed
 | fluidmax} channel <channel id>) #end
```

例：

```
Device#configure dot11Radio <2> {enable | disable} mode {fluidity} channel <36>
```

ポイントツーポイント リレー トポロジの設定例：

メッシュエンド（ME）の設定

```
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fixed
Device#configure dot11Radio 2 channel 36
```

メッシュポイント（MP1）の設定

```
Device#configure fluidity id infrastructure
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fixed
Device#configure dot11Radio 1 channel 36
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fixed
Device#configure dot11Radio 2 channel 149
```

MP2 の設定

```
Device#configure fluidity id infrastructure
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fixed
Device#configure dot11Radio 1 channel 149
```

CLI によるポイントツーポイント リレー トポロジの検証

ポイントツーポイント リレー トポロジの設定を検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio <interface> config
```

メッシュエンド（ME）の統計

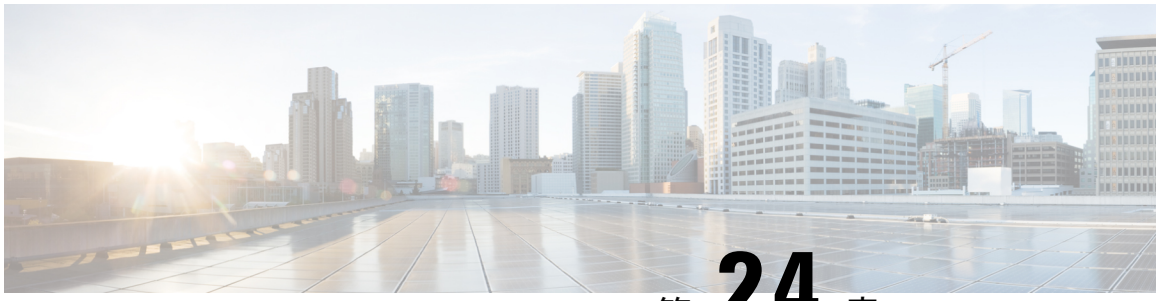
```
Device#show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

メッシュポイント（MP1）の統計

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

MP2 の統計

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
```



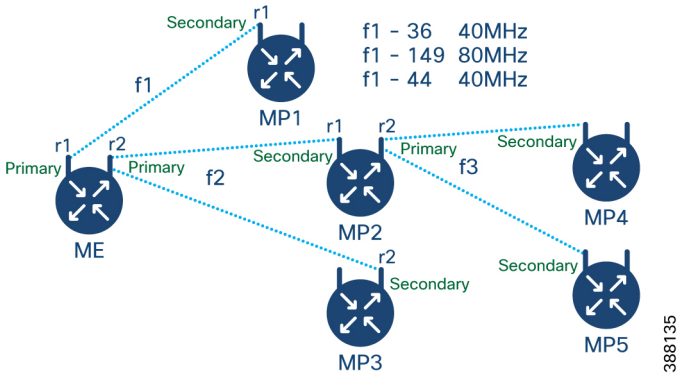
第 24 章

Fluidmax トポロジの設定と検証

Fluidmax（ポイントツーマルチポイント）トポロジの設定と検証

固定インフラストラクチャに関しては、ポイントツーマルチポイント接続を導入するために、Fluidmax モードで動作するようにワイヤレスインターフェイスを設定できます。各インターフェイスは独立した Fluidmax パラメータのセットを使用するため、導入可能なネットワークトポロジの柔軟性が大幅に向上しています。例として、以下の図は、ME（メッシュエンド）ノードが両方の無線機を Fluidmax プライマリモードで使用して、2 つの異なる周波数で複数のセカンダリクライアント（MP1（メッシュポイント）、MP2、および MP3）のために機能する、2 カスケード型ポイントツーマルチポイントクラスタを示しています。MP2 に関しては、最初の無線機は Fluidmax セカンダリモードで動作して ME に接続し、2 番目のインターフェイスは Fluidmax プライマリとして設定されてより多くのダウンストリーム クライアント（MP4 および MP5）のために機能します。

図 *3 : 2* カスケード型 *Fluidmax* トポロジ



CLI によるポイントツーマルチポイント トポロジの設定

Fluidmax（ポイントツーマルチポイント）トポロジを設定するには、次のコマンドを使用します。

```
Device#configure dot11Radio <interface>
```

interface：<0 ～ 3> dot11Radio インターフェイスの番号。

```
Device#configure dot11Radio <interface> {enable | disable}
```

enable または disable：ワイヤレスインターフェイスの管理状態を設定して、実行時に有効または無効にします

```
Device#configure dot11Radio <interface> mode {fluidity | fixed | fluidmax } { primary |
 secondary }
```

mode：指定されたインターフェイスの動作モード（Fluidity、fixed、または Fluidmax）。

primary | secondary：ユニットの Fluidmax ロール（プライマリまたはセカンダリ）。

```
Device#configure dot11Radio <interface> channel <channel id>
```

channel：動作チャンネル ID <1 ～ 256> を設定します。

```
Device#configure dot11Radio <interface> band-width <channel bandwidth>
```

bandwidth：チャンネル帯域幅（MHz）。現在サポートされている値は 20、40、80、160 です。

```
Device#wr
```

ポイントツーマルチポイント（Fluidmax）トポロジ設定の例：

ME（メッシュエンド）の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax primary
Device#configure dot11Radio 1 channel 36
Device#configure dot11Radio 1 band-width 40
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fluidmax primary
Device#configure dot11Radio 2 channel 149
Device#configure dot11Radio 2 band-width 80
```

MP1（メッシュポイント）の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax secondary
Device#configure dot11Radio 1 channel 36
Device#configure dot11Radio 1 band-width 40
```

MP2 の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax secondary
Device#configure dot11Radio 1 channel 149
Device#configure dot11Radio 1 band-width 80
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fluidmax primary
Device#configure dot11Radio 2 channel 44
Device#configure dot11Radio 2 band-width 40
```

MP3 の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax secondary
Device#configure dot11Radio 1 channel 149
Device#configure dot11Radio 1 band-width 80
```

MP4 の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax secondary
Device#configure dot11Radio 1 channel 44
Device#configure dot11Radio 1 band-width 40
```

MP5 の設定

```
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fluidmax secondary
Device#configure dot11Radio 1 channel 44
Device#configure dot11Radio 1 band-width 40
```

Cluster ID：インターフェイスが Fluidmax モードに設定されている場合に割り当てられる ID。この ID は、プライマリ ノードとバックアップ プライマリ ノードで同じである必要があります。同じクラスタに属するデバイスを識別し、グループ化するのに役立ちます。

Tower ID：指定したインターフェイスの Fluidmax タワー ID を有効または無効にします。

（注） タワー ID は、同じタワー ID を持つゲートウェイ＋メッシュポイント（MP）– MP がある構成で使用されます。

Fluidmax モードでインターフェイス、クラスタ ID、およびタワー ID を設定するには、次のコマンドを使用します。

```
Fluidmax - Set the interface in Fluidmax mode.
Primary | Secondary - Fluidmax role for the device, either primary or secondary.
Device# configure dot11Radio [1|2] mode fluidmax cluster id fluidmesh
Cluster id - Set Fluidmax Cluster ID assigned to the interface.
Device# configure dot11Radio [1|2] mode fluidmax tower [enable|disable]
Tower – Enable or disable Fluidmax Tower ID for specified interface.
```

CLI を使用したポイントツーマルチポイント トポロジの検証

このコマンドを使って、ポイントツーマルチポイント（Fluidmax）トポロジ設定を検証します。

```
Device# show dot11Radio <interface> config
```

例：

ME（メッシュエンド）無線機 2

```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax primary
Frequency : 5745 MHz
Channel : 149
…….
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
```

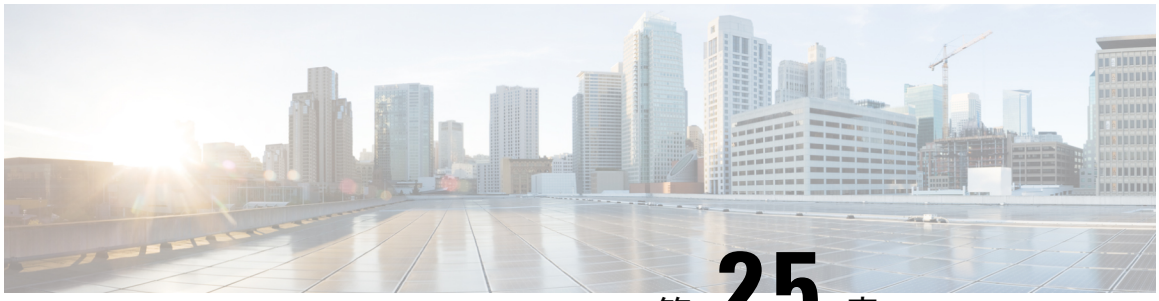
```
Automatic scan : enabled
Automatic scan threshold : disabled
```

MP2（メッシュポイント）

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5745 MHz
Channel : 149
…….
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax primary
Frequency : 5220 MHz
Channel : 44
Channel width : 40
…….
Fluidmax Configuration
Tower ID : 100
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
```

MP4 無線機 1

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5220 MHz
Channel : 44
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
```



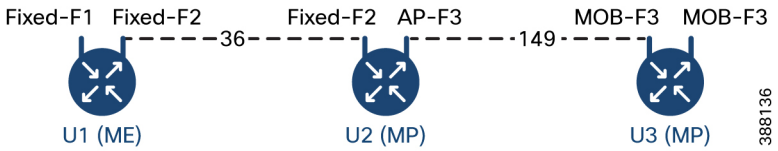
第 25 章

混合モード（固定インフラストラクチャ+Fluidity）トポロジの設定と検証

混合モード（固定インフラストラクチャ + Fluidity）トポロジの設定と検証

混合モード設定により、異なる周波数の多重無線デバイスを柔軟に設定できます。図から、U2は、固定インフラストラクチャ内の 1 つの無線機と、車両接続を同時に受け入れる Fluidity アクセスポイントとしての 2 番目の無線機で設定されています。U3 で両方の無線インターフェイスが Fluidity として設定されている場合、U1 の両方の無線インターフェイスが固定インフラストラクチャとして設定されます。固定インフラストラクチャロールが適切な場合、ワイヤレスインターフェイスは、P2MP（ポイントツーマルチポイント）ロール（プライマリまたはセカンダリ）の制限なしに Fluidmax モードで動作することもできます。

図 *4*:混合モードトポロジ



CLI による混合モードトポロジの設定

混合モードトポロジを設定するには、次の CLI コマンドを使用します。

```
Device# configure fluidity id {vehicle-auto | vehicle ID | infrastructure | wireless-relay}
```

fluidity id：デバイスの Fluidity ロールを設定します。

vehicle-auto：自動車両 ID 選択が使用される車両モード。

vehicle ID（英数字）：手動 ID が使用される車両モード。

infrastructure：デバイスのインフラストラクチャモードを設定します。

wireless-relay：バックホールへのイーサネット接続のないワイヤレスインフラストラクチャ。

```
Device# configure dot11Radio <interface>
```

interface：<0 ～ 3> dot11Radio インターフェイスの番号。

```
Device# configure dot11Radio <interface> {enable | disable}
```

enable または disable：ワイヤレスインターフェイスの管理状態を設定して、実行時に有効または無効にします

```
Device# configure dot11Radio <interface> mode {fluidity | fixed | fluidmax}
```

mode：指定されたインターフェイスの動作モード（Fluidity、Fixed、または Fluidmax）。

```
Device# configure dot11Radio <interface> channel <channel id>
```

channel：動作チャンネル ID <1 ～ 256> を設定します。

```
Device# wr
```

例：

U1 の設定

```
Device# configure dot11Radio 2 enable
Device# configure dot11Radio 2 mode fixed
Device# configure dot11Radio 2 channel 36
```

U2 の設定

```
Device# configure dot11Radio 1 enable
Device# configure dot11Radio 1 mode fixed
Device# configure dot11Radio 1 channel 36
Device# configure dot11Radio 2 enable
Device# configure dot11Radio 2 mode fluidity
Device# configure dot11Radio 2 channel 149
Device# configure fluidity id infrastructure
```

U3 の設定

```
Device# configure fluidity id vehicle-auto
Device# configure dot11Radio 1 enable
Device# configure dot11Radio 1 mode fluidity
Device# configure dot11Radio 1 channel 149
```

CLI による混合モードトポロジの検証

混合モードトポロジを検証するには、次の show コマンドを使用します。

```
Device# show dot11Radio <interface>config
```

U1 の統計：

```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
```

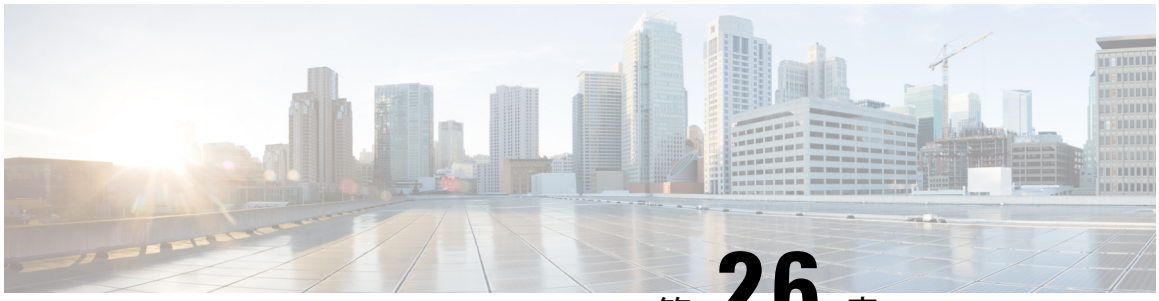
```
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

U2 の統計：

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidity
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

U3 の統計：

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidity
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```



第 26 章

高速フェールオーバーの設定と検証

高速フェールオーバーの概要

高速フェールオーバーは、特定のタイプのフェールオーバー設定です。この設定では、システムがサーバーの正常性を監視し、必要に応じて迅速に切り替えられます。

高速フェールオーバーのメカニズム：

- URWBベースのネットワーク内でハードウェアの冗長性とキャリアグレードの可用性を提供します。
- ハードウェア障害が発生した場合、高速フェールオーバーにより、ネットワークは次の時間内に再度復旧できます。
  - Fluidmax を使用する場合、30 秒未満（ネットワークサイズによって異なる）
  - Fluidity を使用する場合、500 ミリ秒未満

（注） 高速フェールオーバーはすべてのネットワークライセンスに含まれます。

高速フェールオーバーの設定と検証

（注） 高速フェールオーバーの設定と検証は、Fluidmax モードと Fluidity モードの両方に適用されます。

高速フェールオーバーを設定する前に、次の前提条件が満たされるようにします。

1. プライマリノードとバックアップ プライマリ ノードの両方が同じ設定であることを確認します。これには、チャンネルのパラメータ（周波数、チャンネル幅、モード）が同じであることなどが含まれます。Fluidmax が有効になっている場合は、両方のノードでクラスタ ID が同じであることを確認します。
2. ネットワーク内のすべてのデバイスで高速フェールオーバーを有効にします。

（注） Fluidmax 高速フェールオーバーは、イーサネットバックホールを使用した MP から MP または ME から ME へのフェールオーバーのみサポートされます。

CLI による高速フェールオーバーの設定

高速フェールオーバーを設定するには、このコマンドを使用します。

```
Device# configure modeconfig mode meshpoint
```

modeconfig：デバイスの現在の動作モードを設定します。モードは、メッシュエンド（ME）、メッシュポイント（MP）、またはグローバルゲートウェイ（L3）に設定できます。

```
Device# configure mpls fastfail status [enable | disable]
```

mpls：指定したデバイスの mpls データフレームパケットを設定します。

fastfail：高速フェールオーバー機能のステータス（有効または無効）を設定します。

```
Device# configure mpls fastfail timeout <0 - 65535>
```

fastfail timeout：デバイス障害検出の高速フェールオーバーのタイムアウトを設定します。

このコマンドを使用して、プリエンプション遅延を設定します。

```
Device# configure mpls preempt-delay <0- 65535>
```

デフォルトでは、プリエンプション遅延時間は 70 秒です。この期間中、プライマリデバイスはセカンダリデバイスから能動的に更新を収集します。これにより、ネットワークの現在のプリエンプション遅延ステータスを十分に把握できます。

（注） 無線インターフェイス設定は、両方の ME ポイントツーマルチポイントのプライマリで同じであることが必要です。

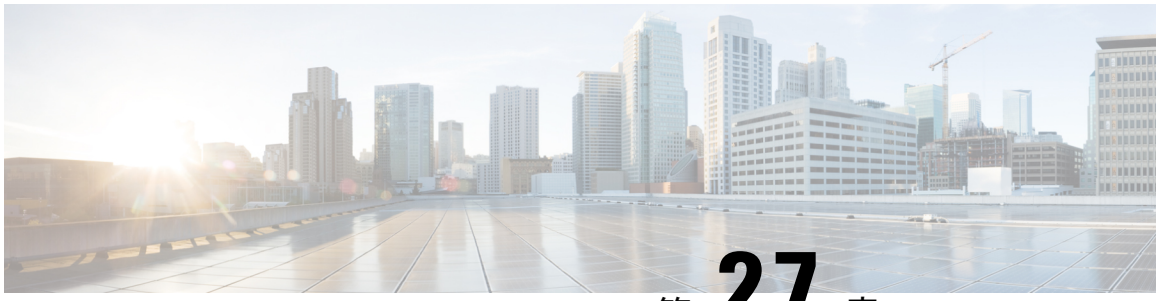
CLI による高速フェールオーバーの検証

このコマンドを使用して、高速フェールオーバーを検証します。

```
Device# show mpls config
Device# show dot11Radio <interface> fluidmax (check Fluidmax Primary ID and working
state)
```

例：

```
Device# show mpls config
layer 2
unicast-fllod
arp-unicast:
reduce-broadcast:
cluster ID
MPLS fast failover: enabled
Node failover timeout: 100 ms
……
MPLS tunnels:
Idp_id 381877266 debug 0 auto_pw 1
Local_gw 5.21.201.116 global_gw 0.0.0.0 pwlist {}
```



第 27 章

屋内展開の設定

屋内展開の設定

Catalyst IW9167E および IW9165 は、CLI を使用した屋内展開の有効化と無効化をサポートしています。

（注） 屋内展開設定を有効にする前に、Catalyst IW9167E または IW9165 が屋内モードに設定されていることを確認します。屋外モードは屋内で使用できますが、5150 ～ 5350 MHz チャンネルは国によっては屋内のみ許可されるため、屋内モードは屋外には適しません。

デフォルトでは、デバイスは屋外モードに設定されています。

屋内展開を有効にするには、次の CLI コマンドを使用します。

```
Device# configure wireless indoor-deployment enable
```

屋内展開を無効にするには、次の CLI コマンドを使用します。

```
Device# configure wireless indoor-deployment disable
```

E の屋内展開を確認するには、次の show コマンドを使用します。

屋内展開が有効になっている場合

```
Device# show Dot11Radio {1|2} config
DFS region : E
DFS radar role : auto
Radar detected : 0
Indoor deployment : enable
```

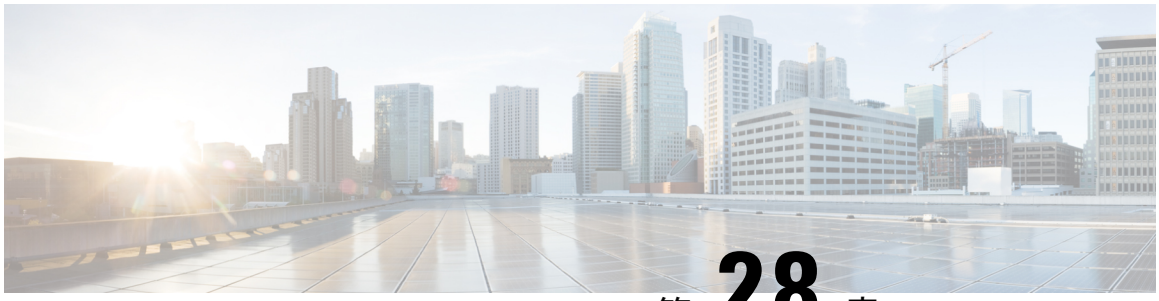
```
Device# show controllers Dot11Radio {1|2}
Radio info summary:
=====================
Radio : 5.0 GHz
Carrier set : (-Ei) GB
Base radio MAC : FC:58:9A:15:B7:C0
Supported channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

屋内展開の設定

屋内展開が無効になっている場合

```
Device# show Dot11Radio {1|2} config
DFS region : E
DFS radar role : auto
Radar detected : 0
Indoor deployment : disable
```

```
Device# show controllers Dot11Radio {1|2}
Radio info summary:
=====================
Radio : 5.0 GHz
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
```



第 28 章

レイヤ2メッシュの透過性の設定

レイヤ2メッシュの透過性の設定

レイヤ2メッシュ透過性機能を使用すると、特定のプロトコルのイーサネットタイプを選択できます。イーサネットタイプを転送するには、CLI コマンドまたは GUI を使用して、ネットワークを有効または無効にします。次のリストにある予約済みイーサネットタイプは設定できません。

表 *8*: 予約済みイーサネットタイプのリスト

イーサネットタイプ（範囲）	転送可能	その他の情報
0x0000 ～ 0x05FF	ユーザー設定可能	イーサネット I フレーム。STP と CDP は他の設定オプションの影響を受けます
0x0800	対応	IPv4
0x0806	対応	ARP（IPv4）
0x0900 ～ 0x09FF	非対応	URWB シグナリングプロトコル
0x8100	対応	IEEE 802.1Q VLAN カプセル化
0x8847 ～ 0x8848	非対応	MPLS
0xFFFF	非対応	IANA 予約済み

MPLS レイヤ 2 モードで使用する場合、URWB データ プレーン メッシュ ネットワークでは次の機能がサポートされます。

- レイヤ 2 メッシュ透過性機能を使用すると、許可されるイーサネットタイプを選択的にフィルタリングすることで、URWB ネットワーク全体で非 IPv4 レイヤ 2 プロトコルを転送します。
- URWB ネットワークに存在するイーサネットタイプが自動的に検出され、レポートされます。
- 許可リストのイーサネットタイプを追加および削除する機能。
- 便利な方法で完全な透過性を設定する（すべてのレイヤ 2 プロトコルを有効にする）機能。
- CLI と GUI の両方がサポートされます。

CLI を使用したレイヤ 2 プロトコル転送の設定と確認

レイヤ 2 プロトコル転送を設定するには、次の CLI コマンドを使用します。

許可リストにイーサネットタイプを追加するには、次の CLI コマンドを使用します。

```
Device# configure mpls ether-filter allow-list add

<0x0-0xffff> ether-type value
         all allow all ether-types
```

例：

```
Device# configure mpls ether-filter allow-list add 0x86DD

Device# show mpls config
        ...
        Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
        ...
```

許可リストのイーサネットタイプを削除するには、次の CLI コマンドを使用します。

```
Device# configure mpls ether-filter allow-list delete
         <0x0-0xffff> ether-type value
```

例：

```
Device# configure mpls ether-filter allow-list delete 0x86DD

Device# show mpls config
        ...
        Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
        ...
```

許可リストのすべてのイーサネットタイプをクリアするには、次の CLI コマンドを使用します。

```
Device# configure mpls ether-filter allow-list clear
```

例：

```
Device# show mpls config
                ...
                Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
                ...
```

```
Device# configure mpls ether-filter allow-list clear
Device# write
Device# reload

Device# show mpls config
...
Ethernet Filter allow-list: none, ethernet-I block
...
```

許可リストにすべてのイーサネットタイプを追加するには、次のCLIコマンドを使用します。

```
Device# configure mpls ether-filter allow-list add all
```

例：

```
Device# configure mpls ether-filter allow-list add all

Device# show mpls config
...
Ethernet Filter allow-list: all, ethernet-I block
```

（注） **all** キーワードは、イーサネットフィルタをオールパスモードに設定するために使用されます（許可リストに単一のエントリ 0x0000 を入力します）。

検出されたイーサネットタイプのリストをクリアするには、次のCLIコマンドを使用します。

```
Device# configure mpls ether-filter table clear
```

例：

```
Device# show mpls ether-filter
               Ether-type Direction Description
               0x8899      INGRESS    ---
               0x86DD      INGRESS    IPv6
        Device# configure mpls ether-filter table clear
               Cisco-81.160.136#show mpls ether-filter
               Ether-type Direction Description
               0x8899      INGRESS    ---
```

（注） 検出プロセスは、検出されたイーサネットタイプをクリアした後、バックグラウンドで動作します。

イーサネットIプロトコルを設定するには、次の CLI コマンドを使用します。

```
Device# configure mpls ether-filter ethernet-I forward
```

例：

```
Device# configure mpls ether-filter ethernet-I forward

Deive# show mpls config
        ...
        Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I forward
        ...


Device# configure mpls ether-filter ethernet-I block
```

例：

```
Device# configure mpls ether-filter ethernet-I block

         Device# show mpls config
         ...
         Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I block
```

許可されたイーサネットタイプのリストを確認するには、次の show コマンドを使用します。

```
Device# show mpls config
```

例：

```
Device# show mpls config
                ...
                Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
                ...
```

検出されたイーサネットタイプのリストを確認するには、次の show コマンドを使用します。

```
Device# show mpls ether-filter table
```

例：

```
Device# show mpls ether-filter table
                Ether-type   Direction   Description
                0x8899        INGRESS       ---
                0x86DD        INGRESS       IPv6
```

GUI を使用したレイヤ 2 プロトコル転送の設定

特定のイーサネットタイプと検出されたイーサネットタイプを許可リストに追加するには、次の手順を実行します。

1. [ADVANCED SETTINGS] で、[ethernet filter] をクリックします。

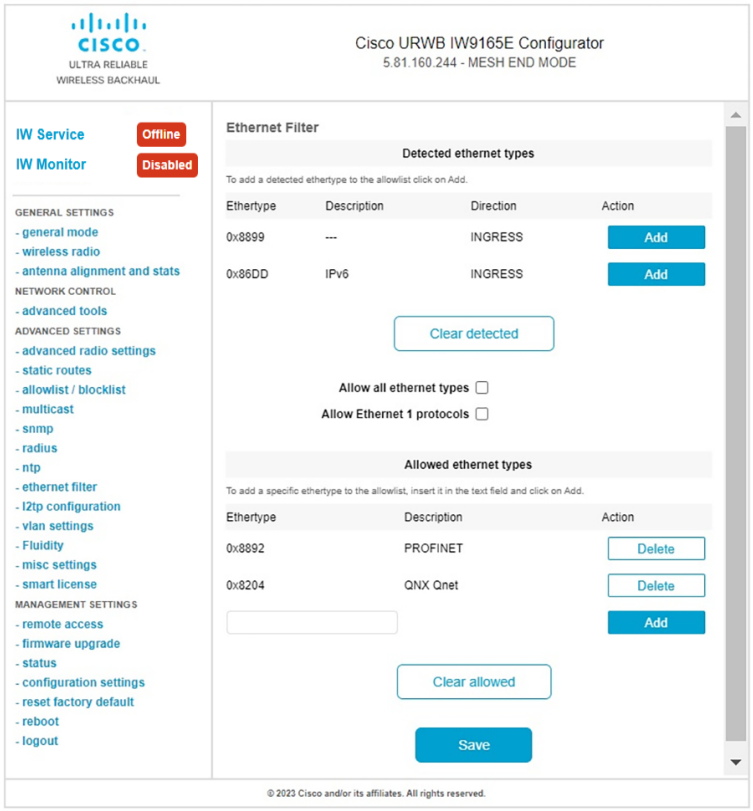
   [Ethernet Filter] ウィンドウが表示されます。

2. [Detected ethernet types] セクションで、[Add] をクリックして許可リストにイーサネットタイプを追加します。

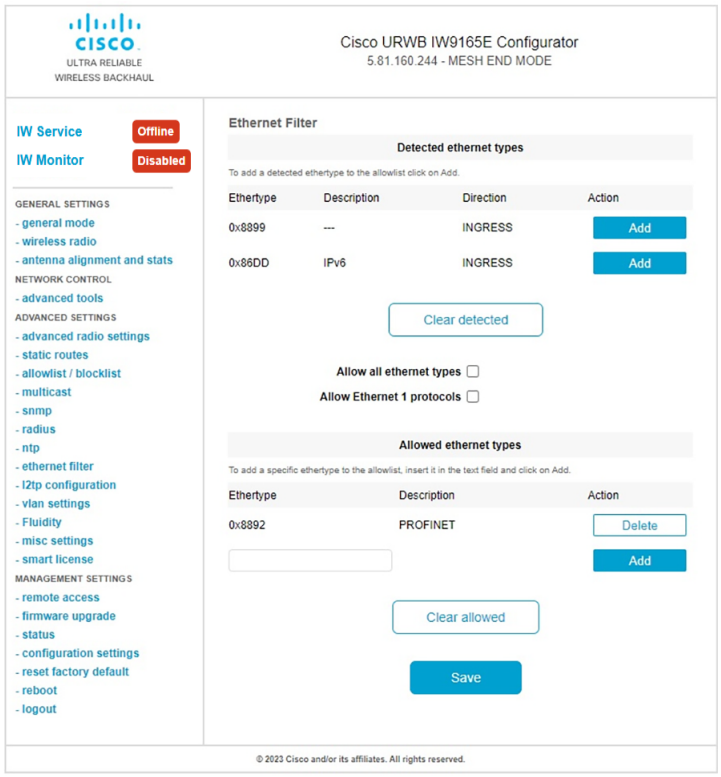
3. 追加し終えると、追加済みのイーサネットタイプが [Allowed Ethernet type] セクションに反映されます。

4. [Allowed ethernet types] セクションで、特定のイーサネットタイプを許可リストに追加するには、テキストボックスに [Ethertype] 名を入力し、[Add] をクリックします。

次の画像は、許可リストに追加された特定のイーサネットタイプと検出されたイーサネットタイプを示しています。


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
ULTRA RELIABLE WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
Ethernet Filter
Detected ethernet types
To add a detected ethertype to the allowlist click on Add.
Ethertype
Description
Direction
Action
0x8899

INGRESS
Add
0x86DD
IPv6
INGRESS
Add
Clear detected
Allow all ethernet types
Allow Ethernet 1 protocols
Allowed ethernet types
To add a specific ethertype to the allowlist, insert it in the text field and click on Add.
Ethertype
Description
Action
0x8892
PROFINET
Delete
0x8204
QNX Qnet
Delete
Add
Clear allowed
Save
© 2023 Cisco and/or its affiliates. All rights reserved.


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
ULTRA RELIABLE WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
Ethernet Filter
Detected ethernet types
To add a detected ethertype to the allowlist click on Add.
Ethertype
Description
Direction
Action
0x8899

INGRESS
Add
0x86DD
IPv6
INGRESS
Add
Clear detected
Allow all ethernet types
Allow Ethernet 1 protocols
Allowed ethernet types
To add a specific ethertype to the allowlist, insert it in the text field and click on Add.
Ethertype
Description
Action
0x8892
PROFINET
Delete
Add
Clear allowed
Save
© 2023 Cisco and/or its affiliates. All rights reserved.

許可リストから許可されたイーサネットタイプをすべてクリアするには、次の手順を実行します。

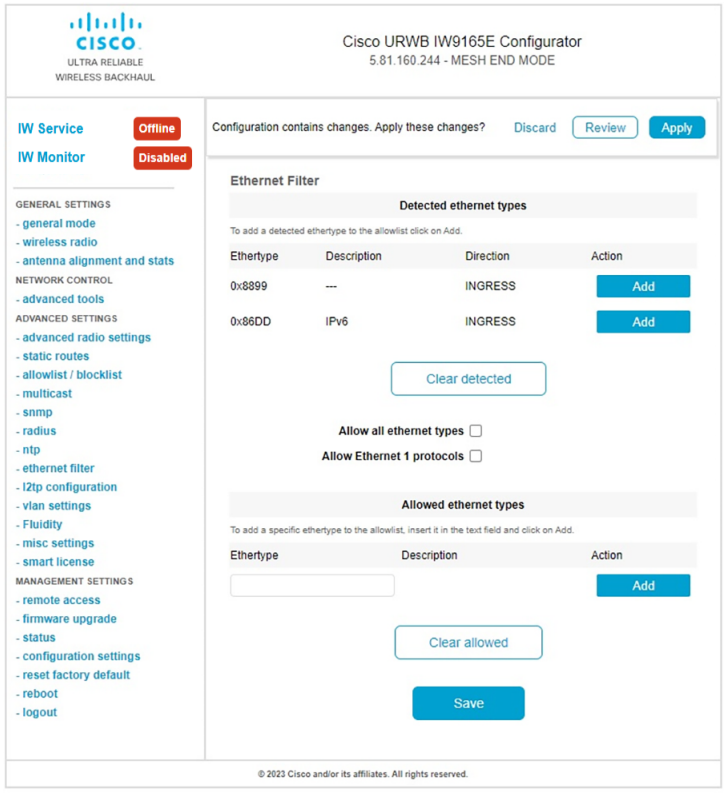
1. [ADVANCED SETTINGS] で、[ethernet filter] をクリックします。

   [Ethernet Filter] ウィンドウが表示されます。

2. 許可リストからすべてのイーサネットタイプをクリアするには、[Allowed ethernet types] セクションで [Clear allowed] をクリックします。

3. [Clear allowed] をクリックすると、許可リストからすべてのイーサネットタイプがクリアされます。

次の画像は、許可リストから許可されたイーサネットタイプがすべてクリアされたことを示しています。



許可リストから検出されたイーサネットタイプをすべてクリアするには、次の手順を実行します。

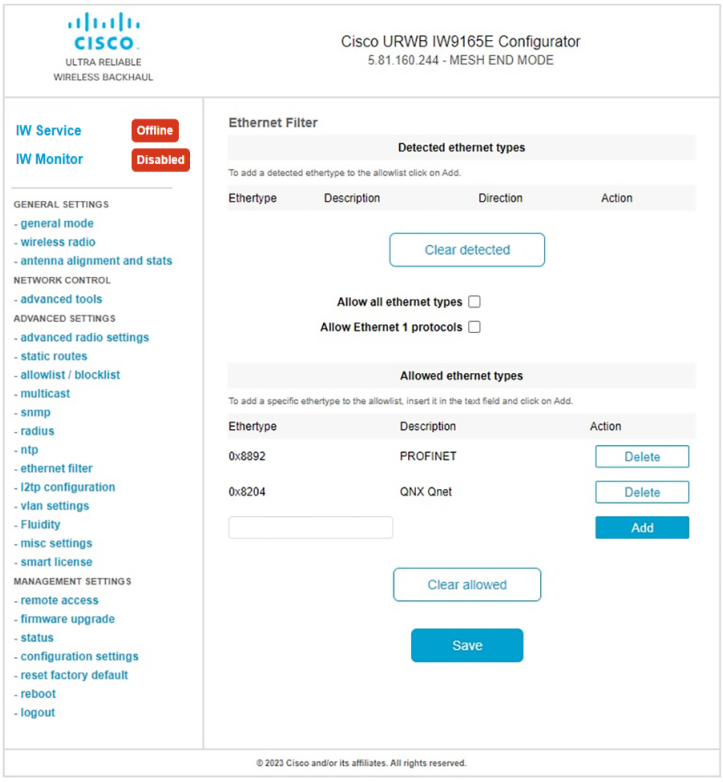
1. [ADVANCED SETTINGS] で、[ethernet filter] をクリックします。

   [Ethernet Filter] ウィンドウが表示されます。

2. [Detected ethernet types] セクションで [Clear detected] をクリックして、許可リストから検出されたイーサネットタイプをクリアします。

3. [Clear detected] をクリックすると、[Detected ethernet types] セクションのイーサネットタイプがクリアされます。

次の画像は、許可リストから検出されたイーサネットタイプがすべてクリアされたことを示しています。



すべてのイーサネットタイプを許可リストに追加する（許可する）には、次の手順を実行します。

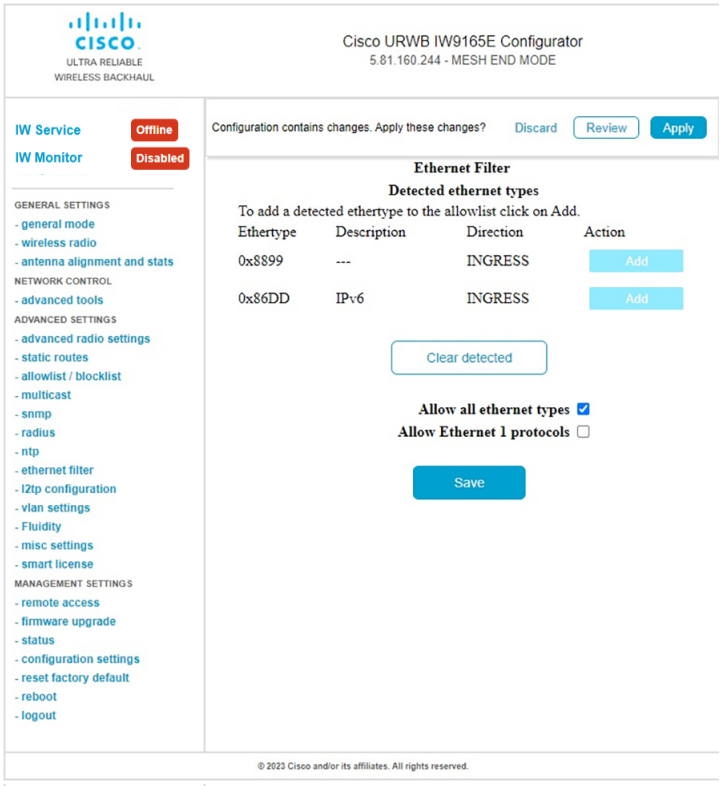
1. [ADVANCED SETTINGS] で、[ethernet filter] をクリックします。

   [Ethernet Filter] ウィンドウが表示されます。

2. [Ethernet Filter] セクションの [Allow all ethernet types] チェックボックスをオンにして、すべてのイーサネットタイプを許可リストで許可します。

3. [Save] に続いて [Apply] をクリックして、設定を変更します。

次の画像では、すべてのイーサネットタイプが許可リストに追加されています。



イーサネット 1 プロトコルを設定するには、次の手順を実行します。

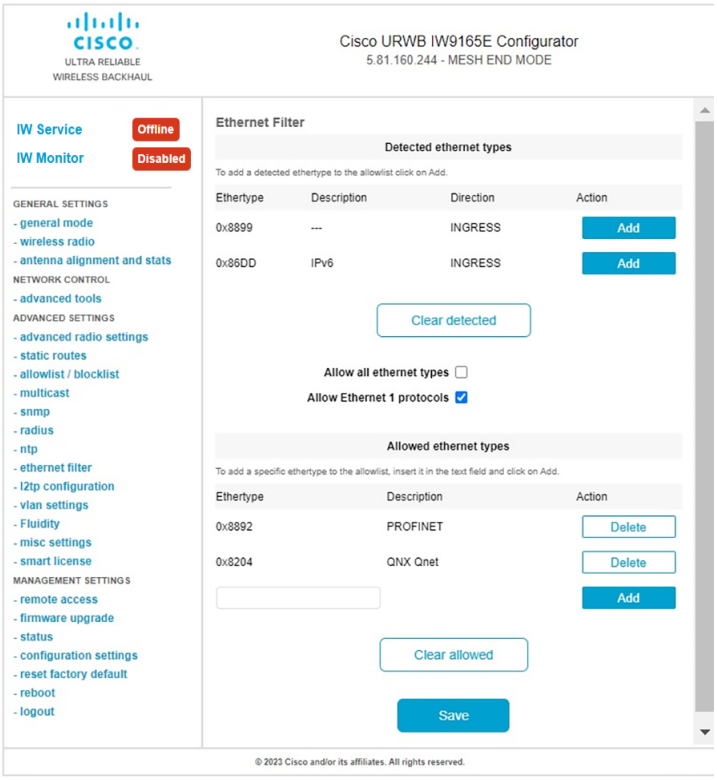
1. [ADVANCED SETTINGS] で、[ethernet filter] をクリックします。

   [Ethernet Filter] ウィンドウが表示されます。

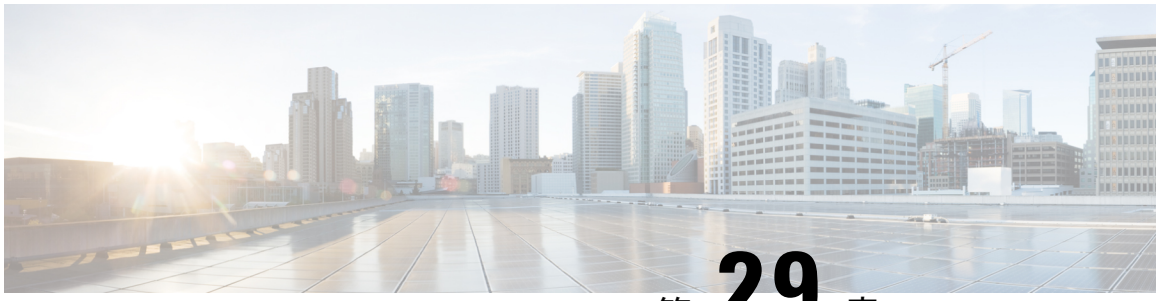
2. [Ethernet Filter] セクションの [Allow Ethernet 1 protocols] チェックボックスをオンにして、イーサネット 1 プロトコルモードを有効にします。

3. [Save] に続いて [Apply] をクリックして、設定を変更します。

次の画像は、イーサネット 1 プロトコルを許可する設定を示しています。


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
ULTRA RELIABLE WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
Ethernet Filter
Detected ethernet types
To add a detected ethertype to the allowlist click on Add.
Ethertype
Description
Direction
Action
0x8899

INGRESS
Add
0x86DD
IPv6
INGRESS
Add
Clear detected
Allow all ethernet types
Allow Ethernet 1 protocols
Allowed ethernet types
To add a specific ethertype to the allowlist, insert it in the text field and click on Add.
Ethertype
Description
Action
0x8892
PROFINET
Delete
0x8204
QNX Qnet
Delete
Add
Clear allowed
Save
© 2023 Cisco and/or its affiliates. All rights reserved.



第 29 章

マルチパス動作の設定

MPO の概要

速で動く移動体システムでは、高速な車上のネットワーク接続が期待されます。これは、途切れることのない高信頼な路車間無線通信を意味します。しかし、ネットワークの動的な性質、無線周波数の環境条件、およびさまざまな Wi-Fi 標準に従うローミングにより、パケット損失が発生します。マルチパスオペレーション（MPO）は、複数のワイヤレスパスにパケットの重複する複製を送信することにより、信頼性を高めます。この特許取得済みのテクノロジーは、優先順位の高いトラフィックを最大 4 倍に複製し、ハードウェア障害を減らして可用性を高め、遅延を短縮し、干渉の影響を軽減します。

MPO は、モバイルシステムとワイヤレスネットワークのバックエンド インフラストラクチャの間に複数のラベルスイッチドパス（LSP）を確立するためのアプローチを採用しています。複数の LSP により、優先順位の高いパケットを冗長パス経由で送信することで、パケット損失を低減できます。

MPO の機能

デフォルトでは、MPLS は、車両とインフラストラクチャ間のデータ伝送用に、単一のワイヤレスリンクを使用して単一のトンネルを確立します。2 つの車載無線機で 2 つの無線インターフェイスを使用する場合は、4 つの MPLS トンネルを設定して MPO 保護対象トラフィックを送信できます。保護対象トラフィックに複数のリンクを使用するように MPO を設定すると、使用可能な各ワイヤレスリンク上に MPLS トンネルが作成されます。各ワイヤレスリンクによって、MPO 保護対象トラフィックが複製されます。1 つのワイヤレスリンクに障害が発生し

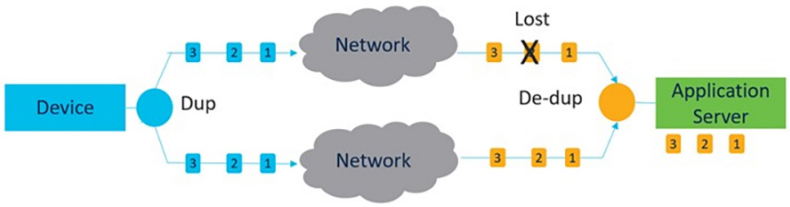
ても、他のリンクがトラフィックを複製します。UIW リリース 17.14.1 では、MPO で高速フェールオーバーがサポートされます。

MPO パケットの複製と重複除去

MPO では、複製されたパケットが複数のワイヤレスチャンネルを介して（さまざまなアクセスポイントに）送信されます。これにより信頼性が確保され、受信側アクセスポイントの空間ダイバーシティにより、少なくとも 1 つの複製が正しく受信される可能性が大幅に向上します。重複除去は、異なるワイヤレスパスで受信されたパケットの重複を解消するための、MPO のもう 1 つの機能です。

その結果、配信されるパケットにはシーケンス番号が割り当てられているため、重複除去アルゴリズムはすでに受信したパケットの複製を削除できます。

複製と重複除去のプロセスを以下に示します。



複製と重複除去のアルゴリズムでは、次の処理が実行されます。

- パケット損失と非対称な高遅延/可変遅延パスに対処します。
- バッファリングによって発生する追加のパケット遅延をなくします。
- 重複パケットとシーケンス外のパケットを削除します。
- CPU、リソース、およびメモリの効率を向上させます。

CLI を使用した MPO 機能の設定

MPO を設定する前に、802.1p ベースの QoS を有効にする必要があります。

MPO 機能を設定するには、次の CLI コマンドを使用します。

```
Device# configure fluidity mpo
```

cos：MPO 冗長性（一度に 1 つの CoS のみ）で保護するトラフィックのサービスクラス（CoS）を設定します。有効な cos の範囲は 0 ～ 7 で、デフォルト値は 6 です。

path：モバイルデバイスのみによって確立される同時冗長パスの最大数を設定します。有効な最大パスリンクの範囲は 1 ～ 4 で、デフォルト値は 1 です。

rssi：ワイヤレスリンクの最小 RSSI しきい値を冗長パス（dB）として設定します（モバイルデバイスのみ）。有効な最小 rssi 値の範囲は 0 ～ 96 で、デフォルト値は 20 です。

telemetry：特定の MPO テレメトリの有効化/無効化を設定します。telemetry 値は、有効：M=1 または無効：M=0（デフォルト）です

```
Device# configure fluidity mpo status
```

disabled：MPO の複製/重複除去を無効にします。

rx-only：MPO ステータスを rx-only に設定します。着信 MPLS トラフィックの重複除去し、発信トラフィックを複製しません。

enabled：MPO を有効にします。発信トラフィックを複製して、着信 MPLS トラフィックを重複除去します。

例：

```
Device# configure fluidity mpo cos C ( C value from 0 to 7 (default 6))
Device# configure fluidity mpo path max N ( N value from 1 to 4 ( default 1))
Device# configure fluidity mpo rssi min R ( R value from 0 to 96 ( default 20))
Device# configure fluidity mpo telemetry T (T can be one of: enabled: M=1
                                              Disabled: M=0 (default))
Device# configure fluidity mpo status S ( S can be one of:
                                          enabled: E=1 F=1
                                          rx-only: E=1 F=0
                                          disabled: E=0 F=1 (default))
```

次に、MPO カウンタを使用した UDP テレメトリストリームの例を示します。

```
Device# configure fluidity mpo telemetry <enabled | disabled>
Device# configure telemetry server 192.168.0.200
Device# configure telemetry export enable
Device# configure fluidity mpo telemetry enabled
```

MPO 設定パラメータを確認するには、次の show コマンドを使用します。

```
Device# show fluidity mpo config
```

例：

```
Device# show fluidity mpo config
                Status: enabled
                Path max links: 2
                RSSI min: 20
                CoS: 6
```

CLI を使用した MPO 機能の確認（MPO 監視）

show mpls config コマンドの出力：

```
Device# show mpls config
                   5.42.42.43:
                   path_id : 0
                   ilm : 136000
                   nhlfe : 16:
                   lbr : 5.42.42.42
                   age : 6.980000028 { 5.42.42.42 5.42.42.43 }

                   path_id : 1
                   ilm : 136001
                   nhlfe : 18:
                   lbr : 5.42.42.42
                   age : 6.970000026 { 5.42.42.42 5.42.42.43 }
```

show fluidity mpo statistics コマンドの出力：

```
Device# show fluidity mpo statistics (on Mesh End)
            table-size 2:

             MAC address : 40:36:5A:15:C8:50        8C:89:A5:83:EB:71
             Tx-1        : 0                        208
             Tx-2        : 0                        208
             Rx-Accept-1 : 178                      0
             Rx-Accept-2 : 30                       0
             Rx-Drop-1   : 30                       0
             Rx-Drop-2   : 178                      0
             Lost-1-only : 0                        0
             Lost        : 0                        0

Device# show fluidity mpo statistics (on Mobile Primary unit)
            table-size 2:

            MAC address : 40:36:5A:15:C8:50        8C:89:A5:83:EB:71
            Tx-1        : 208                      0
            Tx-2        : 208                      0
            Rx-Accept-1 : 0                        182
            Rx-Accept-2 : 0                        26
            Rx-Drop-1   : 0                        26
            Rx-Drop-2   : 0                        182
            Lost-1-only : 0                        0
            Lost        : 0                        0
```

MAC address：パケットを送信している外部ネットワークデバイスの送信元 L2 アドレス。

Tx-1 および Tx-2：重複の対象となるパケットの総数を示しています。

Rx-Accept-1 および Rx-Accept-2：これらのカウンタは、それぞれ、プライマリパスまたはセカンダリパスのいずれかで重複除去プロセスで受信および破棄されたパケットの数を表しています。

Lost-1-only：セカンダリパスの重複除去プロセスで受信されて受け入れられ、プライマリパスでは受信されず受け入れられなかったパケットの数。

Lost：プライマリパスとセカンダリパスの両方で失われたパケットの累積数。

`show fluidity network` コマンドの出力：

```
Device# show fluidity network (on Mesh End and Mobile Primary)

                  unit 5.21.201.60  infrastructure meshend primary
                  vehicles 4  total_mobiles 5
                  infrastructure 1  backbone 0  meshend 5.21.201.60

                  Vehicle ID : + 85313616
                  Path : 0
                  Infrastr.ID : 5.21.201.60
                  Via : R1
                  Mobile ID : 5.21.200.80
                  Via : R2
                  H/O seq : 5710
                  H/O age : 36.597
                  #M: 2
                  Primary ID : 5.21.200.80
                  Secondary IDs : 5.21.201.204

                  Vehicle ID : + 85313616
```

```
Path : 1
Infrastr.ID : 5.21.201.60
Via : R2
Mobile ID : 5.21.201.204
Via : R2
H/O seq : 5711
H/O age : 5.909
#M: 2
Primary ID : 5.21.200.80
Secondary IDs : 5.21.201.204
```

（注） 中間ノード（MP およびモバイルセカンダリ）には、パスのサブセットのみがあります。

MPO パス ID 0：プライマリパス、その他：冗長パス。

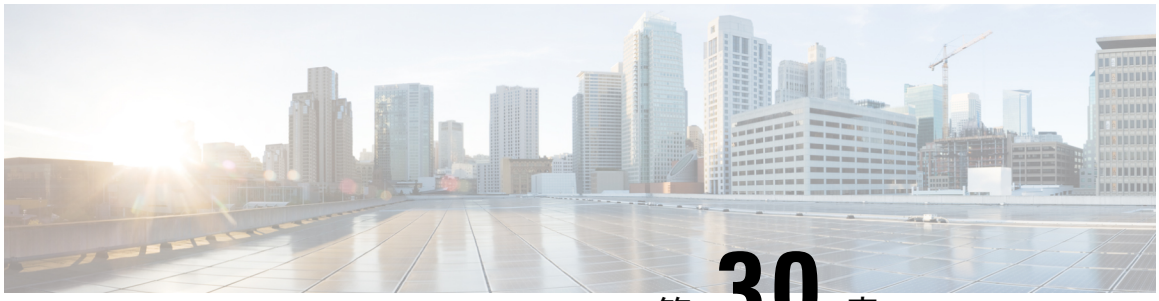
show eng-stats コマンドの出力：

```
Device# show eng-stats (on mobile primary unit)
....
Fluidity role : primary
vehicle id : 0
static  : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile  : 4.21.200.80 [FC:58:9A:15:B9:13]
snr : 42
rssi : -54
dop : 40
chan : 132/40
handoff: 21.518258794
time : 2
Current:
ho_seq: 7  pending: false  age: 21.518303221  primary: 5.21.200.80
[0] - <3.21.201.60 - 4.21.200.80> status SUCCESS seq 6 id 0 age 59.469266332 rssi 42
[1] - <4.21.201.60 - 4.21.201.204> status SUCCESS seq 7 id 1 age 21.518317752 rssi 41
last primary: <3.21.201.60 - 4.21.200.80>
free ids: 7 6 5 4 3 2
current missing path mask: 1111110

HO Table
static  : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile  : 4.21.200.80 [FC:58:9A:15:B9:13]
rssi : 42
dop : 40
chan : 132/40
updated : 74
skip : 0

static  : 4.21.201.60 [FC:58:9A:15:C7:D3]
mobile  :  4.21.201.204 [FC:58:9A:15:E4:D3]
rssi : 41
dop : 40
chan : 100/40
updated : 18
skip : 0
rssi_delta : 6 3
threshold : 35
```

MPO の制限事項

MPO が有効になっている場合、次のハンドオフ機能は使用できません。

- ポール禁止およびポール近接
- 色分け
- 負荷分散



第 30 章

URWB テレメトリプロトコルの設定

URWB テレメトリプロトコルの設定

UIW リリース 17.12.1 より URWB テレメトリプロトコルが導入され、リアルタイムのワイヤレス性能のカスタム外部監視が可能になります。サードパーティアプリケーションおよびカスタムアプリケーションでこのデータを使用できます。定期的に送信される定義済みの構造化 UDP パケットには、さまざまなネットワークメトリックが含まれています。

各アクセスポイントは、その無線機のデータをエクスポートします。このデータは、受信アプリケーションによってライブで解釈することも、キャプチャして後で処理することもできます。

プロトコル形式の詳細については、シスコサポートに連絡して、URWB テレメトリプロトコルの参照ドキュメントをリクエストしてください。

テレメトリ UDP パケットには、次の情報が含まれています。

- パケットの信号強度
- パケットのスループットと移行レート
- 送信および再送信の数
- 変調レート
- パケット損失の詳細
- 各無線機の動作周波数
- ネットワークを記録するイベントに関する情報

CLI を使用した URWB テレメトリプロトコルの設定

デフォルトでは、テレメトリデータは無効になっています。テレメトリパケットを生成するには、次の CLI コマンドを使用します。

URWB テレメトリプロトコルの設定

受信者の IP アドレスと UDP ポートを設定するには、次の CLI コマンドを使用します（マルチキャストアドレスがサポートされています）。

```
Device# configure telemetry server <dest IP [port]>
```

設定された受信者への URWB テレメトリプロトコル送信を有効または無効にするには、次の CLI コマンドを使用します（マルチキャストアドレスがサポートされています）。

```
Device# configure telemetry server <dest IP [port]>
```

設定されたサーバーへの raw UDP テレメトリ送信を有効または無効にするには、次の CLI コマンドを使用します。

```
Device# configure telemetry export [ enable | disable ]
```

例：

```
Device# configure telemetry export enable
Device# configure telemetry server 10.115.11.56 1234
Device# write
Device# reload
```

（注）
- **export enable** CLI コマンドを実行する前に、IP アドレスが設定されていることを確認します。設定されていない場合、コマンドは「please configure the telemetry server IP first」というエラーで拒否されます。
- **export disable** CLI コマンドを実行すると、IP サーバーは同時に 0.0.0.0 に設定されます（ポート値は変更されません）。

テレメトリ設定を確認するには、次の show コマンドを使用します。

```
Device# show telemetry config
Telemetry export: enabled, current (live): disabled
Telemetry server: 10.115.11.56 1234, current (live): 0.0.0.0 30000
```

CLI を使用した URWB テレメトリプロトコルのライブ設定

```
Device# configure telemetry live
Export : enable/disable telemetry export
Server : set telemetry server IP address (and port)
```

（注） ライブ テレメトリ エクスポートを有効にする前に、サーバーの設定が必要です。

例：

```
Device# configure telemetry live export enable
Error: please configure the telemetry server IP first
```

例（サーバー設定後のテレメトリエクスポート）：

```
Device# configure telemetry live server 10.115.11.56 1234
Device# configure telemetry live export enable
Device# show telemetry config
Telemetry export: enabled, current (live): enabled
Telemetry server: 10.115.11.56 1234, current (live): 10.115.11.56 1234
```

（注） live 修飾子が指定されている場合、このコマンドはすぐに現在の設定に影響します。live 修飾子が使用されていない場合は、設定ファイルのみが変更されます。

CLI を使用した GNSS テレメトリプロトコルの設定

GNSS テレメトリを有効にするには、次の CLI コマンドを使用します。

```
Device# configure gnss telemetry enable
```

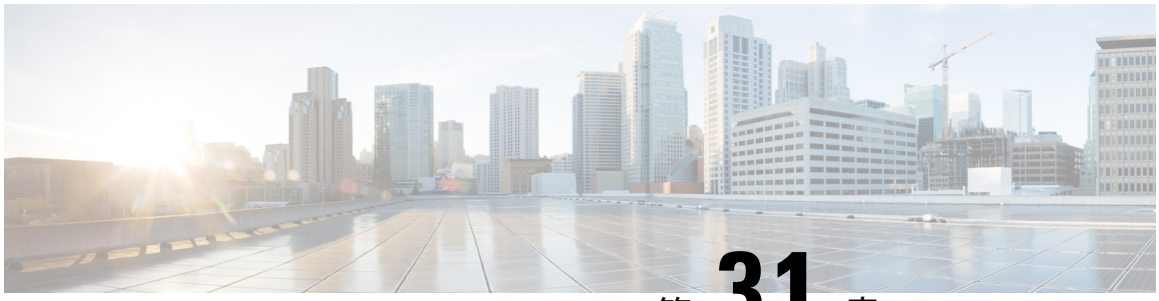
GNSS テレメトリを無効にするには、次の CLI コマンドを使用します。

```
Device# configure gnss telemetry disable
```

GNSS テレメトリを表示するには、次の CLI コマンドを使用します。

```
Device# show gnss telemetry
```

URWB テレメトリプロトコルの設定



第 31 章

IW Monitor 管理の設定

IW Monitor 管理の設定

UIW リリース 17.12.1 では、IW Monitor のサポートが導入されます。これは、次の機能をサポートする、スタンドアロンのオンプレミス監視アプリケーションです。

表 *9 : UIW* リリース *17.12.1* 以降の *IW Monitor* 機能のサポート

機能	説明
RADIUS（Remote Authentication Dial-In User Service）の IW Monitor ログ	モバイルユニットによる Radius 認証の試行が IW Monitor に記録されます
IW Monitor ログ CLI SSH アクセス	SSH 接続の試行が IW Monitor に記録されます
IW Monitor ログ GUI アクセス	GUI へのログインが IW Monitor に記録されます
IW Monitor ログ イーサネット リンク変更	LAN ポートの物理リンクの変更がバッファリングされて IW Monitor に記録されます
IW Monitor ログ設定変更	CLI または GUI を介してユニット設定に適用された変更が Monitor に記録されます

オンプレミス IW Monitor は、次の主要な機能をサポートしています。

- ネットワークステータスを監視するためのダッシュボード
- ネットワークのトポロジ表示
- ワイヤレス主要性能指標（KPI）のリアルタイムチャートと履歴チャート
- リアルタイムの性能監視
- IW デバイスから送信されたテレメトリデータの処理

- ネットワーク イベント ロギング

UIW リリース 17.12.1 では、IW Monitor ダッシュボードの次のサポートが提供されます。

- アタッチおよびデタッチ機能。
- テレメトリプロトコルのサポート。
- CLI および GUI 管理。

CLI を使用した IW Monitor 管理のデタッチ

IW Monitor には設定は不要で、アクセスポイントが IW Monitor に追加されます。次の CLI を使用して、IW Monitor サーバーからデバイスをデタッチし、接続のトラブルシューティングを行います。

```
Device# configure monitor
         detach : detach MONITOR action
```

例：

```
Device# configure monitor detach
```

CLI を使用した IW Monitor 管理の確認

IW Monitor 管理を確認するには、次の show コマンドを使用します。

```
Device# show monitor
```

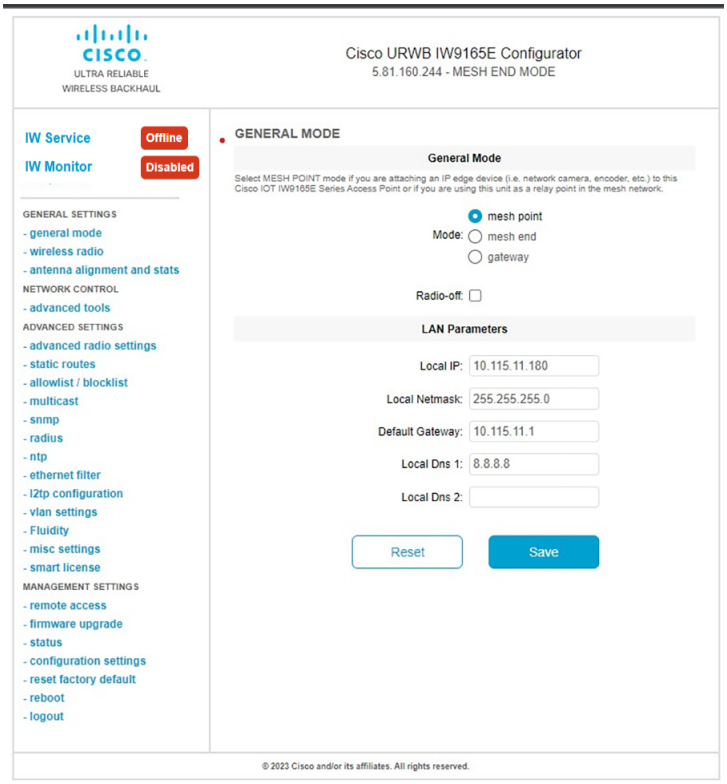
例：

```
Device# show monitor
IW MONITOR: enabled
Status: Connected
```

GUI を使用した IW Monitor 管理の設定

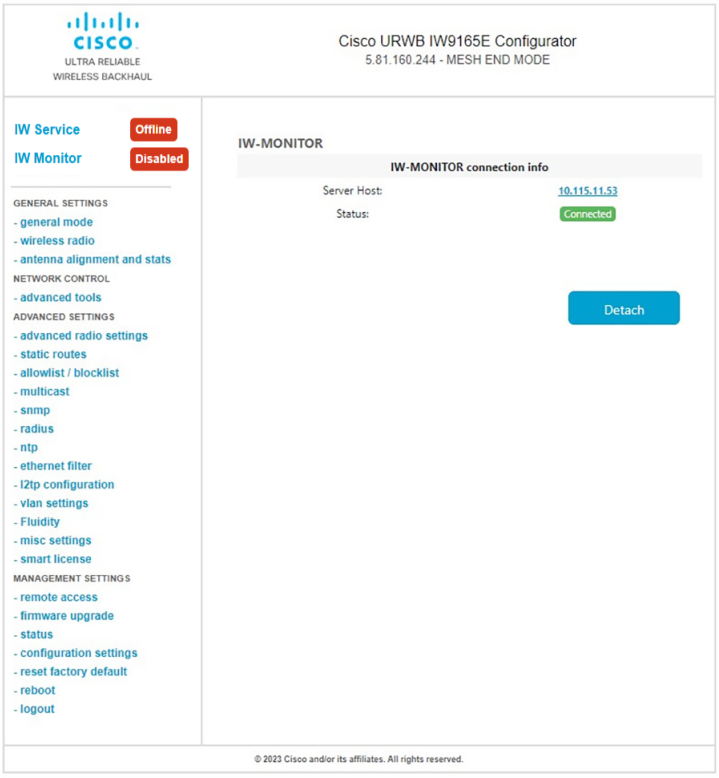
次の画像では、[Cisco URWB IW9165E Configurator] または [Cisco URWB IW9167E Configurator] ウィンドウで [IW MONITOR] オプションが有効になっています。

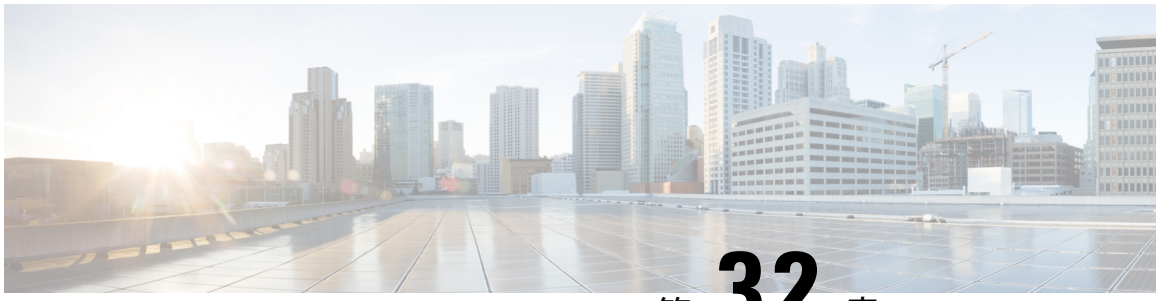
IW Monitor 管理の設定



[IW-MONITOR] オプションを有効にすると、[IW-MONITOR connection info] が次のように表示されます。

IW Monitor 管理の設定





第 32 章

Catalyst IW9167 および IW9165 の LED パターン

Catalyst IW9167 の LED パターン

Catalyst IW9167E は、ブートプロセス中に以下の LED パターンに従います（通常のブートプロセス中は緑色に点滅します）。

表 *10* : ブート中の *LED* パターンの定義

イベント	LED の状態
ブートローダの状態シーケンス DRAM メモリ テスト中 DRAM メモリ テスト OK ボードの初期化中 フラッシュファイルシステムの初期化 フラッシュ メモリ テスト OK イーサネットの初期化中 イーサネット OK AP OS の起動中 初期化成功	緑色の点滅
リセットボタンを長押ししたとき（20秒未満）	赤色の点滅
リセットボタンを長押ししたとき（20秒以上）	赤色の点灯

イベント	LED の状態
リセットボタンを離したとき または リセットボタンを長押ししたとき（60秒以上）	緑色の点滅

アクセスポイントの起動後は、Catalyst IW9167E は以下の LED パターンに従います。

表 *11 : URWB OS LED* パターンの定義

AP の状態	LED の状態
一般的な警告：インラインパワー不足	赤色、緑色、橙色の繰り返し
プロビジョニングモード：フォールバック	橙色の点滅
プロビジョニングモード：DHCP	橙色
SNR（信号対雑音比）最高（25 dB 以上）	緑色の点滅
SNR 良好（15<=X<25 dB）	フェードイン（緑色）
SNR 不良（10<=X<15 dB）	フェードイン（橙色）
SNR 許容範囲外（10 dB 未満）	フェードイン（赤色）

Catalyst IW9165 の LED パターン

Catalyst IW9165E には、赤色、緑色、青色の 3 色 LED があります。Catalyst IW9165D には、赤色、緑色、橙色の LED があり、3 つの明るさレベルがあります。アクセスポイントの明るさレベルは変更できます。コントローラの CLI または GUI は、8 つの異なる設定で明るさを制御します。

URWB スタックのシステム LED には、URWB の状態を示す以下のパターンがあります。

表 *12 : URWB* の状態の *LED* パターン

AP の状態	LED の状態
フォールバック	橙色または青色の点滅
DHCP	橙色または青色

RSSI LED

Catalyst IW9165 には、RF 受信信号強度表示（RSSI）を示す、緑色と橙色の 2 色の LED があります。RSSI LED に異なる明るさレベルはありません。

表 *13 : RSSI LED*

黄色の LED	緑色の LED	説明
点滅	消灯	RSSI が - 86 dBm 未満
点灯	消灯	RSSI が - 86 〜 - 81 dBm
消灯	点滅	RSSI が - 81 〜 - 71 dBm
消灯	点灯	RSSI が - 71 dBm 超

次の表に、Catalyst IW9165E の LED の機能を示します。

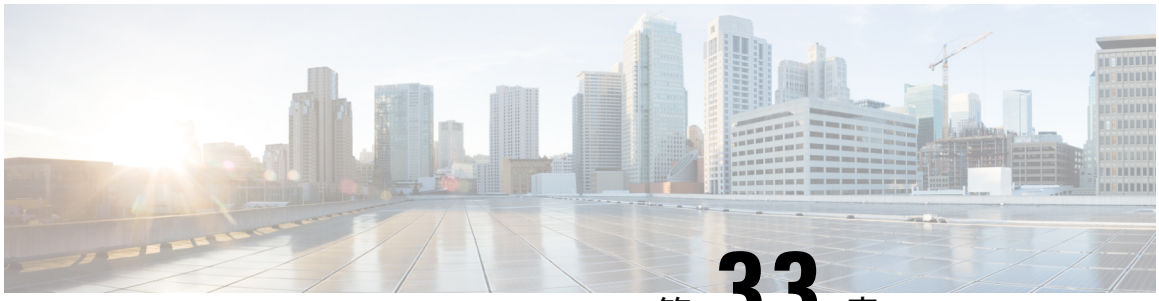
表 *14 : Catalyst IW9165E の URWB LED* の機能

LED 機能ラベル	色/状態	説明（デフォルト = 消灯）
システムステータス	3 色 RGB	さまざまなシステムステータスを示します
RSSI	黄色または緑色	RSSI が - 86 dBm 未満：黄色 - 86 dBm =< RSSI =< - 81 dBM：緑色の点滅 RSSI が - 81 dBm 超：緑色
WAN GE	緑色	ポートがアップ状態、リンクあり
	緑色の点滅	アクティビティが発生しているリンク
	消灯	リンクなしまたはポートがオフ
LAN GE	緑色	ポートがアップ状態、リンクあり
	緑色の点滅	アクティビティが発生しているリンク
	消灯	リンクなしまたはポートがオフ
デジタル IO 1 〜 2	黄色	デジタル入力または出力がアクティブ
	消灯	デジタル入力または出力が非アクティブ

次の表に、Catalyst IW9165D の LED の機能を示します。

表 *15 : Catalyst IW9165D* の *URWB LED* の機能

LED 機能ラベル	色/状態	説明（デフォルト = 消灯）
システムステータス	3 色 RGA	さまざまなシステムステータスを示します
RSSI	黄色または緑色	RSSI が - 86 dBm 未満：黄色 - 86 dBm =< RSSI =< - 81 dBM：緑色の点滅 RSSI が - 81 dBm 超：緑色



第 33 章

ローミングパラメータの設定と確認

パケット再試行回数の制限

UIW リリース 17.15.1 以降では、ユニキャストパケットのパケット再送信回数の制限を設定できます。これには、集約パケットと非集約パケットの両方が含まれます。

（注） パケット再送信の最大再試行回数は 32 回です。

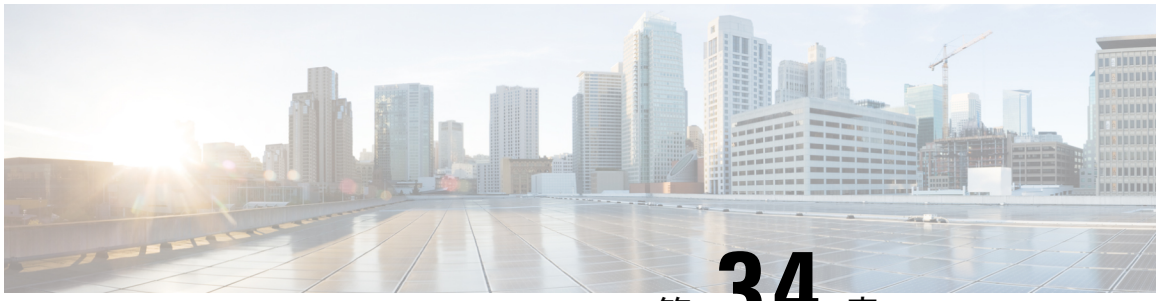
CLI を使用したパケット再送信の試行回数の上限の設定

AP でのパケット再送信の試行回数の上限を設定するには、このコマンドを使用します。

```
Device#configure dot11Radio <N> packet retries <retry-count>
```

CLI を使用したパケット再送信の試行回数の上限の確認

```
Device#show dot11Radio 1 config
.
.
.
DFS region:             Q
DFS radar role:         auto
Radar detected:         0
Indoor deployment:      disable
Rx-SOP Threshold:       0 dBm(AUTO)
Max packet retries:     32
```



第 34 章

ネットワーク アドレス変換

ネットワークアドレス変換の概要

UIW リリース 17.16.1 以降、AP はネットワークアドレス変換（NAT）機能をサポートしています。この機能により、無人搬送車（AGV）用の単一のパブリック IP アドレスを使用して外部ネットワークにアクセスすることで、AGV のためにスムーズで効率的なローミングを行うことができます。AGV での各アプリケーションにポート番号が割り当てられ、ダウンストリームとアップストリームの両方向のデータフローが管理されます。

（注） NAT は、AP のレイヤ 2 モードでのみサポートされます。

この機能は、次の機能をサポートしています。

- ポート変換を設定した NAT（NAPT）
- 送信元 NAT（SNAT）

ダウンストリーム トラフィック用のポート変換を設定したNAT（NAPT）では、着信データパケットが管理されて正しい内部デバイスにルーティングされます。アドレステーブルを使用して特定のアプリケーションの内部プライベート IP アドレスとポート番号が見つけられて、パケットが転送されます。詳細については、「AGV の NAPT を使用したダウンストリーム データ フロー」を参照してください。

アップストリーム トラフィック用の送信元NAT（SNAT）では、外部ネットワークに送信する前に、内部ネットワークデバイスからの発信パケットの送信元 IP アドレスとポート番号が変更されます。詳細については、「AGV の SNAT を使用したアップストリーム データ フロー」を参照してください。

NAT の利点

オンボード車両システムに共通の IP アドレススキームにより、すべての車両機器を一意に識別する複雑さが軽減され、外部システムからのアクセスが容易になります。

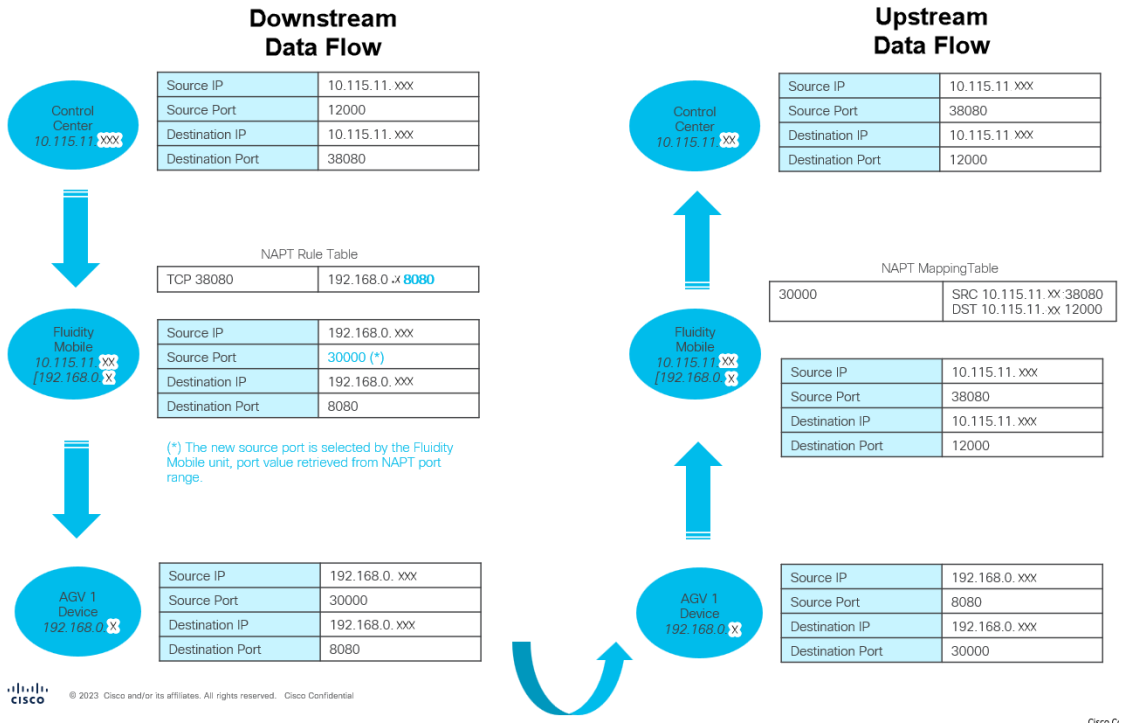
AGV の NAPT を使用したダウンストリーム データ フロー

ダウンストリームとは、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フローを指します。AP は、外部ネットワークと内部ネットワークの間のゲートウェイとして機能します。AP が外部ネットワークからパケットを受信すると、NAPT によってアドレステーブルを使用して特定のアプリケーションの内部プライベート IP アドレスとポート番号が見つけられて、パケットが転送されます。

NAPT を使用すると、次のことができます。

- 外部ネットワークのデバイスが、AGV の内部ネットワークのサービスに接続できます。
- AGVの内部ネットワーク内のAPが、データフローを特定のポートに向かわせることができます。

図 *5 : NAPT* を使用したダウンストリーム データ フローの例 :



AGV の NAPT を使用したポート番号の割り当て

NAPT によって、AGV のさまざまなサービスに異なるポート番号が割り当てられます。これにより、外部ネットワークからの応答が AGV の正しいサービスに送信されるようになります。

NAPT 設定用に予約済みの外部ポート番号

プロトコル/ポート番号	Service	注
TCP および UDP	—	1 ～ 1023 のポート番号は、TCP プロトコルと UDP プロトコルの両方で使用できません。
UDP/1812 ～ 1813	RADIUS	—
UDP/6600 UDP/6610	産業用ワイヤレスモニター	オンプレミスの UDP と ping

プロトコル/ポート番号	Service	注
UDP/<テレメトリポート>	産業用ワイヤレステレメトリ	• 産業用ワイヤレステレメトリのプロトコル用には、さまざまなポート番号が設定されます。 • テレメトリ用に設定されているデフォルト値は 30000 です。

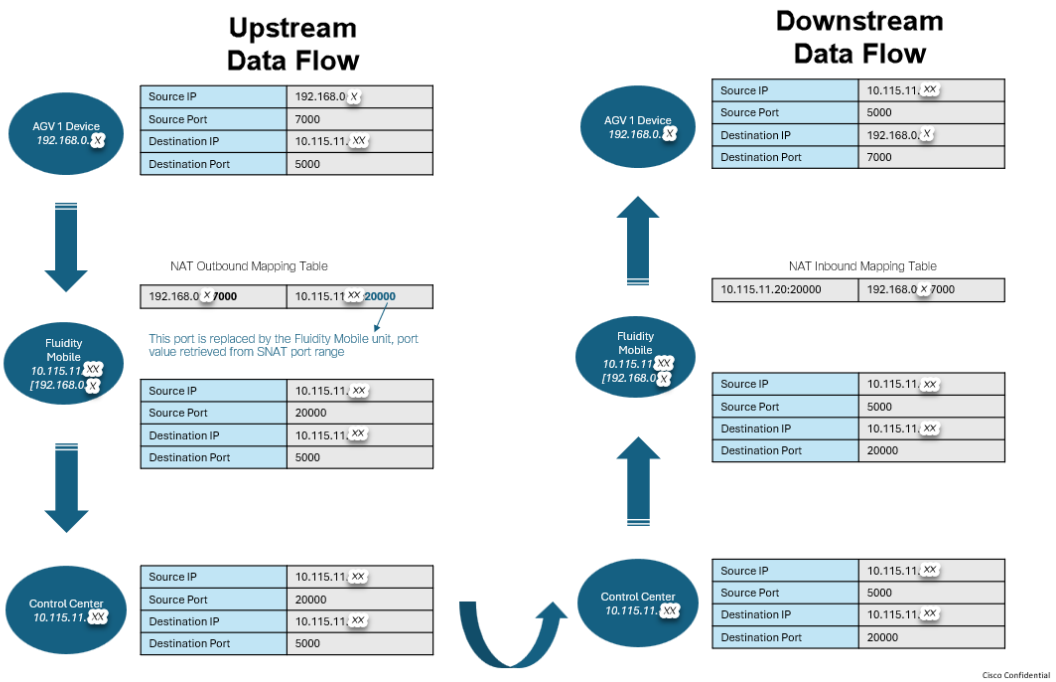
AP の NAPT 規則

NAPT規則により、内部ホストの特定のポートにデータフローが送信されます。一般的なNAPT規則は、`<Protocol, Global Destination Port, Translated Local Destination IP, Translated Local Destination Port>` という構成です。プロトコルにはUDPまたはTCPのいずれかを使用できます。

AGV の SNAT を使用したアップストリーム データ フロー

アップストリームとは、内部ネットワークから外部ネットワークへのデータのフローを指します。APは、内部ネットワークと外部ネットワークの間のゲートウェイとして機能します。APが内部ネットワークから外部ネットワークにパケットを送信するときに、SNATによって発信パケットの送信元IPアドレスと送信元ポートがパブリックのIPとポートと一致するように変更されます。

図 *6 : SNAT* を使用したアップストリーム データ フローの例 :



CLI を使用した NAPT の設定

AP で NAPT 機能を設定してダウンストリーム データ フローを有効にするには、次の作業を実行します。

手順

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

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

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

ステップ 2 **configure ip nat inside ipv4** *ipv4-address netmask* コマンドを使用して、NAT の内部 IPv4 アドレスを設定します。

```
Device#configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

ステップ 3 **configure ip nat inside port range** *left-limit-port-number right-limit-port-number* コマンドを使用して、NAT の内部ポート範囲を設定します。

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

内部ポートの有効範囲は 30000 ～ 35000 です。この範囲は、SNAT 範囲と重複しないようにする必要があります。

ステップ 4 **configure ip nat entry add proto** {**TCP** | **UDP**} **outside port** *outside-port-number* **inside ipv4** *inside-ipv4-address* **port** *inside-port-number* コマンドを使用して、NAT のプロトコル、外部ポート値、内部 IPv4 アドレス、および内部ポート値を設定します。

```
Device#configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2 port
8080
```

ステップ 5 **write** および **reload** コマンドを使用して、現在の設定を保存します。

```
Device#write

Device#reload
```

NAPT の設定例

```
Device#configure ip nat enable
Device#configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device#configure ip nat inside port range 32000 33000
Device#configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2 port
 8080
Device#write
Device#reload
```

CLI を使用した SNAT の設定

AP で SNAT 機能を設定してアップストリーム データ フローを有効にするには、次の作業を実行します。

手順

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

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

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

ステップ 2 **configure ip nat inside ipv4** *ipv4-address netmask* コマンドを使用して、NAT の内部 IPv4 アドレスを設定します。

```
Device#configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

ステップ 3 **configure ip nat outside port range** *left-limit-port-number right-limit-port-number* コマンドを使用して、NAT の外部ポート範囲を設定します。

```
Device#configure ip nat outside port range 22000 23000
```

外部ポートの有効範囲は 20000 ～ 25000 です。この範囲は、NAPT 範囲と重複しないようにする必要があります。

ステップ 4 **write** および **reload** コマンドを使用して、現在の設定を保存します。

```
Device#write
Device#reload
```

SNAT の設定例

```
Device#configure ip nat enable
Device#configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device#configure ip nat outside port range 22000 23000
Device#write
Device#reload
```

CLI を使用した NAT 規則の削除

AP で特定の NAT 規則を削除するには、**configure ip nat entry del** コマンドを使用します。

```
Device#configure ip nat entry del 0
```

CLI を使用したすべての NAT 規則の削除

AP ですべての NAT 規則を削除するには、**configure ip nat entry del all** コマンドを使用します。

```
Device#configure ip nat entry del all
```

CLI を使用した NAT 設定の確認

NAT 設定のステータスを表示するには、**show ip nat config** コマンドを使用します。

```
device#show ip nat config
NAT: enabled
IP: 192.168.1.144
Netmask: 255.255.255.0
NAPT port range: 30000-35000
SNAT port range: 22000-23000
TCP timeout: 300
UDP timeout: 300
NAT max rules: 100
```

CLI を使用した NAT 変換の確認

すべての NAT 変換を表示するには、**show ip nat translations** コマンドを使用します。

```
Device#show ip nat translations

NAT: enabled

Port NAT Translations
---------------------

TCP Translations
(192.168.50.4, 4000, 192.168.50.1, 34200) => (10.115.11.157, 4443, 10.115.11.250, 51010)
(10.115.11.250, 51010, 10.115.11.157, 4443) => (192.168.50.1, 34200, 192.168.50.4, 4000)

UDP Translations
None

Source NAT Translations
-----------------------
TCP Translations
(192.168.50.4, 51178, 10.115.11.250, 4000) => (10.115.11.157, 20292, 10.115.11.250, 4000)
(10.115.11.250, 4000, 10.115.11.157, 20292) => (10.115.11.250, 4000, 192.168.50.4, 51178)
UDP Translations
(10.115.11.250, 3000, 10.115.11.157, 22068) => (10.115.11.250, 3000, 192.168.50.4, 38318)
(192.168.50.4, 38318, 10.115.11.250, 3000) => (10.115.11.157, 22068, 10.115.11.250, 3000)
```

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。