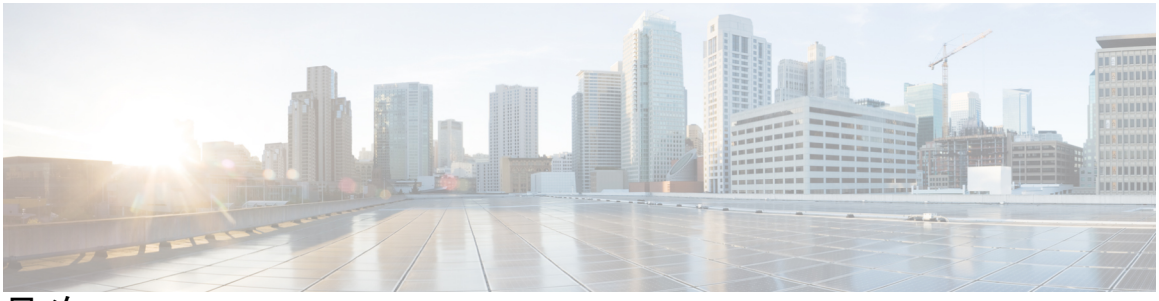
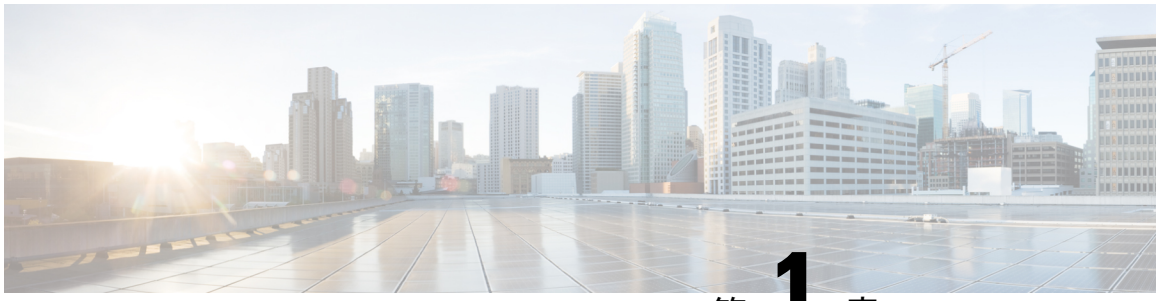
Cisco Catalyst IW9167E Heavy Duty アクセスポイント リリース 17.17.x コンフィギュレーション ガイド

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



第 1 章

はじめに

アクセスポイントの概要

Cisco Catalyst IW9167E Heavy Duty 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ます。IOS XE Cupertino 17.9.3 ソフトウェアリリース以降、Cisco Catalyst Wi-Fi（CAPWAP ）モードまたは Cisco Ultra-Reliable Wireless Backhaul（Cisco URWB）モードでの動作が可能です。IW9167EH アクセスポイントは、動作モードを Wi-Fi から Cisco URWB に、またはその逆に変更できる柔軟性を備えています。

Cisco IOS XE Dublin 17.11.1 以降、ワークグループブリッジ（WGB）とユニバーサル WGB（uWGB）は、Cisco Catalyst IW9167E Heavy Duty アクセスポイントでサポートされています。

このドキュメントでは、IW9167EH アクセスポイントに固有の CAPWAP モードと WGB/uWGB モードの設定について説明します。

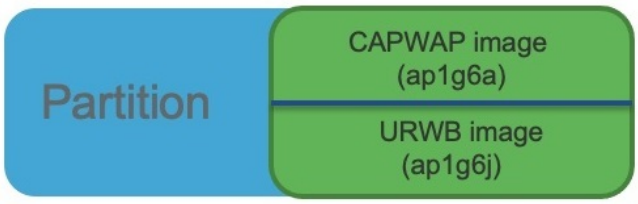
CAPWAP モードでは、アクセスポイントは次のモードで動作可能です。

- ローカル
- FlexConnect
- ブリッジ
- FlexConnect + ブリッジ
- スニファ
- Monitor

- サイトサーベイ

IW9167EH でのイメージの判別

ソフトウェアイメージは、IW9167EH の同じパーティション上の異なるフォルダに保存されます。



AP が稼働しているモード（CAPWAP、Cisco URWB、または WGB/uWGB）に応じて、起動に使用するイメージを選択する必要があります。次の表に、各モードのソフトウェアイメージを示します。

表 *1 : IW9167EH* のソフトウェアイメージ

IW9167EH モード	ソフトウェア イメージ
CAPWAP	**ap1g6a-k9w8-xxx.tar**
Cisco URWB	Unified Industrial Wireless イメージ **ap1g6j-k9c1-xxx.tar**
WGB/uWGB	

IW9167EH が実行しているイメージを判別するには、**show version** コマンドを使用します。

- 次の例に示すように、**show version** の出力に **Cisco AP Software, (ap1g6a)** と表示された場合は、AP が CAPWAP モードをサポートする CAPWAP イメージ **ap1g6a-k9w8-xxx.tar** を実行していることを意味します。

```
Cisco AP Software, (ap1g6a), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Fri Jul 29 01:56:00 PDT 2022

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100

APFC58.9A16.E648 uptime is 0 days, 1 hours, 03 minutes
Last reload time   : Mon Sep 19 02:23:13 UTC 2022
Last reload reason : Image Upgrade

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1757076/1006864K bytes of memory.
```

- 次の例に示すように、**show version** の出力に **Cisco AP Software (ap1g6j)** と表示された場合は、AP が Cisco URWB モードまたは Cisco WGB/uWGB をサポートする **ap1g6j-k9c1-xxx.tar** イメージを実行していることを意味します。

```
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

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1759128/1091316K bytes of memory.
```

異なるイメージを選択して起動するための AP の設定

CAPWAP、URWB、またはWGB/uWGBモードで起動するようにアクセスポイントを設定するには、以下の手順に従います。

（注） 異なるモードに切り替えると、工場出荷時の状態への全面的なリセットが実行されます。すべての設定とデータが完全に削除されます。

手順

ステップ 1 **enable**

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **configure boot mode** {**capwap** | **urwb** | **wgb**}

AP をCAPWAP、URWB、または WGB/uWGB モードに設定します。AP は指定されたモードで再起動します。

WGB/uWGB をサポートするように 17.9.x 搭載の IW9167EH をアップグレートする

IW9167EH が Cisco IOS XE Cupertino 17.9.3 ソフトウェア搭載で出荷され、CAPWAP モードで動作している場合、WGB/uWGB モードをサポートするように AP を Cisco IOS XE Dublin 17.11.1 にアップグレードする場合は、まず AP を Cisco URWB モードに切り替える必要があります。その後、17.11.1 にアップグレードできます。

IW9167EH が CAPWAP モードと Cisco URWB モードのどちらで実行されているかを確認するには、**show version** コマンドを使用します。

- **show version** の出力で **Cisco AP Software (ap1g6a)** と表示される場合、AP は CAPWAP モードで実行されています。
- **show version** の出力で **Cisco AP Software (ap1g6j)** と表示される場合、AP は Cisco URWB モードで実行されています。

Cisco WGB/uWGB モードは、Cisco URWB と同じイメージを共有します。CAPWAP モード（**ap1g6a**）で **ap1g6j** イメージを 17.11.1 にアップグレードすることはできません。**archive download** コマンドではイメージタイプがチェックされるため、イメージタイプが一致しない場合、アップグレードは中止されます。

手順

ステップ 1 CAPWAP モードを Cisco URWB モードに切り替えます。

例：

```
#configure boot mode urwb
       Before image swapping device need factory reset. Are you sure to proceed? (Y/N):y
       Converting to Cisco URWB Mode...
       <rebooting…>
```

ステップ 2 デフォルトログイン情報（Cisco/Cisco/Cisco）でログインします。

ステップ 3 **Offline** モードで動作するように Cisco URWB を設定します。

例：

```
#configure iotod-iw offline
       Switching to IOTOD IW Offline mode...
       Will switch from Provisioning Mode to IOTOD IW offline Mode, device need to reboot: Y/N?  Y
       <rebooting…>
```

ステップ 4 Cisco URWB でネットワーキングを設定します（IP/ネットマスク/ゲートウェイ、パスフレーズ）。

例：

```
Cisco-23.174.76#configure wireless passphrase unit1
Cisco-23.174.76#configure ap address ipv4 static 192.168.1.200 255.255.255.0 192.168.1.1
Cisco-23.174.76#write
Cisco-23.174.76#reload
     <rebooting…>
```

（注）
パスフレーズはオプションですが、同一のレイヤ 2 ネットワークに接続されている複数のユニットを同時にアップグレードする場合は、異なるパスフレーズを割り当てることを推奨します。Cisco URWB では、すべてのノードに同じパスフレーズが設定されている場合は MPLS ネットワークが自動的に形成されるため、付加的な MPLS の設定を行わないと、IP サービスが正常に機能しない可能性があります。

ステップ 5 17.11.1 にアップグレードします。

例：

```
#archive download-sw /reload tftp://<TFTP_SERVER>/<ap1g6j-FILENAME>
          <rebooting…>
```

ステップ 6 AP を Cisco URWB モードから Cisco WGB/uWGB モードに切り替えます。

例：

```
#configure boot mode wgb
          <rebooting…>
```

関連資料

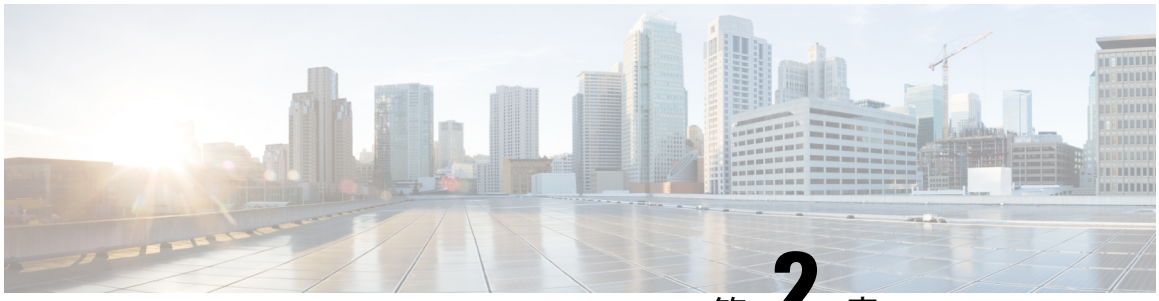
Cisco Catalyst IW9167E Heavy Duty アクセスポイントのすべてのサポート情報については、https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html を参照してください。

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

- IW9167EH ハードウェアの詳細については、『Cisco Catalyst IW9167E Heavy Duty Series Access Point Hardware Installation Guide』を参照してください。
- AP の機能および仕様をすべて網羅したリストは、『Cisco Catalyst IW9167E Heavy Duty Access Point Data Sheet』に記載されています。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定については、https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.htmlを参照してください。
- Cisco URWB モード設定の詳細については、関連するドキュメントを参照してください。

  https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html
- Cisco IOS XE の詳細については、関連するドキュメントを参照してください。

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html



第 2 章

AP モードの設定

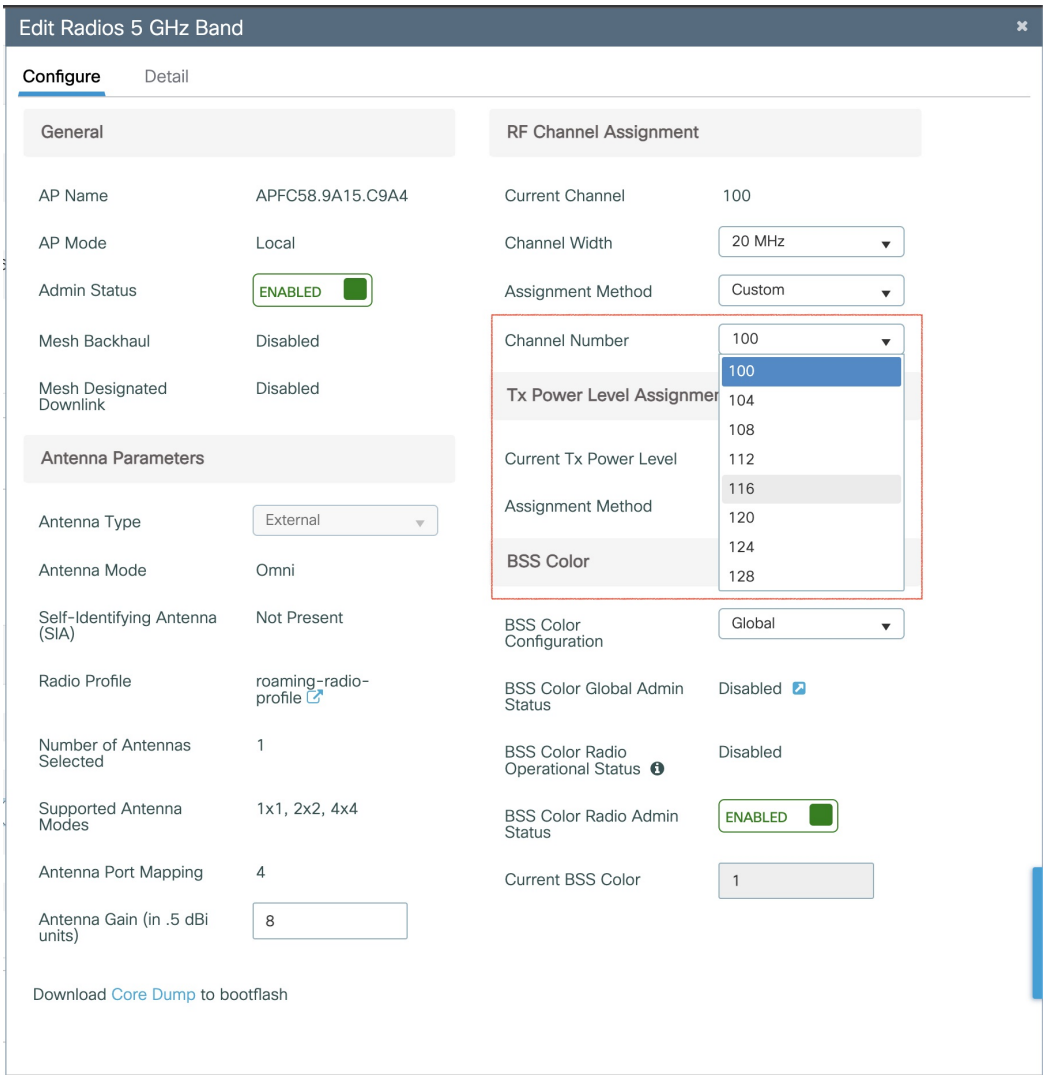
-E ドメインの屋内展開の設定

IW9167EH は、-E ドメインの屋内展開をサポートしています。

デフォルトでは、屋内展開は無効で、5G 無線機はチャンネル 100、104、108、112、116、120、124、128、132、136、140 をサポートします。工場出荷時の状態へのリセット後、屋内展開の設定はデフォルトにリセットされ、無効になります。

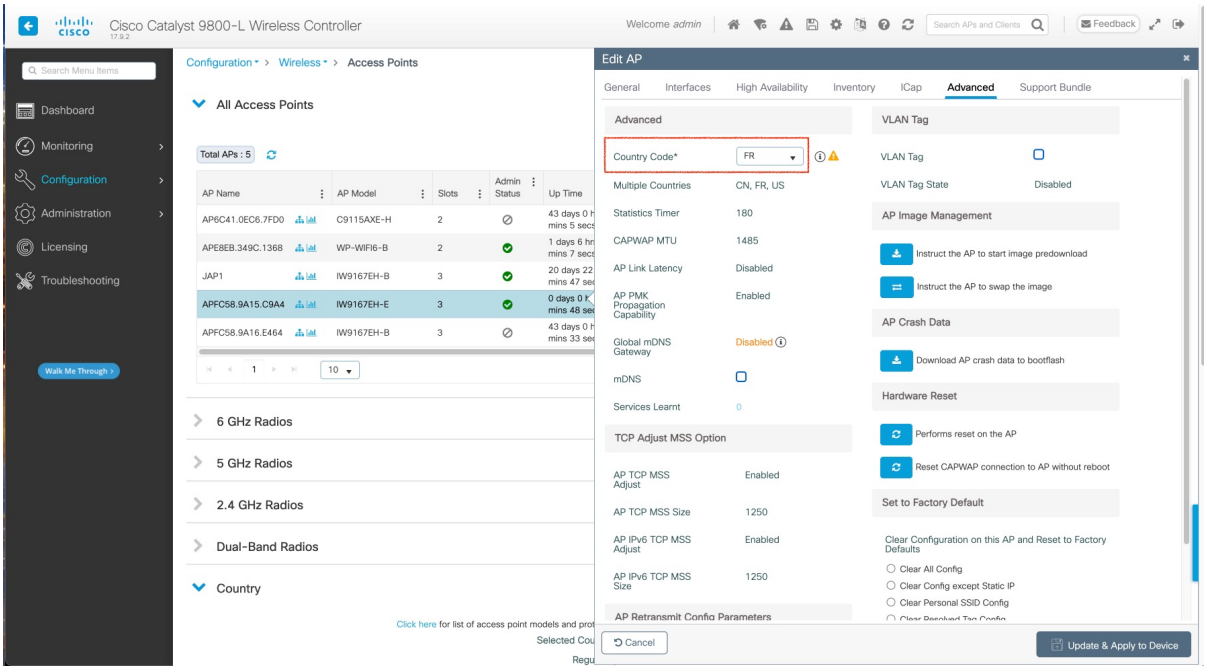
show ap name <ap-name> config general | section Indoor コマンドを使用して AP モードを確認できます。次の例に示すように、コマンド出力中の「Enabled」は、AP が屋内モードであることを意味し、「Disabled」は AP が屋外モードであることを意味します。

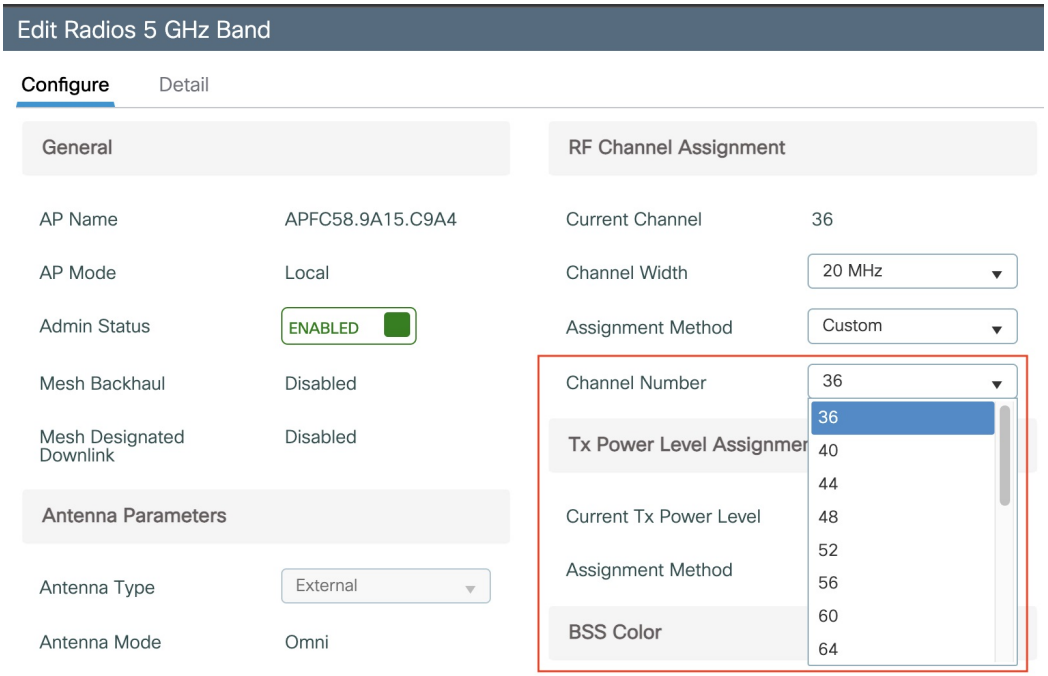
```
#show ap name APFC58.9A15.C9A4 config general | inc Indoor
    AP Indoor Mode                                  : Disabled
```



AP を屋内モードに設定するには、ワイヤレス LAN コントローラから **ap name** <*ap-name*> **indoor** コマンドを使用します。このコマンドは、AP の再起動を開始します。再起動後に AP がワイヤレス LAN コントローラに登録されたら、対応する国番号を AP に割り当てる必要があります。屋内展開が有効になっている場合、5G 無線機はチャンネル 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140 をサポートします。

（注） 屋内展開を無効にするには、**ap name** <*ap-name*> **no indoor** コマンドを使用します。





（注） チャンネルリストは、U-NII-2c から U-NII-1、U-NII-2a、U-NII-2c に拡張されます（チャンネル 144 は除外されます）。

802.11ax 1600ns および 3200ns のガード間隔

802.11ac には、2 つのガード間隔（GI）オプション（長い GI（800ns）と短い GI（400ns））があります。802.11ax では、新しいガード間隔オプションが導入されています。800ns、1600ns、3200ns の 3 種類の GI があります。ガード間隔を長くすると、マルチパスと遅延拡散が生じる環境での性能が向上します。長いガード間隔は、距離の長い屋外展開でのリンクの信頼性を向上させ、屋外環境でのシンボル間干渉を防ぎ、カバー範囲と性能を向上させるのに役立ちます。

次の表では、802.11ax を以前の 2 つの標準規格と比較しています。

表 *2 : 802.11ax* のガード間隔と以前の標準規格のガード間隔の比較

Capabilities	802.11n	802.11ac	802.11ax
物理層（PHY）	高スループット（HT）	超高スループット（VHT）	高効率（HE）
Guard Interval	800/400 ns	800/400 ns	800/1600/3200 ns

802.11ax 長期ガード間隔の設定

HE モードのガード間隔は、RF プロファイルで設定する必要があります。

手順

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
Device#configure terminal
```

例：

```
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

ステップ 2 RF プロファイルを設定し、RF プロファイル コンフィギュレーション モードを開始します。

ap dot11 {**24ghz**|**5ghz**} **rf-profile** *<profile-name>*

例：

```
Device(config)#ap dot11 24ghz rf-profile 24G-RF-profile
```

ステップ 3 RF プロファイルのガード間隔を設定します。

guard-interval {**GUARD_INTERVAL_1600NS** | **GUARD_INTERVAL_3200NS** | **GUARD_INTERVAL_400NS** | **GUARD_INTERVAL_800NS**}

例：

```
Device(config-rf-profile)#guard-interval GUARD_INTERVAL_1600NS
```

- GUARD_INTERVAL_1600NS：1600 ns のガード間隔を設定（HE モードのみ）
- GUARD_INTERVAL_3200NS：3200 ns のガード間隔を設定（HE モードのみ）
- GUARD_INTERVAL_400NS：400 ns のガード間隔を設定（HT VHT モード）
- GUARD_INTERVAL_800NS：800 ns のガード間隔を設定

（注）
HE モードの有効なガード間隔値は、800、1600、および 3200 ns です。デフォルトでは、GI は 800 ns です。

ステップ 4 グローバル コンフィギュレーション モードを終了します。

end

例：

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

ワイヤレスコントローラの設定を確認するには、次のコマンドを使用します。

```
#show ap rf-profile name Demo-24G-RF-profile detail | inc Guard
Guard Interval        : 1600ns
#show ap rf-profile name Demo-5G-RF-profile detail | inc Guard
Guard Interval        : 3200ns
```

例

1. RF プロファイルで GI を定義する

```
ap dot11 24ghz rf-profile Demo-24G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_1600NS
no shutdown
ap dot11 5ghz rf-profile Demo-5G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_3200NS
no shutdown
```

2. RF プロファイルを RF タグに関連付ける

```
wireless tag rf Demo-Guard-Interval-RF-tag
24ghz-rf-policy Demo-24G-RF-profile
5ghz-rf-policy Demo-5G-RF-profile
```

3. RF タグを AP に関連付ける

```
ap fc58.9a15.c83c
rf-tag Demo-Guard-Interval-RF-tag
```

GNSS のサポート

Cisco IOS XE Dublin 17.11.1 以降、GNSS は IW9167EH でサポートされます。AP は、屋外環境に展開されたデバイスの GPS 情報を追跡し、ワイヤレスコントローラに GNSS 情報を送信します。

AP の GNSS 情報を表示するには、次のコマンドを使用します。

ap# **show gnss info**.

AP の GPS 位置情報を表示するには、次のコマンドを使用します。

controller# **show ap geolocation summary**

controller# **show ap name** <*Cisco AP*> **geolocation detail**

RAP イーサネット デイジー チェーン

RAP イーサネット デイジー チェーン機能により、既存のイーサネットブリッジング機能が強化されます。この機能により、ブリッジ AP はイーサネットリンクにとどまるよう強制され、アップリンクバックホールのワイヤレスリンクの選択がブロックされます。イーサネットリンクに障害が発生しても、アクセスポイントがワイヤレスバックホールを介して親を選択することはありません。

次の図は、RAP イーサネット デイジー チェーン トポロジの例を示しています。スタンドアロンの DC 電源が各 RAP に提供されます。

図 *1: RAP* イーサネット デイジー チェーン トポロジ

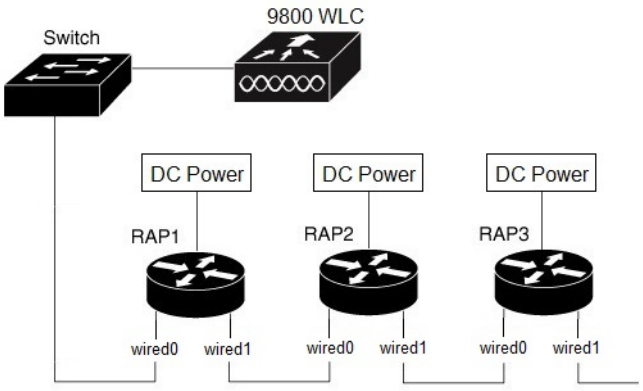


表 *3:* ポート マッピング

パネルラベル	SW インターフェイス
mGig POE 入力ポート	有線 0
SFP	有線 1

（注） この機能でサポートされている SFP モジュールは、1000BASE-T 高耐久性 SFP（Cisco PID：GLC-T-RGD）です。

この機能を設定する際は、次のガイドラインに従ってください。

- デイジーチェーン内のすべての AP は、ルート AP ロールのメッシュブリッジモードまたはFlex+ブリッジモードで動作しています。PoE 入力（wired0）ポートおよびSFP（wired1）ポートはアップリンクポートとして使用することが可能で、PoE 入力（wired0）ポートの優先順位は SFP（wired1）よりも高くなります。
- VLAN の透過性は、すべてのデイジーチェーン RAP で無効にする必要があります。
- 各ルート AP で VLAN サポートを有効にするには、次の手順を実行します。
  - ブリッジモード AP の場合は、**ap name name-of-rap mesh vlan-trunking [native] vlan-id** コマンドを使用して、対応する RAP でトランク VLAN を設定します。
  - Flex + ブリッジ AP の場合は、対応する Flex プロファイルでネイティブ VLAN ID を設定する必要があります。

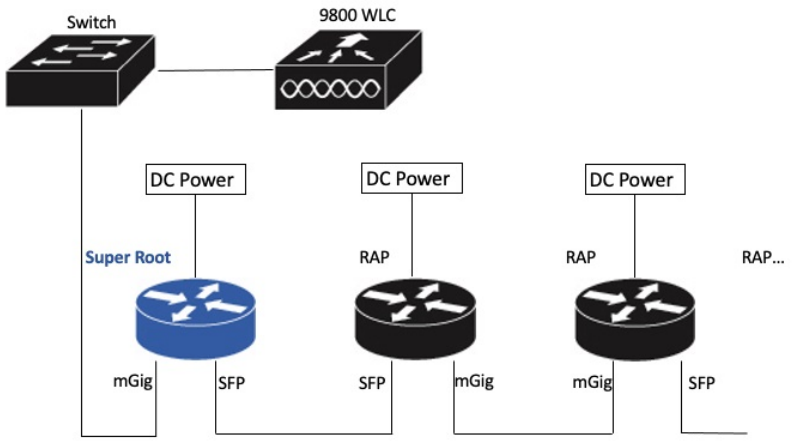
RAP イーサネット デイジー チェーン機能は Cisco IOS XE Cupertino 17.9.3 ですでにサポートされていますが、この機能には以下の制限があります。

- プライマリ イーサネット ポート（mGig ポート）はアップリンクとして使用する必要があります。この場合、SFP ポートから SFP ポートへの接続はサポートされないため、ネットワークのスループットに影響します（SFP が mGig ポートに接続されている場合、2.5 Gbps または 5 Gbps の銅線 SFP は使用できません）。
- 既存のコマンド **persistant-ssid** を再利用して RAP イーサネット デイジー チェーン機能を有効にする方法は、間違いの原因になります。

Cisco IOS XE ダブリン 17.11.1 では、RAP イーサネット デイジー チェーン機能が拡張されており、次の機能がサポートされます。

- ワイヤレス スパニング ツリー プロトコル（WSTP）hello が自動ルートポート検出をサポートするため、RAP は任意のポートをアップリンクとして使用できます。次のトポロジを参照してください。

図 *2 : WSTP* による *RAP* イーサネット デイジー チェーンのトポロジ



- この機能を有効にするために、別個の専用コマンド **rap-eth-dasychain** が導入されました。

WSTP の概要

ワイヤレス LAN スパニングツリープロトコル（WSTP）は、シスコのメッシュネットワークをループフリーのスパニング ツリー プロトコル トポロジに編成します。メッシュネットワークを、安定したループフリーの最適なスパニング ツリー プロトコル トポロジにすばやく設定します。最適なトポロジによって、プライマリイーサネット LAN への最小コストパスが実現します。WSTP Hello メッセージは、WSTP トポロジの構築に使用されます。

WSTP スーパールートは、WSTP スパニングツリープロトコル全体の最高レベルの「スーパー」ルートとして選択される単一の RAP です。スーパールートはプライマリ LAN に直接接続されます。スーパールートは、イーサネットルートポートでゼロコストの WSTP SR Hello メッセージを送信し、プライマリ LAN を RAP にアドバタイズします。

以前のリリースとの比較

次の表は、現在のリリースと 17.11 より前のリリースのデイジーチェーン機能を比較したものです。

	リリース 17.11.1 より前	リリース 17.11.1
トポロジ	**固定型トポロジ** RAP は、デイジーチェーントポロジのアップリンクとして mGig ポートを使用する必要があります。	**柔軟なトポロジ** RAP は、AP で WSTP を有効にすることにより、デイジーチェーントポロジで mGig ポートと SFP ポートのいずれかをアップリンクとして使用できます。

	リリース 17.11.1 より前	リリース 17.11.1
機能の有効化	AP プロファイルの **Persistant-ssid** [1]	メッシュプロファイルの **rap-eth-dayschain**
リングトポロジ	サポート対象外。[2]	サポート対象外

[1] **Persistent-ssid** は 17.11 でも引き続きサポートされているため、古い設定で以前のリリースから 17.11 にアップグレードした後でも、デイジーチェーン機能が影響を受けることはありません。ただし、**Persistent-ssid** は 17.11 では推奨されず、新しい **rap-eth-dayschain** コマンドが推奨されます。

[2] **daisychain-stp-redundancy** を有効にすることで、IW6300 アクセスポイントでのみサポートされます。詳細については、『Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide』の「RAP Ethernet Daisy Chain Redundancy for STP Ring Topology」セクションを参照してください。

RAP イーサネット デイジー チェーンの設定

このセクションでは、RAP イーサネット デイジー チェーンの設定手順について説明します。

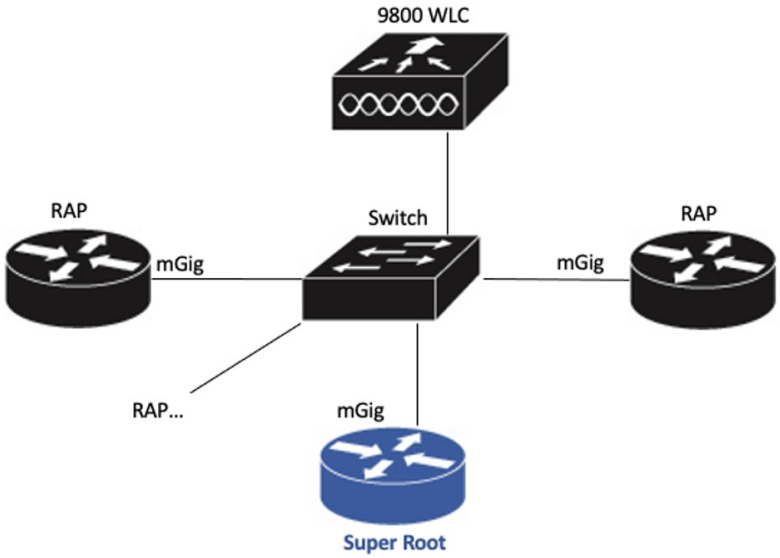
フィールド展開の前に RAP イーサネット デイジー チェーンを事前設定する

このセクションでは、フィールド展開でのセットアップの前にラボで完了する必要がある事前設定について説明します。

手順

ステップ 1 開梱し、接続して、AP の電源を入れます。

ステップ 2 mGig ポートを使用して各 AP をコントローラに接続します。詳細については、次の図を参照してください。



ステップ 3 AP をブリッジモードに設定し、AP ロールをルート AP に設定します。

この設定手順の詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-11/config-guide/b_wl_17_eleven_cg/m_mesh_ewlc.html#task_pnb_bwy_mlb を参照してください。

ステップ 4 RAP イーサネット デイジー チェーンを設定します。

a) メッシュプロファイルを作成し、RP イーサネット デイジー チェーン機能を有効にします。

RAP イーサネット デイジー チェーンの有効化 （17 ページ）を参照してください。

b) プロファイルをすべての RAP にアタッチします。

c) 1 つの AP を、ワイヤレスコントローラへのファーストホップとなるスーパールートとして設定します。

スーパールートの設定 （18 ページ）を参照してください。

d) SFP ポートをアップリンクとして使用する場合は、スーパールート AP でプライマリ イーサネット ポートを設定します。

プライマリ イーサネット ポートの設定 （19 ページ）を参照してください。

ステップ 5 イーサネットブリッジングを有効にして、イーサネットポートを設定します。

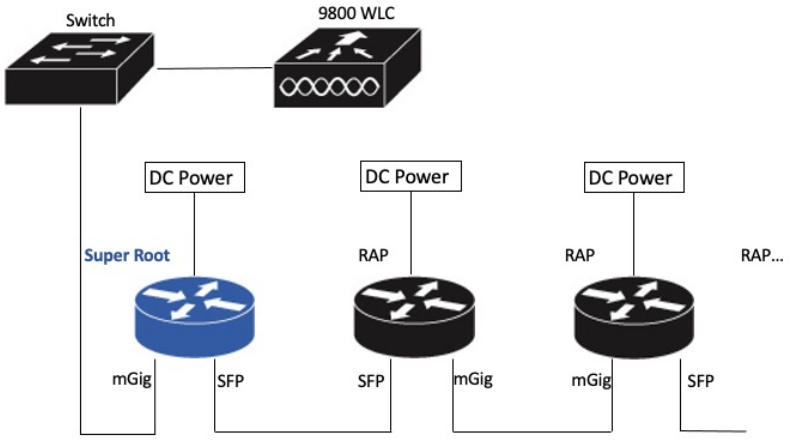
イーサネットブリッジングとイーサネットポートの設定 （19 ページ）を参照してください。

a) イーサネットブリッジングを有効にします。

b) ポートモードと VLAN を含む、ポート 0 とポート 1 の両方でイーサネットポートを設定します。ポートをトランクモードに設定することを推奨します。

ステップ 6 デイジーチェーントポロジでの動作を確認します。

a) 有線ポートを介して RAP を 1 つずつ接続します。



（注）
上の図に示されているように、ワイヤレスコントローラからの最初のホップである RAP は、スーパールートとして設定する必要があります。

b) 各ホップの RAP がコントローラに接続できることを確認します。

（注）
フィールド展開で、この手順のステップ 6 を繰り返してください。最初のホップを必ずスーパールートに設定します。

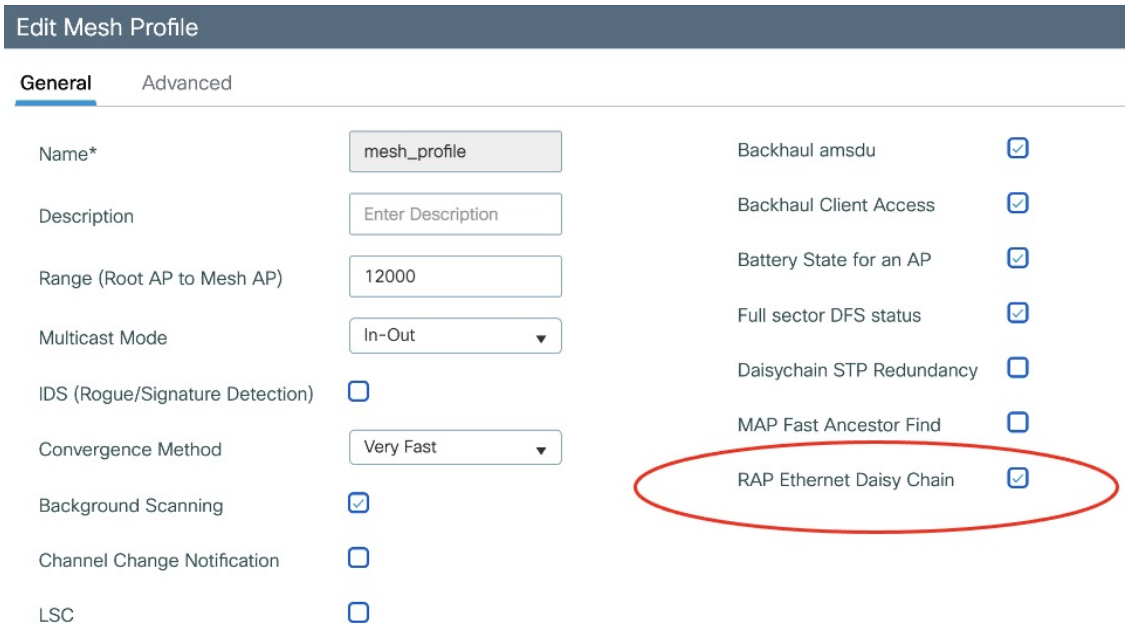
RAP イーサネット デイジー チェーンの有効化

RAP イーサネット デイジー チェーン機能を有効にするには、**rap-eth-dayschain** コマンドを使用するか、GUI から設定します。

次の例は、CLI からこの機能を有効にする方法を示しています。

```
#configure terminal
(config)#wireless profile mesh default-mesh-profile
(config-wireless-mesh-profile)#ethernet-bridging
(config-wireless-mesh-profile)#rap-ethernet-daisychain
```

次の図は、GUI からこの機能を有効にする方法を示しています。



設定を確認するには、次の例に示すように、ワイヤレスコントローラから **show wireless profile mesh detailed** コマンドまたは **show wireless mesh ethernet dasy-chain summary** コマンドを使用します。

```
#show wireless profile mesh detailed <profile name>
…
RAP ethernet daisychain       : ENABLED

#show wireless mesh ethernet daisy-chain summary
AP Name      BVI MAC        BGN        Backhaul          Ethernet      STP Red
Super Root
-----------------------------------------------------------------------------------------------
APxxxxxx     xxxxxxx       xxxxx       Ethernet0          Up Up          NA
Enabled
```

または、次の例に示すように、AP で **show mesh config** コマンドを使用します。

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Disabled
```

スーパールートの設定

上流に位置するスイッチに接続する最初の RAP は、スーパールートとして設定する必要があります。つまり、すべての WSTP hello の送信元となるように設定します。他の RAP は、hello の受信後に初めて hello を開始します。

ワイヤレスコントローラまたは AP からスーパールートを設定できます。

- ワイヤレスコントローラから、**ap name <name> [no] mesh rap-eth-daisychain super-root** コマンドを使用してスーパールートを設定します。

  設定を確認するには、次のコマンドを使用します。

```
#show ap name <name> config general
…
RAP ethernet daisychain                 : Enabled
Super Root                              : Enabled
```

- AP で、**capwap ap mesh wstp super-root** コマンドを使用してスーパールートを設定します。

  設定を確認するには、次のコマンドを使用します。

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
```

プライマリ イーサネット ポートの設定

スーパールートは、プライマリ イーサネット ポートを使用して、上流に位置するスイッチに接続する必要があります。IW9167EH の場合、デフォルトのプライマリ イーサネット ポートはイーサネットポート 0 です。プライマリ イーサネット ポートを手動で設定するには、ワイヤレスコントローラから **ap name <name> mesh backhaul ethernet <0/1>** コマンドを使用します。

設定を確認するには、ワイヤレスコントローラから次のコマンドを使用します。

```
#show ap name <name> config general
…
AP Primary Ethernet port                          : 1
RAP ethernet daisychain                           : Enabled
Super Root                                        : Disabled
```

または、AP で次のコマンドを使用します。

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
AP Primary ethernet backhaul interface: 1

#show mesh adjacency parent
AdjInfo: Wired Backhaul: 1 [xx:xx:xx:xx:xx:xx]
```

イーサネットブリッジングとイーサネットポートの設定

イーサネットブリッジングの設定（CLI）

MAPのイーサネットポートはデフォルトで無効になっています。有効にするには、ルートAPと他の各 MAP でイーサネット ブリッジングを設定する必要があります。AP でイーサネットブリッジングを有効にするには、次の手順に従います。

手順

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
Device#configure terminal
```

ステップ 2 メッシュプロファイルを作成します。

wireless profile mesh *profile-name*

例：

```
(config)#wireless profile mesh rap-eth-daisy
```

ステップ 3 **ethernet-bridging**

例：

```
(config-wireless-mesh-profile)#ethernet-bridging
```

リモートの有線ネットワークを相互に接続します。

ステップ 4 VLAN 透過性を無効にして、ブリッジが VLAN を認識するようにします。

no ethernet-vlan-transparent

例：

```
(config-wireless-mesh-profile)#no ethernet-vlan-transparent
```

ステップ 5 グローバル コンフィギュレーション モードを終了します。

end

例：

```
(config-wireless-mesh-profile)#end
```

例

設定を確認するには、次のコマンドを使用します。

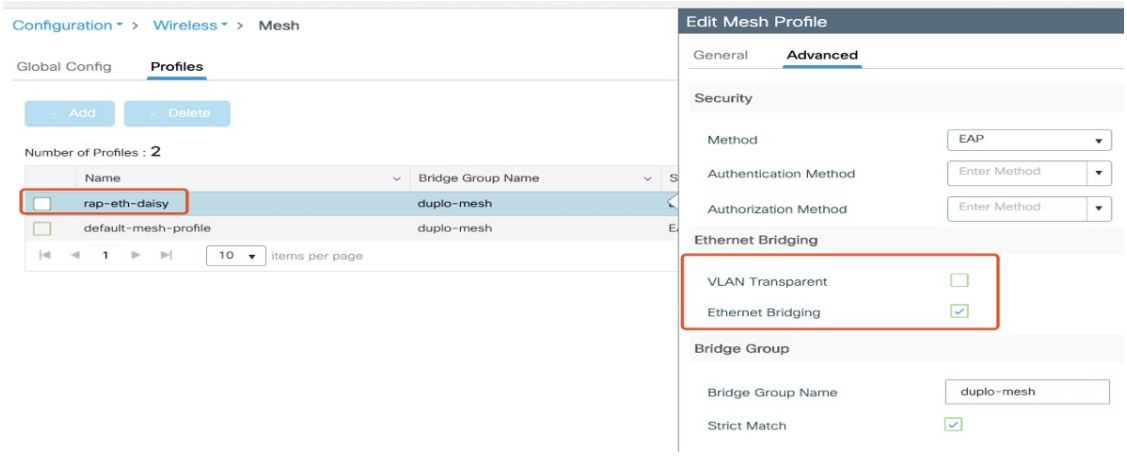
```
#show wireless profile mesh detailed rap-eth-daisy

Mesh Profile Name           : rap-eth-daisy
--------------------------------------
Description                 :
Bridge Group Name           : unconfigured
Strict match BGN            : DISABLED
Amsdu                       : ENABLED
Background Scan             : DISABLED
Channel Change Notification : DISABLED
Backhaul client access      : DISABLED
Ethernet Bridging           : ENABLED
Ethernet Vlan Transparent   : DISABLED
Daisy Chain SP Redundancy   : DISABLED
Full Sector DFS             : ENABLED
```

イーサネットブリッジングの設定（GUI）

ワイヤレスコントローラ GUI からイーサネットブリッジングを設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
ステップ 2 [Add] をクリックします。
ステップ 3 [General] タブで、メッシュプロファイルの [Name] を入力します。
ステップ 4 [Advanced] タブで、[VLAN Transparent] チェックボックスをオフにして、VLAN 透過性を無効にします。
ステップ 5 [Advanced] タブで、[Ethernet Bridging] チェックボックスをオンにします。
ステップ 6 [Apply to Device] をクリックします。



イーサネットポートの設定（CLI）

RAPイーサネットのセカンダリポートは、アクセスモードとトランクモードをサポートしています。イーサネットポートモードを設定するには、次の手順に従います。

- 次のコマンドを使用して、アクセスモードを設定します。

  #**ap name** *ap-name* **mesh ethernet 1 mode access** *Vlan-ID*

- 次のコマンドを使用して、トランクモードを設定します。事前に VLAN サポートを有効にし、メッシュプロファイルでVLANトランスペアレントを無効にする必要があります。
  - 対応する RAP でトランク VLAN を設定します。

    #**ap name** *ap-name* **mesh vlan-trunking native** *Vlan-ID*

  - トランクポートのネイティブ VLAN を設定します。

    #**ap name** *ap-name* **mesh ethernet 1 mode trunk vlan native** *Vlan-ID*

  - トランクポートの許可VLANを設定します。メッシュまたはルートアクセスポイントのイーサネットポートでVLANフィルタリングを許可します。メッシュプロファイルで VLAN 透過性が無効になっている場合にのみアクティブです。

#ap name *ap-name* **mesh ethernet 1 mode trunk allowed** *Vlan-ID*

イーサネットポートの設定（GUI）

ワイヤレスコントローラ GUI からイーサネットポートを設定するには、次の手順に従います。

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] を選択します。

ネットワーク内のすべての設定済み AP が一覧表示される [All Access Points] セクションが、対応する詳細情報とともに表示されます。

ステップ 2 設定されたメッシュ AP をクリックします。

[Edit AP] ウィンドウが表示されます。

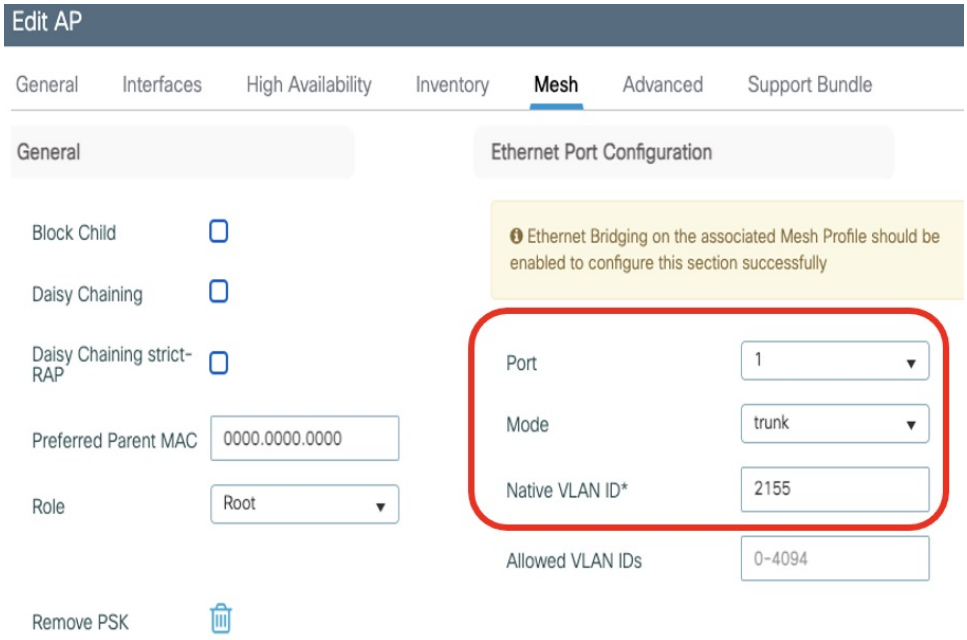
ステップ 3 [Mesh] タブを選択します。

ステップ 4 [Ethernet Port Configuration] セクションの [Port] ドロップダウンリストから、設定するポートを選択します。

ステップ 5 [Mode] ドロップダウンリストで、アクセスモードまたはトランクモードを選択します。

ステップ 6 [Native VLAN ID] フィールドに、トランクポートのネイティブ VLAN を入力します。

ステップ 7 [Update and Apply to Device] をクリックします。



Show コマンドと Debug コマンド

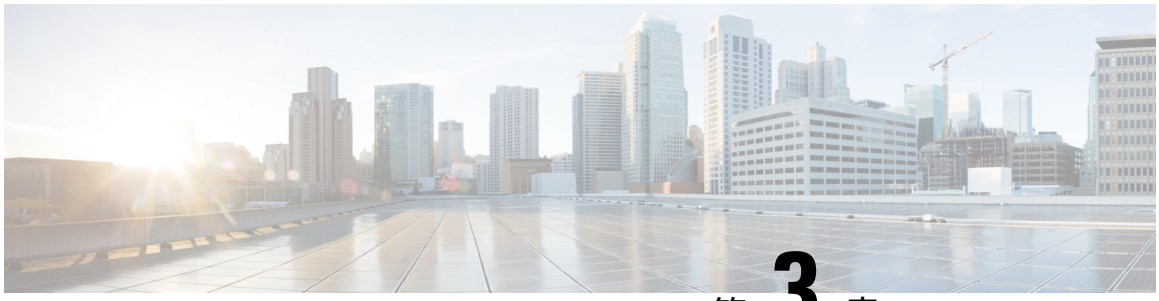
- WTP をデバッグするには、次のコマンドを使用します。

```
AP#debug mesh wstp
  error    Mesh wstp error debugs
  events   Mesh wstp events debugs
  packets  Mesh wstp packet debugs
```

```
03:05:24.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:24.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:24.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
03:05:26.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:26.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:26.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
```

- WSTP 統計を表示するには、次のコマンドを使用します。

```
AP#show mesh stats
WSTP stats:
Attach-Cnt Hello-TX Hello-Rx TCN-TX TCN-RX SR-Chg-Cnt ST-Roam-Cnt
         0       58       58      0      0          0           0
```



第 3 章

ワークグループ ブリッジ

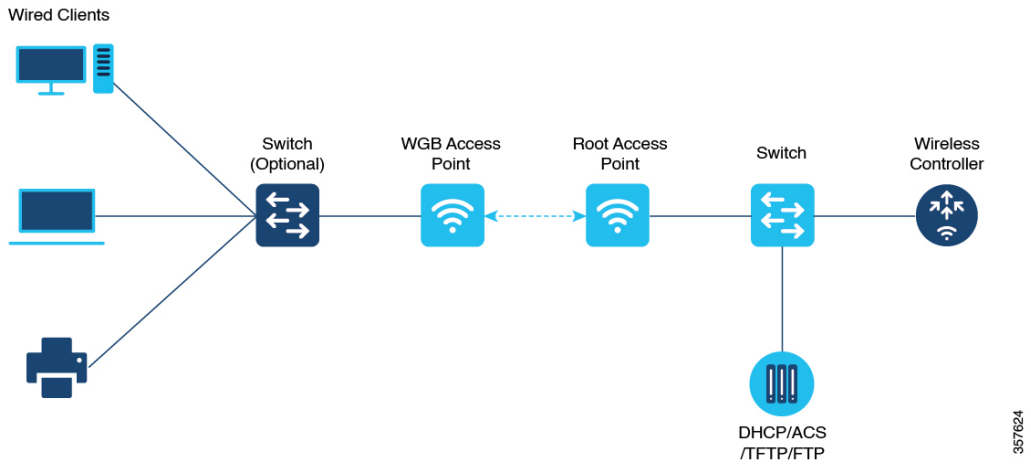
• uWGB でのポートアドレス変換 （109 ページ）
• Cisco IW9167EH WGB での速度 10 Mbps のポートのサポート （117 ページ）

概要

アクセスポイント（AP）モードのワークグループブリッジ（WGB）は、イーサネットポートで WGB AP に接続される有線クライアントへのワイヤレス接続を提供します。WGB はイーサネットインターフェイス上の有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol（IAPP）メッセージングを使用してインフラストラクチャ AP 経由で WLC に報告することで、1 つのワイヤレスセグメントを介して有線ネットワークに接続します。WGB はルート AP への単一のワイヤレス接続を確立し、ルート AP は WGB をワイヤレスクライアントとして扱います。

ユニバーサル WGB（uWGB）は、uWGB に接続された有線クライアントとシスコおよびシスコ以外のワイヤレスネットワークを含むワイヤレスインフラストラクチャとの間のワイヤレスブリッジとして機能する WGB 機能の補完モードです。ワイヤレスインターフェイスの 1 つは、アクセスポイントとの接続に使用されます。無線 MAC は、AP との関連付けに使用されます。

図 *3 : WGB* の例



Cisco IOS XE Dublin 17.11.1 以降、WGB は Cisco Catalyst IW9167E Heavy Duty アクセスポイントでサポートされています。

制限事項と制約事項

ここでは、WGB および uWGB モードの制限事項について説明します。

• WGB は Cisco Lightweight アクセスポイントとのみアソシエートできます。ユニバーサル WGB は、サードパーティのアクセスポイントと関連付けることができます。

- WPA1 セキュリティを使用する Cisco Meraki ワイヤレス インフラインフラストラクチャでは、uWGB はどの SSID にも関連付けられません。
- 速度とデュプレックスは、ローカルに接続されたエンドポイントの機能に応じて自動的にネゴシエートされ、AP の有線 0 および有線 1 インターフェイスで手動で設定することはできません。
- 次の機能を WGB と使用することはサポートされていません。
  - アイドル タイムアウト
  - Web 認証
- レイヤ3のローミングでは、WGBが別のコントローラ（外部コントローラなどに）にローミングした後で、有線クライアントをその WGB ネットワークに接続すると、有線クライアントの IP アドレスはアンカー コントローラにのみ表示され、外部コントローラには表示されません。
- コントローラから WGB レコードの認証を解除すると、すべての WGB 有線クライアントのエントリも削除されます。
- 次の機能は、WGB に接続された有線クライアントにはサポートされていません。
  - MAC フィルタリング
  - リンク テスト
  - アイドル タイムアウト
- Adaptive 802.11r 向けに設定された WLAN との WGB のアソシエーションはサポートされません。
- WGB は、IPv4 が有効になっている場合にのみ IPv6 をサポートします。ただし、WGB 有線クライアントの IPv6 トラフィックへの影響はありません。
- WGB のアップリンク アソシエーションが完了すると、WGB 管理 IPv6 は機能しません。アソシエーションが成功すると、WGB は IPv6 アドレスを取得できます。ただし、IPv6 ping は WGB から、あるいは WGB へは受け渡されません。ワイヤレスまたは有線クライアントから WGB 管理 IPv6 への SSH は機能していません。ピン可能な問題の回避策として、IPv6 がすでに有効になっていて、IPv6 アドレスが割り当て済みであっても、IPv6 を再度有効にします。
- uWGB モードは、それ自体への SSH 接続をサポートしていません。
- uWGB モードは、TFTP も SFTP もサポートしていません。ソフトウェアアップグレードは、WGB モードから実行する必要があります。詳細については、uWGB イメージのアップグレード （30 ページ）を参照してください。
- uWGB はホスト IP サービスをサポートしていません。無線アップリンクによるイメージのアップグレードや SSH セッションによるリモート管理など、一部の機能はサポートされていません。

- IW9167EH WGB/uWGB モードの場合、**packet retries [N] drop** コマンドは IOS XE リリース 17.11.1 で機能しません。
- DFS チャンネルは、リリース 17.13.1 以降の IW9167EH WGB/uWGB でサポートされています。
- IW9167EH WGB/uWGB のワイヤレスアップリンクとして使用できるのは、Dot11Radio 0 および Dot11Radio 1 インターフェイスのみです。
- インフラストラクチャ AP が非 DFS（動的周波数選択）チャンネルで動作しているときに、そのチャンネル帯域幅が変更された場合、WGB は元のチャンネル帯域幅を使用してインフラストラクチャ AP への接続を維持します。

  WGB が正しいチャンネル帯域幅で AP に接続していることを確認するには、ワイヤレスコントローラで **wireless client mac-address** <*wgb-wireless-client-mac-address*> **deauthenticate** コマンドを使用して、WGB ワイヤレスクライアントの認証を解除します。

Day 0 における強力なパスワードの設定

初回ログイン後に WGB/uWGB に強力なパスワードを設定する必要があります。ユーザー名と強力なパスワードは次のルールに従う必要があります。

1. ユーザー名の長さは 1 ～ 32 文字です。
2. パスワードの長さは 8 ー 120 文字です。
3. パスワードには、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの句読点を含める必要があります。
4. 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）
5. パスワードには、3 つの連続した順番の文字を含めることはできません。
6. パスワードには、同じ文字を 3 回連続して含めることはできません。
7. ユーザー名と同じ文字列や、ユーザー名を逆にした文字列はパスワードに使用できません。
8. 新しいパスワードは、現在のパスワードと 4 文字以上異なる必要があります。

たとえば、デフォルトのログイン情報は次のとおりです。

- ユーザー名：Cisco
- パスワード：Cisco
- イネーブルパスワード：Cisco

このログイン情報を、次の強力なパスワードを使って再設定します。

- ユーザー名：demouser
- パスワード：DemoP@ssw0rd
- イネーブルパスワード：DemoE^aP@ssw0rd

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

% First Login: Please Reset Credentials

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

% Credentials changed, please re-login

[*04/18/2023 23:53:44.8926] chpasswd: password for user changed
[*04/18/2023 23:53:44.9074]
[*04/18/2023 23:53:44.9074] Management user configuration saved successfully
[*04/18/2023 23:53:44.9074]


User Access Verification
Username: demouser
Password: DemoP@ssw0rd
APFC58.9A15.C808>enable
Password:DemoE^aP@ssw0rd
APFC58.9A15.C808#
```

（注） 上記の例では、デモンストレーションのためにすべてのパスワードがプレーンテキストで表示されています。実際には、アスタリスク（*）で隠されています。

WGB のコントローラ設定

WGB をワイヤレスネットワークに接続するには、コントローラの WLAN および関連するポリシープロファイルで特定の設定を行う必要があります。

Cisco Client Extensions オプションを設定し、WLAN で Aironet IE のサポートを設定するには、次の手順を実行します。

1. WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。

   ```
   #wlan profile-name
   ```

2. Cisco Client Extensions オプションを設定し、WLAN で Aironet IE のサポートを設定します。

   ```
   #ccx aironet-iesupport
   ```

（注） この設定がないと、WGB は AP にアソシエートできません。

WLAN ポリシープロファイルを設定するには、次の手順を実行します。

1. ワイヤレス ポリシー コンフィギュレーション モードを開始します。

   #**wireless profile policy** *profile-policy*

2. VLAN にプロファイル ポリシーを割り当てます。

   #**vlan** *vlan-id*

3. WGB VLAN クライアントのサポートを設定します。

   #**wgb vlan**

uWGB イメージのアップグレード

uWGB モードは、TFTP も SFTP もサポートしていません。ソフトウェアアップグレードを実行するには、次の手順に従います。

手順

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

ステップ 2 無線インターフェイスを [Administratively Down] 状態にします。

configure Dot11Radio <0|1> disable

例：

```
#configure Dot11Radio 0 disable
#configure Dot11Radio 1 disable
```

ステップ 3 uWGB を WGB モードに変換します。

configure Dot11Radio *slot_id* **mode wgb ssid-profile** *ssid_profile_name*

例：

```
#configure Dot11Radio 1 mode wgb ssid-profile a_uwgb_demo_ssid

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

（注）
ssid_profile_name には、ユーザーが設定した既存の SSID プロファイルを指定できます。

ステップ 4 再起動後、WGB に静的 IP アドレスを割り当てます。

configure ap address ipv4 static *IPv4_address netmask Gateway_IPv4_address*

例：

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

ステップ 5 ICMP ping で動作を確認します。

ping *server_IP*

例：

```
#ping 192.168.1.20
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds

PING 192.168.1.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.858/0.932/1.001 ms
```

ステップ 6 ソフトウェアをアップグレードします。

archive download /reload <**tftp | sftp | http**>*://server_ip/file_path*

ステップ 7 WGB を uWGB に戻します。

configure Dot11Radio *slot_id* **mode uwgb** *wired_client_mac_addr* **ssid-profile** *ssid_profile_name*

例：

```
#configure Dot11Radio 1 mode uwgb 00b4.9e00.a891 ssid-profile a_uwgb_demo_ssid
```

WGB の設定

一般的な WGB の設定には、次の手順が含まれます。

1. SSID プロファイルを作成します。
2. 無線機をワークグループとして設定し、SSID プロファイルを無線に関連付けます。
3. 無線機をオンにします。

WGB アップリンクは、次のようなさまざまなセキュリティ方式をサポートしています。

- オープン（非セキュア）
- PSK
- Dot1x（LEAP、PEAP、FAST-EAP、TLS）

（注） WGB で EAP-TLS セキュリティが必要な場合は、次の順序に従って設定してください。

1. デバイスのユーザー名/パスワード、NTP サーバー、ホスト名、および有効な IP アドレスを設定します。
2. トラストポイントを作成し、お好みの方法で証明書をインポートします。
3. （オプション）dot1x ログイン情報を設定します。
4. EAP プロファイルを作成し、メソッド、トラストポイント名、dot1x ログイン情報（オプション）をマッピングします。
5. EAP プロファイルを SSID プロファイルに結び付けます。
6. SSID プロファイルを優先される無線機にバインドします。

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

EAP プロファイル を SSID プロファイルにもう一度アタッチするには、**configure ssid-profile <ssid_prof_name> ssid authentication eap profile <eap_prof_name> key-management <key_type>** コマンドを使用します。

```
Device#configure ssid-profile <ssid_prof_name> ssid <ssid name> authentication eap profile
 <eap_prof_name> key-management <key_type>
```

次に、Dot1x FAST-EAP の設定例を示します。

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 0 mode wgb ssid-profile demo-FAST
configure dot11radio 0 enable
```

以下のセクションで、WGB の設定について詳しく説明します。

IP アドレスの設定

IPv4 アドレスを設定する

- DHCP を使用して IPv4 アドレスを設定するには、**configure ap address** *ipv4 dhcp* コマンドを使用します。

```
Device#configure ap address ipv4 dhcp
```

- 静的 IPv4 アドレスを設定するには、**configure ap address** *ipv4 static ipv4_addr netmask gateway* コマンドを使用します。設定すると、アップリンク接続なしで有線インターフェイスを使用してデバイスを管理できます。

```
Device#configure ap address ipv4 static ipv4_addr netmask gateway
```

現在の IP 設定の確認

現在の IP アドレス設定を表示するには、**show ip interface brief** コマンドを使用します。

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

IPv6 アドレスを設定する

静的 IPv6 アドレスを設定するには、**configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* コマンドを使用します。この設定により、アップリンク接続なしで有線インターフェイスを介して AP を管理できます。

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

IPv6 自動設定の有効化

AP で IPv6自動設定を有効にするには、**configure ap address ipv6 auto-config enable** コマンドを使用します。

```
Device#configure ap address ipv6 auto-config enable
```

（注）

- AP で IPv6 自動設定を無効にするには、**configure ap address ipv6 auto-config disable** コマンドを使用します。
- IPv6 SLAAC を有効にするには、**configure ap address ipv6 auto-config enable** コマンドを使用します。SLAAC は WGB の CoS には適用されないことに注意してください。このコマンドでは、SLAAC の代わりに DHCPv6 を使用して IPv6 アドレスを設定します。

DHCP を使用した IPv6アドレスの設定

DHCP を使用して IPv6 アドレスを設定するには、**configure ap address** *ipv6 dhcp* コマンドを使用します。

```
Device#configure ap address ipv6 dhcp
```

現在の IP 設定の確認

現在の IP アドレス設定を確認するには、**show ipv6 interface brief** コマンドを使用します。

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

Dot1x ログイン情報を設定します。

Dot1x ログイン情報を設定するには、**configure dot1x credential** *profile-name* **username** *name* **password** *pwd* コマンドを使用します。

```
Device#configure dot1x credential profile-name username name password pwd
```

WGB EAP Dot1x プロファイルの確認

WGB EAP Dot1x プロファイルの状態を表示するには、**show wgb eap dot1x credential profile** コマンドを使用します。

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

WGB 有線クライアントの認証解除

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

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

EAP プロファイルの設定

EAP プロファイルを設定するには、以下のステップを実行します。

1. Dot1x ログイン情報プロファイルを EAP プロファイルにアタッチします。
2. EAP プロファイルを SSID プロファイルにアタッチします。
3. SSID プロファイルを無線機にアタッチします。

手順

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

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

（注）
EAP プロファイル方式を選択します。

- fast
- peap
- tls

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

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

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

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

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

```
Device#configure eap-profile profile-name delete
```

端末のトラストポイントの手動登録設定

手順

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

quit を入力して、証明書を終了します。

（注）
中間証明書を使用する場合は、トラストポイントのすべての証明書チェーンをインポートします。

例：

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name* **enroll** コマンドを使用して、秘密鍵と証明書署名要求（CSR）を生成します。

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

CA サーバーの CSR 出力を使用して、デジタル署名付き証明書を作成します。

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

quit を入力して、証明書を終了します。

```
Device#quit
```

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

ステップ 8 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 9 トラストポイント用に作成された証明書の内容を表示するには、**show crypto pki trustpoint certificate** コマンドを使用します。

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

WGB のトラストポイント自動登録の設定

手順

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

このコマンドは、CA サーバーから CA 証明書を自動的に取得します。

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

CA サーバーのデジタル署名付き証明書を要求します。

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

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

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

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

ステップ 8 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 9 特定のトラストポイントの証明書の詳細を表示するには、**show crypto pki trustpoint** *trustpoint-name* **certificate** コマンドを使用します。

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

ステップ 10 Public Key Infrastructure（PKI）タイマー情報を表示するには、**show crypto pki timers** コマンドを使用します。

show crypto pki timers

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

TFTP サーバーを使用した手動での証明書の登録設定

手順

ステップ 1 登録方法を指定します。

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

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

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name***enroll** コマンドを使用して、秘密鍵と証明書署名要求（CSR）を生成します。

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

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

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

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

ステップ 7 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 8 トラストポイント用に作成された証明書の内容を表示するには、**show crypto pki trustpoint certificate** コマンドを使用します。

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

SSID の設定

SSID の設定は、次の 2 つの部分で構成されます。

1. SSID プロファイルの作成 （39 ページ）
2. ワークグループブリッジの無線インターフェイスの設定 （40 ページ）

SSID プロファイルの作成

SSID プロファイルを設定するには、次のいずれかの認証プロトコルを選択します。

1. オープン認証
2. 事前共有鍵（PSK）認証
   - PSK WPA2 認証
   - PSK Dot11r 認証
   - PSK Dot11w 認証
3. Dot1x 認証

オープン認証を使用した SSID プロファイルの設定

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

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

PSK 認証を使用した SSID プロファイルの設定

PSK 認証を使用して SSID プロファイルを設定するには、次の認証プロトコルのいずれかを選択します。

- PSK WPA2 認証を使用した SSID プロファイルの設定
- PSK Dot11r 認証を使用した SSID プロファイルの設定
- PSK Dot11w 認証を使用した SSID プロファイルの設定

PSK WPA2 認証を使用した SSID プロファイルの設定

PSK WPA2 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

PSK Dot11r 認証を使用した SSID プロファイルの設定

PSK Dot11r 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

PSK Dot11w 認証を使用した SSID プロファイルの設定

PSK Dot11w 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Dot1x 認証を使用した SSID プロファイルの設定

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

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
 profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Dot1x EAP-PEAP 認証による SSID プロファイルの設定

以下の例は、Dot1x EAP-PEAP 認証を使用した SSID プロファイルの設定を示しています。

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

ワークグループブリッジの無線インターフェイスの設定

- 使用可能な 2 つの無線インターフェイスから、一方の無線インターフェイスで WGB モードを設定する前に、もう一方の無線インターフェイスをルート AP モードに設定します。

  次のコマンドを入力して、無線インターフェイスをルート AP としてマッピングします。

  # **configure dot11radio** *radio-slot-id* **mode root-ap**

  例

  ```
  # configure dot11radio 0 mode root-ap
  ```

（注） アクティブな SSID または EAP プロファイルが変更された場合、更新されたプロファイルをアクティブにするには、プロファイルを無線インターフェイスに再度関連付ける必要があります。

- 次のコマンドを入力して、無線インターフェイスにWGB SSIDプロファイルをマッピングします。

  # **configure dot11radio** *radio-slot-id* **mode wgb ssid-profile** *ssid-profile-name*

  例

  ```
  # configure dot11radio 1 mode wgb ssid-profile psk_ssid
  ```

- 次のコマンドを入力して、無線インターフェイスを設定します。

  # **configure dot11radio** *radio-slot-id*{ **enable** | **disable** }

  例

  ```
  # configure dot11radio 0 disable
  ```

（注） 1 つの無線機またはスロットのみに WGB モードでの動作が許可されます。

WGB/uWGB タイマーの設定

タイマー設定 CLI は、WGB と uWGB で共通です。タイマーを設定するには、次のコマンドを使用します。

- 次のコマンドを入力して、WGB アソシエーション応答のタイムアウトを設定します。

  # **configure wgb association response timeout** *response-millisecs*

  デフォルト値は 100 ミリ秒です。有効な範囲は 100 ～ 5000 ミリ秒です。

- 次のコマンドを入力して、WGB 認証応答のタイムアウトを設定します。

  # **configure wgb authentication response timeout** *response-millisecs*

  デフォルト値は 100 ミリ秒です。有効な範囲は 100 ～ 5000 ミリ秒です。

- 次のコマンドを入力して、WGB EAP タイムアウトを設定します。

  # **configure wgb eap timeout** *timeout-secs*

  デフォルト値は 3 秒です。有効な範囲は、2 ～ 60 秒です。

- 次のコマンドを入力して、WGBブリッジクライアント応答のタイムアウトを設定します。

  # **configure wgb bridge client timeout** *timeout-secs*

  デフォルトのタイムアウト値は 300 秒です。有効な範囲は 10 ～ 1000000 秒です。

uWGB の設定

ユニバーサル WGB は、アップリンク無線機 MAC アドレスを使用してシスコ以外のアクセスポイントと相互運用できます。このため、ユニバーサル ワークグループ ブリッジのロールは 1 つの有線クライアントのみをサポートします。

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

configure dot11 <**0**|**1**> **mode uwgb** <*uwgb_wired_client_mac_address*> **ssid-profile** <*ssid-profile*>

次に、Dot1x FAST-EAP の設定例を示します。

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 0 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 0 enable
```

以下のセクションで、uWGB の設定について詳しく説明します。

IP アドレスの設定

IPv4 アドレスを設定する

- DHCP を使用して IPv4 アドレスを設定するには、**configure ap address** *ipv4 dhcp* コマンドを使用します。

  ```
  Device#configure ap address ipv4 dhcp
  ```

- 静的 IPv4 アドレスを設定するには、**configure ap address** *ipv4 static ipv4_addr netmask gateway* コマンドを使用します。設定すると、アップリンク接続なしで有線インターフェイスを使用してデバイスを管理できます。

  ```
  Device#configure ap address ipv4 static ipv4_addr netmask gateway
  ```

現在の IP 設定の確認

現在の IP アドレス設定を表示するには、**show ip interface brief** コマンドを使用します。

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

IPv6 アドレスを設定する

静的 IPv6 アドレスを設定するには、**configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* コマンドを使用します。この設定により、アップリンク接続なしで有線インターフェイスを介して AP を管理できます。

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

IPv6 自動設定の有効化

AP で IPv6自動設定を有効にするには、**configure ap address ipv6 auto-config enable** コマンドを使用します。

```
Device#configure ap address ipv6 auto-config enable
```

（注）
- AP で IPv6 自動設定を無効にするには、**configure ap address ipv6 auto-config disable** コマンドを使用します。
- IPv6 SLAAC を有効にするには、**configure ap address ipv6 auto-config enable** コマンドを使用します。SLAAC は WGB の CoS には適用されないことに注意してください。このコマンドでは、SLAAC の代わりに DHCPv6 を使用して IPv6 アドレスを設定します。

DHCP を使用した IPv6アドレスの設定

DHCP を使用して IPv6 アドレスを設定するには、**configure ap address** *ipv6 dhcp* コマンドを使用します。

```
Device#configure ap address ipv6 dhcp
```

現在の IP 設定の確認

現在の IP アドレス設定を確認するには、**show ipv6 interface brief** コマンドを使用します。

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

Dot1x ログイン情報を設定します。

Dot1x ログイン情報を設定するには、**configure dot1x credential** *profile-name* **username** *name* **password** *pwd* コマンドを使用します。

```
Device#configure dot1x credential profile-name username name password pwd
```

WGB EAP Dot1x プロファイルの確認

WGB EAP Dot1x プロファイルの状態を表示するには、**show wgb eap dot1x credential profile** コマンドを使用します。

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

EAP プロファイルの設定

EAP プロファイルを設定するには、以下のステップを実行します。

1. Dot1x ログイン情報プロファイルを EAP プロファイルにアタッチします。
2. EAP プロファイルを SSID プロファイルにアタッチします。
3. SSID プロファイルを無線機にアタッチします。

手順

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

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

（注）
EAP プロファイル方式を選択します。

- fast
- peap
- tls

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

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

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

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

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

```
Device#configure eap-profile profile-name delete
```

端末のトラストポイントの手動登録設定

手順

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

quit を入力して、証明書を終了します。

（注）
中間証明書を使用する場合は、トラストポイントのすべての証明書チェーンをインポートします。

例：

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name* **enroll** コマンドを使用して、秘密鍵と証明書署名要求（CSR）を生成します。

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

CA サーバーの CSR 出力を使用して、デジタル署名付き証明書を作成します。

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

quit を入力して、証明書を終了します。

```
Device#quit
```

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

ステップ 8 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 9 トラストポイント用に作成された証明書の内容を表示するには、**show crypto pki trustpoint certificate** コマンドを使用します。

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

WGB のトラストポイント自動登録の設定

手順

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

このコマンドは、CA サーバーから CA 証明書を自動的に取得します。

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

CA サーバーのデジタル署名付き証明書を要求します。

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

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

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

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

ステップ 8 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 9 特定のトラストポイントの証明書の詳細を表示するには、**show crypto pki trustpoint** *trustpoint-name* **certificate** コマンドを使用します。

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

ステップ 10 Public Key Infrastructure（PKI）タイマー情報を表示するには、**show crypto pki timers** コマンドを使用します。

show crypto pki timers

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

TFTP サーバーを使用した手動での証明書の登録設定

手順

ステップ 1 登録方法を指定します。

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

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

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

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

ステップ 5 **configure crypto pki trustpoint** *ca-server-name***enroll** コマンドを使用して、秘密鍵と証明書署名要求（CSR）を生成します。

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

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

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

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

ステップ 7 **show crypto pki trustpoint** コマンドを使用して、トラストポイントの概要を表示します。

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

ステップ 8 トラストポイント用に作成された証明書の内容を表示するには、**show crypto pki trustpoint certificate** コマンドを使用します。

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

SSID の設定

SSID の設定は、次の 2 つの部分で構成されます。

1. SSID プロファイルの作成 （39 ページ）
2. uWGB の無線インターフェイスの設定 （50 ページ）

SSID プロファイルの作成

SSID プロファイルを設定するには、次のいずれかの認証プロトコルを選択します。

1. オープン認証
2. 事前共有鍵（PSK）認証
   - PSK WPA2 認証
   - PSK Dot11r 認証
   - PSK Dot11w 認証
3. Dot1x 認証

オープン認証を使用した SSID プロファイルの設定

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

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

PSK 認証を使用した SSID プロファイルの設定

PSK 認証を使用して SSID プロファイルを設定するには、次の認証プロトコルのいずれかを選択します。

- PSK WPA2 認証を使用した SSID プロファイルの設定
- PSK Dot11r 認証を使用した SSID プロファイルの設定
- PSK Dot11w 認証を使用した SSID プロファイルの設定

PSK WPA2 認証を使用した SSID プロファイルの設定

PSK WPA2 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

PSK Dot11r 認証を使用した SSID プロファイルの設定

PSK Dot11r 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

PSK Dot11w 認証を使用した SSID プロファイルの設定

PSK Dot11w 認証を使用して SSID プロファイルを設定するには、**configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** コマンドを使用します。

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Dot1x 認証を使用した SSID プロファイルの設定

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

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
 profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Dot1x EAP-PEAP 認証による SSID プロファイルの設定

以下の例は、Dot1x EAP-PEAP 認証を使用した SSID プロファイルの設定を示しています。

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

uWGB の無線インターフェイスの設定

- 使用可能な 2 つの無線インターフェイスから、一方の無線インターフェイスで WGB モードを設定する前に、もう一方の無線インターフェイスをルート AP モードに設定します。

  次のコマンドを入力して、無線インターフェイスをルート AP としてマッピングします。

  # **configure dot11radio** *radio-slot-id* **mode root-ap**

  例

  ```
  # configure dot11radio 0 mode root-ap
  ```

（注） アクティブな SSID または EAP プロファイルが変更された場合、更新されたプロファイルをアクティブにするには、プロファイルを無線インターフェイスに再度関連付ける必要があります。

- 次のコマンドを入力して、無線インターフェイスに WGB SSID プロファイルをマッピングします。

  # **configure dot11radio** *radio-slot-id* **mode uwgb** *uwgb-wired-client-mac-address* **ssid-profile** *ssid-profile-name*

- 次のコマンドを入力して、無線インターフェイスを設定します。

  # **configure dot11radio** *radio-slot-id*{ **enable** | **disable** }

  例

  ```
  # configure dot11radio 0 disable
  ```

（注） SSID プロファイルにアップリンクを設定した後、変更をアクティブにするために無線機の無効化と有効化を行うことをお勧めします。

（注） 1 つの無線機またはスロットのみに uWGB または WGB モードでの動作が許可されます。

WGB と uWGB 間の変換

WGB から uWGB に変換するには、次のコマンドを使用します。

#**configure dot11radio** <**0**|**1**> **mode uwgb** <*WIRED_CLIENT_MAC*> **ssid-profile** <*SSID_PROFILE_NAME*>

uWGB から WGB に変換するには、次のコマンドを使用します。この変換を行うと、AP が再起動されます。

```
#configure Dot11Radio 1 mode wgb ssid-profile <SSID_PROFILE_NAME>

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

LED パターン

2 つの新しい LED パターンが IW9167EH WGB モードに追加されました。

- WGB のアソシエーションが解除された状態では、システム LED は赤色に点滅します。
- WGB と親 AP との関連付けが成立すると、システム LED は緑色に点灯します。

HT 速度制限の設定

WGBがフィールドを移動する展開では、高スループット（HT）変調符号化方式（MCS）を使用して伝送レート制限を手動で設定できます。

次に、802.11n HT m4. m5. レートで送信するように設定する場合のWGBの設定例を示します。

Config dot11radio [**1**|**2**] **802.11ax disable**

Config dot11radio [**1**|**2**] **802.11ac disable**

Config dot11radio [**1**|**2**] **speed ht-mcs m4. m5.**

WGB では、レガシーレートの設定もサポートされます。

- 802.11b/g の場合、レガシーレートは次のように設定されます。

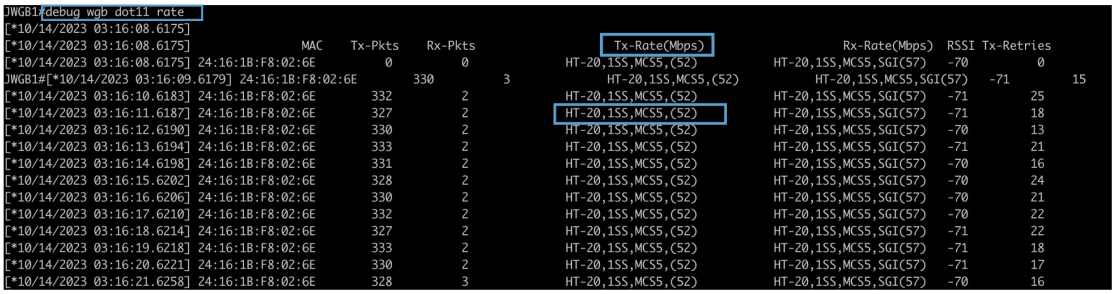
```
configure dot11radio 0 speed legacy-rate
1.0 Allow 1.0 Mb/s rate
11.0 Allow 11.0 Mb/s rate
12.0 Allow 12.0 Mb/s rate
18.0 Allow 18.0 Mb/s rate
2.0 Allow 2.0 Mb/s rate
24.0 Allow 24.0 Mb/s rate
36.0 Allow 36.0 Mb/s rate
48.0 Allow 48.0 Mb/s rate
5.5 Allow 5.5 Mb/s rate
54.0 Allow 54.0 Mb/s rate
6.0 Allow 6.0 Mb/s rate
9.0 Allow 9.0 Mb/s rate
basic-1.0 Require 1.0 Mb/s rate
basic-11.0 Require 11.0 Mb/s rate
basic-12.0 Require 12.0 Mb/s rate
basic-18.0 Require 18.0 Mb/s rate
basic-2.0 Require 2.0 Mb/s rate
basic-24.0 Require 24.0 Mb/s rate
basic-36.0 Require 36.0 Mb/s rate
basic-48.0 Require 48.0 Mb/s rate
basic-5.5 Require 5.5 Mb/s rate
basic-54.0 Require 54.0 Mb/s rate
basic-6.0 Require 6.0 Mb/s rate
basic-9.0 Require 9.0 Mb/s rate
default Set default legacy rates
```

- 802.11a の場合、レガシーレートは次のように設定されます。

```
configure dot11radio [1|2] speed legacy-rate
12.0 Allow 12.0 Mb/s rate
18.0 Allow 18.0 Mb/s rate
24.0 Allow 24.0 Mb/s rate
36.0 Allow 36.0 Mb/s rate
48.0 Allow 48.0 Mb/s rate
54.0 Allow 54.0 Mb/s rate
6.0 Allow 6.0 Mb/s rate
9.0 Allow 9.0 Mb/s rate
basic-12.0 Require 12.0 Mb/s rate
basic-18.0 Require 18.0 Mb/s rate
basic-24.0 Require 24.0 Mb/s rate
basic-36.0 Require 36.0 Mb/s rate
basic-48.0 Require 48.0 Mb/s rate
basic-54.0 Require 54.0 Mb/s rate
basic-6.0 Require 6.0 Mb/s rate
basic-9.0 Require 9.0 Mb/s rate
default Set default legacy rates
```

レガシーレートは、802.11 管理フレームと制御フレームで使用されます。WGB レガシーレートは、AP のレガシーレートに一致するか、少なくともこれら 2 つのレートが重複している必要があります。そうでない場合には、レートの不一致が原因で WGB アソシエーションが拒否されます。

WGB Tx MCS レートを確認するには、**debug wgb dot11 rate** コマンドを使用します。次に、このコマンドの出力例を示します。



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

無線機統計コマンド

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

```
Device# debug wgb dot11 rate

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

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

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

```
Device# show interfaces dot11Radio 1 statistics

Dot11Radio Statistics:
        DOT11 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx K Bytes:         965570/0       Host Tx K Bytes:       1611903/0
Unicasts Rx:             379274/0       Unicasts Tx:           2688665/0
Broadcasts Rx:          3166311/0       Broadcasts Tx:               0/0
Beacons Rx:           722130099/1631    Beacons Tx:          367240960/784
Probes Rx:            588627347/2224    Probes Tx:            78934926/80
Multicasts Rx:          3231513/0       Multicasts Tx:           53355/0
Mgmt Packets Rx:      764747086/1769    Mgmt Packets Tx:     446292853/864
Ctrl Frames Rx:         7316214/5       Ctrl Frames Tx:              0/0
RTS received:                 0/0       RTS transmitted:             0/0
Duplicate frames:             0/0       CTS not received:            0/0
MIC errors:                   0/0       WEP errors:            2279546/0
FCS errors:                   0/0       Retries:                896973/0
Key Index errors:             0/0       Tx Failures:              8871/0
                                        Tx Drops:                    0/0

Rate Statistics for Radio::
[Legacy]:
6 Mbps:
 Rx Packets:     159053/0            Tx Packets:      88650/0
                                     Tx Retries:       2382/0
9 Mbps:
 Rx Packets:          43/0           Tx Packets:         23/0
                                     Tx Retries:         71/0
12 Mbps:
 Rx Packets:           1/0           Tx Packets:        119/0
                                     Tx Retries:        185/0
18 Mbps:
 Rx Packets:           0/0           Tx Packets:          5/0
                                     Tx Retries:        134/0
24 Mbps:
 Rx Packets:         235/0           Tx Packets:      20993/0
                                     Tx Retries:       5048/0
36 Mbps:
 Rx Packets:           0/0           Tx Packets:        781/0
                                     Tx Retries:        227/0
54 Mbps:
 Rx Packets:         133/0           Tx Packets:       9347/0
                                     Tx Retries:       1792/0

[SU]:
M0:
 Rx Packets:           7/0           Tx Packets:          0/0
                                     Tx Retries:          6/0
M1:
 Rx Packets:        1615/0           Tx Packets:      35035/0
                                     Tx Retries:       3751/0
M2:
 Rx Packets:       15277/0           Tx Packets:     133738/0
                                     Tx Retries:      22654/0
M3:
 Rx Packets:       10232/0           Tx Packets:       1580/0
                                     Tx Retries:      21271/0
M4:
```

```
 Rx Packets:     218143/0            Tx Packets:     190408/0
                                     Tx Retries:      36444/0
M5:
 Rx Packets:     399283/0            Tx Packets:     542491/0
                                     Tx Retries:     164048/0
M6:
 Rx Packets:    3136519/0            Tx Packets:     821537/0
                                     Tx Retries:     329003/0
M7:
 Rx Packets:    1171128/0            Tx Packets:     303414/0
                                     Tx Retries:     154014/0



Beacons missed: 0-30s 31-60s 61-90s 90s+
                     2      0      0    0
```

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

```
AP# show wgb dot11 uplink latency

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

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

```
AP# show wgb dot11 uplink

HE Rates: 1SS:M0-11 2SS:M0-11
Additional info for client 8C:84:42:92:FF:CF
RSSI: -24
PS  : Legacy (Awake)
Tx Rate: 278730 Kbps
Rx Rate: 410220 Kbps
VHT_TXMAP: 65530
CCX Ver: 5
Rx Key-Index Errs: 0
             mac     intf TxData TxUC TxBytes TxFail TxDcrd TxCumRetries MultiRetries
MaxRetriesFail RxData RxBytes RxErr                TxRt(Mbps)                RxRt(Mbps)
   LER PER stats_ago
8C:84:42:92:FF:CF wbridge1   1341 1341  184032      0      0          543            96
            0    317   33523     0 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8 (458)
 27272   0  1.370000
Per TID packet statistics for client 8C:84:42:92:FF:CF
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s)
       0      35    1314            0             8
       1       0       0            0             0
```

```
       2       0       0            0            0
       3       0       0            0            0
       4       0       0            0            0
       5       0       0            0            0
       6     182      24            1            0
       7       3       3            0            0
Rate Statistics:
Rate-Index    Rx-Pkts    Tx-Pkts Tx-Retries
         0         99          3          0
         4          1          1          9
         5         21         39         35
         6         31        185         64
         7         26        124         68
         8         28        293         82
         9         77        401        151
        10         32        140         97
        11          2        156         37
```

Syslog

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

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

イベントロギング

WGBフィールド展開の場合、イベントロギングは有用な情報（WGBの状態変更やパケットのRx/Txなど）を収集して分析し、ログ履歴を提供して、特にローミングケースにおける問題のコンテキストを提示します。

probe、auth、assoc、EAP、dhcp、icmp、arpなど、すべての管理パケットタイプに対してWGBトレースフィルタを設定できます。WGB トレースを有効または無効にするには、次のコマンドを使用します。

#config wgb event trace {**enable**|**disable**}

次の 4 種類のイベントタイプがサポートされています。

- **Basic event**：WGB の基本レベルの情報メッセージのほとんどをカバーします。

- **Detail event**：基本イベントと追加のデバッグレベルメッセージをカバーします。
- **Trace event**：有効になっている場合、wgb トレースイベントを記録します。
- **All event**：トレースイベントと詳細イベントをバンドルします。

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

異常な状況が発生した場合は、次の show コマンドを使用して、eventlog メッセージをメモリに手動でダンプできます。このコマンドでは、WGB ロギングも表示されます。

#**show wgb event** [**basic**|**detail**|**trace**|**all**]

次に、**show wgb event all** の出力例を示します。

```
APC0F8.7FE5.F3C0#show wgb event all
[*08/16/2023 08:18:25.167578] UP_EVT:4 R1 IFC:58:9A:17:B3:E7] parent_rssi: -42 threshold:
 -70
[*08/16/2023 08:18:25.329223] UP_EVT:4 R1 State CONNECTED to SCAN_START
[*08/16/2023 08:18:25.329539] UP_EVT:4 R1 State SCAN_START to STOPPED
[*08/16/2023 08:18:25.330002] UP_DRV:1 R1 WGB UPLINK mode stopped
[*08/16/2023 08:18:25.629405] UP_DRV:1 R1 Delete client FC:58:9A:17:B3:E7
[*08/16/2023 08:18:25.736718] UP_CFG:8 R1 configured for standard: 7
[*08/16/2023 08:18:25.989936] UP_CFG:4 R1 band 1 current power level: 1
[*08/16/2023 08:18:25.996692] UP_CFG:4 R1 band 1 set tx power level: 1
[*08/16/2023 08:18:26.003904] UP_DRV:1 R1 WGB uplink mode started
[*08/16/2023 08:18:26.872086] UP_EVT:4 Reset aux scan
[*08/16/2023 08:18:26.872096] UP_EVT:4 Pause aux scan on slot 2
[*08/16/2023 08:18:26.872100] SC_MST:4 R2 reset uplink scan state to idle
[*08/16/2023 08:18:26.872104] UP_EVT:4 Aux bring down vap - scan
[*08/16/2023 08:18:26.872123] UP_EVT:4 Aux bring up vap - serv
[*08/16/2023 08:18:26.872514] UP_EVT:4 R1 State STOPPED to SCAN_START
[*08/16/2023 08:18:26.8727091 SC_MST:4 R1 Uplink Scan Started.
[*08/16/2023 08:18:26.884054] UP_EVT:8 R1 CH event 149
```

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

次の clear コマンドは、メモリの WGB イベントを消去します。

#**clear wgb event** [**basic**|**detail**|**trace**|**all**]

すべてのイベントログを WGB フラッシュに保存するには、次のコマンドを使用します。

#**copy event-logging flash**

パッケージファイルは、ログレベルが異なる 4 つの個別のログファイルで構成されます。

次のコマンドを使用して、イベントログをリモートサーバーに保存することもできます。

#**copy event-logging upload** <**tftp** | **sftp** | **scp**>**:**//A.B.C.D[/*dir*][/*filename.tar.gz*]

次に、イベントログを TFTP サーバーに保存する例を示します。

```
APC0F8.7FE5.F3C0#copy event-logging upload
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz
Starting upload of WGB config
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz ...
It may take a few seconds. If longer, please cancel command, check network and try again.
```

```
########################################################################## 100.0%
Config upload completed.
```

（注） 一方、**copy event-logging upload** <**tftp** | **sftp** | **scp**>**:**//A.B.C.D[/*dir*][/*filename.tar.gz*] コマンドは引き続きサポートされます。UIW リリース 17.17.1 以降では、以下の transfer コマンドを使用して、より包括的な診断情報を取得することを推奨します。

イベントログを収集および転送するようにWGBでリモートサーバーとプロトコルタイプ（TFTPまたは SFTP）を設定するには、以下のタスクを使用します。

- **transfer upload mode**{**ftp** | **tftp**} コマンドを使用して、ログ転送のプロトコルを選択します。

  ```
  Device#transfer upload mode sftp
  ```

- SFTP を使用する場合は、**transfer upload username** *username* **password** *password* を使用して、ユーザー名とパスワードを設定します。

  ```
  Device#transfer upload username Cisco password Cisco123
  ```

- **transfer upload server-ip** *remote-server-ip* を使用して、リモートサーバーの IP アドレスを設定します。

  ```
  Device#transfer upload server-ip 192.168.71.11
  ```

- （オプション）**transfer upload server-ip** *remote-server-ip* **path** *remote-server-path* を使用して、リモートサーバーのパスを設定します。

  ```
  Device#transfer upload server-ip 192.168.71.11 path /upload/wgb
  ```

（注） 上記の静的設定は持続的で、デバイスのリロード後も引き続き有効です。

- **transfer upload start** コマンドを使用して、イベントログを収集し、リモートサーバーに転送します。

  ```
  Device#transfer upload start
  ```

リモートサーバーが設定されると、デバイスは以下のデータを収集および転送します。

- デバイスは、障害対応を目的としてコアファイルを収集します。
- syslog ファイルを収集して、システムのイベントとアクティビティを監視します。
- WGB または uWGB の実行コンフィギュレーションが設定のバックアップのために取得されます。
- 無線機のリセット履歴は、潜在的な接続の問題を特定するために記録されます。
- システム性能とインシデントを追跡するために、イベントロギングデータが転送されます。

802.11v 機能

802.11v は、ワイヤレスネットワーク管理の標準規格で、

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

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

802.11v のサポートによるローミングの機能拡張

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

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

基本サービスセット移行要求フレーム

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

WLC を使用して AP のクライアントとの関連付けを解除する

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

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

その他の参考情報

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

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

補助走査の設定

補助走査モードは、ローミング性能の向上を目的に、WGB 無線機 2（5 GHz）で走査専用モードまたはハンドオフモードのいずれかに設定できます。ローミングが開始されると、WGB は、走査テーブルを参照して最適な親 AP を検索します。走査テーブルは、2.4 GHz の場合は無線機 0 または無線機 4、5 GHz の場合は無線機 1 または無線機 4 を使用して更新されます。

- 走査専用モードの概要
- 走査専用モードの設定
- 走査専用モードの無線機 4
- 補助走査ハンドオフモードの設定
- デュアル無線機 WGB によるローミングの最適化

走査専用モード

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

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

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

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

走査専用モード

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

ローミングが開始されると、アルゴリズムによって走査テーブルで候補が検索され、テーブルが空でなければ走査段階はスキップされます。その後、WGBがその候補APとの関連付けを行います。

走査専用モードの設定

走査専用モードを設定するには、**configure dot11Radio 2 mode scan only** コマンドを使用します。

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

チャンネルリストの手動設定

チャンネルリストにチャンネルを手動で追加するには、**configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **add** コマンドを使用します。

```
Device#configure wgb mobile station interface dot11Radio 1 scan <channel> [add|delete]
```

（注） チャンネルリストからチャンネルを手動で削除するには、**configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **delete** コマンドを使用します。

走査テーブルタイマーの設定

タイマーを調整するには、**configure wgb scan radio 2 timeout***1500* コマンドを使用します。デフォルトでは、走査テーブルの候補APエントリは1200ミリ秒で自動的に削除されます。

```
Device#configure wgb scan radio 2 timeout 1500
```

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

走査テーブルの確認

走査テーブルを確認するには、**show wgb scan** コマンドを使用します。

```
Device#show wgb scan
Best AP expire time: 5000 ms
```

```
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:E2:4F     84     136       1531
FC:58:9A:15:DE:4F     37     136       41

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4F    37     136       41
```

走査専用モードの無線機 4

Cisco IOS-XE 17.15.1 リリースより前は、無線機 2（5 GHz）のみを走査用に設定できました。Cisco IOS-XE 17.15.1 リリース以降、無線機 4（IW9167E AP）を走査専用モードで設定できます。

無線機 4 には、以下の送受信アンテナがあります。

- 2.4 GHz および 5 GHz の周波数帯域からデータを送信するための送信アンテナ 1 基。
- 2.4 GHz、5 GHz、および 6 GHzの周波数帯域からデータを受信するための受信アンテナ 2 基。

（注） 無線機 2 と無線機 4 の両方が同時に走査機能に関して有効になっている場合、WGB は無線機 4 を走査に使用し、無線機 2 は非アクティブになります。

無線機 4 を走査専用モードとして使用する利点

- WGB の補助走査およびローミングでは、2.4 GHz と 5 GHz の両方の周波数がサポートされるようになりました。
- 走査用無線機はサービス無線機とアンテナを共有するため、アンテナリソースを節約できます。

（注） ローミング性能は、無線機 2 での WGB 補助走査機能と同じレベルに保たれます。

走査専用モードについての無線機 2 と無線機 4 の比較

走査のサポート	無線機 2（5 GHz）	無線機 4（専用補助無線機）
2.4 GHz	非対応	はい
5 GHz	対応	対応
走査専用モード	対応	対応
走査ハンドオフモード	対応	非対応

走査のサポート	無線機 2（5 GHz）	無線機 4（専用補助無線機）
補助走査アンテナの要件	RF カバレッジのダイバーシティを利用するには、追加のアンテナが必要です。	走査用無線機は、サービス無線機のアンテナを使用します。

専用補助無線機とサービス無線機間の接続マップ

専用補助無線機	サービス無線機
2.4 GHz 伝送	アンテナ 1
5 GHz 伝送	アンテナ 4
2.4 GHz 受信	アンテナ 2 アンテナ 3
5 GHz 受信	アンテナ 3 アンテナ 2

無線機 4 の走査専用モードへの設定

無線機 4 を走査専用モードで動作するように設定するには、次のコマンドを使用します。

```
#config wgb aux-radio scan
```

無線機 4 の走査専用モードを無効にするには、次のコマンドを使用します。

```
#config wgb aux-radio disable
```

無線機 4 走査専用モードの設定の確認

無線機 4 が走査専用モードであることを確認するには、次のコマンドを使用します。

```
#show running-config
AP Name             : APFC58.9A16.E538
AP Mode             : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring : Enabled
SSH State            : Enabled
AP Username          : cisco
Session Timeout     : 300
WGB Trace           : Disabled
Syslog Host          : 0.0.0.0
Radio and WLAN-Profile Mapping
=====================================
Radio ID    Radio Mode    SSID-Profile       SSID         Authentication
-------------------------------------------------------------------------------
1           WGB           wyj-open           wyj-open     OPEN
2           SCAN          wyj-open           wyj-open     OPEN

Radio Configurations
   .
   .
   .
```

```
   Radio Id                    : 2
   Admin state              : ENABLED
   Mode                     : SCAN - Handoff
   Spatial Stream           : AUTO
   Guard Interval           : 800 ns
   Dot11 type               : 11ax
   11v BSS-Neighbor         : Disabled
   A-MPDU priority          : 0x3f
   A-MPDU subframe number   : 255
   RTS Protection           : 2347(default)
   Rx-SOP Threshold         : AUTO
   Radio profile            : NA
Radio Id                    : 4 (Aux Radio)
   Admin state              : ENABLED
   Mode                     : SCAN
```

次の show コマンドで表示される走査結果：

```
#show wgb scan
 Aux Scanning Configure:
 Radio Id: 1
        Admin State: ENABLED
        Mode: WGB
Radio Id: 2
        Admin State: ENABLED
        Mode: SCAN - Handoff
Radio Id: 4 (Aux Radio)
        Admin State: ENABLED
        Mode: SCAN
Best AP expire time: 5000 ms
Aux Scanning State: RUNNING
Aux Scanning Radio Results (Radio 4)
************[ AP List]***************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D9:B6:8E     35     149       2914

***********[ Best AP]****************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D9:B6:8E    35     149       2914

Aux Serving Radio Results (Radio1)
************[ AP List]***************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D0:A3:8E     18     36        4

***********[ Best AP]****************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D0:A3:8E    18     36       5
```

補助走査ハンドオフモードの設定

スロット 2 の無線機がハンドオフモードに設定されている場合、無線機 1 と無線機 2 の両方がアップリンクの候補となります。一方の無線機がワイヤレスアップリンクを維持している間に、もう一方の無線機がチャンネルの走査を継続します。走査リストは、手動で設定することも、802.11v によって学習させることもできます。

無線機 2 は無線機 1 と同じ MAC アドレスを共有し、走査機能、アソシエーション、およびデータ伝送をサポートします。どちらの無線機も、[serving] または [scanning] ロールで動作できます。ローミングが開始されると、アルゴリズムによって走査データベース（内部の表）が検索され、最適な候補 AP を選択して接続が確立されます。無線機のロールとトラフィック

は、各ローミングの後にスロット1とスロット2の間で動的に切り替わります。WGBは常に、[scanning] ロールで動作している無線機を使用して、新しいAPへのローミングアソシエーションを完了します。この設定により、ローミング中断時間を 20 ～ 50 ミリ秒に改善できます。

次の表では、さまざまなメカニズムでのローミング瞬断時間（3 チャンネルの場合）を比較します。

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

WGB スロット 2 の無線機を補助走査モードに設定するには、次のコマンドを使用します。

configure dot11Radio 2 mode scan handoff

show run コマンドを使用して、設定を確認します。

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

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

```
APFC58.9A15.C808#show wgb scan
Best AP expire time: 2500 ms

Aux Scanning Radio Results (slot 2)
************[ AP List ]***************
BSSID               RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     54     153       57
FC:58:9A:15:E2:4E     71     153       64
```

```
***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    54     153       57

Aux Serving Radio Results
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     58     153       57
FC:58:9A:15:E2:4E     75     153       133

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    58     153       57
```

デュアル無線機 WGB によるローミングの最適化

Cisco IOS-XE 17.15.1 リリース以降、デュアル無線機構成のデバイスのローミング効率が向上しました。ビーコンフレームが連続して欠落するかパケットの再試行回数が上限に達することで、ローミングが開始されます。2 つ目の無線機により、WGB は走査段階を飛ばし、候補となる AP の走査表を直接確認できます。このプロセスにより、サービスのダウンタイムが短縮されます。

ローミングの契機となる要因

ローミングは以下のイベントで開始されます。

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

デュアル無線機設定

デュアル無線機構成において、IW9167E AP で可能な設定は次のとおりです。

デュアル無線機	AP
2.4 GHz 無線機 0 + 無線機 4（専用補助無線機）	IW9167E
5 GHz 無線機 1 + 無線機 2（走査専用モード）	
5 GHz 無線機 1 + 無線機 2（補助走査ハンドオフモード）	
5 GHz 無線機 1 + 無線機 4（専用補助無線機）	

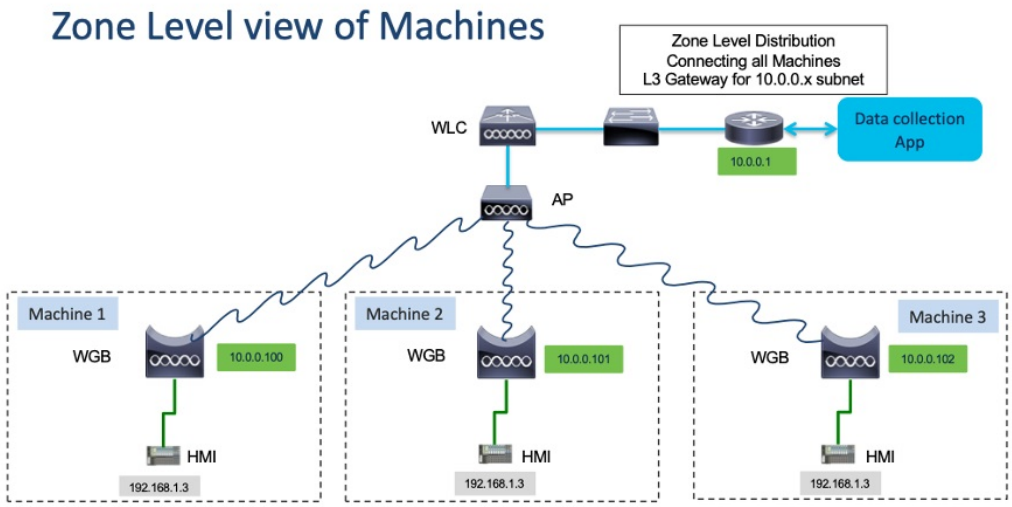
レイヤ 2 NAT

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

レイヤ 2 NAT は、次の 2 つの変換表を維持します。

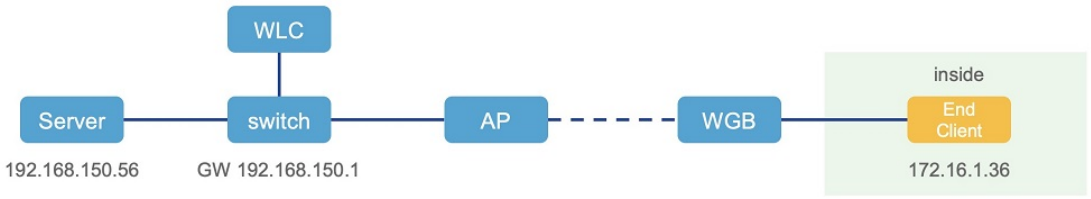
- プライベートからパブリックへのサブネット変換
- パブリックからプライベートへのサブネット変換

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



ホスト IP アドレス変換の設定例

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



レイヤ 2 NAT の設定例

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

```
Device# show l2nat config

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

レイヤ 2 NAT ルールの例

レイヤ 2 NAT ルールの例を以下に示します。

```
Device# show l2nat rule

Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

レイヤ 2 NAT エントリの例

現在のレイヤ 2 NAT エントリの例を以下に示します。

```
Device# show l2nat entry

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

WGB 有線クライアントの例

ブリッジを介した WGB 有線クライアントの例を以下に示します。

レイヤ 2 NAT の有効化前：

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

レイヤ 2 NAT の有効化後：

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

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

レイヤ 2 NAT パケット変換統計の例

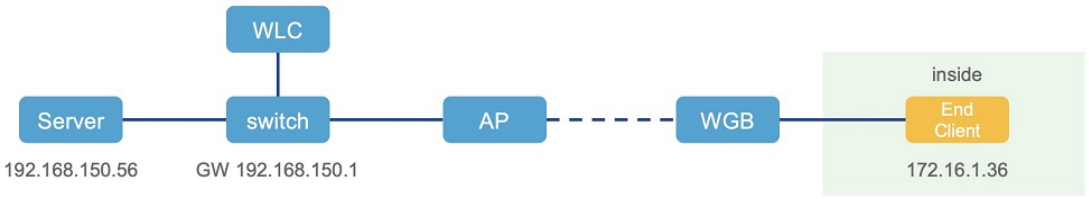
レイヤ 2 NAT パケット変換統計の例を以下に示します。

```
Device# show l2nat stats

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

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

ネットワークアドレス変換の設定例

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



このシナリオで使用するコマンドは次のとおりです。

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

イーサネットポートのネイティブ VLAN

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

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

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

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

低遅延プロファイル

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

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

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

WGB の [Optimized-Video] EDCA プロファイルの設定

ビデオのユースケースに最適化された低遅延プロファイルを設定するには、次のコマンドを使用します。

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-video** {**enable** | **disable**}

設定を確認するには、次のコマンドを使用します。

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-video
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 4 10 11 0 0
AC_BK L 6 10 11 0 0
AC_VI L 3 4 2 94 0
AC_VO L 2 3 1 47 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

WGB の [Optimized-Automation] EDCA プロファイルの設定

自動化のユースケースに最適化された低遅延プロファイルを設定するには、次のコマンドを使用します。

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-automation** {**enable** | **disable**}

設定を確認するには、次のコマンドを使用します。

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-automation
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 7 10 12 0 0
AC_BK L 8 10 12 0 0
AC_VI L 7 7 3 0 0
AC_VO L 3 3 1 0 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
```

```
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

WGB の [customized-wmm] EDCA プロファイルの設定

カスタマイズされた Wi-Fi マルチメディア（WMM）プロファイルを設定するには、次のコマンドを使用します。

#**configure dot11Radio** <*radio_slot_id*> **profile customized-wmm** {**enable** | **disable**}

カスタマイズされたWMMプロファイルパラメータを設定するには、次のコマンドを使用します。

#**configure dot11Radio** {**0**|**1**|**2**} **wmm** {**be** | **vi** | **vo** | **bk**} {**cwmin** <*cwmin_num*> | **cwmax** <*cwmax_num*> | **aifs** <*aifs_num*> | **txoplimit** <*txoplimit_num*>}

パラメータの説明：

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

WGB での低遅延プロファイルの設定

WGB で低遅延プロファイルを設定するには、次のコマンドを使用します。

AP# **configure dot11Radio** <*radio_slot_id*> **profile low-latency** [**ampdu** <*length*>] [**sifs-burst** {**enable** | **disable**}] [**rts-cts** {**enable** | **disable**}] [**non-aggr** <*length*>] [**aggr** <*length*>]

iot-low-latency プロファイルの EDCA の詳細なパラメータを表示するには、次のコマンドを使用します。

```
#show controllers dot11Radio 1 | beg EDCA
EDCA config
L: Local C:Cell A:Adaptive EDCA params
  AC   Type  CwMin  CwMax Aifs Txop ACM
AC_BE     L      4      6   11    0   0
AC_BK     L      6     10   11    0   0
AC_VI     L      3      4    1    0   0
AC_VO     L      0      2    0    0   1
AC_BE     C      4     10   11    0   0
AC_BK     C      6     10   11    0   0
AC_VI     C      3      4    2   94   0
AC_VO     C      2      3    1   47   1
```

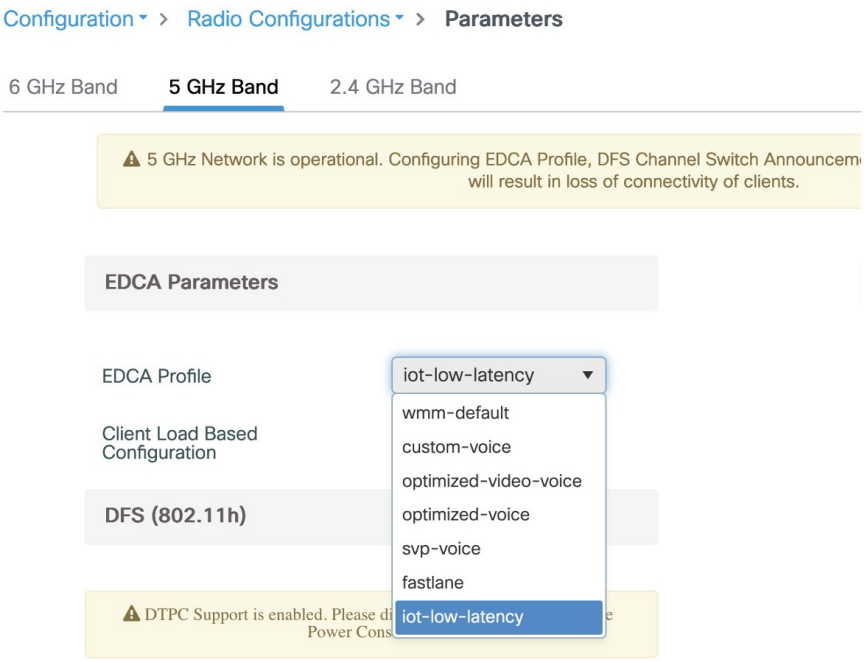
コントローラ GUI を使用した EDCA パラメータの設定

手順

ステップ 1 [Configuration] > [Radio Configuration] > [Parameters] を選択します。このページを使用して、6 GHz、5 GHz、および 2.4 GHz 無線機のグローバルパラメータを設定できます。

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

ステップ 2 [EDCA Parameters] セクションで、[EDCA Profile] ドロップダウン リストから EDCA プロファイルを選択します。Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality-of-Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。



ステップ 3 [Apply] をクリックします。

EDCA パラメータの設定（ワイヤレスコントローラ CLI）

手順

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
Device# configure terminal
```

ステップ 2 無線ネットワークを無効にします。

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

例：

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

ステップ 3 5 GHz、2.4 GHz、または 6 GHz ネットワークの iot-low-latency EDCA プロファイルを有効にします。

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency**

例：

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

ステップ 4 無線ネットワークを有効にします。

no ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

例：

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

ステップ 5 特権 EXEC モードに戻ります。

end

例：

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

ステップ 6 現在の設定を表示します。

show ap dot11 {**5ghz** | **24ghz** | **6ghz**} **network**

例：

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

A-MPDU の設定

集約は、パケット データ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。

A-MPDUパラメータは、集約パケットのサイズを定義し、集約パケット間の適切な間隔を定義して、受信側 WLAN ステーションがパケットを適切に復号化できるようにします。

2.4G、5G、および 6G 無線機でプロファイルベースの A-MPDU を設定するには、次のコマンドを使用します。

WLC(config)# **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** <*profile-name*>

WLC(config-rf-profile)# [**no**] **dot11n a-mpdu tx block-ack window-size** <*1-255*>

グローバル設定は、次のコマンドを使用して設定できる特殊なプロファイルです。

WLC(config)#[**no**] **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** <*1-255*>

異なる RF プロファイルを無線 RF タグにバインドするには、次のコマンドを使用します。

WLC(config)# **wireless tag rf** <*rf-tag-name*>

WLC (config-wireless-rf-tag)# **5ghz-rf-policy** <*rf-profile-name*>

（注） RF プロファイルレベルで設定された **a-mpdu tx block-ack window-size** 値は、グローバルに設定された値に優先します。

A-MPDU の長さの設定値を表示するには、次のコマンドを使用します。

show controllers dot11Radio <*radio_slot_id*>

```
AP# show controllers dot11Radio 1
Radio Aggregation Config:
=========================

TX A-MPDU Priority: 0x3f
TX A-MSDU Priority: 0x3f
TX A-MPDU Window:   0x7f
```

WGB/uWGB 無線パラメータの設定

WGB 無線アンテナの設定

WGB 無線アンテナの利得を設定するには、次のコマンドを使用します。デフォルトのアンテナ利得は 4 dBi です。

configure dot11 <**0|1|2**> **antenna gain** <*1-30*>

WGB 無線アンテナを設定するには、次のコマンドを使用します。デフォルトは abcd-antenna です。

```
configure dot11 <0|1|2> antenna <a-antenna|ab-antenna|abcd-antenna>
```

802.11ax 1600ns および 3200ns のガード間隔

802.11ax は、複数のガード間隔（GI）値（800ns、1600ns、および3200ns）をサポートします。デフォルトでは、GI は 800ns に設定されています。とはいえ別の値に設定することもできます。

長い GI は、一般的に屋外展開で使用されます。

```
#configure dot11radio <0|1|2> guard-interval
  1600  Configure 1600 ns guard interval (only in HE mode)
  3200  Configure 3200 ns guard interval (only in HE mode)
  800   Configure 800 ns guard interval
```

カスタマイズされた送信電力

デフォルトでは、無線機の送信電力は AUTO(0) レベルに設定されています。

無線機の送信電力を手動で設定するには、次のコマンドを使用します。

```
# configure Dot11Radio <0|1|2> txpower-level <0-8>
```

-ROW PID を使用して WGB/uWGB に国コードを割り当てる

最初に、-ROW 規制ドメインを使用して、適切な国コードを WGB/uWGB に割り当てる必要があります。WGB は、再起動後に対応する送信電力表を読み込みます。

国コードを割り当てるには、次のコマンドを使用します。

```
#configure countrycode
  Supported ROW country codes:
  GB VN

  WORD  Select one of above ROW country codes.
```

（注） ROW の国コードが設定された後、設定を別の国に変更する場合は、まず工場出荷時の設定にリセットしてから、新しい国コードを設定する必要があります。

-E ドメインと英国での屋内展開

IW9167EH は、-E ドメインと、- ROW ドメイン内の GB の屋内展開をサポートしています。

屋外展開の場合、IW9167EH 5G 無線機はチャンネル 100、104、108、112、116、120、124、128、132、136、140 をサポートします。屋内展開が有効になっている場合、5G 無線機はチャ

ンネル 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140 をサポートします。

屋内モードを設定するには、**configure wireless indoor-deployment enable** コマンドを使用します。

屋内モードを無効にするには、**configure wireless indoor-deployment disable** コマンドを使用します。

```
#configure wireless indoor-deployment
  disable  Disable indoor deployment
  enable   Enable indoor deployment
```

屋内モードまたは屋外モードを確認するには、**show controllers Dot11Radio [1|2]** コマンドを使用します。次の例に示すように、コマンド出力では、「-Ei」は屋内モードが有効であることを意味し、「-E」は屋内モードが無効であることを意味します。CLI 出力には、サポートされるチャンネルも表示されます。

```
#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-Ei)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140

#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-E)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
100 104 108 112 116 120 124 128 132 136 140
```

WGB ローミングパラメータの設定

再接続を開始するしきい値の継続時間と信号強度を設定するには、以下のコマンドを使用します。デフォルト値は、期間が 20 秒、しきい値が -70db です。

```
# configure wgb mobile period <time> <rssi-threshold>
```

再接続を開始するビーコン欠落数を設定するには、次のコマンドを使用します。デフォルト値は 10 です。

```
# config wgb beacon miss-count <count>
```

再接続を開始する最大パケット再試行回数を設定するには、次のコマンドを使用します。デフォルト値は 64 です。

```
# configure wgb packet retries <retry-count>
```

静的ローミングチャンネルを設定するには、次のコマンドを使用します。

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> add
```

モバイルチャンネルを削除するには、次のコマンドを使用します。

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> delete
```

すべてのチャネルを走査するには、次のコマンドを使用します。

```
# configure wgb mobile station interface Dot11Radio 1 scan all
```

WGB 設定のインポートとエクスポート

既存の WGB の稼働中の設定をサーバーにアップロードしてから、新たに展開した WGB にダウンロードします。

設定をサーバーにアップロードするには、次のコマンドを使用します。

```
#copy configuration upload <sftp:|tftp://> ip-address [directory] [file-name]
```

展開内のすべての WGB にサンプル設定をダウンロードするには、次のコマンドを使用します。

```
#copy configuration download <sftp:|tftp://> ip-address [directory] [file-name]
```

copy configuration download コマンドを実行すると、実行後にアクセスポイントが再起動します。インポートされた設定は、再起動後に有効になります。

WGB および uWGB の設定の確認

show run コマンドを使用して、AP が WGB モードか uWGB モードかを確認します。

- WGB：

```
#show run
AP Name              : APFC58.9A15.C808
AP Mode              : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring  : Enabled
SSH State            : Disabled
AP Username          : admin
Session Timeout      : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
---------------------------
1           WGB           myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
```

```
   Mode              : WGB
   Dot11 type        : 11ax
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
```

- uWGB：

```
#show run
AP Name               : APFC58.9A15.C808
AP Mode               : WorkGroupBridge
CDP State             : Enabled
Watchdog monitoring   : Enabled
SSH State             : Disabled
AP Username           : admin
Session Timeout       : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
---------------------------
1           UWGB          myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
   Mode              : UWGB
   Uclient mac       : 0009.0001.0001
   Current state     : WGB
   UClient timeout   : 0 Sec
   Dot11 type        : 11ax
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
```

show wgb dot11 associations コマンドを使用して、WGB および uWGB の設定を確認します。

- WGB：

```
#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:99:9A:15:B4:91
SSID Name : roam-m44-open
Parent AP Name : APFC58.9A15.C964
Parent AP MAC : 00:99:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Dot11 type : 11ax
Channel : 100
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 86/86 Mbps
Max Datarate : 143 Mbps
RSSI : 53
IP : 192.168.1.101/24
```

```
Default Gateway : 192.168.1.1
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```

- uWGB：

```
#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:09:00:01:00:01
SSID Name : roam-m44-open
Parent AP MAC : FC:58:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Uclient mac : 00:09:00:01:00:01
Current state : UWGB
Uclient timeout : 60 Sec
Dot11 type : 11ax
Channel : 36
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 77/0 Mbps
Max Datarate : 143 Mbps
RSSI : 60
IP : 0.0.0.0
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```

SNMP 機能

WGB 上の Simple Network Management Protocol（SNMP）は、

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

WGB の SNMP フレームワークには、以下が含まれます。

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

SNMP プロセス

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

図 *4 : SNMP* プロセス

SNMP バージョン

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

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

サポートされる SNMP MIB ファイル

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

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

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

SNMP パラメータの設定

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

- SNMP 機能を有効にする前に、CLI コマンド **configure snmp enabled** を使用して、すべての SNMP パラメータを設定します。

• SNMP 機能を無効にすると、すべての SNMP 設定が自動的に削除されます。

手順

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

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

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

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

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

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

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

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

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

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

length の有効な範囲は 8 ～ 64 文字です。

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

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

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

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

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

length の有効な範囲は 8 ～ 64 文字です。

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

```
Device#configure snmp enabled
```

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

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

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

```
Device# configure snmp disabled
```

SNMP の確認

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

SNMP version v3

```
Device# show snmp

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

SNMP version v2c

```
Device# show snmp

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

QoS ACL 分類およびマーキング

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

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

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

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

ルールベースのトラフィック分類

ルールベースのトラフィック分類は、次のようなネットワーク管理技術です。

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

ルール設定の基準

次のパラメータを使用して、マッピングルールを設定できます。

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

パケットの分類と割り当て

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

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

ルールベースのマッピングの利点

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

- QoS ポリシーの効果的な適用
- 重要なアプリケーションとサービスの優先順位付け
- 時間的制約のあるトラフィックの遅延を低減

- ネットワーク性能とユーザーエクスペリエンスの向上

QoS および ACL トラフィック分類方式

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

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

レイヤ 2 分類フィールド

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

レイヤ 3 分類フィールド

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

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

レイヤ 4 分類フィールド

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

サービスクラスへのトラフィックの割り当て

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

分類におけるデータ プレーンの役割

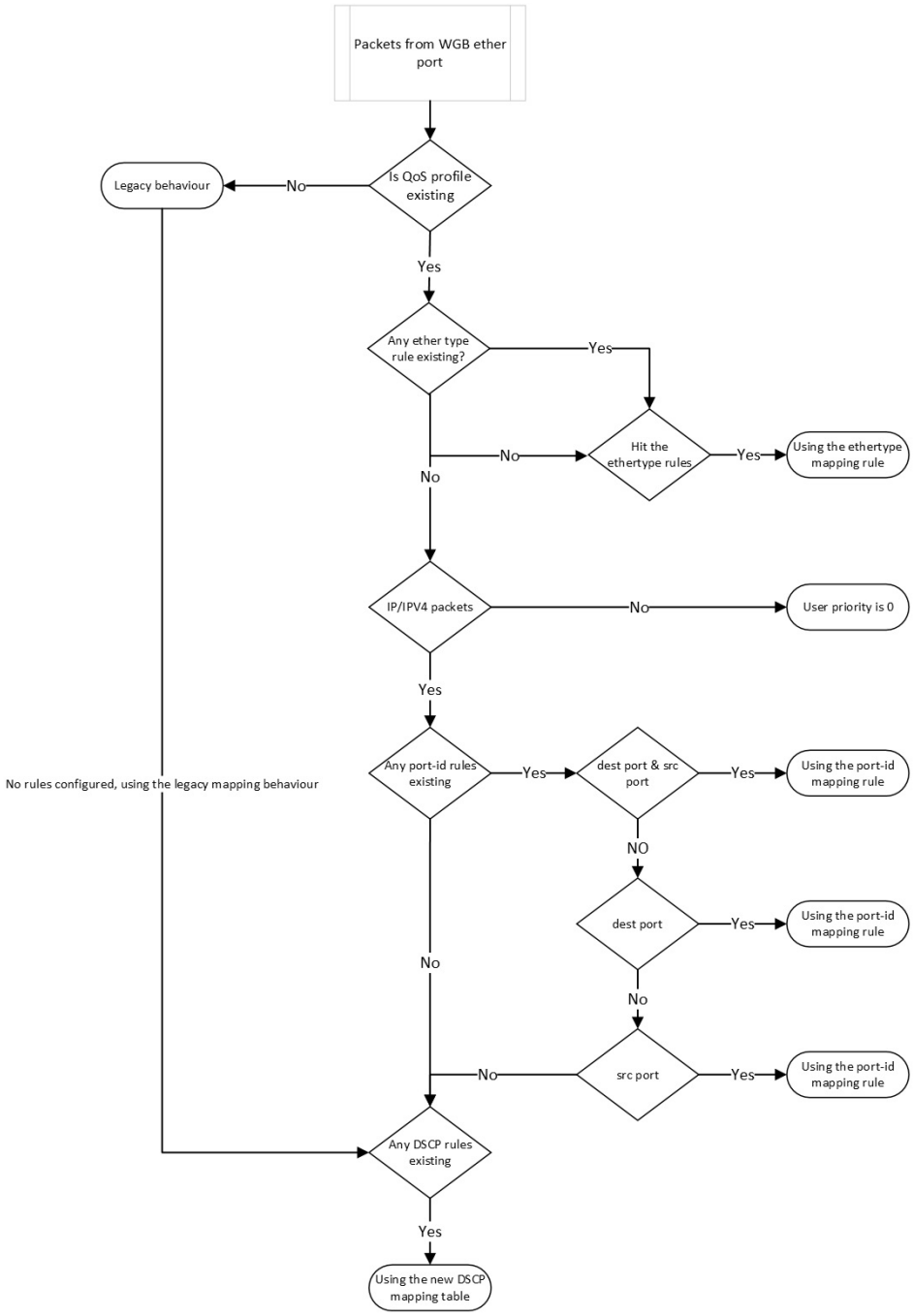
データプレーン統計には、トラフィックが各ルールと一致した回数を示すカウンタが表示されます。これらのカウンタは、管理者がルールの有効性を分析し、性能を最適化するのに役立ちます。

分類におけるコントロールプレーンの役割

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

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

図 *5 : WGB* イーサネットポートからのトラフィックフローのフローチャート



QoS マッピングプロファイルの設定

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Quality of Service マップの確認

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

```
Device# show wgb qos-mapping

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

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

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

```
Device# show datapath qos-mapping rule

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

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

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

```
Device# show datapath qos-mapping statistics

======= pkt stats per dscp-mapping rule =======
dscp up pkt_cnt
16 7 0
```

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

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

パケットキャプチャ：WGB での TCP ダンプ

パケットキャプチャ：TCP ダンプユーティリティ

TCP ダンプユーティリティは、ネットワーク パケット アナライザで、

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

「WGB での TCP ダンプ」の章では、Catalyst IW9167EH の WGB 有線インターフェイスを介して TCP ダンプを有効にする方法について説明します。

TCP ダンプユーティリティの目的

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

TCP ダンプユーティリティは

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

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

パケットキャプチャモード

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

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

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

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

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

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

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

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

プロトコル パケット キャプチャ機能

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

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

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

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

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

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

パケットキャプチャのフィルタ式

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

修飾子は 3 種類あります。

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

  例：port 20

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

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

- Proto：特定のプロトコルに限定してキャプチャします。

  例： tcp port 21

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

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

WGB の有線パケットキャプチャの有効化

手順

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

1. デフォルトフィルタを使用した PCAP：

   Device#**debug traffic wired** [*0* | *1*] {**ip** | **tcp** | **udp**} [**verbose** | **capture**]

   [0 ～ 1]：有線インターフェイス番号を指定します。選択されていない場合は、すべての有線インターフェイスからパケットをキャプチャします。

   次の表に、Default、Verbose、および Capture モードの PCAP の例を示します。

モード	例
Default：IP プロトコルヘッダーパケットをキャプチャします。	Device#**debug traffic wired 1 ip** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:35:50.529851 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 13721, seq 1, length 64 2 08:35:50.534813 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 13721, seq 1, length 64

モード	例
Verbose：UDP プロトコルパケットの詳細情報をキャプチャします。	Device#**debug traffic wired 1 udp verbose** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:25:59.696990 IP6 fe80::322c:712c:5787:f246.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit 0x0000: 3333 0001 0002 fc58 9a16 e428 86dd 6001 0x0010: 7b92 006d 1101 fe80 0000 0000 0000 322c 0x0020: 712c 5787 f246 ff02 0000 0000 0000 0000 0x0030: 0000 0001 0002 0222 0223 006d 00a6 010c 0x0040: d064 0008 0002 ffff 0006 001e 0034 0011 0x0050: 0015 0016 0017 0018 001f 0038 0040 0043 0x0060: 0052 0053 005e 005f 0060 0001 000a 0003 0x0070: 0001 fc58 9a16 e428 0014 0000 0027 0013 0x0080: 0006 4150 4643 3538 0439 4131 3604 4534 0x0090: 3238 0000 0300 0c00 0000 0100 0000 0000 0x00a0: 0000 00
Capture：TCP パケット情報を PCAP ファイルに書き込みます。	Device#**debug traffic wired 1 tcp capture** % Writing packets to "/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)

2. カスタムフィルタを使用した PCAP：

（注）
有効にする PCAP プロセスは一度に 1 つとしてください。フィルタ式では、" ` $ ^ & | \ > < ? ; ~ などのサポートされていない文字を使用しないでください。

Device#**debug traffic wired** [*0*|*1*] **filter** *expression* [**verbose**|**capture**]

次の表に、Default、Verbose、および Capture モードの PCAP の例を示します。

モード	例
Default：IP プロトコルヘッダーパケットをキャプチャします。	Device#**debug traffic wired 0 filter icmp** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 10:38:59.948729 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 16204, seq 1, length 64 2 10:38:59.954308 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 16204, seq 1, length 64

モード	例
Verbose：UDP プロトコルパケットの詳細情報をキャプチャします。	Device#**debug traffic wired 1 filter icmp verbose** APXXXX.XXXX.XXXX##reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 17:13:30.706493 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 986, seq 1, length 64 0x0000: fc58 9a17 afd4 f8e4 3b9d 7322 0800 4500 0x0010: 0054 57a0 4000 4001 889e c0a8 6cc8 c0a8 0x0020: 6c51 0800 940c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637 17:13:30.710567 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 986, seq 1, length 64 0x0000: f8e4 3b9d 7322 fc58 9a17 afd4 0800 4500 0x0010: 0054 9102 0000 4001 8f3c c0a8 6c51 c0a8 0x0020: 6cc8 0000 9c0c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637
Capture：TCP パケット情報を PCAP ファイルに書き込みます。	Device#**ddebug traffic wired 1 filter icmp capture** % Writing packets to "/tmp/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)

フィルタ式の詳細については、TCP ダンプの PCAP フィルタに関するドキュメントを参照してください。

3. カスタムフィルタを使用した複数 VLAN の PCAP：

（注）
一部のカスタムフィルタでは、非ネイティブ VLAN のトラフィックをキャプチャできません。たとえば、カスタムフィルタコマンド **#debug traffic wired 0 filter icmp** では、非ネイティブ VLAN のダウンリンク ICMP トラフィックをキャプチャできません。

非ネイティブ VLAN でダウンリンクトラフィックをキャプチャするには、次の 2 つのオプションがあります。

- フィルタ式に VLAN を加えることで、非ネイティブ VLAN の有線クライアントの双方向トラフィックをキャプチャする。

```
Device#debug traffic wired 0 filter "icmp or (vlan and icmp)"
1  12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64
2  12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1, length 64
```

- デフォルト IP フィルタを使用して、ネイティブ VLAN と非ネイティブ VLAN を含むすべての IP トラフィックをキャプチャする。

```
Device#debug traffic wired 0 ip
1  12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64
```

```
2  12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1,
length 64
```

有線 PCAP を無効にするには、「WGB の有線パケットキャプチャの無効化」を参照してください。

ステップ 2 パケットを外部サーバーにアップロードするには、次のコマンドを使用します。

（注）
パケットをアップロードする前に、PCAP プロセスを完了し、パケットをファイルに保存します。

TFTP、SFTP、または SCP サーバーを使用して、PCAP ファイルを外部サーバーにアップロードします。

Device#**copy pcap APxxxx.xxxx.xxxx_capture.pcap0 <tftp|sftp>://A.B.C.D[/dir][/filename]**

copy pcap APxxxx.xxxx.xxxx_capture.pcap0 scp://username@A.B.C.D[:port]:/dir[/filename]

例：

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

有線パケットキャプチャの無効化

手順

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

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

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

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

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

有線パケットキャプチャの確認

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

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

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

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

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

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

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

 1  09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920,
 seq 1, length 64
 2  09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920,
seq 1, length 64
```

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

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

AAA ユーザー認証のサポート

AAA ユーザー認証

AAA ユーザー認証は、以下を実行するネットワーク管理メカニズムです。

- ユーザー認証を介してネットワークリソースへのアクセスを制御し、

- 差別化された権限レベルをユーザーに割り当て、
- ユーザー名とパスワードを AAA サーバーで一元的に管理します。

リリース 17.15.1 以降、IW9167EH WGB では AAA ベースのユーザー管理および認証がサポートされます。

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

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

AAA ベースのユーザー管理および認証の機能

AAA ベースのユーザー管理および認証には、以下の機能が含まれます。

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

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

AAA サーバーの設定

始める前に

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

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

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

手順

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

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

ログインユーザーの RADIUS 認証の有効化または無効化

手順

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

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

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

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
.
```

ログインユーザーの TACACS+ 認証の有効化または無効化

手順

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

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

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

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

AAA 認証の設定例

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

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
.
```

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

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

ポートアドレス変換

ポートアドレス変換

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

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

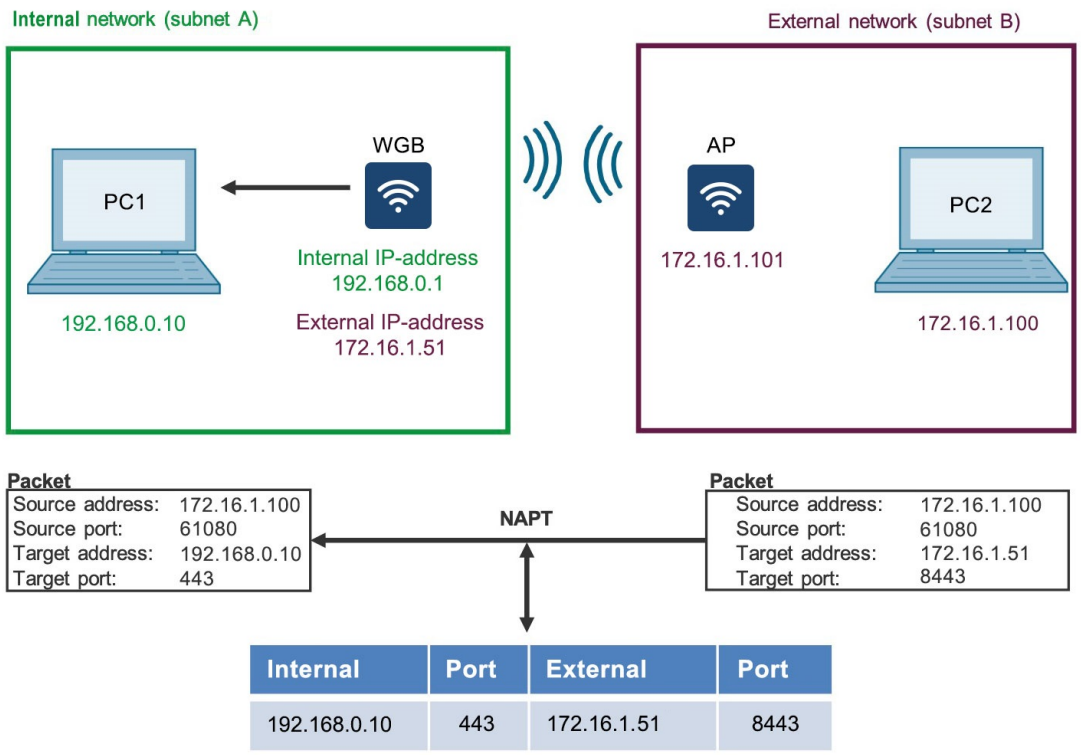
プライベート IP アドレスは、内部ネットワーク内のみで使用されます。パブリック IP アドレスは、グローバルに一意であり、インターネット上で使用されます。NAPT マッピングでは、IP アドレスとポート番号の両方が使用されます。両方を使用することにより、複数の内部ホストからのパケットを、異なるポート番号を使用して同じ外部 IP アドレスにマッピングできます。その結果、内部ローカルサブネット内のクライアントデバイスは、複数の無人搬送車（AGV）で同じ IP アドレスを再利用できるようになります。

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

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

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

図 *6*: 内部ネットワークと外部ネットワーク間の *NAPT* 変換



サポートされているプロトコル

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

WGB の制限事項

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

uWGB の制限事項

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

NAPT ルールとマッピングテーブル

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

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

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

NAPT マッピングテーブル

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

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

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

次の表に NAPT マッピングの例を示します。

表 *4 : NAPT* マッピングテーブル

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

上りと下りのデータ流

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

- ネットワークアドレスおよびポート変換（NAPT）を使用して送信元アドレスまたは宛先アドレスを変換し、
- 内部ネットワークと外部ネットワークの間でデータを安全に転送できるようにし、
- IP アドレスのプライバシーと完全性を維持します。

NAPT を使用した下りのデータ流

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

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

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

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

図 *7: WGB* での *NAPT* を使用した上りと下りのデータ流

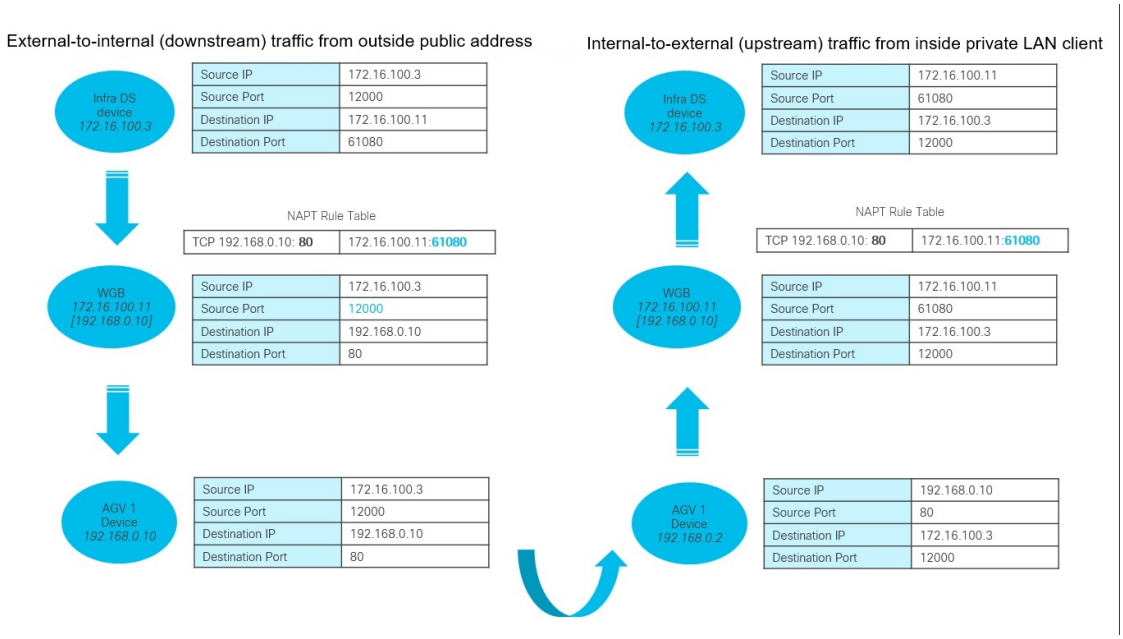
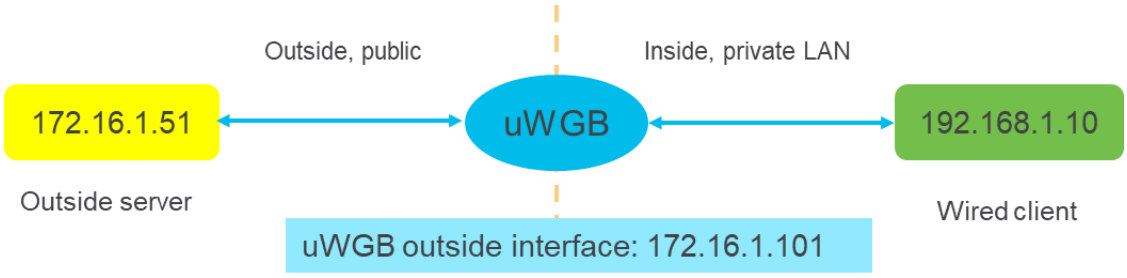


図 *8 : uWGB* での *NAPT* を使用した上りと下りのデータ流



SNAT を使用した上りのデータ流

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

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

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

WGB での NAPT 変換

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

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

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

外側のポート番号は、設定された NAPT 範囲内である必要があります。

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

```
Device# show ip nat configuration

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

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

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

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

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

NAPT マッピングルールの削除

この手順では、NAPT 設定エントリを削除する方法について説明します。inside と outside パラメータを指定することで特定の NAPT マッピングルールを削除できます。ルール ID でルールを削除したり、設定からすべての NAPT ルールを消去したりできます。特定のルールを削除するか、あるいは NAPT 設定全体をリセットするかに基づいて、方法を選択します。

手順

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

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

NAPT IP アドレスの削除

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

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

手順

次のいずれかのオプションを使用して、NAPT IP アドレスを削除します。

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

WGB での NAPT の確認

NAPT 設定の確認

WGB の現在の NAPT 設定を出力するには、**show ip nat configuration** コマンドを使用します。

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

NAPT エントリの確認

NAPT ルールテーブルから現在の NAPT 変換エントリを出力するには、**show ip nat translations** コマンドを使用します。

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

```
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port    direction
    expiry_time
(192.168.0.10, 80, 172.16.100.3, 443) => (172.16.100.11, 30000, 172.16.100.3, 443)
[forward] exp: 138
(172.16.100.3, 443, 172.16.100.11, 30000) => (172.16.100.3, 443, 192.168.0.10, 80)
[reverse] exp: 138
```

出力中の forward は WGB によって処理されたデータパケットのログ詳細を参照します。これには送信元、接続先、実行された変換などの詳細情報が含まれます。

reverse は、WGB によって転送された元のパケットに基づく戻りトラフィックのログの詳細を参照します。この操作により、元のトラフィックの方向を逆にして、接続先からの応答が送信元に正常に到達するようになります。

uWGB でのポートアドレス変換

ポートアドレス変換

UIW リリース 17.16.1 以降、ポートアドレス変換（PAT）は、各無人搬送車（AGV）の IW9167EH uWGB でサポートされています。

PAT は、ネットワークアドレスポート変換（NAPT）とも呼ばれ、パケットを外部ネットワークに送信する前に、複数の内部有線クライアントのプライベート IP アドレスとポート番号を一意のパブリック IP アドレスとポート番号に変換します。

プライベートまたは内部 IP アドレスは内部ネットワークでのみ使用されますが、パブリックまたは外部 IP アドレスはインターネット上で使用され、グローバルに一意です。

NAPT マッピングは、IP アドレスとポート番号に基づいています。NAPT を使用すると、複数の内部ホストからのパケットが、異なるポート番号を使用して同じ外部 IP アドレスにマッピングされます。

内部ローカルサブネット内のクライアントデバイスは、複数の AGV 間で同じ IP アドレスを再利用できます。

前提条件

NAPT 展開では、内部ローカルサブネット内の AGV デバイスに事前設定された IP アドレスがあります。

サポートされているプロトコル

NAPT は、内部および外部ネットワークのデバイス間で通信するための TCP または UDP をサポートします。

NAPT の制限事項

NAPT に関する制限事項は次のとおりです。

- NAPT は、アクセス制御リスト（ACL）をサポートしません。

- NAPT は、1 つのプライベート LAN のみを NAPT の内側のネットワークとしてサポートします。

NAPT ルールとマッピングテーブル

NAPT ルール

uWGB は、設定された IP アドレスに基づいてデフォルトのマッピングルールを作成し、内部クライアントデバイスによって開始されたトラフィックフローを変換します。

外部ホストからの着信トラフィックの変換を管理する NAPT マッピングルールを設定します。

デフォルトのマッピングルールは次の要素で構成されます。`<inside-IP-address, inside-tcp-or-udp-port>`、`<outside-ip-address, predefined port range>`、`<protocol>`（プロトコルは UDP と TCP のいずれか）

NAPT マッピングテーブル

uWGB は、トラフィックルールと NAPT ルールに基づいてマッピングテーブルを作成し管理します。

NAPT は、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、IP プロトコル（TCP または UDP）などのフロー識別子を使用して、NAPT マッピングテーブルのインデックスを作成します。

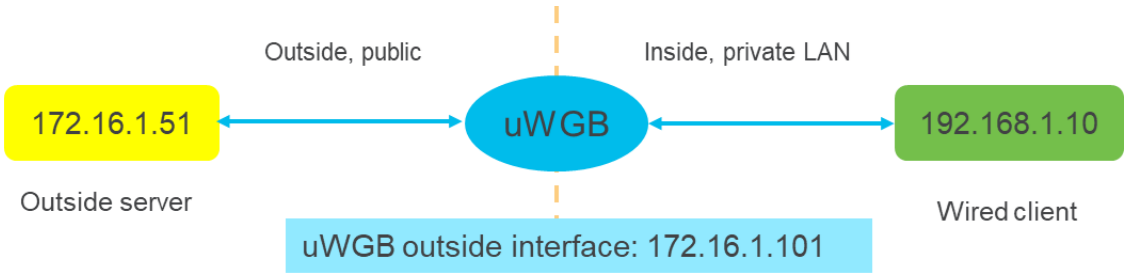
（注） NAPT 変換テーブル内のマッピングエントリの最大数は 4096 で、これらのエントリは自動的にペアで表示されます。

表 *5: NAPT* マッピングテーブル

プロトコル	内側ローカル IP アドレスおよびポート	uWGB グローバル IP アドレス	外側グローバル IP アドレスおよびポート
TCP	192.168.1.10: 80	172.16.1.101	172.16.1.101: 61080

上りと下りのデータ流

図 *9 : NAPT* を使用した上りと下りのデータ流



SNAT を使用した上りのデータ流

上りのデータ流とは、内部ネットワークから外部ネットワークへのパケットの流れを指します。uWGB は、内部ネットワークと外部ネットワーク間のゲートウェイとして機能します。uWGB は、送信元ネットワークアドレス変換（SNAT）を使用して、内部ネットワークから外部ネットワークへのすべての発信パケットを変換します。

SNAT は、uWGB を通過するパケットの送信元 IP アドレスを uWGB クライアント IP アドレスに置き換えて変換します。この変換により、内部 IP アドレスが外部ネットワークに公開されることがなくなります。

NAPT を使用した下りのデータ流

下りのデータ流とは、外部ネットワークから AGV の内部ネットワークへのデータの流れを指します。uWGB は、外部ネットワークと内部ネットワーク間のゲートウェイとして機能します。

uWGB は、外部 IP アドレスとポートでパケットを受信すると、マッピングテーブルをチェックして、着信パケットの宛先 IP アドレスと宛先 TCP または UDP ポートを照合します。

ルールが一致すると、uWGB はテーブル内の一致したエントリに従って宛先 IP アドレスとポート番号を変換し、パケットを内部ネットワークに転送します。

uWGB での NAPT 設定

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

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

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

外側のポート番号は、上りのデータ流用に自動的に生成されます。

この設定は、内部から外部へのトラフィックフローをサポートします。

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

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

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

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

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

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

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

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

外側のポート番号は、設定された NAPT 範囲内である必要があります。

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

```
Device# show ip nat configuration

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

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

```
Device#show ip nat translations

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

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

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

NAPT マッピングルールの削除

uWGB の NAPT マッピングルールを削除するには、次の手順に従います。

手順

必要に応じて、指定されたコマンドを使用して設定を削除します。

- **config ip nat rule delete inside ip** *inside- ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} コマンドを使用して、NAPT マッピングルールを削除します。

```
Device#config ip nat rule delete inside ip 192.168.1.10 port 80 outside port 61080 protocol tcp
```

- ルール ID に従って NAPT マッピングルールを削除するには、**configure ip nat entry delete** *rule-id* コマンドを使用します。

```
Device#configure ip nat entry del 0
```

（注）
ルール ID を表示するには、**show ip nat configuration** コマンドを使用します。

- uWGB のすべての NAPT マッピングルールを削除するには、**configure ip nat entry delete** *all* コマンドを使用します。

```
Device#configure ip nat entry delete all
```

NAPT IP アドレスの削除

uWGB の NAPT 機能 IP アドレスを削除するには、次の手順に従います。

（注） NAPT 設定を完全に削除するには、IP アドレスとインターフェイスを削除します。

手順

必要に応じて、下記のコマンドを使用して NAPT 機能の必要な IP アドレスを削除します。

- 内部 IPv4 アドレスを削除するには、**config ip nat address delete** コマンドを使用します。

```
Device#Device#config ip nat address delete
```

- 外部 IPv4 アドレスを削除するには、**configure interface nat-outside address delete** コマンドを使用します。

```
Device#configure interface nat-outside address delete
```

NAPT 展開での uWGB の管理

NAPT 展開で uWGB を管理するには、次の手順に従います。

始める前に

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

手順

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

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

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

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

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

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

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

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

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

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

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

```
Device#show wgb dot11 associations
Uplink Radio ID            : 1
```

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

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

uWGB での NAPT の確認

NAPT 設定の確認

uWGB の現在の NAPT 設定を出力するには、**show ip nat configuration** コマンドを使用します。

```
Device#show ip nat configuration

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

NAPT エントリの確認

NAPT ルールテーブルから現在の NAPT 変換エントリを出力するには、**show ip nat translations** コマンドを使用します。

```
Device#show ip nat translations
ICMP:
    src_ip    dst_ip    port     =>       src_ip    dst_ip    port      direction
expiry_time
(172.16.1.1, 172.16.1.101, 30257) => (172.16.1.1, 192.168.1.10, 267) [reverse] exp: 272
(192.168.1.10, 172.16.1.1, 11) => (172.16.1.101, 172.16.1.1, 30001) [forward] exp: 272
===================================
```

```
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.1.10, 20000, 172.16.1.51, 35200) => (172.16.1.101, 61001, 172.16.1.51, 35200)
[reverse] exp: 214
(192.168.1.10, 51184, 172.16.1.51, 22000) => (172.16.1.101, 30001, 172.16.1.51, 22000)
[forward] exp: 161
(172.16.1.51, 35200, 172.16.1.101, 61001) => (172.16.1.51, 35200, 192.168.1.10, 20000)
[forward] exp: 214
(172.16.1.51, 22000, 172.16.1.101, 30001) => (172.16.1.51, 22000, 192.168.1.10, 51184)
[reverse] exp: 161
====================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.1.10, 44155, 172.16.1.51, 23000) => (172.16.1.101, 30002, 172.16.1.51, 23000)
[forward] exp: 238
(172.16.1.51, 23000, 172.16.1.101, 30002) => (172.16.1.51, 23000, 192.168.1.10, 44155)
[reverse] exp: 238
====================================
```

出力中の forward は、uWGB が処理して転送する実際のトラフィックストリームからのエントリを意味します。uWGB を介して変換および送信されたパケットの詳細がログに記録されます。

reverse は、既存の forward の方向を逆にしたエントリを意味します。最初に転送されたトラフィックから予想される戻りパスまたは応答が記録されます。

Cisco IW9167EH WGB での速度 10 Mbps のポートのサポート

イーサネットポートでの 10 Mbps 速度ネゴシエーション

Cisco IOS XE リリース 17.16.1 以前の IW9167EH WGB は、イーサネットポートで 10 Mbps の速度をサポートしていません。とはいえ、一部のクライアントは引き続き 10 Mbps イーサネットポートを備えたデバイスを使用します。これらのデバイスとの互換性を実現するには、以下の手順に従います。

Cisco IOS XE リリース 17.16.1 以降、IW9167EH WGB は有線 0 ポートでの 10 Mbps 速度ネゴシエーションをサポートします。このドキュメントでは、WGB 有線 0 ポートで 10 Mbps 速度ネゴシエーションを有効または無効にする方法について説明します。

WGB 有線 0 ポートによって、有線デバイスが WGB に接続され、有線およびワイヤレス ネットワーク セグメントがブリッジされます。

速度ネゴシエーション

速度ネゴシエーション（自動ネゴシエーション）は、接続された 2 台のイーサネットデバイスが最適な共通伝送パラメータ（速度やデュプレックスモードなど）を自動的に選択して通信を最適化するプロセスです。

速度とデュプレックスは、ローカルに接続されたエンドポイントの機能に基づいて自動ネゴシエーションされます。

（注） 100 Mbps および 1 Gbps をサポートするデバイスを接続する場合は、10 Mbps 機能を無効にします。

利点

この機能により、10 Mbps イーサネットデバイスを他のデバイスに置き換えずに IW9167EH WGB AP に接続できます。

Cisco IW9167EH WGB での速度 10 Mbps のポートの有効化

イーサネットポートで 10 Mbps の速度を有効にするには、以下のタスクを使用します。**show** コマンドは必要に応じて実行することが可能で、特定のシーケンスに従う必要はありません。

手順

ステップ 1 **enable** コマンドを使用して、特権 EXEC モードを有効にします。

```
Device>enable
```

ステップ 2 **configure wired** *wired-port-number* **speed** *port-speed* **enable** コマンドを使用して、有線 0 ポートで速度 10 Mbps の機能を有効にします。

```
Device#configure wired 0 speed 10 enable
```

ステップ 3 （オプション）有線 0 ポートで速度 10 Mbps のポートのステータスを確認するには、**show running-config** コマンドを使用します。

```
Device#show running-config
feature 10M speed

Interface wired0 10Mbps Configuration:
====================================
Status: Enable
```

ステップ 4 **show ip interface brief** コマンドを使用して、有線 0 ポートの速度ネゴシエーションを確認します。

```
Device#show ip interface brief
Interface            IP-Address      Method   Status   Protocol   Speed      Duplex
*wired0              unassigned      unset    up       up         10         full
wired1               n/a             n/a      down     down       n/a        n/a
auxiliary-client     192.168.163.91  static   up       up         n/a        n/a
wifi0                n/a             n/a      down     down       n/a        n/a
wifi1                n/a             n/a      up       up         n/a        n/a
wifi2                n/a             n/a      up       up         n/a        n/a
```

Cisco IW9167EH WGB での速度 10 Mbps のポートの無効化

イーサネットポートで 10 Mbps の速度を無効にするには、このタスクを使用します。**show** コマンドは必要に応じて実行することが可能で、特定のシーケンスに従う必要はありません。

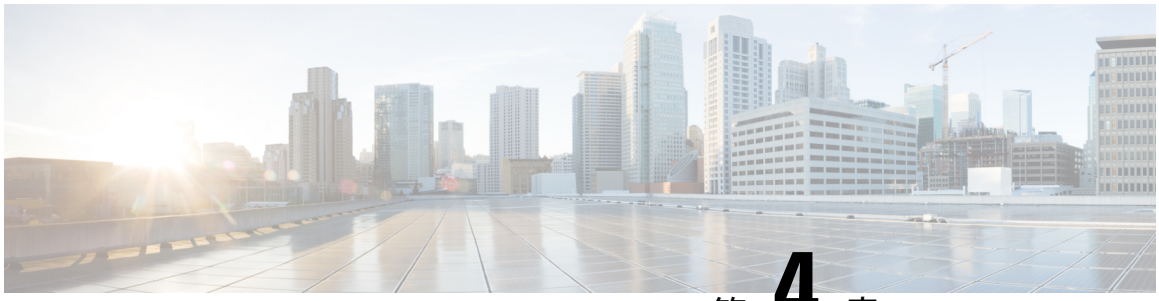
手順

ステップ 1 有線 0 ポートで速度 10 Mbps の機能を無効にするには、**configure wired** *wired-port-number* **speed** *port-speed* **disable** コマンドを使用します。

```
Device# configure wired 0 speed 10 disable
```

ステップ 2 （オプション）有線 0 ポートで速度 10 Mbps のポートのステータスを確認するには、**show running-config** コマンドを使用します。

```
Device#show running-config
feature 10M speed

Interface wired0 10Mbps Configuration:
=====================================
Status: Disable
```



第 4 章

自動周波数調整

6 GHz 標準出力モードの AFC サポート

Cisco Catalyst IW9167EH アクセスポイントには、指定された 3 つの SIA ポートに繋いだ Self-Identifiable Antenna（SIA）、デュアルバンドアンテナ、シングルバンドアンテナなど、複数のアンテナ選択肢をサポートする 8 つの N 型メスコネクタがあります。IW9167EH には、6 GHz バンドの SIA アンテナとの互換性があります。

IW9167EH は、自動周波数調整（AFC）6 GHz 標準出力モードをサポートします。標準出力 AP がシステムに接続されます。標準出力を有効にする前に、AP は AFC システムから使用可能な周波数と各周波数範囲の出力を取得する必要があります。

AFC システムは、規制機関（米国の場合は FCC、）から提供される情報に基づいて、使用可能な周波数と最大許容出力を計算します。応答がコントローラに返送され、AFC システムから返された許可チャンネルリストに基づいて標準出力チャンネルが AP に割り当てられます。

標準出力 AP は、AFC サービスを通じて調整を行います。AFC は情報にアクセスし、AP の地理位置情報とアンテナの特性に加え、AP の干渉半径をモデル化したトポグラフィック伝達マップを作成します。このマップを使用することで、最大送信電力を割り当て、チャンネル設定を調整または設定して干渉を回避できます。

（注） 初めて SIA アンテナを取り付けた後は、電源を一度切って入れ直す必要があります。

表 *6 :* 無線機の *6 GHz* 出力モードの対応

展開モード	屋内低出力への対応	標準出力への対応
屋外	非対応	はい

送信電力の実効等方放射電力（EIRP）は最大 36 dBm に制限されており、 AFC サービスを使用して AP を調整する必要があります。米国では、AP の運用は 5.925 GHz ～ 6.425 GHzの UNII-5 周波数帯域と、6.525 GHz ～ 6.875 GHzの UNII-7 周波数帯域で許可されています。

表 *7: 6 GHz* 目標出力

アンテナ利得	経路ごとの最大伝導出力（SP/AFC）		Tx x Rx チェーン	最大 EIRP（SP/AFC）
	20 ～ 80 MHz	160 MHz		
7 dBi	17 dBm	17 dBm	4 X 4	30 dBm

AP の AFC ステータスの確認

AP の AFC 要求および応答データを確認するには、**show rrm afc** コマンドを実行します。

```
Device#show rrm afc
Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor axis:
 9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

現在稼働中の出力モードを確認するには、**show controllers dot11Radio 2 | i Radio** コマンドを実行します。

```
Device#show controllers dot11Radio 2 | i Radio
Dot11Radio2     Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

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。