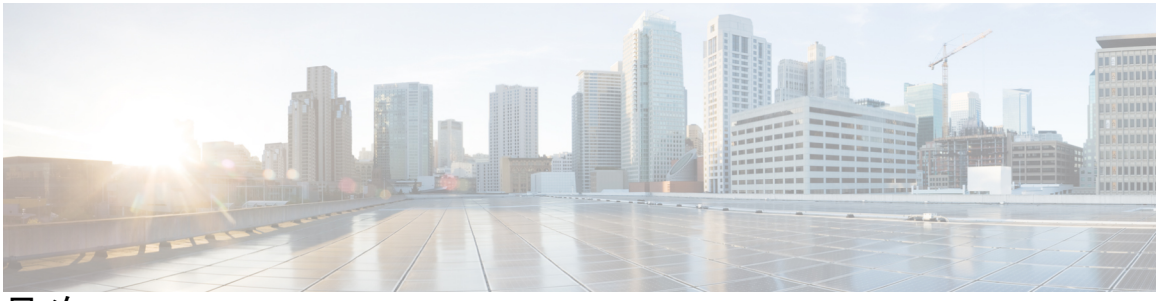
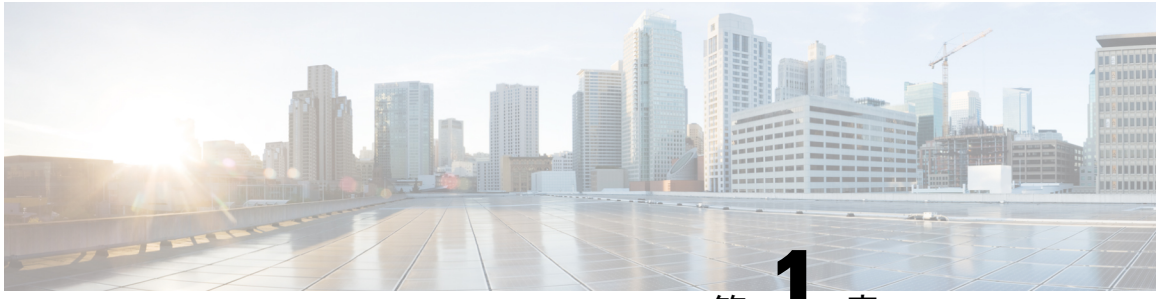
Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント設定ガイド、Cisco IOS XE 17.15.x

最終更新：2025 年 1 月 26 日

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



目 次



第 1 章

はじめに

アクセスポイントの概要

Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント（以下、*IW9165E*）は、外部アンテナを備えた 2x2 Wi-Fi 6E 設計をサポートし、移動中の車両やマシンに超高信頼ワイヤレス接続を付加する設計となっています。低消費電力、堅牢な IP30 設計、小型フォームファクタにより、Catalyst IW9165E は産業資産に非常に簡単に統合できます。

IW9165E は、移動する車両やマシンに超高信頼ワイヤレス接続を付加するように設計されています。IW9165E は、Cisco Unified Industrial Wireless (UIW) ソフトウェアリリース 17.12.1 以降、Cisco Ultra-Reliable Wireless Backhaul（Cisco URWB）として動作できます。これにより、シームレスなハンドオフが可能になり、高可用性、低遅延、ゼロパケット損失が実現します。

IW9165E は、Cisco Unified Industrial Wireless ソフトウェアリリース 17.13.1 以降、シスコのアクセス ポイント インフラストラクチャに接続できるワークグループブリッジ（WGB）モードと、サードパーティのアクセス ポイント インフラストラクチャに接続できるユニバーサル WGB（uWGB）モードの Wi-Fi クライアントとしても動作できます。どちらのモードも、WGB の背後にある有線クライアントをインフラストラクチャ側のアクセスポイントにブリッジするのに役立ちます。

Catalyst IW9167E は、Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、Lightweight AP（Control And Provisioning of Wireless Access Points（CAPWAP））モード、超高信頼ワイヤレスバックホール（URWB）モード、または WGB モードで動作できます。

IW9165E には、ハードウェアを変更することなく、CAPWAP、WGB、または URWB モードで IW9165E を動作させるためにソフトウェアを更新するだけで、イメージを切り替えるオプションがあります。

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。

- **ローカルモード**：これは AP のデフォルトモードです。このモードでは、AP はクライアントにサービスを提供します。ローカルモードでは、AP は、コントローラ接続用に 2 つの CAPWAP トンネルを作成します。1 つは管理用で、他方はデータトラフィック用です。これは中央スイッチングと呼ばれます。データトラフィックが AP からコントローラにスイッチング（ブリッジ）されるためです。
- **FlexConnect モード**：FlexConnect モードでは、データトラフィックはローカルにスイッチングされ、コントローラには送信されません。このモードでは、シスコの AP は自律 AP のように動作しますが、コントローラによって管理されます。このモードの場合、コントローラへの接続が失われても、AP は機能し続けます。
- **Fabric モード**：ファブリックモードの AP には、AP が接続されているファブリックエッジへの VxLAN トンネル（アクセストンネル）が構築されます。AP が拡張ノード（EN）またはポリシー拡張ノード（PEN）に接続されている場合。アクセストンネルは、アクセスポイント（AP）と、拡張ノードがアップリンクされている各ファブリックエッジとの間に構築されます。AP とファブリックエッジ間の VxLAN トンネルは、アクセスポイントまでセグメンテーションを維持するためのものです。アクセスポイントは、ファブリックエッジへの VxLAN トンネルに SGT タグを挿入します。
- **Sniffer モード**：ワイヤレススニファモードでは、AP は指定されたチャンネルで無線のスニッフィングを開始します。AP は、指定されたチャネル上のすべてのパケットを取得し、AiroPeek または Wireshark（IEEE 802.11 無線 LAN のパケットアナライザ）を実行するリモートマシンに転送します。これには、タイムスタンプ、信号強度、パケットサイズなどの情報が含まれます。

（注） スニファモードでは、データの送信先サーバーが、ワイヤレスコントローラ管理 VLAN と同じ VLAN 上にあることが必要です。それ以外の場合は、エラーメッセージが表示されます。

- **Monitor モード**：モニターモードでは、AP がクライアントとインフラストラクチャ間のデータトラフィックの処理から除外されます。AP は、ロケーションベースのサービス（LBS）、不正 AP 検出、および侵入検知システム（IDS）の専用センサーとして機能します。AP がモニターモードの場合、AP は電波をアクティブにモニタリングし、通常はクライアントにサービスを提供しません。
- **Site Survey モード**：AP GUI が有効になり、サイト調査の RF パラメータの設定に使用されます。詳細については、『*Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*』の「Access Points Survey Mode」のセクションを参照してください。

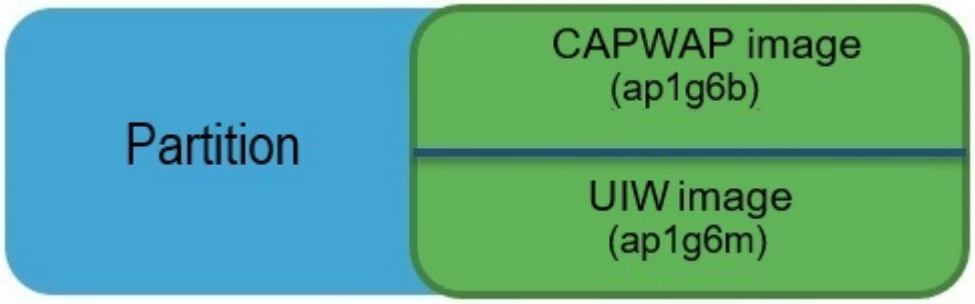
サポートされない機能

- 2.4G 無線機はサポートされません。
- 走査用無線機はサポートされません。

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

イメージの決定

ソフトウェアイメージは、IW9165E 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 : IW9165E* ソフトウェアイメージ

IW9165E のモード	ソフトウェア イメージ
CAPWAP	**ap1g6b-k9w8-xxx.tar**
URWB	Unified Industrial Wireless イメージ **ap1g6m-k9c1-xxx.tar**
WGB/uWGB	

IW9165E 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, (ap1g6b)** 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 **ap1g6b-k9w8-xxx.tar** を実行していることを意味します。

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

- 次の例に示すように、**show version** の出力に **Cisco AP Software (ap1g6m)** と表示された場合は、AP が URWB モードまたは WGB/uWGB をサポートする **ap1g6m-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, (ap1g6m), C9165, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Tue Feb 20 23:04:29 GMT 2024
```

Catalyst IW9165E Lightweight アクセスポイントは、CAPWAP、URWB、WGB など、単一のハードウェアプラットフォームで3つのワイヤレステクノロジーをサポートします。Catalyst IW9165E には、ハードウェアを変更することなく、CAPWAP、WGB、または URWB モードで Catalyst IW9165E を動作させるためにソフトウェアを更新するだけで、イメージを切り替えるオプションがあります。

イメージ変換の設定

IW9165E アクセスポイントを Wi-Fi モード（CAPWAP AP）または URWB モードまたは WGB モードに変換するには、次の手順を実行します。

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

   configure boot mode urwb

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

   configure boot mode capwap

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

   configure boot mode wgb

（注） イメージを変換すると、工場出荷時の状態への完全なリセットが実行され、設定とデータが完全に削除されます。

関連資料

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

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

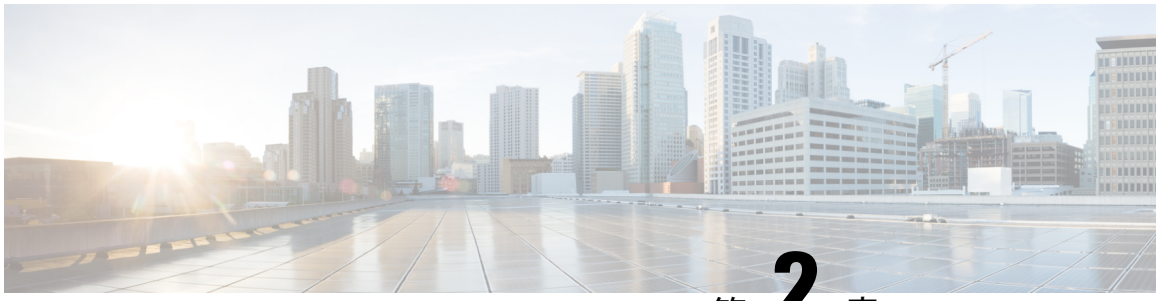
- IW9165E ハードウェアの詳細については、『Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント ハードウェア設置ガイド』を参照してください。
- AP の機能および仕様をすべて網羅したリストは、『Cisco Catalyst IW9165 シリーズ データシート』に記載されています。

- Cisco URWB モード設定の詳細については、関連するドキュメントを参照してください。

  https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html。

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

関連資料



第 2 章

ワークグループ ブリッジ

概要

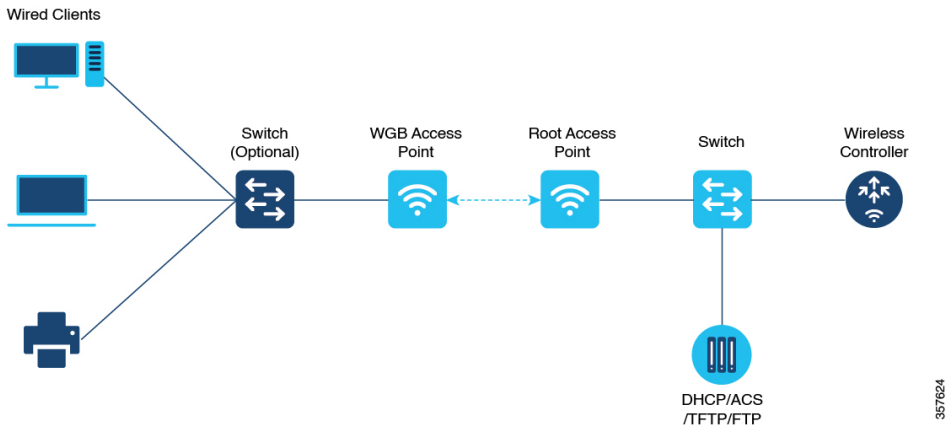
ワークグループ ブリッジ モード

ワークグループブリッジ（WGB）は、アクセスポイント（AP）のモードであり、有線クライアントへのワイヤレス接続を提供します。これらのクライアントは、WGB AP のイーサネットポートに接続されます。WGBは、有線ネットワークと単一のワイヤレスセグメント間のブリッジのように機能します。この機能を果たすため、WGB はイーサネット上の有線クライアントの MAC アドレスを学習します。WGB は、Internet Access Point Protocol（IAPP）メッセージングを使用し、インフラストラクチャ AP を介してこれらの識別子をワイヤレス LAN コントローラ（WLC）と共有します。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 ワークグループ ブリッジ モード

ユニバーサル ワークグループ ブリッジ（uWGB）モードは、WGB 機能を補完するモードです。uWGB モードは、uWGB に接続された有線クライアントとワイヤレス インフラストラクチャ間のワイヤレスブリッジとして機能します。このインフラストラクチャには、シスコとシスコ以外のワイヤレスネットワークが含まれます。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。無線機 MAC は、AP とのアソシエーションに使用されます。

図 *1 : WGB* の例



Cisco Unified Industrial Wireless ソフトウェアリリース 17.13.1 以降、WGB は Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアントでサポートされます。

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。uWGB は、サードパーティのアクセスポイントとのみアソシエートできます。
- 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。
- 有線およびワイヤレスのネットワークの切り替えでループを検出し、防止するため、VLAN ごとのスキャン ツリー（PVST）とパケットが使用されます。WGB は STP パケットを透過的にブリッジします。WGB は 2 つの有線セグメント間での STP パケットをブリッジできます。有線セグメント内の STP の設定が誤っていたり、整合性がない場合は、アクセスポイントまたは WGB に接続されたスイッチによって、WGB ワイヤレス リンクがブロックされる可能性があります。これにより、STP が有線ネットワーク内のスイッチ ポートをブロックし始めるため、WGB が AP から切断されるか、またはコントローラへの AP の接続解除がドロップされ、有線クライアントが IP アドレスを受信しなくなる場合があります。管理者が WGB で有線セグメント間の STP のブリッジを無効にする必要がある場合、ワイヤレス ネットワーク内の直接接続されているスイッチ上で STP を無効にすることを推奨します。
- 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、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 （12 ページ）を参照してください。
- Cisco Unified Industrial Wireless ソフトウェアリリース 17.13.1 以降、uWGB モードの AP は SSH による管理をサポートし、有線クライアントが検出されない場合はイメージのアップグレードを実装できます。
  - 有線クライアントが検出されると、uWGB モードの AP が uWGB 状態に変わり、AP を管理できなくなります。
  - 有線クライアントが検出されない場合、uWGB モードの AP は WGB 状態に変わり、AP を管理できます。

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 *slot_id* **disable**

例：

```
#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*

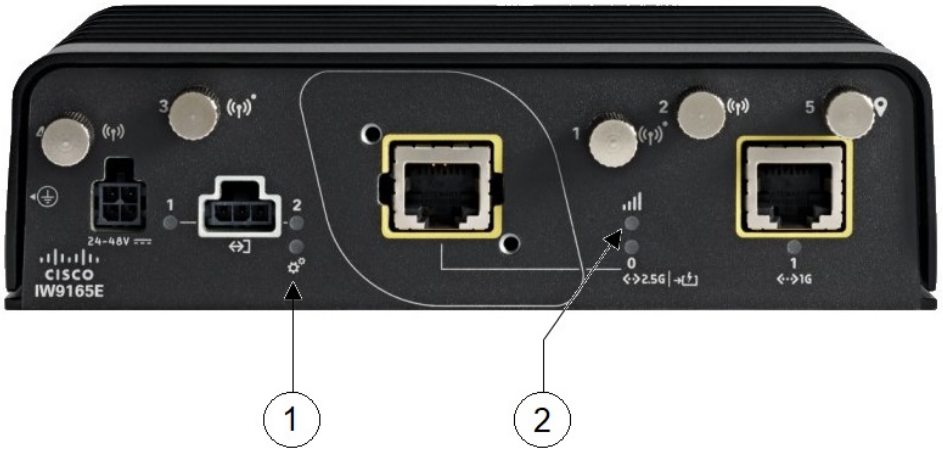
例：

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

LED パターン

次の図に示すように、AP の前面パネルには、システムステータス LED と RSSI LED の 2 つの LED があります。

図 *2 : IW9165E の LED*



1	システム ステータス LED • 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 とのアソシエーションが成立すると、システム LED は緑色に点灯します。	2	RSSI ステータス LED • RSSI が -71dBm 以上の場合、RSSI LED は緑色に点灯します。 • RSSI が -81 dBm 以上 -70 dBm 未満の場合、RSSI LED は緑色に点滅します。 • RSSI が -81 dBm より大きく -95 dBm 未満の場合、RSSI LED は黄色に点灯します。 • それ以外の場合は消灯します。

IP アドレスの設定

IPv4 アドレスの設定

次のコマンドを入力して、AP の IPv4 アドレスを設定します。

- DHCP によって IPv4 アドレスを設定するには、次のコマンドを使用します。

  #**configure ap address ipv4 dhcp**

- 静的 IPv4 アドレスを設定するには、次のコマンドを使用します。これにより、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デバイスを管理できます。

  #**configure ap address ipv4 static** *ipv4_addr netmask gateway*

- 現在の IP アドレス設定を表示するには、次のコマンドを使用します。

  #**show ip interface brief**

IPv6 アドレスの設定

次のコマンドを入力して、AP の IPv6 アドレスを設定します。

- 静的 IPv6 アドレスを設定するには、次のコマンドを使用します。これにより、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デバイスを管理できます。

  #**configure ap address ipv6 static** *ipv6_addr prefixlen* [*gateway*]

- #**configure ap address ipv6 auto-config** {**enable**|**disable**}

（注） **configure ap address ipv6 auto-config enable** コマンドは、IPv6 SLAAC を有効にするように設計されています。ただし、SLAAC は cos WGB には適用されません。この CLI 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 によって IPv6 アドレスを設定するには、次のコマンドを使用します。

  #configure ap address ipv6 dhcp

- 現在の IP アドレス設定を表示するには、次のコマンドを使用します。

  #show ipv6 interface brief

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）

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 1 mode wgb ssid-profile demo-FAST
configure dot11radio 1 enable
```

以下の項で、WGB の設定について詳しく説明します。

SSID の設定

SSID の設定は、次の 2 つの部分で構成されます。

SSID プロファイルの作成

SSID プロファイルの認証プロトコルとして、次のいずれかを選択します。

オープン認証による 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、次のコマンドを使用します。

configure ssid-profile *ssid-profile-name* **ssid** *radio-serv-name* **authentication open**

PSK 認証による 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、次のコマンドを使用します。

configure ssid-profile *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2**

PSK Dot11r 認証を使用して SSID 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 ssid-profile *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r**

PSK Dot11w 認証を使用して SSID 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 ssid-profile *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w**

Dot1x 認証による 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、次のコマンドを使用します。

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

次に、Dot1x EAP-PEAP 認証を使用した SSID プロファイルの設定例を示します。

```
configure dot1x credential c1 username wgbusr password cisco123456
configure eap-profile p1 dot1x-credential c1
configure eap-profile p1 method peap
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

IW9165E には 2.4 GHz 無線機がありません。スロット 1（dot11radio 1）のみをアップリンクとして設定し、WGB モードで動作させることができます。

- 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 1 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 1** { **enable** | **disable** }

  例

  ```
  #configure dot11radio 1 disable
  ```

Dot1X ログイン情報の設定

次のコマンドを入力して、dot1x ログイン情報を設定します。

configure dot1x credential *profile-name* **username** *name* **password** *pwd*

次のコマンドを入力して、WGB EAP dot1x プロファイルの概要を表示します。

 # show wgb eap dot1x credential profile

WGB 有線クライアントの認証解除

このコマンドを入力して、WGB 有線クライアントの認証を解除します。

clear wgb client {**all** |**single** *mac-addr*}

EAP プロファイルの設定

EAP プロファイルを設定するには、次の手順を実行します。

1. dot1x ログイン情報プロファイルを EAP プロファイルにバインドします。
2. EAP プロファイルを SSID プロファイルにバインドします。
3. SSID プロファイルを無線機にバインドします。

手順

ステップ 1 次のコマンドを入力して、EAP プロファイルの方式タイプを設定します。

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

ステップ 2 次のコマンドを入力して、TLS 用の CA トラストポイントを接続します。デフォルトプロファイルでは、WGB は認証に内部 MIC 証明書を使用します。

 # configure eap-profile *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*}

ステップ 3 次のコマンドを入力して、dot1x-credential プロファイルをバインドします。

 # configure eap-profile *profile-name* **dot1x-credential** *profile-name*

ステップ 4 [オプション] 次のコマンドを入力して、EAP プロファイルを削除します。

 # configure eap-profile *profile-name***delete**

ステップ 5 次のコマンドを入力して、EAP プロファイルと dot1x プロファイルの概要を表示します。

 # show wgb eap profile all

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 次のコマンドを入力して、WGB にトラストポイントを作成します。

 # configure crypto pki trustpoint *ca-server-name* **enrollment terminal**

ステップ 2 次のコマンドを入力して、トラストポイントを手動で認証します。

 # configure crypto pki trustpoint *ca-server-name* **authenticate**

Base 64 でエンコードされた CA 証明書を入力し、新しい行に **quit** と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、ユーザーはトラストポイントに完全な証明書チェーンをインポートする必要があります。

例：

```
#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 次のコマンドを入力して、秘密鍵のサイズを設定します。

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

ステップ 4 次のコマンドを入力して、サブジェクト名を設定します。

 # 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 次のコマンドを入力して、秘密鍵と証明書署名要求（CSR）を生成します。

 # configure crypto pki trustpoint *ca-server-name* **enroll**

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 次のコマンドを入力して、WGB に署名付き証明書をインポートします。

 # configure crypto pki trustpoint *ca-server-name* **import certificate**

Base 64 でエンコードされた CA 証明書を入力し、新しい行に **quit** と入力して証明書を終了します。

ステップ 7 [オプション] 次のコマンドを入力して、トラストポイントを削除します。

 # configure crypto pki trustpoint *trustpoint-name* **delete**

ステップ 8 次のコマンドを入力して、トラストポイントの概要を表示します。

 # show crypto pki trustpoint

ステップ 9 次のコマンドを入力して、トラストポイント用に作成された証明書の内容を表示します。

 # show crypto pki trustpoint *trustpoint-name* **certificate**

ワークグループブリッジのトラストポイントの自動登録設定

手順

ステップ 1 次のコマンドを入力して、サーバー URL を使用して WGB にトラストポイントを登録します。

 # configure crypto pki trustpoint *ca-server-name* **enrollment url** *ca-server-url*

ステップ 2 次のコマンドを入力して、トラストポイントを認証します。

 # 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 次のコマンドを入力して、秘密鍵のサイズを設定します。

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

ステップ 4 次のコマンドを入力して、サブジェクト名を設定します。

 # 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 次のコマンドを入力して、トラストポイントを登録します。

 # 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 次のコマンドを入力して、自動登録を有効にします。

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

コマンドで disable 構文を使用することで、自動登録を無効にできます。

ステップ 7 [オプション] 次のコマンドを入力して、トラストポイントを削除します。

 # configure crypto pki trustpoint *trustpoint-name* **delete**

ステップ 8 次のコマンドを入力して、トラストポイントの概要を表示します。

 # show crypto pki trustpoint

ステップ 9 次のコマンドを入力して、トラストポイント用に作成された証明書の内容を表示します。

 # show crypto pki trustpoint *trustpoint-name* **certificate**

ステップ 10 次のコマンドを入力して、PKI タイマー情報を表示します。

 # 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 次のコマンドを入力して、WGB のトラストポイントの CA 証明書とクライアント証明書を取得するための登録方式を指定します。

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

ステップ 2 次のコマンドを入力して、トラストポイントを手動で認証します。

 # configure crypto pki trustpoint *ca-server-name* **authenticate**

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は、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 次のコマンドを入力して、秘密鍵のサイズを設定します。

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

ステップ 4 次のコマンドを入力して、サブジェクト名を設定します。

 # 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 次のコマンドを入力して、秘密鍵と証明書署名要求（CSR）を生成します。

 # configure crypto pki trustpoint *ca-server-name* **enroll**

証明書要求を生成し、この要求を TFTP サーバーに書き込みます。書き込まれるファイル名には「.req」という拡張子が付加されます。

ステップ 6 次のコマンドを入力して、WGB に署名付き証明書をインポートします。

 # configure crypto pki trustpoint *ca-server-name* **import certificate**

許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。WGB は、同じファイル名とファイル名に「.crt」拡張子を付けたものを使用して、TFTP を使用して付与された証明書の取得を試行します。

ステップ 7 次のコマンドを入力して、トラストポイントの概要を表示します。

 # show crypto pki trustpoint

ステップ 8 次のコマンドを入力して、トラストポイント用に作成された証明書の内容を表示します。

 # show crypto pki trustpoint *trustpoint-name* **certificate**

WGB または 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 <*slot_id*> **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 1 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 1 enable
```

以下の項で、uWGB の設定について詳しく説明します。

- SSID の設定
- Dot1X ログイン情報の設定
- EAP プロファイルの設定
- 端末のトラストポイントの手動登録設定
- ワークグループブリッジのトラストポイントの自動登録設定
- TFTP サーバーを使用した手動での証明書の登録設定
- WGB または uWGB タイマーの設定

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** <*radio_slot_id*> **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]
```

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
```

Syslog の設定

Syslogは、デバイスがイベントデータログを中央に送信して保存するために使用する一般的なプロトコルです。現在、UDP モードのみがサポートされています。WGB でデバッグコマンドが有効になっている場合には、追加のデバッグログが収集されます。収集されSyslogサーバーに送信されるログはすべて、「kernel」ファシリティおよび「warning」レベルとなります。

- WGB syslog を有効にするには、次のコマンドを使用します。

  # **logging host enable** <*server_ip*> **UDP**

- WGB syslog を無効にする（デフォルト）には、次のコマンドを使用します。

  # **logging host enable 0.0.0.0 UDP**

- 現在の syslog 設定を表示するには、次のコマンドを使用します。

  # **show running-config**

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）変調および符号化方式（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.**

（注） WGB では、レガシーレートの設定もサポートされます。

Config dot11radio [**1**|**2**] **speed legacy-rate basic-6.0 9.0 12.0 18.0 24.0**

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。

```
DWGB1#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
DWGB1#[*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
```

802.11v のサポート

802.11v は、IEEE 802.11 標準ファミリのワイヤレスネットワーク管理の標準規格です。802.11v の機能拡張の 1 つは、WLAN が関連付けられたクライアントに要求を送信し、クライアントがより適切なアソシエート先 AP を選択できるように助言するネットワーク支援型ローミングです。これは、ロード バランシングと、接続が不安定なクライアントの管理の両方に役立ちます。

WGB に 802.11v のサポートを追加することで、WGB はアソシエーションが解除される前に切断が迫っていることを認識し、自発的にローミングを開始し、ネイバー AP のリストから適切な AP を選択できます。WGB は最新のネイバー AP を定期的にクエリし、次のローミング時に最適な AP に関連付けることができます。

ネイバー AP のチャンネル情報は Basic Service Set（BSS）移行要求フレームに含まれるため、複数のチャンネルを展開する場合は、ネイバー AP のチャンネルのみを走査することでローミング遅延を低減できます。

ワイヤレスコントローラは、AP 側のロードバランス、RSSI、およびデータレートに基づいてクライアントのアソシエーションを解除できます。このアソシエーションの解除は、発生する前に 802.11v クライアントに通知できます。ワイヤレスコントローラは、一定期間（設定可能）内にクライアントと別の AP との再アソシエーションが成立しない場合、一定期間経過後にクライアントとのアソシエーションを解除できます。ネットワーク支援型ローミングによるクライアントのアソシエーション解除を有効にするには、ワイヤレスコントローラからアソシエーション解除通知設定をオンにします。BSS 移行管理要求フレーム内のオプションフィールド（[disassociation imminent]）がこれに相当します。

ワイヤレスコントローラでの 802.11v 設定の詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-13/config-guide/b_wl_17_13_cg/m_802_11v_ewlc.html を参照してください。

WGB で 802.11v のサポートを設定するには、次のコマンドを使用します。

- WGB で 802.11v のサポート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。802.11v のサポートを有効にすると、WGB はネイバーリストから学習したチャンネルのみを走査します。

  # **configure wgb mobile station interface dot11Radio** *<radio_slot_id>* **dot11v-bss-transition** [**enable**|**disable**]

- WGB が親 AP に BSS 移行クエリメッセージを送信する時間の間隔を設定するには、次のコマンドを使用します。明示的に設定されていない場合、デフォルト値は 10 秒です。タイマーは秒単位で設定します。

  # **configure wgb neighborlist-update-interval** *<1 ～ 900>*

- 関連付けられた AP から受信したネイバーリストを確認するには、次のコマンドを使用します。

  # **show wgb dot11v bss-transition neighbour**

- dot11v ネイバーのチャンネルリスト、走査済みの補助無線機、走査済みの残存チャンネルを確認するには、次のコマンドを使用します。

  # **show wgb dot11v bss-transition channel**

- ネイバーリストをクリアしてエラー状態を回復するには、次のコマンドを使用します。

  # **clear wgb dot11v bss-transition neighbor**

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。

走査専用モードの概要

- AP は無線機に、クライアント接続の提供のためではなく、走査を目的とした動作のみを許可します。
- AP はワイヤレス環境を継続的に走査して、ネットワーク性能、干渉、不正デバイス、およびその他の重要な計量値に関するデータを収集します。

走査専用モードの設定

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。

ローミングが発動すると、アルゴリズムによって走査表から候補が検索され、表が空でなければ走査段階は飛ばされます。その後、WGB がその候補 AP とのアソシエーションを行います。

走査専用モードを設定するには、次のコマンドを使用します。

configure dot11Radio 2 mode scan only

チャンネルリストを手動で設定するには、次のコマンドを使用します。

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

デフォルトでは、走査表の候補 AP エントリは 1200 ミリ秒でエージアウトします。次のコマンドを使用して、このタイマーを調整できます。

#**configure wgb scan radio 2 timeout**

<1 ～ 5000> AP 走査の有効期限

（注） AP 選択アルゴリズムにより、走査表から最適な RSSI を持つ候補が選択されます。この RSSI 値が古い値になっている場合があります。この場合には、ローミングで障害が発生する可能性があります。

show wgb scan コマンドを使用して、走査表を確認します。

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

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

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

補助走査ハンドオフモードの設定

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。ローミングが発動すると、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。

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

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

次の表では、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、ローミングが発動します。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。

ローミングが発動する要因

ローミングは、次のイベントで発動します。

- 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。

デュアル無線機構成

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。

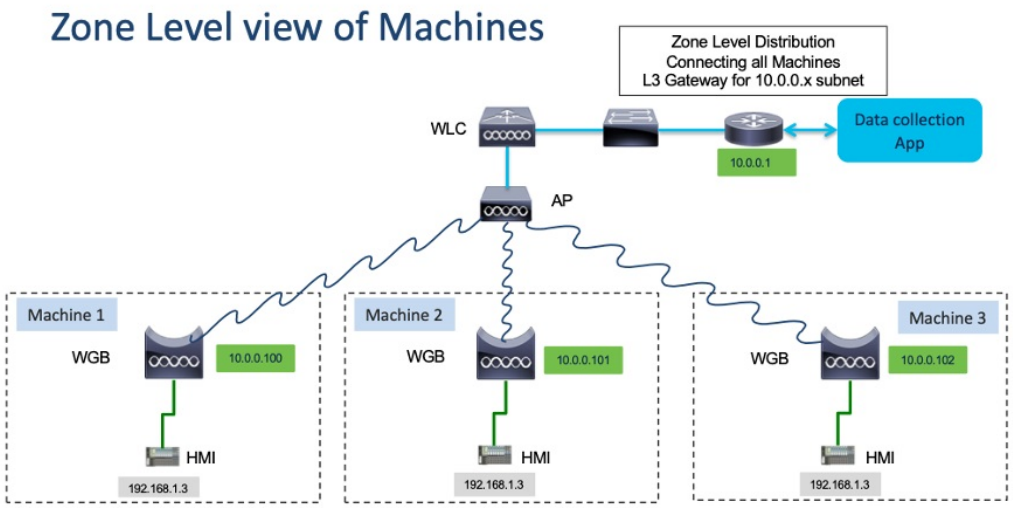
デュアル無線機	AP
5 GHz 無線機 1 + 無線機 2（走査専用モード）	IW9165E
5 GHz 無線機 1 + 無線機 2（補助走査ハンドオフモード）	

レイヤ 2 NAT の設定

1 対 1（1：1）レイヤ 2 NAT は、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）に割り当てるサービスであり、エンド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なります。レイヤ 2 NAT には、プライベートからパブリックおよびパブリックからプライベートへサブネットの変換を定義できる 2 種類の変換表があります。

産業分野における、すべての HMI（ロボットなどのお客様のマシン）に同じファームウェアがプログラムされているシナリオでは、マシン間のファームウェアの重複は、IP アドレスが HMI

間で再利用されることを意味します。この機能は、パブリックネットワークと通信する産業用ネットワークで重複する同じ IP アドレスを持つ複数のエンドデバイスの問題を解決します。



次の表に、レイヤ 2 NAT を設定するためのコマンドを示します。

表 *2 :* レイヤ *2 NAT* 設定コマンド

コマンド	説明
#**configure l2nat** {**enable**|**disable**}	L2 NAT を有効または無効にします。
#**configure l2nat default-vlan** <*vlan_id*>	すべての NAT ルールが適用されるデフォルトの VLAN を指定します。*vlan_id* が指定されていない場合、すべての NAT ルールが vlan 0 に適用されます。
#**configure l2nat** {**add**|**delete**} **inside from host** <*original_ip_addr*> **to** <*translated_ip_addr*>	プライベート IP アドレスをパブリック IP アドレスに変換する NAT ルールを追加または削除します。 • *original_ip_addr*：WGB イーサネットポートに接続された有線クライアントのプライベート IP アドレス。 • *Translation_ip_addr*：パブリックネットワークで有線クライアントを表すパブリック IP アドレス。

コマンド	説明
#**configure l2nat** {**add**|**delete**} **outside from host** <*original_ip_addr*> **to** <*translated_ip_addr*>	パブリック IP アドレスをプライベート IP アドレスに変換する NAT ルールを追加または削除します。 • *original_ip_addr*：外部ネットワークホストのパブリック IP アドレス。 • *Translation_ip_addr*：プライベートネットワークで外部ネットワークホストを表すプライベート IP アドレス。
#**configure l2nat** {**add**|**delete**} **inside from network** <*original_nw_prefix*> **to** <*translated_nw_prefix*> <*subnet_mask*>	プライベート IP アドレスサブネットをパブリック IP アドレスサブネットに変換する NAT ルールを追加または削除します。 • *original_nw_prefix*：プライベート IP ネットワークプレフィックス。 • *Translation_nw_prefix*：パブリック IP ネットワークプレフィックス。
#**configure l2nat** {**add**|**delete**} **outside from network** <*original_nw_prefix*> **to** <*translated_nw_prefix*> <*subnet_mask*>	パブリック IP アドレスサブネットをプライベート IP アドレスサブネットに変換する NAT ルールを追加または削除します。 • *original_nw_prefix*：パブリック IP ネットワークプレフィックス。 • *Translation_nw_prefix*：プライベート IP ネットワークプレフィックス。

次の表に、レイヤ 2 NAT 設定を確認およびトラブルシュートするための show コマンドと debug コマンドを示します。

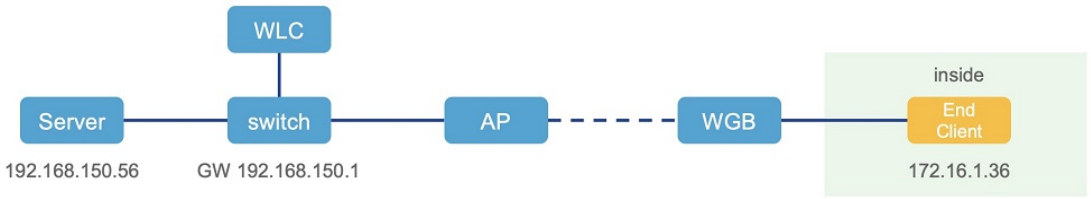
表 *3*：レイヤ *2 NAT* の *Show* コマンドと *Debug* コマンド

コマンド	説明
#**show l2nat entry**	レイヤ 2 NAT の実行中エントリを表示します。
#**show l2nat config**	レイヤ 2 NAT 設定の詳細を表示します。
#**show l2nat stats**	レイヤ 2 NAT パケット変換統計を表示します。
#**show l2nat rules**	設定からレイヤ 2 NAT ルールを表示します。

コマンド	説明
#clear l2nat statistics	パケット変換統計をクリアします。
#clear l2nat rule	レイヤ 2 NAT ルールをクリアします。
#clear l2nat config	レイヤ 2 NAT 設定をクリアします。
#debug l2nat	パケット変換プロセスのデバッグを有効にします。
#debug l2nat all	パケット着信時に、NAT エントリに一致する結果を出力します。 **注意** この debug コマンドにより、コンソールに大量のログが出力される可能性があります。特に Syslog サービスがブロードキャストアドレスで有効になっている場合、このコマンドが原因でコンソールからの応答が失われる可能性があります。
#undebug l2nat	パケット変換プロセスのデバッグを無効にします。

ホスト IP アドレス変換の設定例

このシナリオでは、WGB に接続されたエンドクライアント（172.16.1.36）は、ゲートウェイに接続されたサーバー（192.168.150.56）と通信する必要があります。レイヤ 2 NAT は、外部ネットワーク（192.168.150.36）上でのエンドクライアントのアドレスと内部ネットワーク（172.16.1.56）上でのサーバーのアドレスを提供するように設定されています。



次の表は、このシナリオの設定作業を示しています。

コマンド	目的
#configure l2nat add inside from host 172.16.1.36 to 192.168.150.36 **#configure l2nat add outside from host 192.168.150.56 to 172.16.1.56**	NAT ルールを追加して、内部クライアントと外部サーバーが相互に通信できるようにします。

コマンド	目的
#configure l2nat add inside from host 172.16.1.1 to 192.168.150.1 **#configure l2nat add inside from host 172.16.1.255 to 192.168.150.255**	ゲートウェイとブロードキャストアドレスの NAT を追加します。

次の show コマンドにより、設定を表示します。

- 次のコマンドは、レイヤ 2 NAT 設定の詳細を表示します。出力の I2O は「内部から外部」を意味し、O2I は「外部から内部」を意味します。

```
#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
```

- 次のコマンドは、レイヤ 2 NAT ルールを表示します。

```
#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
```

- 次のコマンドは、レイヤ 2 NAT 実行中エントリを表示します。

```
#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
```

- 次のコマンドは、ブリッジを介した WGB 有線クライアントを表示します。
  - レイヤ 2 NAT の有効化前：

```
#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：

```
#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
```

NAT の有線クライアントに E2E トラフィックの問題が発生した場合は、次のコマンドを使用してクライアント登録プロセスを再起動します。

```
#clear wgb client single B8:AE:ED:7E:46:EB
```

- 次のコマンドは、レイヤ 2 NAT パケット変換の統計を表示します。

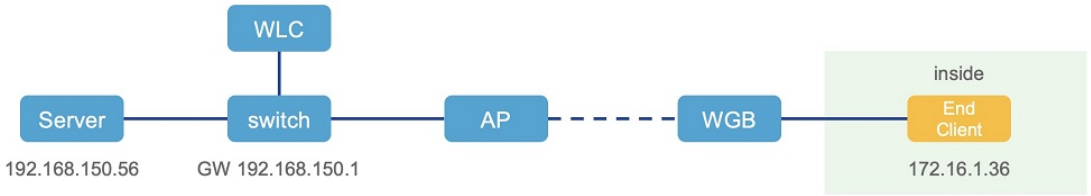
```
#show l2nat stats
Direction          Original              Substitute            ARP  IP   ICMP UDP
TCP
inside-to-outside  172.16.1.1@2660       192.168.150.1@2660    1    4    4    0
0
inside-to-outside  172.16.1.36@2660      192.168.150.36@2660   3    129  32   90
1
inside-to-outside  172.16.1.56@2660      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
```

統計情報をリセットするには、次のコマンドを使用します。

```
#clear l2nat stats
```

ネットワークアドレス変換の設定例

このシナリオでは、内部アドレスを 172.16.1.0 255.255.255.0 サブネットから 192.168.150.0 255.255.255.0 サブネットのアドレスに変換するようにレイヤ 2 NAT が設定されています。この変換で置き換えられるのは、ネットワークプレフィックスのみです。IP アドレスのホストビットは変わりません。



このシナリオ向けに、次のコマンドが設定されています。

```
#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でのネイティブ VLAN の設定

WGB の一般的な展開では、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（または WLC/AP/WGB）管理

VLAN と同じ VLAN 上にある必要があります。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 を設定する必要があります。

（注） 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） 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 DS 側のクライアントがパッシブクライアントの背後でこの 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** と **configure wgb ethport native-vlan id X**（X は WGB（または WLC/AP/WGB）管理 VLAN と同じ VLAN）コマンドを追加で設定します。

次の表に、ネイティブ VLAN を設定するためのコマンドを示します。

表 *4:* ネイティブ *VLAN* 設定コマンド

コマンド	説明
#**config wgb ethport native-vlan** {**enable**|**disable**} 例： `#config wgb ethport native-vlan enable`	ネイティブ VLAN 設定を有効または無効にします。
#**config wgb ethport native-vlan id** <*vlan-id*> 例： `#config wgb ethport native-vlan id 2735`	ネイティブ VLAN ID を指定します。

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

IEEE 802.11 ネットワークは、拡張型分散チャンネルアクセス（EDCA）、集約 MAC プロトコルデータユニット（AMPDU）、集約または非集約パケット再試行を適用することで、低遅延と QoS の要件を満たすモノのインターネット（IoT）のサポートと展開において大きな役割を果たします。

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。

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
```

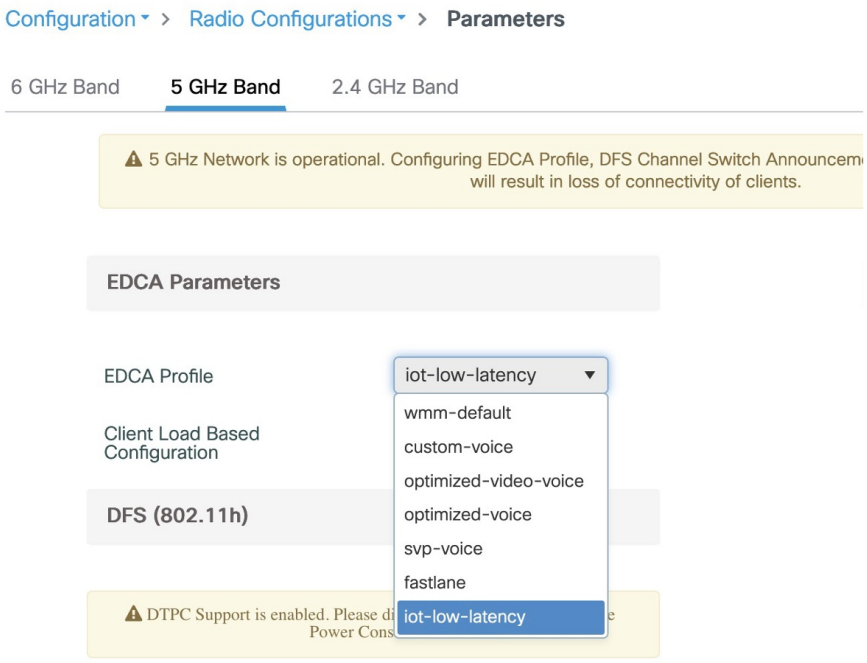
EDCA パラメータの設定（ワイヤレスコントローラ GUI）

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 を使った SNMP の設定と検証

簡易ネットワーク管理プロトコル（SNMP）は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。SNMPはネットワーク デバイスの監視や管理に使用される標準化されたフレームワークと共通言語を提供します。

WGB は、ネットワーク管理者に SNMP インターフェイスを提供し、さまざまな状態やカウンタをポーリングできます。これにより、管理者は現場で WGB の正常性を簡単に監視できます。

デフォルトでは、SNMP は無効です。

SNMP フレームワークには、次のコンポーネントがあります。

- **SNMP Manager**：Simple Network Management Protocol（SNMP）マネージャは、SNMP を使用するネットワークホストのアクティビティを制御および監視するシステムです。最も一般的な管理システムは、ネットワーク管理システム（NMS）です。NMS という用語は、ネットワーク管理に使用する専用デバイスを意味する場合と、このようなデバイス上で使用するアプリケーションを意味する場合があります。
- **SNMP Agent**：Simple Network Management Protocol（SNMP）エージェントは、デバイスに対してデータを保守し、このデータを必要に応じて管理システムにレポート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です。
- **SNMP MIB**：SNMP エージェントには、SNMP マネージャが Get 操作や Set 操作を通じて要求したり変更したりできる MIB 変数が含まれています。マネージャは、エージェントからの値の取得またはエージェントへの値の保存が可能です。エージェントは、デバイスパラメータやネットワーク データに関する情報のリポジトリである SNMP MIB から値を収集します。エージェントは、マネージャのデータ取得要求やデータ設定要求に応答もできます。

次の図に、SNMP プロセスを示します。SNMP エージェントは SNMP クライアントからリクエストを受信し、そのリクエストをサブエージェントに渡します。その後、サブエージェントは SNMP エージェントに応答を返し、エージェントは SNMP 応答パケットを作成し、リクエストの発信元であるリモートネットワーク管理ステーションに応答を送信します。

図 *3 : 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のデータベースです。管理対象オブジェクト、つまり変数を設定したり読み取ったりして、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、階層状に構成できます。MIB は、オブジェクト識別子によって識別される管理対象オブジェクトの集まりで構成されます。MIB には、SNMP などのネットワーク管理プロトコルを使用してアクセスします。

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 階層内における MIB オブジェクトの位置が識別され、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提供されます。

次に、SNMP Management Information Base（MIB）：CISCO-DOT11-ASSOCIATION-MIB でサポートされるオブジェクトのリストを示します。

表 *5 :* サポートされる *OID*

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

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

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

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

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

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

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

WGB CLI による SNMP の設定

次の CLI コマンドが、SNMP の設定に使用されます。

（注）

- SNMP CLI ロジックは SNMP 設定用に変更されています。SNMP 機能を有効にする前に、CLI：configure snmp enabled により、SNMP のパラメータをすべて設定する必要があります。
- SNMP 機能を無効にすると、SNMP に関連するすべての設定が自動的に削除されます。

手順

ステップ 1 [SNMP v2c community ID] 番号を入力します（SNMP v2c のみ）。

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

ステップ 2 **SNMP プロトコルのバージョン**を指定します。

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

ステップ 3 **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** | **sha>**

ステップ 4 **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 **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 8-64>**

ステップ 6 **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** | **aes** | **none**}

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

ステップ 7 **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 8-64>**

ステップ 8 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 ～ 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 **SNMP 設定を無効**にします。

Device#**configure snmp disabled**

SNMP を無効にすると、関連するすべての設定が削除されます。

例

SNMP の設定例。

- **SNMP v2c を設定するための CLI** ：

```
Device#configure snmp v2 community-id <length 1-64>
Device#configure snmp version v2c
Device#configure snmp enabled
```

- **SNMP v3 を設定するための CLI（セキュリティレベル AuthPriv）** ：

```
Device#configure snmp auth-method <md5|sha>
Device#configure snmp v3 username <length 32>
Device#configure snmp v3 password <length 8-64>
Device#configure snmp secret <length 8-64>
Device#configure snmp encryption <aes|des>
Device#configure snmp version v3
Device#configure snmp enabled
```

- **SNMP v3 を設定するための CLI（セキュリティレベル AuthNoPriv）** ：

```
Device#configure snmp auth-method <md5|sha>
Device#configure snmp v3 username <length 32>
Device#configure snmp v3 password <length 8-64>
Device#configure snmp encryption none
Device#configure snmp version v3
Device#configure snmp enabled
```

WGB CLI による SNMP の確認

SNMP 設定を確認するには、次の show コマンドを使用します。

- **SNMP バージョン v3 の出力の表示**：

```
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 バージョン v2c の出力の表示**：

```
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 の分類とマーキングのサポート

Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、WGB では、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従って異なるアクセス制御ドライバキューにマークできます。

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、現場環境に基づいて異なるアクセス制御キューに割り当てる必要があります。

概要

WGB では、イーサネットポートからの着信パケットをワイヤレス側の特定の優先キューにマッピングするカスタムルールを作成できます。WGB には、IEEE 802.1p（dot1p）または DiffServ コードポイント（DSCP）のいずれかに基づいてアップストリームデータ トラフィックをマッピングする機能があります。

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、および DSCP に基づいてルールを設定できます。ワイヤレスネットワーク上のさまざまなアクセス制御キューにパケットを転送し、効率的な QoS の適用を促進します。

イーサネットポートに着信したパケットは、カスタマイズされたルールベースのマッピングを使用して、ワイヤレス側の特定のアクセス制御キューに転送されます。

カスタマイズされたルールによって、送信元および宛先 IP アドレス、ポート番号、プロトコルタイプなどのあらかじめ定義された条件に基づいて、パケットの分類とさまざまなアクセス制御キューへの割り当てが規定されます。ルールを定義すると、定義されたルールによって着信パケット内の重要なサービスまたはトラフィックが識別されます。定義されたルールによってこうした重要なサービスを照合することで、一致するサービスをネットワーク インフラストラクチャ内の優先度の高いキューにマッピングできます。

WGB におけるルールベースのトラフィックの分類とマッピングを使用することで、ネットワークトラフィックを効果的に管理し、優先順位付けを行い、重要なアプリケーションやサービスに固有の要求を満たせます。このアプローチにより、ネットワーク内で QoS ポリシーを効果的に適用して、最適なネットワーク性能を維持し、重要なサービスの遅延を最小限に抑え、ユーザー体験全般を向上できます。

QoS と ACL に基づくトラフィックの分類

分類とは、パケット内のフィールドを検証して、トラフィックを区別するプロセスです。デバイスでは、QoS が有効になっている場合にのみ分類が有効になります。

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 ラベルは、パケットに対して実行するすべての QoS アクションを示し、パケットの送信元キューを識別します。

レイヤ2イーサネットフレームでは、[Ethertype]フィールドに分類情報が含まれます。[Ethertype]フィールド（通常、サイズは2バイト）は、通常、フレームにカプセル化されたデータのタイプを示します。

レイヤ 3 IP パケットでは、8 ビットの [Type of Service（TOS）] フィールドに分類情報が含まれます。[ToS] フィールドには、IP precedence 値または Diffserv コード ポイント（DSCP）値のいずれかが含まれます。IP precedence 値の範囲は 0 ～ 7 です。DSCP 値の範囲は 0 ～ 63 です。

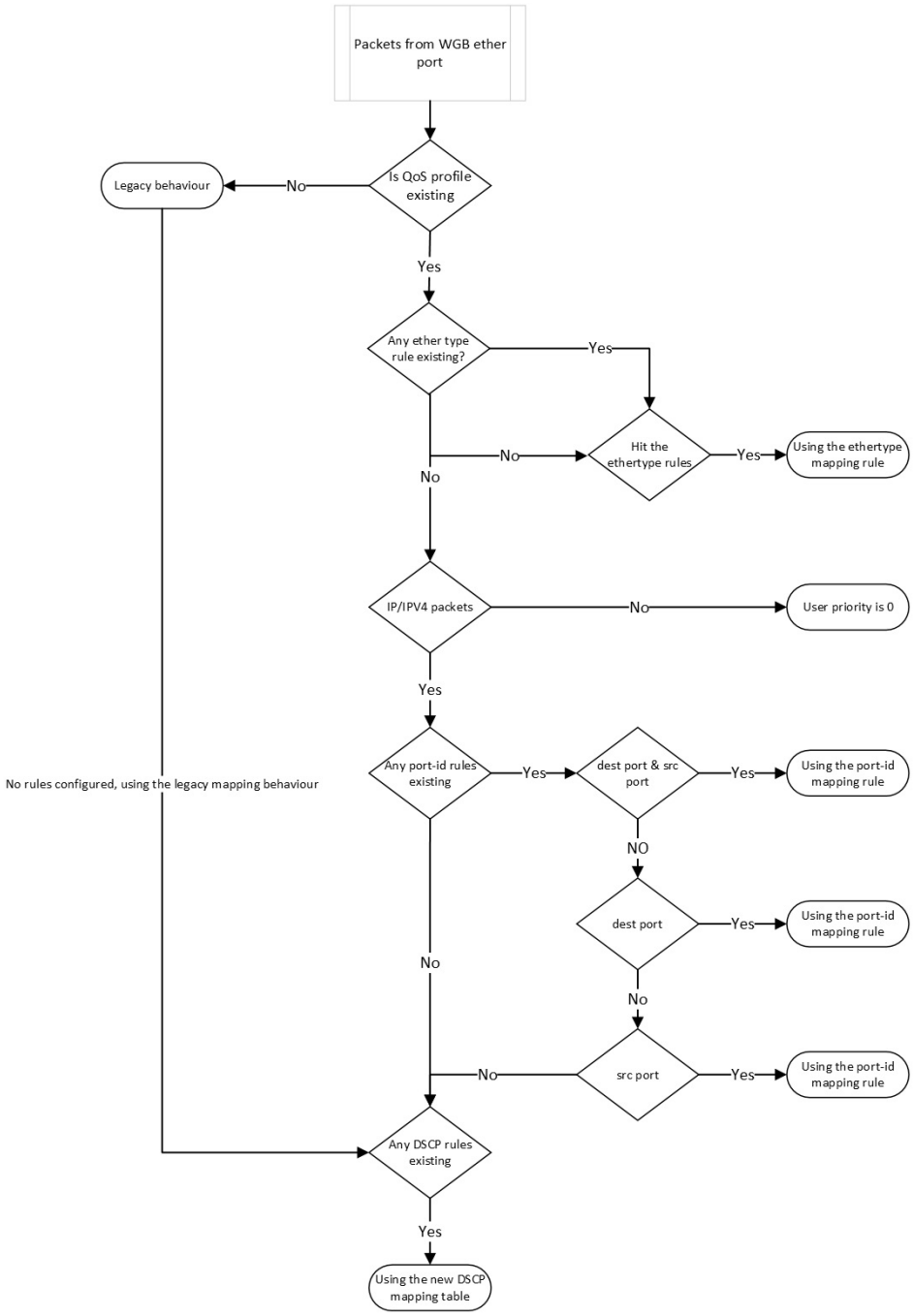
レイヤ 4 TCP セグメントまたは UDP データグラムでは、[Source Port] フィールドまたは [Destination Port] フィールドに分類情報が含まれます。これらのポートフィールドは、データの送信者と受信者に関連付けられたポート番号を指定します。これにより、ネットワーキングデバイスは、事前に定義された条件に基づいてトラフィックを分類できます。

システムにより、イーサネットタイプ、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、サービスクラス内のパケットが一貫して処理されます。WGBは、2つの有線ポートからのさまざまなパケットを分類し、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するのに役立ちます。

データプレーン統計は、ネットワークトラフィックが各ルールにヒットした回数を示します。これらのカウンタは、ネットワーク管理者がルールとポリシーの有効性を分析し、ネットワーク性能を最適化する上で不可欠です。

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ネットワークアーキテクチャの一部です。

図 *4 : 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 が無効になっている場合、アクセスポイントは従来のマッピング動作に従い、次の処理を実行します。

1. 指定された Ethertype 0x8100 の VLAN 要素からタグ制御情報（TCI）の優先順位を取得します。

2. Ethertype 0x8892（Profinet）QoS マッピングについては、TCI の優先順位に 6 を割り当てます。
3. Ethertype 0x0800（IP）および 0x86DD（IPv6）については、DSCP の優先順位はデフォルトの dscp2dot1p マッピング表に従って設定されます。

```
======= 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
```

QoS が有効になっている場合、アクセスポイントは次の処理を実行します。

1. Ethertype 0x8892（Profinet）QoS マッピングの優先順位は、構成の設定に基づきます。
2. Ethertype 0x0800（IP）および 0x86DD（IPv6）については、優先順位はポートまたは DSCP を考慮したマッピングルールに基づきます。
   - UDP/TCP ポート（またはポート範囲）ルールを確認します。
   - DSCP ルールを確認します。
3. 非 IPv4/IPv6 パケットのユーザー優先順位として値 0 を割り当てます。
4. ルールが設定されていない場合、QoS プロファイルは従来のマッピング動作に従います。

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

Quality of Service マッピングプロファイルの設定

次のコマンドを使用すると、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 QoS マッピングプロファイルを有効にします。

Device#**config wgb qos-mapping <profile-name> enable**

例：

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

ステップ 2 **イーサネットタイプ**に基づく WGB QoS マッピング プロファイル ルール。

次のコマンドを使用して、イーサネットフレームタイプに基づいてルールを設定します。

- イーサネットタイプに基づいてルールを追加します。

  Device#**config wgb qos-mapping** <**profile-name**> **add ethtype hex** <**number**> **priority** <**0-7**>

例：

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

コマンドにより存在しないプロファイルを指定した場合、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。

- イーサネットタイプに基づくルールの削除

  Device#**config wgb qos-mapping** <**profile-name**> **delete ethtype hex** <**number**>

例：

```
Device#configure wgb qos-mapping demo-profile delete ethtype hex 8892
```

このコマンドの場合、存在しないプロファイルを指定すると、警告メッセージが発行されます。さらに、指定した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には、そのプロファイルは自動的に削除されます。

ステップ 3 **ポートの ID または範囲**に基づくルール。

次のコマンドを使用して、L4 ポートの ID または範囲に基づいてルールを設定します。

- ポートの ID または範囲に基づいてルールを追加します。

  Device#**config wgb qos-mapping** <**profile-name**> add **srcport** <**number**> | <**range** <**start-number**> <**end-number**>> [**dstport** <**number**> | <**range** <**start-number**> <**end-number**>>] **priority** <**0-7**>

例：

```
Device#configure wgb qos-mapping demo-profile add srcport range 5050 5070 dstport 8000 priority 3
```

コマンドにより存在しないプロファイルを指定した場合、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。

- ポートの ID または範囲に基づいてルールを削除します。

  Device#**config wgb qos-mapping** <**profile-name**> delete [**srcport** <**number**> | <**range** <**start-number**> <**end-number**>> [**dstport** <**number**> | <**range** <**start-number**> <**end-number**>>]]

例：

```
Device#configure wgb qos-mapping demo-profile delete srcport range 5050 5070 dstport 8000
```

このコマンドの場合、存在しないプロファイルを指定すると、警告メッセージが発行されます。さらに、指定した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には、そのプロファイルは自動的に削除されます。

ステップ 4 **DSCP** に基づくルール。

次のコマンドは、IPv4/IPv6 パケットの DSCP 値に基づいてルールを設定するために使用されます。

- [Add

Device#**config wgb qos-mapping** <**profile-name**> add dscp <**number**> priority < **0-7**>

例：

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

コマンドにより存在しないプロファイルを指定した場合、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。

- 削除（Delete）

  Device#**config wgb qos-mapping** <**profile-name**> delete dscp <**number**> priority < **0-7**>

例：

```
Device#configure wgb qos-mapping demo-profile delete dscp 63
```

このコマンドの場合、存在しないプロファイルを指定すると、警告メッセージが発行されます。さらに、指定した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には、そのプロファイルは自動的に削除されます。

（注）
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 QoS マッピングプロファイルを無効にします。

Device#**config wgb qos-mapping** <**profile-name**> disable

例：

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

無効にすると、コマンドによってプロファイルがデータパスからクリアされ、WGB 構成ファイルに保持されます。指定されたプロファイルが存在しない場合、コマンドは警告メッセージを発行し、新しい空のプロファイルは作成されません。

ステップ 6 QoS マッピングプロファイルを削除します。

Device#**config wgb qos-mapping** <**profile-name**> delete

例：

```
Device#configureure 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 設定から削除されます。

WGB の Quality of Service マッピングの確認

コントロールプレーンの WGB 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

WGB での TCP ダンプ

TCP ダンプユーティリティは、ネットワーク監視およびデータ取得に広く使用されるネットワーク パケット アナライザです。TCP ダンプを WGB に適用すると、WGB の有線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、表示、および保存できます。

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

TCP ダンプユーティリティの目的

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

TCP ダンプユーティリティの機能

- 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する
- 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

- 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 ファイルはクリアされます。

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。

WGB のプロトコル 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。

- 伝送制御プロトコル
- Internet Control Message Protocol（ICMP）および 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
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
```

WGB の有線パケットキャプチャの無効化

手順

PCAP を無効にするには、次のコマンドを使用します。

1. デフォルトフィルタ：

   Device#**no debug traffic wired** [*0-3*] {**ip** | **tcp** | **udp**} [**verbose** | **capture**]

2. カスタムフィルタ：

   Device#**no debug traffic wired** [*0-3*] **filter** *expression* [**verbose** | **capture**]

（注）
キャプチャプロセスを終了するには、**no debug** または **undebug all** コマンドを使用します。

WGB の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 ユーザー認証のサポートに関する情報

この章では、AAA によって（認証を通じて）ネットワークリソースの使用を制御し、（承認を通じて）許可されるアクションを定義する方法を説明します。リリース 17.15.1 以降、IW9165E WGB では AAA ベースのユーザー管理および認証がサポートされます。

AAA サーバーは、Authorization-Reply メッセージを使用して、0 ～ 15 の権限レベルをクライアントに割り当てます。現在、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おり、レベル 2 ～ 14 は予約済みです。AAA サーバーにユーザーを追加する際、権限レベル 0 および 2 ～ 14 は使用しないでください。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は次のとおりです。

- 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 を活用したユーザー認証
- 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 リリース以降から 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 以前のリリースから 17.15.1 リリース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。このため、再度 RADIUS サーバーポートの設定が必要です。

手順

ステップ 1 次のコマンドを使用して、AAA サーバー（RADIUS または TACACS+）を設定します。

Device# **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**} **address** {**ipv4** | **ipv6**} *ip-address* **port** *port-number* **secret** *secret-string*

（注）
secret-string パラメータには、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（“”）などのサポートされていない文字は使用しないでください。

ステップ 2 （オプション）AAA サーバー（RADIUS または TACACS+）を削除するには、次のコマンドを使用します。

Device# **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**} **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 次のコマンドを実行して、ログインユーザーの AAA RADIUS 認証を有効にします。

Device# **config ap management aaa radius enable**

ステップ 2 （オプション）次のコマンドを実行して、ログインユーザーの AAA RADIUS 認証を無効にします。

Device# **config ap management aaa radius disable**

ログインユーザーの TACACS+ 認証の有効化または無効化

始める前に

手順

ステップ 1 次のコマンドを実行して、ログインユーザーの AAA TACACS+ 認証を有効にします。
Device# **config ap management aaa tacplus enable**

ステップ 2 （オプション）次のコマンドを実行して、ログインユーザーの AAA TACACS+ 認証を無効にします。
Device# **config ap management aaa tacplus disable**

AAA 認証設定の確認

AAA サーバー（RADIUS または TACACS+）の設定を確認するには、**show running-configuration** コマンドを使用します。

次に、AAA RADIUS 認証が有効になっている場合の出力例を示します。

```
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
.
.
.
```

次に、AAA tacplus 認証が有効になっている場合の出力例を示します。

```
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
.
.
.
```

無線機統計コマンド

無線接続の問題をトラブルシュートするには、次のコマンドを使用します。

- **#debug wgb dot11 rate**

```
#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**

```
#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**

```
AP4C42.1E51.A050#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**

```
AP4C42.1E51.A050#show wgb dot11 uplink

HE Rates: 1SS:M0-11 2SS:M0-11
Additional info for client 8C:84:42:92:FF:CF
RSSI: -24
PS  : Legacy (Awake)
Tx Rate: 278730 Kbps
Rx Rate: 410220 Kbps
VHT_TXMAP: 65530
CCX Ver: 5
Rx Key-Index Errs: 0
            mac    intf TxData TxUC TxBytes TxFail TxDcrd TxCumRetries MultiRetries
 MaxRetriesFail RxData RxBytes RxErr                TxRt(Mbps)
RxRt(Mbps)   LER PER stats_ago
8C:84:42:92:FF:CF wbridge1   1341 1341  184032      0      0          543
 96            0   317   33523    0 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8
 (458) 27272   0  1.370000
Per TID packet statistics for client 8C:84:42:92:FF:CF
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s)
       0      35    1314            0             8
       1       0       0            0             0
       2       0       0            0             0
       3       0       0            0             0
       4       0       0            0             0
       5       0       0            0             0
       6     182      24            1             0
```

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

イベントロギング

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**

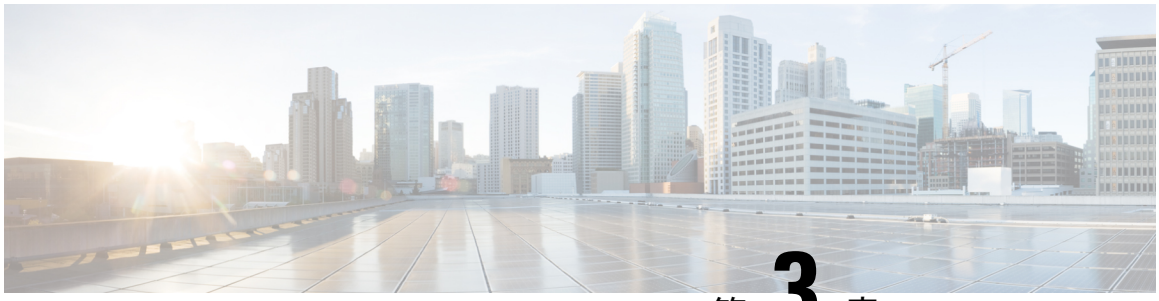
パッケージファイルは、ログレベルが異なる 4 つの個別のログファイルで構成されます。

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.
```



第 3 章

Control and Provisioning of Wireless Access Points

概要

CAPWAP は、ワイヤレス LAN コントローラが複数の AP とワイヤレス LAN コントローラ（WLC）を管理し、セキュア通信トンネルを介してコントロールプレーンとデータプレーン情報を交換できるようにする IEEE 標準規格プロトコルです。

CAPWAP はレイヤ 3 でのみ動作し、AP と WLC の両方で IP アドレスの提示を必要とします。CAPWAP は、UDP ポート 5246 および 5247 で、それぞれ IPv4 および IPv6 用のトンネルを確立します。Datagram Transport Layer Security（DTLS）暗号化により、一層セキュリティが強化されます。

DTLS は、AP と WLC 間のセキュリティを担保するプロトコルとして機能し、通信の暗号化を促進することで中間者攻撃による盗聴や改ざんを防ぎます。

デフォルトでは、DTLS は CAPWAP の制御チャンネルを保護し、AP と WLC 間のすべての CAPWAP 管理トラフィックおよび制御トラフィックを暗号化します。

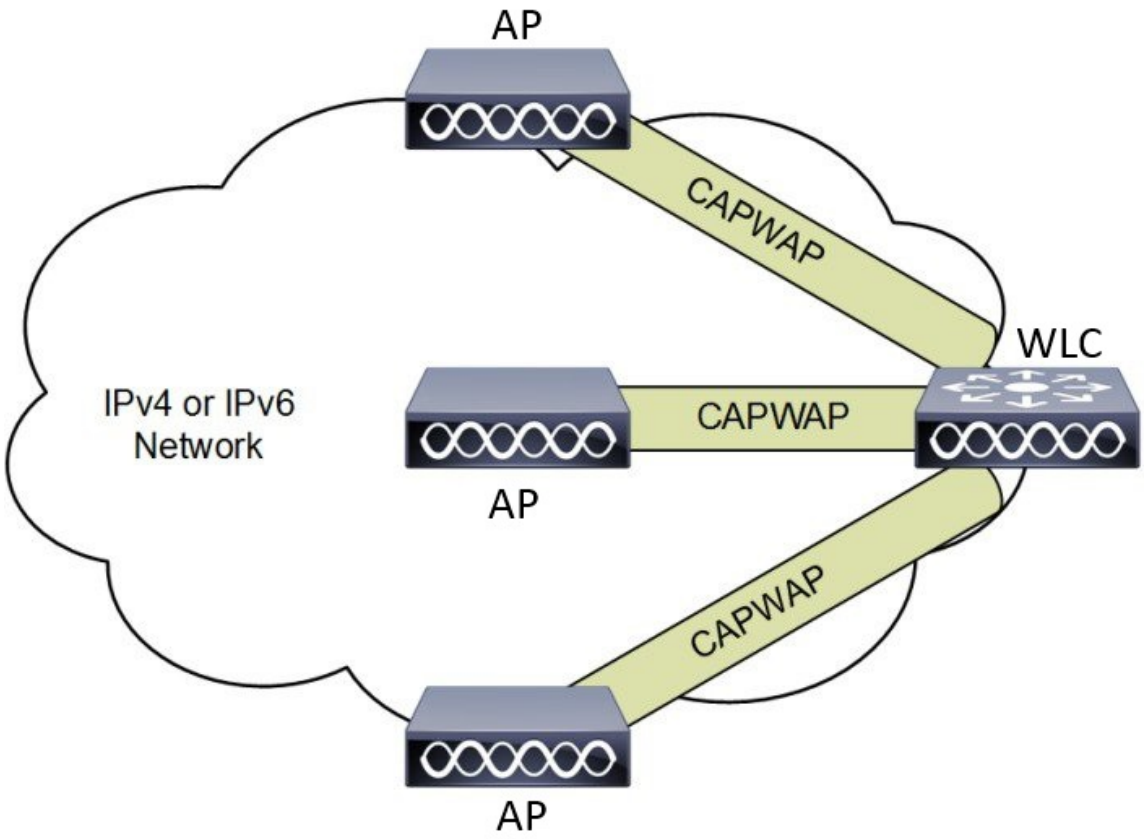
データチャンネルはデフォルトでは無効であり、AP と WLC 間を移動するクライアントデータは暗号化されません。CAPWAP データ暗号化を有効にするかどうかは任意であり、AP でアクティブ化する前に WLC に DTLS ライセンスをインストールする必要があります。

AP が DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンのみ有効となり、データプレーンの DTLS セッションは確立されません。

AP がデータ DTLS をサポートしている場合は、コントローラから新しい設定を受信した後にデータ DTLS を有効にします。AP は、ポート 5247 で DTLS ハンドシェイクを実行し、ハンドシェイクが成功すると DTLS セッションを確立します。すべてのデータトラフィック（AP からコントローラ、およびコントローラから AP）が暗号化されます。

CAPWAP によって、管理者はワイヤレスネットワーク全体を中央で一元的に管理できます。IW9165E は、コントローラとネットワーク上の他の AP 間の通信に Internet Engineering Task Force（IETF）標準規格の CAPWAP を使用します。

図 *5: WLC* に接続された *CAPWAP AP*



Lightweight アクセス ポイントでの証明書プロビジョニング

LAP で新しい証明書をプロビジョニングするには、CAPWAP モードの間に LAP が新しい署名付き X.509 証明書を取得できる必要があります。そのために、LAP はコントローラに certRequest を送信します。コントローラは CA プロキシとして機能し、CA により署名された LAP 用 certRequest の取得を支援します。

certReq および certResponse は LWAPP ペイロードを使用して LAP に送信されます。

LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動的に再起動します。システムは、次回起動時には LSC を使用するように設定されているため、AP は join 要求の一部として LSC デバイス証明書をコントローラに送信します。join 応答の一部として、コントローラは新しいデバイス証明書を送信し、新しい CA ルート証明書を使用して受信 LAP 証明書も検証します。

次の作業

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニング機能を使用する必要があります。

AP の CAPWAP 接続について

CAPWAP を有効にすると、最初の機能として、ディスカバリフェーズが開始されます。ワイヤレス AP は、ディスカバリ要求メッセージを送信してコントローラを検索します。ディスカバリ要求を受信すると、コントローラはディスカバリ応答を返します。この時点で、この2台のデバイスの間に、CAPWAP 制御メッセージとデータメッセージを交換するための Datagram Transport Layer Security（DTLS）プロトコルを使ったセキュアな接続が確立されます。

AP は CAPWAP ディスカバリメカニズムを使用して、コントローラに CAPWAP 接続要求を送信します。コントローラは AP に CAPWAP 接続応答を送信し、AP がコントローラに接続できるようにします。APがワイヤレスコントローラに接続すると、ワイヤレスコントローラによって AP の構成、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

CAPWAP には、制御とデータの 2 つのチャンネルがあります。AP は制御チャンネルを使用して、設定メッセージの送信、イメージとクライアント鍵のダウンロード、またはコンテキストの受信を行います。現在の実装では、制御チャンネルには単一のウィンドウが設けられます。AP は、コントローラから送信されたすべてのメッセージを単一のウィンドウ内で確認する必要があります。AP は、前の制御パケットの確認応答が終わるまで、次の制御パケットを送信しません。

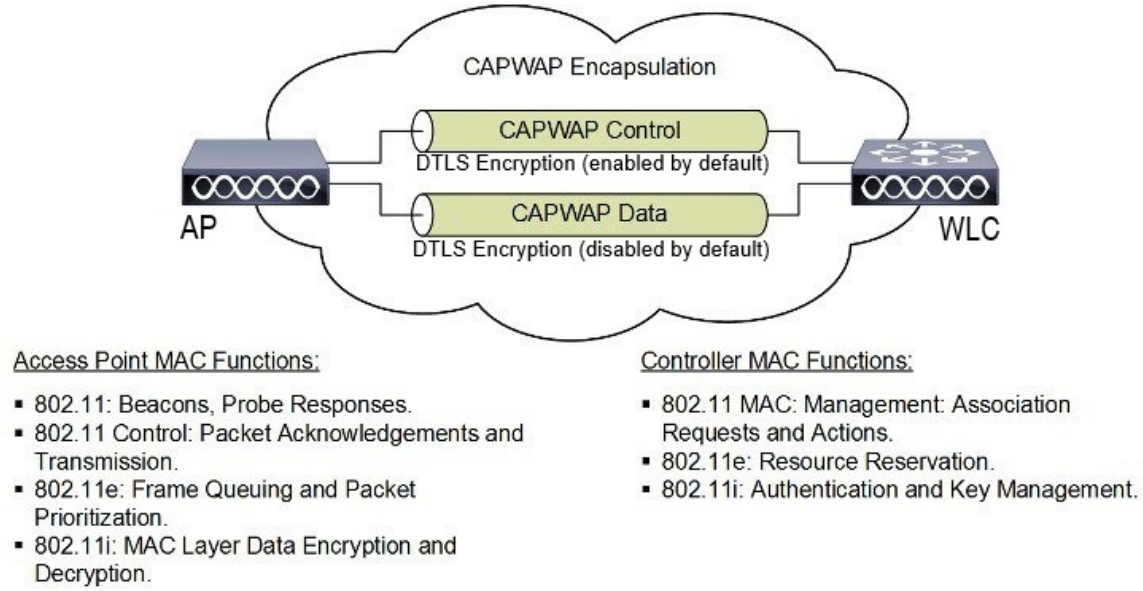
CAPWAP データチャンネルは、AP と WLC 間のユーザーデータトラフィックのカプセル化とトンネリングを担います。これにより、ユーザーデータフローの中央管理が可能になり、WLC はポリシーを適用し、Quality of Service（QoS）を適用し、ワイヤレスネットワーク全体で一貫したセキュリティ対策を確保できます。ユーザーデータは CAPWAP フレーム内でカプセル化され、AP と WLC 間で転送できるようになります。

IETF に従い、CAPWAP は 2 つの動作モードをサポートしています。

- **Split Media Access Control（MAC）**：CAPWAP の主要なコンポーネントの 1 つに、スプリット MAC という概念があります。これは、802.11 プロトコルでの動作の一部を CAPWAP AP が管理し、残りの部分を WLC が管理するというものです。

  スプリット MAC モードでは、CAPWAP プロトコルがすべてのレイヤ 2 ワイヤレスデータおよび管理フレームをカプセル化し、これらのデータやフレームが WLC と AP 間で交換されます。

図 *6 :* スプリット *MAC* アーキテクチャ



- **Local MAC**：ローカル MAC モードでは、データフレームをイーサネットフレームとしてローカルにブリッジまたはトンネリングできます。

  ローカル MAC では、すべてのワイヤレス MAC 機能が AP で実行されます。管理フレームおよび制御フレームの処理を含む完全な 802.11 MAC 機能が AP に常駐します。

どちらのモードでも、AP はレイヤ 2 ワイヤレス管理フレームをローカルで処理してから、コントローラに転送します。

リセットボタンの設定

IW9165E では、（ブートローダがリセット信号を受信した後に）LED が赤色の点滅に変わると、次のリセットアクションが実行されます。デバイスの電源を入れる前に、必ずデバイスのリセットボタンを押します。

- 完全にリセットするには、ボタンを長押し（20 秒未満）します。
- 工場出荷時の状態まで完全にリセットする（FIPS フラグをクリアする）には、ボタンを長押し（20 秒以上 60 秒未満）します。

CAPWAP モードでのイーサネットポートの使用状況

Catalyst IW9165E では、2 つの 2x2 Multiple Input and Multiple Output（MIMO）と 2 つのイーサネットポート（2.5G mGig および 1G）により、最大 3.6 Gbps の物理データレートがサポートされています。

Catalyst IW9165E には、以下の内部ポートマッピングルールがあります。

- Wired0：802.3af、802.3at、802.3bt PoE をサポートする 1 つの mGig（2.5 Gbps）イーサネットポート。

（注） AP のローカルモードや FlexConnect モードでは、wired0 ポートは CAPWAP アップリンクポートとして使用されます。

- Wired1：1Gig イーサネット LAN ポート。

（注） 17.14.1 リリース以降、RLAN 機能は wired1 ポートではサポートされません。

屋内展開の設定

IW9165E は、規制ドメイン -B（米国）、-E（EU）、-A（カナダ）、-Z（オーストラリア、ニュージーランド）の屋内および屋外展開をサポートします。

デフォルトでは、AP の展開モードは屋内です。

-B ドメインでは屋外と屋内の周波数は同じです。

表 *6 :* 無線機の *6G* 出力モードの対応表

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	対応

（注） 屋外モードは屋内で使用できますが、5150 ～ 5350 MHz のチャンネルは -E の国々では屋内のみであるため、屋内モードを屋外で使用することはできません。

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

このコマンドは、AP の再起動を発動します。再起動後に AP がワイヤレスコントローラに登録されたら、対応する国番号を AP に割り当てる必要があります。

屋内展開の確認

WLC で屋内展開が有効になっているかどうかを確認します。

#show ap name <AP_Name> config general | inc Indoor コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor
    AP Indoor Mode                                  : Enabled
```

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor
    AP Indoor Mode                                  : Disabled
```

AP の屋内展開のステータスを確認するには、**show controllers Dot11Radio [1|2]** コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します。

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

（注） コマンド出力の「-Ei」は、屋内モードが有効になっていることを示します。

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します。

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

（注） コマンド出力の「-E」は、屋内モードが無効になっていることを示します。

CLI 出力には、サポートされるチャンネルも表示されます。

AP Radio Slot

Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、Cisco Catalyst IW9165E では、2x2 5GHz Wi-Fi 専用無線機と 5 GHz および 6 GHz のデュアルバンド（XOR）2x2 無線機が使用できます。

Catalyst IW9165E には、5G バンドと 6G バンドを切り替えるオプションがあります。5G バンドと 6G バンドを切り替えるには、次の CLI コマンドを使用します。

```
ap name <ap-name> dot11 dual-band band 6ghz/5ghz
```

（注） デフォルトでは、管理状態は無効です。

スロット 2 の XOR 無線機は 5G に固定されています。

表 *7 : AP Wi-Fi* 無線機アーキテクチャモード

モード	**5 GHz** **スロット 1**	**5/6 GHz** **スロット 2**
5G + 5G	5GHz 2x2:2SS（20/40/80 MHz）	5G 2x2:2SS（20/40/80/160 MHz）
5G + 6G	5GHz 2x2:2SS（20/40/80 MHz）	6G 2x2:2SS（20/40/80/160 MHz）

固定ドメインと国コードのサポート

ROW 規制ドメインにより、特定のドメインがマッピングされていないすべての国コードの製造プロセスのドメイン管理が簡素化されます。この項では、Catalyst IW9165E アクセスポイントの固定ドメインと国コードのサポートについて説明します。

サポートされている固定ドメイン

ドメイン	国番号
A	CA（カナダ）
B	US（米国）

ドメイン	国番号
E	

ドメイン	国番号
	• AT（オーストラリア） • AT（オーストラリア） • BE（ベルギー） • BG（ブルガリア） • HR（クロアチア） • CY（キプロス） • CZ（チェコ共和国） • DK（デンマーク） • EE（エストニア） • FI（フィンランド） • FR（フランス） • DE（ドイツ） • GR（ギリシャ） • HU（ハンガリー） • IS（アイスランド） • IE（アイルランド） • IT（イタリア） • LV（ラトビア） • LI（リヒテンシュタイン） • LT（リトアニア） • LU（ルクセンブルク） • MT（マルタ） • NL（オランダ） • NO（ノルウェー） • PL（ポーランド） • PT（ポルトガル） • RO（ルーマニア） • SK（スロバキア共和国）

ドメイン	国番号
	• SI（スロベニア） • ES（スペイン） • SE（スウェーデン） • CH（スイス）
F	ID（インドネシア）
Q	JP（日本）
Z	• AU（オーストラリア） • NZ（ニュージーランド）

Catalyst IW9165 でサポートされている国コード（ROW）

ドメイン	国番号
ROW	• CL（チリ） • KR（韓国） • GB（英国） • VN（ベトナム）

使用している AP の各国における認可状況については、お客様にご確認いただく必要があります。認可状況および特定の国に関連する規制ドメインの確認方法。詳細については、「Cisco Product Approval Status」[英語] を参照してください。

無線アンテナ配置の設定

Catalyst IW9165E は、RP-SMA（f）コネクタで 4 つの外部アンテナをサポートしています。無線機 1 はアンテナポート 1 および 2 に接続します。無線機 2 はアンテナポート 3 および 4 に接続します。

IW9165E は、6G バンドの Self Identifiable Antenna（SIA）アンテナとの互換性があります。アンテナポート 1 および 3 では、SIA アンテナをサポートできます。アンテナの詳細については、『Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアント ハードウェア設置ガイド』を参照してください。

（注） 初めて SIA アンテナを取り付けた後は、電源を一度切ってから再度オンにする必要があります。

SIA は、アンテナ IW-ANT-OMV-2567-N および IW-ANT-OMH-2567-N のみをサポートします。

表 *8 :* アンテナ利得（*dBm*）

5 GHz スロット 1	5 GHz スロット 2	6 GHz スロット 2
3 4 7 8 10 13 15	3 4 7 8 10 13 15	7

以下の項で、SIA テストを確認するための CLI コマンドについて説明します。

コントローラの SIA ステータスを確認するには、**show ap config slots <AP>** コマンドを実行します。

```
Device#show ap config slot ap_name

show ap config slots AP2CF8.9B1C.CE78
Cisco AP Name : AP4C42.1E51.A144
Attributes for Slot 2
SIA Status       : Present(RPTNC)
SIA Product ID   : IW-ANT-OMV-2567-N
```

6G 標準出力モードの AFC サポート

Cisco Catalyst IW9165E は、自動周波数調整（AFC）6 GHz 標準出力モードをサポートします。標準出力 AP がシステムに接続されます。標準出力を有効にする前に、AP は AFC システムから使用可能な周波数と各周波数範囲の出力を取得する必要があります。

AFC システムは、規制機関（米国の場合は FCC）から提供される情報に基づいて、使用可能な周波数と最大許容出力を計算します。応答がコントローラに返送され、AFC システムから返された許可チャンネルリストに基づいて標準出力チャンネルが AP に割り当てられます。

標準出力 AP は、AFC サービスを通じて調整を行います。AFC は情報にアクセスし、AP の地理位置情報とアンテナの特性に加え、AP の干渉半径をモデル化したトポグラフィック伝達マップを作成します。このマップを使用することで、最大送信電力を割り当て、チャンネル設定を調整または設定して干渉を回避できます。

表 *9 :* 無線機の *6 GHz* 出力モードの対応

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	対応

送信電力の実効等方放射電力（EIRP）は最大 36 dB に制限され、 AFC サービスを通じて AP を調整する必要があります。これらの AP は、-B（米国）ドメインでは、UNII-5（5.925 ～ 6.425 GHz）および UNII-7（6.525 ～ 7.125 GHz）での運用が許可されます。

表 *10 : 6 GHz* 目標出力

経路ごとの導体出力		アンテナ利得	Tx x Rx チェーン	最大 EIRP	最大 EIRP（SP/AFC）
20 ～ 80Mhz	**160Mhz**				
17 dBm	17 dBm	7 dBi*	2 X 2	27 dBm*	36 dBm

AP の AFC ステータスの確認

AP の AFC 要求および応答データを確認するには、**show rrm afc** コマンドを実行します。

```
Device#show rrm afc
Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor axis:
 9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

現在稼働中の出力モードを確認するには、**show controllers dot11Radio 2 | i Radio** コマンドを実行します。

```
Device#show controllers dot11Radio 2 | i Radio
Dot11Radio2     Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

GNSS のサポート

IW9165E では、全地球航法衛星システム（GNSS）がサポートされます。AP は、屋外環境に展開されたデバイスの GPS 情報を追跡し、ワイヤレスコントローラに GNSS 情報を送信します。

AP の GNSS 情報を表示するには、次のコマンドを使用します。

```
ap# show gnss info
```

AP の GPS 位置情報を表示するには、次のコマンドを使用します。

```
controller# show ap geolocation summary
```

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

アンテナ切断検知について

アクセスポイント（AP）の送信機と受信機に複数のアンテナがあると、性能と信頼性が向上します。複数のアンテナによって、受信機側でより強い信号を選択するか、個々の信号を組み合わせることで受信状態が改善します。したがって、障害のあるアンテナやアンテナの物理的な破損を検出することは、AP の信頼性を確保する上で重要です。

アンテナの切断検知機能は、受信機のアンテナ間における信号強度の差分に基づきます。この差分が一定期間に定義された制限を超えると、そのアンテナは問題があると見なされます。

設定した検知期間ごとに、AP はアンテナの状態を伝える Inter-Access Point Protocol（IAPP）メッセージを送信します。このメッセージは、問題が検知された場合に一度だけ送信され、コントローラ トラップ メッセージ、SNMP トラップ、およびコントローラデバッグログに表示されます。

設定ワークフロー

1. AP を設定します。
2. AP プロファイルを設定します。
3. AP プロファイルで機能を有効にします。
4. 機能のパラメータを設定します。
5. 設定を確認します。

ワイヤレスコントローラでのアンテナ切断検知の設定方法について詳しくは、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』を参照してください。

アンテナ切断検知の確認

AP のアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Conroller#sh ap name AP4C42.1E51.A144 config general

Cisco AP Name   : AP4C42.1E51.A144
================================================

Cisco AP Identifier                             : 8c84.4292.f840
Country Code                                    : Multiple Countries :
US,CN,GB,HK,DE,IN,CZ,NZ
Regulatory Domain Allowed by Country            : 802.11bg:-ACE^   802.11a:-ABCDEHNSZ^
  802.11 6GHz:-BEZ^
Radio Authority IDs                             : None
AP Country Code                                 : CZ  - Czech Republic
AP Regulatory Domain
  802.11bg                                      : -E
  802.11a                                       : -E
MAC Address                                     : 8c84.4292.f840
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.33.3
IP Netmask                                      : 255.255.255.0
```

```
Gateway IP Address                              : 9.9.33.1
Fallback IP Address Being Used                  :
Domain                                          :
Name Server                                     :
CAPWAP Path MTU                                 : 1485
Capwap Active Window Size                       : 1
```

APプロファイルのアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Controller#show ap profile name ap-profile detailed

AP Profile Name: ap-profile
.
.
.
AP broken antenna detection:
  Status                                                : ENABLED
  RSSI threshold                                        : 40
  Weak RSSI                                             : -80
  Detection Time                                        : 120
```

トラブルシューティング

このドキュメントでは、アクセスポイント（AP）とワイヤレスコントローラ間の Control And Provisioning of Wireless Access Points（CAPWAP）/Lightweight Access Point Protocol（LWAPP）トンネルが切断される理由を理解するためのユースケースを紹介します。詳細については、「コントローラからのアクセスポイントの関連付け解除のトラブルシューティング」を参照してください。

（注） ソフトウェアまたはハードウェアの変更により、コマンドが動作しなくなったり、構文が変更されたり、リリースによって GUI や CLI の見た目が異なったりする場合があります。

フィードバックのリクエスト

ユーザー入力が役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始

されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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