# WIM の一般的な展開モード

この章は、次の項で構成されています。



## 一般的な導入シナリオ

ここでは、WIM の展開に関する一般的なシナリオをいくつか説明します。

ワイヤレス インターフェイス モジュールは、機能面で Cisco Catalyst シリーズ 9105AXI アクセスポイントとよく似ています。

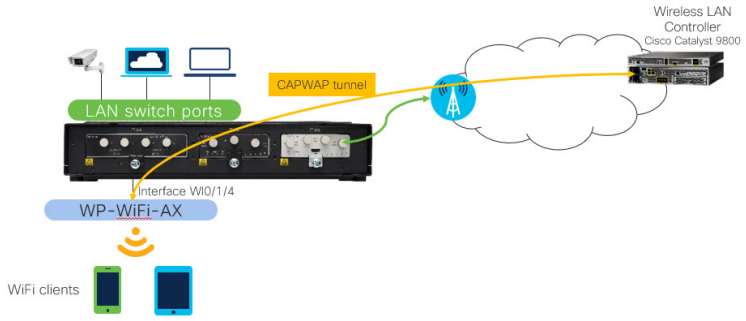
ホストルータのワイヤレス挿入モジュールとして、ワイヤレスアクセスポイント（CAPWAP APモード）として機能するWIMモジュールのプロビジョニングをサポートできます。これにより、ルータはWi-Fiワイヤレスクライアントにネットワークアクセスを提供でき、同時に中央ワイヤレスコントローラによって AP 機能を管理できます。AP 機能を管理するための中央ワイヤレスコントローラを展開しない場合は、EWC モードで WIM を展開できます。この場合、ホストルータはワイヤレスクライアントにネットワークアクセスを提供でき、同時にローカル EWC コントローラによって AP 機能を管理できます。

WGBモードで動作するようにWIMをプロビジョニングすると、ホストルータの設定により、Wi-Fiワイヤレス接続をバックホールリンク候補として使用できます。17.11.1 UIW ソフトウェアの機能拡張により、ホストルータは 1 つの無線機を WGB バックホール用に、もう 1 つの無線機をワイヤレス クライアント アクセス用に使用できるようになります。

# Control And Provisioning of Wireless Access Points（CAPWAP）

アクセス ポイントでは、コントローラとネットワーク上のその他のワイヤレス アクセス ポイント間の通信に、標準の Control and Provisioning of Wireless Access Points Protocol（CAPWAP）を使用します。アクセスポイントの役割を果たす WP-WIFI6 は、有線 LAN に直接接続され、無線ユーザーへの接続ポイントとして機能します。

CAPWAP モードに使用されるイメージは ap1g8-k9w8 です。




## IR1800 で CAPWAP アクセスポイント構成を設定するための前提条件

アクセス ポイントをネットワークでアクティブにするには、コントローラがそのアクセス ポイントを検出する必要があります。CAPWAP はレイヤ 2 をサポートしていません。アクセス ポイントでは、レイヤ 3、DHCP、DNS、または IP サブネットのブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。

ここでは、WIM CAPWAP AP がコントローラと通信するための、DHCP サーバーとルータの SVI インターフェイスの基本設定を示します。追加の NAT、ドメインネームシステム（DNS）、およびその他のルーティング設定の変更については、IR1800 設定ガイド [英語] を参照してください。

（注） AP がすでに CAPWAP モードになっている場合、AP はリブートしません。AP が EWC または WGB モードの場合、モードが CAPWAP に変更されてから AP がリブートします。

## IR1800 での CAPWAP アクセスポイント構成設定手順

次のステップを実行します。

| ステップ | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **ip dhcp pool** *name*<br>**network** *ip address subnet mask*<br>**default-router***ip address*<br>**dns-server** *ip address*<br>**option 43 hex** <*value*><br>例：<br>`Router(config)#ip dhcp pool wireless`<br>`Router(dhcp-config)#network 10.10.10.0 255.255.255.0`<br>`Router(dhcp-config)#default-router 10.10.10.1`<br>`Router(dhcp-config)#dns-server 192.0.2.1`<br>`Router(dhcp-config)#option 43 hex f108c0a80a05c0a80a14` | スイッチ仮想インターフェイス（SVI）に使用される IP アドレスの DHCP サーバーアドレスプールを作成します。ステップ 4 を参照してください。<br>プールのデフォルトゲートウェイとドメインネームシステム（DNS）サーバーアドレスを割り当てます。 |
| ステップ 2 | **interface GigabitEthernet** *slot/subslot/port*<br>**ip address dhcp**<br>**ip nat outside**<br>例：<br>`Router(config)#interface GigabitEthernet 0/0/0`<br>`Router(config-if)#ip address dhcp`<br>`Router(config-if)#ip nat outside` | ルータのアップリンク WAN ポートの IP アドレスを設定し、NAT コマンドを使用してインターフェイスを外部ネットワークに接続します。 |
| ステップ 3 | **interface Wlan-GigabitEthernet** *slot/subslot/port*<br>**switchport mode trunk**<br>**switchport trunk native vlan** *number*<br>例：<br>`Router(config)#interface Wlan-GigabitEthernet 0/1/4`<br>`Router(config-if)#switchport mode trunk`<br>`Router(config-if)#switchport trunk native vlan 10` | WIM 内部スイッチインターフェイスのスイッチポートモードとネイティブ VLAN を設定します。ネイティブ VLAN は AP 管理 VLAN である必要があります。 |
| ステップ 4 | **interface vlan** *number*<br>**description** <*name*><br>**ip address** *ip-address subnet_mask*<br>**ip nat inside**<br>例：<br>`Router(config)#interface vlan 10`<br>`Router(config-if)#description Wireless`<br>`Router(config-if)#ip address 10.10.10.1 255.255.255.0`<br>`Router(config)#ip nat inside` | スイッチ仮想インターフェイス（SVI）を作成し、DHCP プールから IP アドレスを割り当て、インターフェイスを内部ネットワークに接続します。 |

| ステップ | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **ip route 10.10.10.10 10.10.10.10** *default gateway ip-address*<br>例：<br>`Router(config)#ip route 10.10.10.10 10.10.10.10 192.0.2.1` | すべてのトラフィックをルータのデフォルトゲートウェイに転送します。 |
| ステップ 6 | **ip nat inside source list** *number* **interface GigabitEthernet** *slot/subslot/port* **overload**<br>**ip access-list standard** *number*<br>*number* **permit** *ip address wildcard mask*<br>例：<br>`Router(config)#ip nat inside source list 10 interface GigabitEthernet 0/0/0 overload`<br>`Router(config)#ip access-list standard 10`<br>`Router(config)#10 permit 10.10.10.0 0.0.0.255` | アクセスリストを指定して、動的送信元変換を確立します。<br>トラフィックを許可または拒否する ACL を作成します。 |

# アクセスポイントの設定と配置

ワイヤレス インターフェイス モジュールが CAPWAP モードで実行されている場合、モジュールに IP アドレスが設定されると、Cisco 9800 シリーズなどの WLC を介して通信し、管理されます。設定プロセスは、コントローラで行います。

CAPWAP とシスコ ワイヤレス LAN の詳細については、次の資料を参照してください。

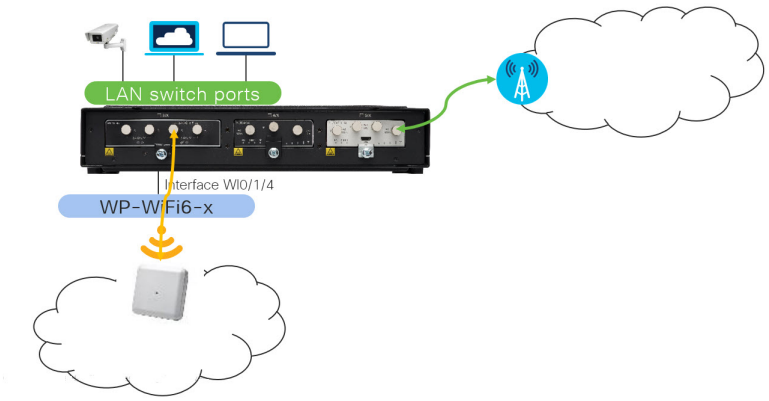
- Configure DHCP OPTION 43 for Lightweight Access Points Guide [英語]
- Cisco Catalyst 9800 Series Configuration Best Practices
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x [英語]

# ワークグループブリッジ（WGB）

ワークグループブリッジ（WGB）のシナリオでは、次のことが可能になります。

- 低コスト、高速 Wi-Fi アップリンク
- 1 つの無線機のみに uWGB または WGB モードでの動作が許可される
- WGB は最大 20 の有線クライアントをサポート
- uWGB は単一のクライアント MAC アドレスをサポート（Wl0/1/4 が、バックホールリンクである Wi-Fi のルーテッドインターフェイスである設定における、VLAN10 インターフェイスなど）

重要　IR1800 の WGB モードは、固定型の展開でのみ推奨されます。




ワークグループ ブリッジ モードは、インフラストラクチャ Wi-Fi を介したデータオフロードに使用される特殊なモードです。このモードで実行中の WIM は、ワイヤレスステーションのように動作します。通常、（ギガビットポートを介して WIM に接続されている）有線クライアントをワイヤレス インフラストラクチャにブリッジするために使用されます。

このモードを使用するシナリオの例として、IR1800 の有線イーサネットポートに接続されているカメラやその他のデバイスに Wi-Fi バックホールを提供する場合が考えられます。WGB モードは、ワイヤレスインフラストラクチャがシスコ製であることが前提条件となりますので、ご注意ください。

Cisco IOS-XE リリース 17.8.1 以降、WIM でユニバーサル WGB モードがサポートされます。

ユニバーサル WGB（uWGB）は、uWGB に接続された有線クライアントとシスコおよびシスコ以外のワイヤレスネットワークを含むワイヤレスインフラストラクチャとの間のワイヤレスブリッジとして機能する WGB 機能の補完モードです。

WGB および uWGB の設定の詳細については、次を参照してください。

Cisco Wave 2 Access Points as Workgroup Bridges [英語]

Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide [英語]

# IR1800 で WGB を設定するための前提条件

ここでは、有線クライアントとインフラストラクチャ Wi-Fi トラフィックをブリッジする IR1800 の基本設定を示します。NAT、ACL、およびその他特定の設定については、IR1800 設定ガイド [英語] を参照してください。

| ステップ | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **vlan** *number-number*<br>例：<br>`Router(config)#vlan 2001-2002` | さまざまな有線クライアントトラフィック用VLANとして固有のVLANを作成します。<br>有線クライアントプリンタ用のVLAN 2001。<br>ビデオカメラ用の VLAN 2002。 |
| ステップ 2 | **interface Wlan-GigabitEthernet** *slot/subslot/port*<br>**switchport mode trunk**<br>**switchport trunk allowed vlan** *number*<br>例：<br>`Router(config)#interface Wlan-GigabitEthernet 0/1/4`<br>`Router(config-if)#switchport mode trunk`<br>`Router(config-if)#switchport trunk allowed vlan 2001-2002` | **Wlan-GigabitEthernet** コマンドを使用して、内部スイッチインターフェイスの Wi-Fi カードを接続します。スイッチポートモードと、許可された有線クライアントトラフィック VLAN パススルーを設定します。 |
| ステップ 3 | **interface GigabitEthernet** *slot/subslot/port*<br>**description** *name*<br>**switchport mode trunk**<br>**switchport trunk native vlan** *number*<br>**interface GigabitEthernet** *slot/subslot/port*<br>**description** *name*<br>**switchport mode access**<br>**switchport access vlan** *number*<br>例：<br>`Router(config)#interface GigabitEthernet 0/1/0`<br>`Router(config-if)#description Printer`<br>`Router(config-if)#switchport mode trunk`<br>`Router(config-if)#switchport trunk native vlan 2001`<br>`Router(config)#interface GigabitEthernet 0/1/1`<br>`Router(config-if)#description Camera`<br>`Router(config-if)#switchport mode access`<br>`Router(config-if)#switchport access vlan 2002` | 有線クライアント接続ポートごとにスイッチポートモードと VLAN を設定します。 |

# WGB の設定と展開

ここでは、WP-WIFI6 モジュールに必要な最低限の WGB CLI 設定を示します。モード間の変換のガイダンスに従って、まず WP-WIFI6 モジュールを WGB で起動します。WGB の詳細な設定については、『Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide』[英語] を参照してください。

手順

**ステップ 1** SSID プロファイルを設定します。

**例**：

```
WIM-WGB# configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

**ステップ 2** 無線インターフェイスを WGB モードに設定し、SSID プロファイルをマッピングします。ワイヤレス インフラストラクチャにより規定された認証を選択します。

**例**：

```
WIM-WGB# configure dot11Radio 1 mode wgb ssid-profile Test
WIM-WGB# configure dot11Radio 1 encryption mode ciphers aes-ccm
WIM-WGB# configure dot11Radio 1 enable
```

**ステップ 3** 未使用の無線機をルート AP として設定し、オフにします。本稿執筆時点では、WGB は単一の無線機を使用します。

**例**：

```
WIM-WGB# configure dot11Radio 0 mode root-ap
WIM-WGB# configure dot11Radio 0 disable
WIM-WGB# configure wgb antenna band mode single
```

**ステップ 4** WIM で **show configuration** を使用して、WGB の基本設定を確認します。

**例**：

```
WIM-WGB# show configuration
AP Name : WIM-WGB
AP Mode : WorkGroupBridge
SSH State : Enabled
AP Username : Cisco1
Syslog Host : 0.0.0.0

Radio and WLAN-Profile mapping:-
===================================
Radio ID Radio Mode SSID-Profile SSID Authentication
-------------------------------------------------------------------------------------------------------------
1 WGB Test Free PSK

Radio configurations:-
==============================
Radio Id : 0
Admin state : DISABLED
Mode : RootAP
Radio Id : 1
Admin state : ENABLED
Mode : WGB

WGB specific configuration:-
===================================
WGB Radio Id : 1
Mode State : Enable
SSID Profile : Test

Antenna Band Mode : Single
```

**ステップ 5** WIM で **show wgb dot11 associations** コマンドを使用して、WGB アソシエーションの **Uplink State** と **RSSI** を確認します。

**例：**

```
WIM-WGB# show wgb dot11 associations

Uplink Radio ID : 1
Uplink Radio MAC : BC:E7:12:0C:FF:6F
SSID Name : Free
Connected Duration : 0 hours, 0 minutes, 5 seconds
Parent AP Name : AP60E6.F0D4.4E34
Parent AP MAC : 60:E6:F0:D4:4A:6A
Uplink State : CONNECTED
Auth Type : PSK
Key management Type : WPA2
Dot11 type : 11ax
Channel : 124
Bandwidth : 40 MHz
Current Datarate : 6 Mbps
Max Datarate : 573 Mbps
RSSI : 40
IP : 192.168.56.107/24
Default Gateway : 192.168.56.1
DNS Server1 : 192.168.71.2
Domain : iottest.local
IPV6 : ::/128
Assoc timeout : 5000 Msec
Auth timeout : 5000 Msec
Dhcp timeout : 60 Sec
Country-code : US
```

**ステップ 6** WIM で **show wgb bridge** コマンドを使用して、ブリッジテーブルから WGB の **wired client mac**、**IP**、**vlan id** を確認します。

**例：**

```
WIM-WGB# show wgb bridge
***Client ip table entries***
mac vap port vlan_id seen_ip confirm_ago fast_brg
60:E6:F0:D4:4A:6A 0 wbridge1 0 0.0.0.0 24.082000 true
E4:62:C4:49:96:F4 0 wired0 2256 192.168.56.108 6.668000 true
```

# uWGB の設定と展開

ここでは、WP-WIFI6 モジュールに必要な最低限の uWGB 設定を示します。モード間の変換に記載されている手順に従って、まず WP-WIFI6 モジュールを WGB で起動します。uWGB の詳細な設定については、『Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide』[英語] を参照してください。

0/3 へのセッションを開始したら、**show configuration** を確認します。次の内容を参照してください。

- 2.4GHz 無線機（dot11 radio 0）がオフになっている
- 5GHz 無線機（dot11 radio 1）がサードパーティの AP に接続するように設定されている

（注） 2.4GHz または 5GHz のいずれかを uWGB モードに設定できます。

次に、サードパーティアプリケーションに接続するための uWGB 設定手順の概要を示します。

手順

**ステップ 1** SSID プロファイルを設定します。

例：

```
configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

**ステップ 2** 無線インターフェイスを uWGB モードに設定し、SSID プロファイルをマッピングします。ワイヤレス インフラストラクチャにより規定された認証を選択します。次の例では、c44d.849b.0a8c は、インフラからアドレスを取得する uWGB 有線クライアントデバイスの MAC アドレスです。

例：

```
configure dot11radio 1 mode uwgb c44d.849b.0a8c ssid-profile Test
configure dot11radio 1 encryption mode ciphers aes-ccm
configure dot11radio 1 enable
```

**ステップ 3** 未使用の無線機をルート AP として設定し、オフにします。本稿執筆時点では、uWGB は単一の無線機を使用します。

例：

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

## uWGB 設定例

次に、uWGB の設定例を示します。

```
APBCE7.120C.DAA8#show config
AP Name              : APBCE7.120C.DAA8
AP Mode              : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring : Enabled
SSH State            : Disabled
AP Username          : Cisco
Session Timeout      : 300

Radio and WLAN-Profile mapping:
=====================================
Radio ID   Radio Mode   SSID-Profile   SSID   Authentication
1          UWGB         Test           Free   PSK

Radio Configuration:
Radio Id           : 0
  Admin state      : DISABLED
  Mode             : RootAP
  Beacon Period    : 100 mSec
```

```
Radio Id           : 1
  Admin state      : ENABLED
  Mode             : UWGB
  Uclient mac      : C44D.849B.0A8C
  Current state    : WGB
  UClient timeout  : 0 Sec
  Dot11 type       : 11ax
  Encryption mode  : AES128

WGB specific configuration:
====================================
WGB Radio Id         : NA
  Mode State         : NA
  SSID Profile       : NA
UWGB Radio Id        : 1
  Mode Enable        : Enable
  SSID Profile       : Test
  Uclient MAC Address: C44D.849B.0A8C
```

IR1800 に接続されている有線デバイスを確認します。

```
#show wgb bridge
***Client ip table entries***
mac vap                 port  vlan_id   seen_ip       confirm_ago  fast_brg
10:DD:B1:CE:B2:E6       0     wired0    192.168.10.25 0.016000      true
```

アソシエーションを確認します。次の例では、uWGB ステータスを表示するためには、クライアントが接続されている必要があります。有線クライアントからまたは有線クライアントへのトラフィックがない場合は、WGB にフォールバックします。

```
#show wgb dot11 associations
Uplink Radio ID       : 1
Uplink Radio MAC      : BC:E7:12:0C:F1:CF
SSID Name             : Free
Parent AP MAC         : 08:02:8E:8D:52:9A
Uplink State          : CONNECTED
Auth Type             : PSK
Key management Type   : WPA2
Uclient mac           : C4:4D:84:9B:0A:8C
Current state         : UWGB
Uclient timeout       : 60 Sec
Dot11 type            : 11ac
Channel               : 36
Bandwidth             : 80 MHz
Current Datarate      : 433 Mbps
Max Datarate          : 1200 Mbps
RSSI                  : 53
IP                    : 0.0.0.0
IPV6                  : ::/128
Assoc timeout         : 5000 Msec
Auth timeout          : 5000 Msec
Dhcp timeout          : 60 Sec
```

# uWGB または WGB アップリンクとルート AP モードの無線機の同時使用

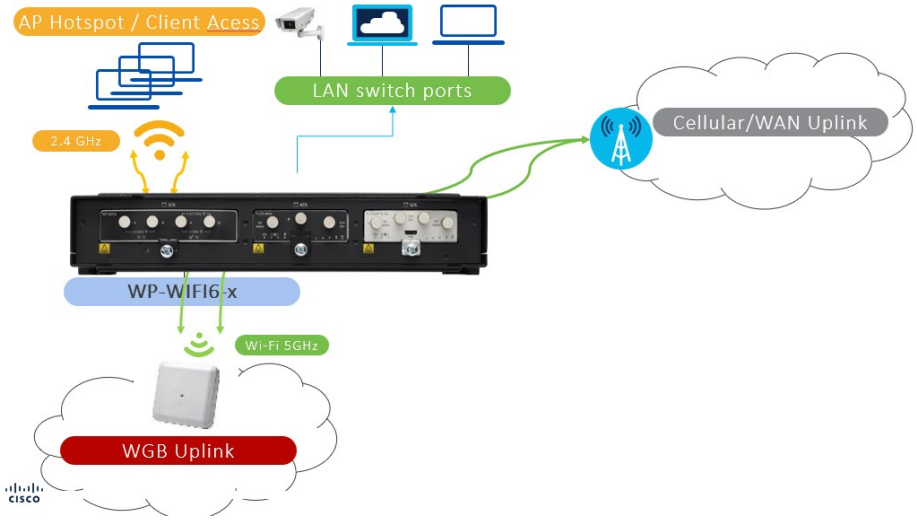
Cisco IOS XE 17.11.1 では、新たな Unified Industrial Wireless イメージ（ap1g8t-k9c1）による WGB アップリンクとルート AP モードの無線機の同時使用機能が導入されました。1 つ目の無

線機を WGB アップリンク（2.4G または 5G）に設定し、2 つ目の無線機をローカル ワイヤレス クライアント用の WGB ルート AP モード（ホットスポット Wi-Fi とも呼ばれる）に設定して個別にサービスを提供するか、両方の無線機をルート AP モードに設定できます。

17.14.1 以降、Wi-Fi モジュールは無線機の同時使用に対応し、一方の無線機は uWGB モードのアップリンクバックホールとして機能し、もう一方はルート AP 無線機として機能します。

この機能により、WLAN-VLAN マッピングが異なるワイヤレス クライアント トラフィックを内部イーサネットポートにブリッジできます。IR1800 ルータは、用途と設定に応じて、これらのワイヤレス クライアント トラフィックを異なるアップリンクにルーティングおよび転送します。

一般的な用例については、次の図を参照してください。




**ルート AP 無線機（2 つ目の無線機）に接続されたワイヤレスクライアントのトラフィックフロー：**

- クライアントにサービスを提供する無線機のトラフィックは、ワイヤレスバックホールに直接ブリッジされません。
- ワイヤレスクライアントのトラフィックは、内部 gig0 を介して統合ルータにブリッジされます。
- ワイヤレスクライアントは、ルータの内部 DHCP サーバーから DHCP を介して IP アドレスを取得します。
- その後、ルータを NAT/ip ルートで設定して、それに応じてワイヤレスクライアントからインフラストラクチャ ネットワークにパケットをルーティングし、トラフィックを転送できます（用途による）。

**無線機の同時使用が対応するシナリオとワイヤレスクライアント数の上限**：

Wi-Fi モジュールの端末接続を担っている無線機に関連づけられ認証されたワイヤレスクライアントは、それらがローカルに接続されてることから、インフラのルート AP には決して更新されません。

1. シナリオ 1
   - 無線機 0：WGB モードに設定中。ステータス：Disabled（アップリンク無線機が無効）
   - 無線機 1：ルート AP モード。最大 100 のワイヤレスクライアントを接続可能
2. シナリオ 2
   - 無線機 0：WGB モードに設定中。ステータス：Enabled（アップリンクが有効）
   - 無線機 1：ルート AP モード。100 のワイヤレスクライアントをサポート
3. シナリオ 3
   - 無線機 0：ルート AP モード。100 のワイヤレスクライアントをサポート
   - 無線機 1：ルート AP モード。100 のワイヤレスクライアントをサポート

（注） 上記のシナリオでは、ルート AP 無線機と WGB アップリンク無線機は、要件に応じて無線機 0 または無線機 1 に設定できます。

# 無線機の同時使用に必要なルータ設定

ここでは、必要な設定を表示するためのコマンドの例を示します。

**IR1800 でのアップリンク VLAN の設定**：

アップリンク VLAN に固有の MAC 設定は、WP-WIFI6 への（および WP-WIFI6 からの）パケットのトラバース効率を高めるため、IR1800 では必須の設定です。次に、例を示します。

```
interface Vlan119            ->This is the interface that can carry the data from local
 network to the infrastructure n/w.
 mac-address c014.fe60.ef8d   ->unique mac address configuration
 ip address dhcp              ->Uplink VLAN gets ip from infra via DHCP
 ip nat outside               ->This config should be done to NAT the downlink/wireless
 client traffic from vlan 4094 to vlan 119
```

（注） Gig0/0/0 MAC アドレス + 4 によって、固有の MAC アドレスが作られます。

アップリンクに uWGB を使用する場合は、uWGB 設定 CLI の実行時に、[wired client mac] として固有の MAC アドレスを指定する必要があります。

configure dot11radio <0/1> mode uwgb <*c014.fe60.ef8d*> *ssid-profile* <*ssid profile name*>

MAC アドレスを取得するには、**show int GigabitEthernet0/0/0** コマンドを使用します。

```
Router#show int GigabitEthernet0/0/0
GigabitEthernet0/0/0 is administratively down, line protocol is down
  Hardware is IR1821-1x1GE, address is c014.fe60.ef80 (bia c014.fe60.ef80)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is Auto Select
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

次に、WGB ブリッジテーブルの出力例を示します。

```
AP84EB.EF55.1438#sh wgb bridge
    ***Client ip table entries***
mac vap            port  vlan_id     seen_ip              confirm_ago     fast_brg
A0:E7:0B:D5:99:95  12    apr0v12     4094  192.168.94.13   158.708000      true
76:68:82:01:86:C9  13    apr0v13     4094  192.168.94.2    0.000000        true
C0:14:FE:60:EF:8D  0     wired0      0     10.119.119.229  1.814000        true
```

（注） ブリッジテーブルエントリでは、アップリンク VLAN（119）に基づく SVI/有線クライアントと、ダウンリンク VLAN に基づくワイヤレスクライアントのみが学習されます。ダウンリンク VLAN（4094）に基づく SVI アドレスは、ここでは学習されません。IR1800 に設定されたアップリンク VLAN（VLAN 119）は、ネイティブ VLAN であるため、VLAN ID「0」として学習されます

**IR1800 でのダウンリンク VLAN の設定**：

次の例を参照してください。

```
interface Vlan4094           ->Downlink VLAN for wireless client traffic
  ip address 192.168.94.1 255.255.255.0
  ip nat inside            ->Should be provided in the local network VLAN to communicate
 with infrastructure VLAN
```

**ダウンリンク VLAN インターフェイスの DHCP プール設定**：

次の例を参照してください。

```
ip dhcp pool vlan4094  -> Downlink VLAN's are the used for wireless client(Root ap:
WLAN-VLAN mapping)
  network 192.168.94.0 255.255.255.0
  default-router 192.168.94.1
  dns-server 8.8.8.8
```

**Wl0/1/4 ポート設定**：

次に、Wl0/1/4 ポートの設定例を示します。AP をルータに接続する内部 Gig0 ポートです。

```
interface Wlan-GigabitEthernet0/1/4
  switchport trunk native vlan 119
  switchport trunk allowed vlan 119,4094
  switchport mode trunk
```

（注） vlan 119 は WBG アップリンク VLAN、vlan 4094 はワイヤレスクライアントのトラフィックに使用されるダウンリンク VLAN です。

**NAT ACL の設定**：

次に、NAT ACL ルールを作成するための設定例を示します。

```
ip access-list extended NAT_ACL
  10 permit ip 192.168.94.0 0.0.0.255 any
//subnet of Downlink VLAN 4094 interface
   route-map RM_WGB_ACL permit 10   ->Used for Routing table mapping
   match ip address NAT_ACL         ->NAT list used for translation
   match interface Vlan119          ->NAT interface (infrastructure VLAN)
```

**外部ネットワークと通信するためのルートマップ**：

```
ip nat inside source route-map RM_WGB_ACL interface Vlan119 overload
```

（注） その他のルータトポロジのシナリオについては、『Cisco Connected Mass Transit System Implementation Guide (Cisco Validated Design)』を参照してください。

# 無線インターフェイスの WGB/uWGB モードおよびルート AP モードへの設定

ワイヤレスクライアントのサポートには、さまざまな項目の管理設定が必要です。この機能をサポートするには、次の CLI を使用します。

### CAPWAP モードからユニファイド WGB モードに設定する

次のコマンドを使用します。

```
configure boot mode wgb
```

### 無線インターフェイスで WGB アップリンクまたはルート AP の SSID を設定する

次のコマンドを使用します。

```
configure ssid-profile <profile-name> ssid <ssid-name>
authentication <auth-type> key-management <key-mgmt>
```

### 無線機を WGB モードに設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> mode wgb ssid-profile <ssid profile name>
configure dot11Radio <0|1> enable
```

### 無線機を uWGB モードに設定する

次のコマンドを使用します。

```
configure dot11Radio<0|1>mode uwgb <client mac> ssid-profile<ssid profile name>
```

（注） <client mac> - uWGB がアップリンクの場合、uWGB 設定 CLI の実行時に、ルータ SVI または PC 有線クライアント MAC 固有の MAC アドレスを <wired client mac> として指定できます。

アップリンクバックホールが uWGB モードの場合に同時ルート AP 無線機モードを機能させるには、CLI でルータスイッチ仮想インターフェイス（SVI）固有の MAC アドレスを「wired client mac」として指定します。この手順により、Wi-Fi モジュールが uWGB モードに設定されている間、ルータ SVI が IP アドレスを取得できるようになります。ルータ SVI はアップリンク VLAN になり、IP ルーティングまたは NAT 設定が適用されると、ワイヤレスクライアントなどのダウンリンク VLAN からのパケットを転送できるようになります。

詳細については、「無線機の同時使用に必要なルータ設定」を参照してください。

### 無線機をルート AP モードに設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> mode root-ap
```

### SSID を VLAN ID を含めてルート AP モードの無線インターフェイスにマッピングする

次のコマンドを使用します。

```
configure dot11Radio <0|1> wlan add <profile-name> <wlan id> vlan <vlan-id>
```

（注） 上記のコマンドでは、クライアントにサービスを提供する無線機での VLAN の作成が wired0 にブリッジされるため、ワイヤレスクライアントからのトラフィックがルータに直接転送されます。WLAN ID の範囲は 2 ～ 16 です（最大 15 の WLAN をサポート）。

ルート AP 関連の設定は、ルート AP 無線機を切り替えてはじめて保存され、有効になります。

WGB のブロードキャストタギングが有効になっている場合、ルート AP はワイヤレスクライアント接続をサポートできません。ブロードキャストタギング設定は、デフォルトで無効になります。

```
configure dot11Radio <0|1> wlan delete <profile-name>
```

### ルート AP 無線インターフェイスの SSID をブロードキャストするよう無線チャンネルを設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> channel <channel number> <width>
```

（注） 設定済みのチャンネルでレーダーが検出された場合、そのチャンネルは自動的に変更され、設定したチャンネルには戻りません。

### 無線インターフェイスのアンテナの設定

次のコマンドを使用します。

```
configure dot11Radio <0|1> antenna <dot11 antenna a/ab>
```

### QoS プロファイルを設定して SSID プロファイルにアタッチする（オプション）

次のコマンドを使用します。

```
configure qos profile <qos-prof-name> <bronze|gold|platinum|silver> configure ssid-profile
<profile-name> ssid <ssid> qos profile <qos-prof-name>
```

### 802.11 のタイプの有効化または無効化

次のコマンドを使用します。

```
configure dot11radio <slot-id> 802.11ax <enable/disable>
configure dot11radio <slot-id> 802.11n <enable/disable>
configure dot11radio <slot-id> 802.11ac <enable/disable>
```

### 出力制限とチャンネルのスイッチ数の設定

次のコマンドを使用します。

**configure dot11radio** *<slot-id>* **802.11h power-constraint** *<value>* **channel-switch-count** *<value>*

### 無線インターフェイスの tx-power の設定

次のコマンドを使用します。

**configure dot11Radio** *<0|1>* **tx-power** *<1-8>*

## uWGB をアップリンクバックホールとして使用する場合のルート AP の無線機設定例

次に、uWGB をアップリンクバックホールとして使用する場合のルート AP の無線機設定例を示します。

```
WIFI module uWGB configuration:
==============================
AP6879.0974.F728#sh running-config
AP Name : AP6879.0974.F728
AP Mode : WorkGroupBridge
CDP State : Enabled
Watchdog monitoring : Enabled
SSH State : Enabled
AP Username : admin
Session Timeout : 0
WGB Trace : Disabled
Syslog Host : 0.0.0.0

Radio and WLAN-Profile mapping:-
===================================
Radio ID Radio Mode SSID-Profile SSID
Authentication
0 RootAP root_wlan root_wlan
OPEN
1 UWGB Test Test
OPEN

Radio configurations:-
==============================
Radio Id : 0
Admin state : ENABLED
Mode : RootAP
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Channel(Band) : 1 (20)
Beacon Period : 100 mSec
Tx Power : 1
802.11ac : Disabled
802.11ax : Enabled
802.11n : Enabled
Encryption mode : AES128
Radio Id : 1
Admin state : ENABLED
Mode : UWGB
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Uclient mac : C014.FE60.EF8D
```

```
Current state : UWGB
UClient timeout : 0 Sec
Dot11 type : 11ax
11v BSS-Neighbor : Disabled
A-MPDU priority : 0x3f
A-MPDU subframe number : 255
RTS Protection : 2347(default)
Rx-SOP Threshold : AUTO
Radio profile : NA
Encryption mode : AES128

List of Root-AP SSID-Profiles:
=======================================
Radio id : 0, SSID-Profile_8 : root_wlan

WGB specific configuration:-
===================================
WGB Radio Id : NA
Mode State : NA
SSID Profile : NA
UWGB Radio Id : 1
Mode Enable : Enable
SSID Profile : Test
Uclient MAC Address: C014.FE60.EF8D

Password Policy configured:-
===================================
password policy : Enable
password minimum length : 8
password lifetime : Disable
Upper Case Required : 1
Lower Case Required : 1
Digit Required : 1
Special Character Required : 1

Rx Beacon Missing Action : Enable
Rx Beacon Missing Count : 100
Packet retries Action : Reconnect
Packet retries Value : 64
RSSI Threshold Value : 70 dBm
Threshold timeout : 5 Sec
HSR-Scan status : Disable
Auth response timeout : 5000 Msec
Assoc response timeout : 5000 Msec
11v neighbor query timeout : 10 sec
WGB channel scan timeout : 20 Msec
Dhcp response timeout : 60 Sec
EAP timeout : 3 sec
Bridge table aging-time : 300 Sec
Probe pak data rate type : NA
Probe pak data rate : 0
Antenna Band Mode : Dual
Broadcast tagging : Disable
Wired Client 802.1x Auth : Disable
IGMP querier IP address : ::
Offchan scan status : Disable

Total configurations size on different structure:-
=====================================================
Total channels : 0
Total SSID-Profiles : 3
Total Root-AP SSID-Profile : 1
```

```
Total EAP Profiles : 0
Total QOS Profiles : 0
Total dot1x credentials : 0
Total PKI truspoints : 0
Total bridge groups : 0


Total SSID profiles configured are:
=========================================
SSID-Profile : Test
SSID Name : Test
SSID Profile path : /data/platform/wbridge/Test
Auth type : OPEN
DTIM Period : 1
QOS profile :
SSID-Profile : root_wlan
SSID Name : root_wlan
SSID Profile path : /data/platform/wbridge/root_wlan
Auth type : OPEN
DTIM Period : 1
QOS profile :


L2NAT Configuration are:
===================================
Status: disabled
Default Vlan: 0
The Number of L2nat Rules: 0
Dir Inside Outside Vlan


Ethernet Port Native VLAN Configuration are:
===================================
Ethernet Port: 0
Status: disabled
Native VLAN ID: 0
Ethernet Port: 1
Status: disabled
Native VLAN ID: 0


Total QoS Mapping profiles configured are:
=========================================
Number of QoS Mapping Profiles: 0


Configuration command list:
============================
### WGB Running config - Hostname: AP6879.0974.F728 ###
configure ap management add username admin password $1$$khxfBj0qAAV4gFMFboJcg. s
ecret $1$$khxfBj0qAAV4gFMFboJcg.
configure ssid-profile Test ssid Test authentication open
configure ssid-profile root_wlan ssid root_wlan authentication open
configure dot11Radio 1 mode uwgb C014.FE60.EF8D ssid-profile Test
configure dot11Radio 1 enable
configure wgb mobile period 5 70
configure dot11Radio 0 mode root-ap
configure dot11Radio 0 wlan add root_wlan 8 vlan 10
configure dot11Radio 0 encryption mode ciphers aes-ccm
configure dot11Radio 0 antenna ab-antenna
configure dot11Radio 0 channel 7 20
configure dot11Radio 0 802.11ac disable
configure dot11Radio 0 tx-power 1
configure dot11Radio 0 enable
configure dot11Radio 1 encryption mode ciphers aes-ccm
configure dot11Radio 1 tx-power 1
```

# WGB ルート AP での Web 認証

## Web 認証の概要

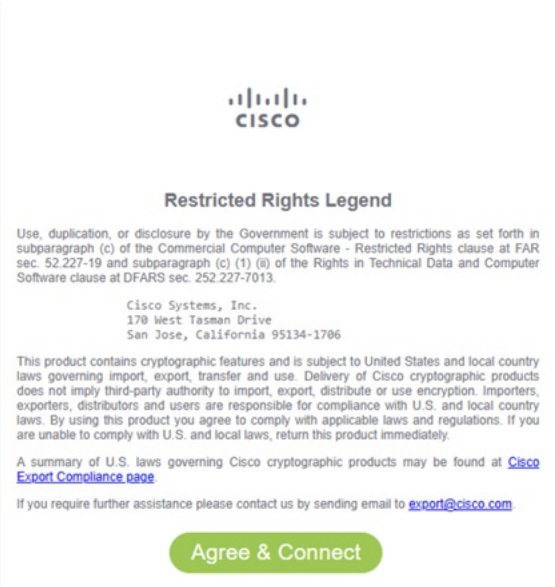
Web 認証は、ゲストアクセスネットワークを設定するためのレイヤ 3 セキュリティ機能の役割を果たします。ワイヤレスクライアントの Web ブラウザを介して認証され、ユーザープロファイルを作成せずにオープン SSID に接続できます。

Cisco IOS XE リリース 17.15.1 以降では、WGB ルート AP で Web 認証を設定およびカスタマイズできます。Web 認証を設定すると、WP-WIFI6 の WGB ルート AP でキャプティブポータルがアクティブ化されます。Web ポータルの利用規約に同意して、インターネットにアクセスします。

Web 認証の設定により、デフォルトの Web ページまたはカスタマイズされた Web ページのいずれかを使用できます。

次の図は、デフォルトのキャプティブポータルページです。

**図 *1*: デフォルトのキャプティブポータルページ**




また、次のように Web 認証をカスタマイズできます。

- キャプティブポータル Web ページに同意した後で、希望する URL をリダイレクトする。
- カスタマイズした同意 Web ページを WIM にコピーし、WGB ルート AP の Web 認証に使用する。
- キャプティブポータル Web ページのカスタム仮想インターフェイス IP アドレスを割り当てる。
- キャプティブポータル Web ページで利用規約に同意する前に、特定のインターネット接続先にアクセスするための事前認証アクセス制御リスト（ACL）ルールを追加する。

たとえば、現在のキャプティブポータル Web ページに外部 Web サイトの広告を表示する場合などです。

（注） Web 認証は、Android、iOS、macOS、および Windows ワイヤレスクライアントをサポートします。

## Web 認証プロセス

1. **Wi-Fi への接続**：ホットスポット SSID を選択し、パブリック Wi-Fi ネットワークに接続して、デバイスで接続を確立します。
2. **キャプティブポータルの検出**：デバイスは、SSID に接続すると、関連付けられたキャプティブポータルを自動的に検出します。
3. **Web 認証のアクティブ化**：デバイスは Web ブラウザをアクティブ化し、特定の同意 Web ページを表示します。
4. **認証の完了**：Web 認証ページの手順を読んで理解したら、同意 Web ページの [Agree & Connect] ボタンをクリックしてサービス利用規約に同意します。
5. **インターネットへのアクセス**： キャプティブ ポータル アシスタントから求められる手順を完了すると、ネットワーク経由でインターネットにアクセスできるようになります。

（注） **クライアントキャッシュ**：Web 認証の完了後 5 分以内に再接続する場合は、デバイスによって同意ページがバイパスされます。

## Web 認証設定の前提条件

Wi-Fi モジュールとルータを設定するには、次の手順を実行します。

### 手順

**ステップ 1** 無線インターフェイスを WGB モードおよびルート AP モードに設定します。無線インターフェイスの WGB/uWGB モードおよびルート AP モードへの設定 （15 ページ）を参照してください。

**ステップ 2** ルータに無線機の同時使用を設定します。無線機の同時使用に必要なルータ設定 （12 ページ）を参照してください。

**ステップ 3** WGB の静的 IP アドレスに ping を実行するように、ルータの IP サービスレベル契約（SLA）を設定します。

```
Device(config)#ip sla number
```

例：

```
Router(config)#ip sla 10
Router(config-ip-sla)#icmp-echo 192.0.2.1 source-interface Vlan4094
Router(config-ip-sl-echoa)#frequency 5
Router(config)#ip sla schedule 10 start-time now
```

（注）

- 192.0.2.1 は WGB の静的 IP アドレスで、Vlan4094 はルータと WGB の間で通信するためのダウンリンク VLAN です。
- ルータの IP SLA は、WGB の静的 IP アドレスに ping を実行します。
- WGB ルート AP に静的 IP アドレスが割り当てられている場合は、リロード後に ping を実行するか、WGB から ping を開始して、WGB の静的 IP アドレスをアクティブ化する必要があります。これを行わないと、Web 認証ページが正常に表示されません。
- ルータの IP SLA 設定によって WGB の静的 IP アドレスがアクティブ化され、手動で ping を行わなくても Web 認証ページがポップアップ表示されます。

## Web 認証の制限事項

Web 認証は、事前認証アクセス制御リスト（ACL）の IPv4 アドレスと IP アドレスだけをサポートするように設計されています。完全修飾ドメイン名（FQDN）ACL はサポートされません。

リダイレクト URL の設定は、Android クライアントでは必須です。

## Web 認証の設定

### Web 認証の有効化

AP で、次の手順を実行して Web 認証を設定します。

手順

**ステップ 1** コマンドを実行して、HTTPd サービスを有効にします。

Device#**configure ap http enable**

（注）

デフォルトでは、HTTPd サービスは有効になっています。**configure ap http disable** コマンドを実行して、HTTPd サービスを無効化します。

**ステップ 2** コマンドを実行して、Web 認証を有効にします。

Device#**configure webauth enable**

（注）

**configure webauth disable** コマンドを実行して、Web 認証を無効にします。

**ステップ 3** コマンドを実行して、ルート AP WLAN の Web 認証を設定します。

Device#**configure dot11Radio** {**0** | **1**} **wlan add** <**profile-name**> <**wlan id**> **vlan** <**vlan id**> **webauth** {**default_webpage**/**customized_webpage**}

（注）
デフォルトの Web ページは、webauthpassthrough.html です。必要に応じて、カスタム Web ページを使用できます。

カスタム Web ページが WGB にアップロードされていない場合、AP は警告を出力し、デフォルトの Web ページを使用します。

**例**：

次に、デフォルトおよびカスタム Web ページの設定例を示します。

- デフォルト Web ページ：

```
Device#configure dot11Radio 1 wlan add WebAuth 4 vlan 4094 webauth default_webpage
```

- カスタム Web ページ：

```
Device#configure dot11Radio 1 wlan add WebAuth-customize 5 vlan 4094 webauth customized_webpage
```

## Web 認証設定のカスタマイズ

AP で、次の手順を実行して Web 認証設定をカスタマイズします。

### 手順

**ステップ 1** サーバーから WIM ストレージにカスタマイズする Web ページをコピーします。

Device#**copy webpage {tftp|sftp}://<server-ip>[/dir][/filename]**

Device#**copy webpage scp://username@<server-ip>[:port]:/dir[/filename]**

（注）
.tar ファイルまたは HTML ファイルをコピーできます。.tar ファイルのサイズは 10 MB を超えてはいけません。

**例**：

```
Device#copy webpage scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar
copy "scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar" to
"/storage/webauth/customized_webpage" (Y/N)Y
root@100.10.10.3's password:
wp_wifi6_web.tar                              100%   30KB   6.4MB/s   00:00
[*04/24/2024 08:27:34.1830] wp_wifi6_web/
[*04/24/2024 08:27:34.1830] wp_wifi6_web/logo.jpg
[*04/24/2024 08:27:34.1830] wp_wifi6_web/webauth.css
[*04/24/2024 08:27:34.1830] wp_wifi6_web/reg_customized_webpage.html
[*04/24/2024 08:27:34.1840] % Customized webpage will use wp_wifi6_web/reg_customized_webpage.html
 as index.html
```

ストレージパス（/storage/webauth/customized_webpage/）にファイルを保存します。tar パッケージをこのディレクトリに抽出し、HTML ページの名前を index.html に変更します。

**ステップ 2** リダイレクト URL を設定します。

Device#**configure webauth redirect-url** {**customized|default**}**RedirectURL**

**例**：

```
Device#configure webauth redirect-url customized https://www.example.com/
```

（注）
カスタムリダイレクト URL を削除するには、**configure webauth redirect-url default** コマンドを使用します。

**ステップ 3** Web 認証インターフェイスで仮想インターフェイスを設定します。

Device# **configure interface webauth address ipv4 static**<**interface_ip**> <**netmask**>

**例**：

```
Device#configure interface webauth address ipv4 static 10.10.10.10 255.255.255.255
```

（注）
デフォルトでは、Web認証インターフェイスはIPアドレス 1.1.1.1 を使用します。これは仮想インターフェイス IP（同意ページの Web サイトの IP アドレス）です。

**ステップ 4** 事前認証 ACL を設定します。

Device#**configure webauthpreauth-acl add** <**aclrules**>

**例**：

```
Device#configure webauth preauth-acl add "allow true and dst 192.168.93.1 mask 255.255.255.0 and ip
 proto 6″
```

ACL ルールのフォーマットの例を次に示します。

- {allow/deny} {icmp/tcp/udp}
- {allow/deny} {icmp/tcp/udp} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <> {and/or} {ip proto <>}
- {allow/deny} true
- {allow/deny} all
- {allow/deny} true {and/or} {tcp/udp} {src/dst} port <>

（注）
- 事前認証 ACL は、クライアントが WEBAUTH_REQD 状態になるとアクティブ化されます。
- ACL ルールの最大長は 255 文字です。ACL エントリの件数に制限はありません。
- 事前認証 ACL を削除するには、**configure webauth pre-authentication acl delete** コマンドを実行します。

• 事前認証 ACL を削除すると、すべての事前認証 ACL エントリがクリアされます。

## WGB 設定のインポートとエクスポート

既存の WGB と同様の設定を作成する場合は、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。

```
Device#copy configuration upload {sftp:|tftp:|scp:}// 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。

```
Device#copy configuration download {sftp:|tftp:|scp:}// 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。

## Web 認証の確認

### Web 認証

Web 認証の設定を確認するには、次の例に示すように **show webauth** を使用します。

```
Device#show webauth

WEBAUTH Configuration are:
==================================
HTTP Status: enabled
Webauth Status: enabled
Webauth Redirect-URL: https://www.example.com/
Webauth Preauth-ACL: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6,
 allow icmp dst 198.51.100.1 mask 255.255.255.0,  allow icmp src 198.51.100.1 mask
255.255.255.0
Customized Webpage Exists: Yes
Customized Webpage MD5 HASH: 05ff0f8944e5466e484c342cba6fc403
```

### Web 認証の現在のステータス

ルート AP WLAN ステータスを表示するには、次の例に示すように **show controller dot11radio {0|1} wlan** を使用します。

```
Device#show controllers dot11Radio 1 wlan

apr1v0    Link encap:Ethernet  HWaddr 68:79:09:B8:03:8F
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:60425858
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:38

radio vap id              mac               ssid state ml_enabled              mld
webauth
```

```
    1      3 68:79:09:B8:03:8C            WebAuth    UP          No 00:00:00:00:00:00
  Yes
    1      4 68:79:09:B8:03:8B  WebAuth-customize    UP          No 00:00:00:00:00:00
  Yes

NON_ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr1v3   3051 2976    75 2376573    919      0   2902 2556   346  575037     0  4.196000
apr1v4    427  402    25  289034     31      0    460  344   116   70123     0  4.196000
ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr1v3      0    0     0       0      0      0      0    0     0       0     0  4.196000
apr1v4      0    0     0       0      0      0      0    0     0       0     0  4.196000

Vlan BSSID Pri/U/M EncryPolicy Key0 Key1 Key2 Key3 iGTK                SSIDs MFP
2290   38C   3 3 3       NONE                      DIS              WebAuth   0
2290   38B   3 3 3       NONE                      DIS     WebAuth-customize   0

VAP-ID                 SSID  Bridging Type
     3              WebAuth Local-Switched
     4     WebAuth-customize Local-Switched
```

## Web 認証クライアントのステータス

クライアントの Web 認証ステータスを表示するには、次の例に示すように **show controller dot11radio {0|1} client** を使用します。

```
Device#show controllers dot11Radio 1 client

             mac radio vap aid        state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D     1   3   2 WEBAUTH_REQD OPEN MCS112SS    HE  HE        false
00:00:00:00:00:00         No        Yes             No
00:50:54:27:A2:9F     1   3   1          FWD OPEN MCS112SS    HE  HE        false
00:00:00:00:00:00         No        Yes             Yes

APAP6879.0974.FD08#show client summary

Radio Driver client Summary:
============================
apr1v3
-------
STA BC:6E:E2:67:CD:9D
  chanspec 153 (0xd099)
  state: AUTHENTICATED ASSOCIATED AUTHORIZED
  per antenna rssi of last rx data frame: -34 -34 0 0
  per antenna average rssi of rx data frames: -34 -33 0 0
  per antenna noise floor: -82 -84 0 0
smoothed rssi: -33
tx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 2xLTF GI 1.6us auto
rx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 4xLTF GI 3.2us auto

apr1v4
-------

WCP client Summary:
====================

             mac radio vap aid        state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D     1   3   2 WEBAUTH_REQD OPEN MCS112SS    HE  HE        false
```

```
00:00:00:00:00:00         No        Yes             No

Assoc time:
=============
              mac      assoc_time
BC:6E:E2:67:CD:9D 00d:00h:04m:08s
```

（注） 同意ページで同意するまでは、クライアントの状態は [WEBAUTH_REQD] であり、Web 認証が完了すると、クライアントの状態は [FWD]（転送）に変わります。

### 事前認証 ACL

クライアントの現在の事前認証ACLを表示するには、次の例に示すように **show client access-lists pre-auth all client mac-address** を使用します。

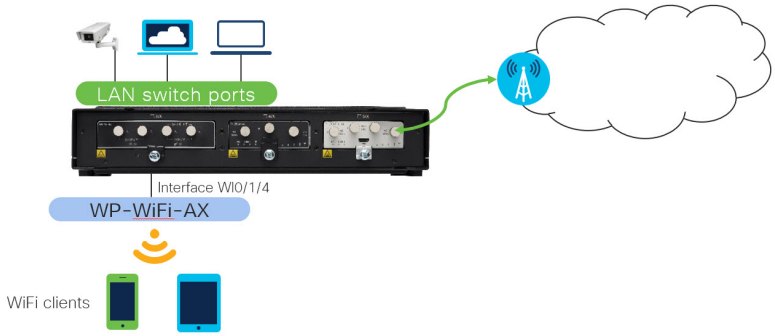
```
Device#show client access-lists pre-auth all BC:6E:E2:67:CD:9D
Pre-Auth URL ACLs for Client: BC:6E:E2:67:CD:9D
IPv4 ACL: PREAUTH
IPv6 ACL:
ACTION    URL-LIST
Resolved IPs for Client: BC:6E:E2:67:CD:9D
HIT-COUNT      URL        ACTION    IP-LIST
PREAUTH
    rule 0: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6
    rule 1: allow icmp dst 198.51.100.1 mask 255.255.255.0
    rule 2: allow icmp src 198.51.100.1 mask 255.255.255.0

No IPv6 ACL found
Redirect URL for client: BC:6E:E2:67:CD:9D

Acl name Quota Bytes left In bytes Out bytes In pkts Out pkts Drops-in Drops-out
 PREAUTH     0          0        0       148       0        2       21       201
CLIENT STATE: WEBAUTH_REQD
WEBAUTH_REQUIRED: TRUE
DNS POST AUTH:  FALSE
PREAUTH ENABLED: TRUE
POSTAUTH ENABLED: FALSE
```

# Cisco Embedded Wireless Controller（EWC）

Embedded Wireless Controller（EWC）のシナリオでは、次の機能が提供されます。

- 自己管理
- トラフィックのローカルスイッチング
- C9105 + IR1800 の性能に合わせて調整されたカスケード AP を管理できる場合もある
- WebUI 管理
- Cisco Catalyst ワイヤレス モバイル アプリケーション（iPhone/Android）

EWC モードは通常、公共交通機関/運輸の遠隔および移動体資産に使用されます。




ワイヤレスインターフェイスモジュールがEWCモードで実行されている場合、ワイヤレスコントローラかつアクセスポイント（通常、内部APと呼ばれる）として機能します。EWCは、専用ワイヤレスコントローラ（C9800 シリーズなど）と同様の方法で他の AP を管理します。

CiscoEWCネットワークでは、ワイヤレスコントローラ機能を実行するアクセスポイント（AP）がアクティブ AP として指定されます。このアクティブ AP によって管理される他のアクセスポイントは従属 AP と呼ばれます。

EWC モードに使用されるイメージは C9800-AP-iosxe-wlc.bin です。

アクティブ EWC には以下の 2 つの役割があります。

- ワイヤレス LAN コントローラ（WLC）として機能し、従属 AP を管理および制御する。従属 AP は、クライアントにサービスを提供する中央管理型アクセスポイントとして機能します。
- クライアントにサービスを提供するアクセスポイントとして機能する。

Wi-Fi ランディングページ機能（Web ベース認証）のサポートについては、『Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide』[英語] の「Web-Based Authentication」の章を参照してください。

Cisco Embedded Wireless Controller の詳細については、次を参照してください。

Cisco Embedded Wireless Controller on Catalyst Access Points FAQ [英語]

Cisco Embedded Wireless Controller on Catalyst Access Points（EWC）ホワイトペーパー

# IR1800 で EWC アクセスポイントを設定するための前提条件

ルータで EWC アクセスポイントを設定する前に、次の前提条件が満たされていることを確認します。

- Cisco Embedded Wireless Controller（EWC）ネットワークのセットアップ時や毎日の運用時に、同じネットワークに他の Cisco Wireless LAN Controller（アプライアンスも仮想も）を実装しないことを推奨します。
- DHCP サーバーは、アクセス ポイントおよびクライアントが IP アドレスを取得できるように、ネットワーク上で使用可能である必要があります。

- IR1800 シリーズ ルータに統合された EWC および AP を設定するには、ルータで DHCP サーバー、SVI インターフェイス、および NAT を設定する必要があります。AP の設定に関する詳細は、IR1800 で CAPWAP アクセスポイント構成を設定するための前提条件 （2 ページ）の項を参照してください。
- Embedded Wireless Controller（EWC）では、管理トラフィックはタグなしで、スイッチポートのネイティブ VLAN として設定する必要があります。WIM と WLAN がすべて異なる VLAN 上にある場合は、ルータの WIM 接続ポートをトランクとして設定する必要があり、個々の WLAN のトラフィックはそれぞれの VLAN でローカルにスイッチングされます。次に、異なる VLAN 上の WIM と WLAN を使用したルータ設定を示します。

| コマンド | 目的 |
|---|---|
| **interface Wlan-GigabitEthernet** *slot/subslot/port*<br>**switchport mode trunk**<br>**switchport trunk native vlan** *number*<br>**switchport trunk allowed vlan** *numbers* | WIM 内部スイッチインターフェイスのスイッチポートモードとネイティブ VLAN を設定します。ネイティブ VLAN 10 は AP 管理 VLAN である必要があります。VLAN 20 および 30 は WLAN トラフィックに使用されます。 |

次の例を参照してください。

```
Router(config)#interface Wlan-GigabitEthernet 0/1/4
Router(config-if)#switchport mode trunk
Router(config-if)#switchport trunk native vlan 10
Router(config-if)#switchport trunk native vlan 10,20,30
```

# Day 0 プロビジョニングを使用した EWC の設定

Day 0 プロビジョニングを使用して AP を設定するには、次の 3 つの方法があります。

1. 「EWC の導入」[英語] の手順に従って、SSID を CiscoAirProvision-XXXX に接続します。
2. 携帯電話で Catalyst ワイヤレスアプリケーションを使用して QR コードをスキャンすることもできます。『User Guide for Cisco Catalyst Wireless Mobile Application』[英語] の手順に従ってください。
3. 「Day 0 ウィザードを使用したコントローラの設定（CLI）」の手順に従うか、「オプション 1 初期 CLI 設定」（『Catalyst 9100 アクセスポイントの Embedded Wireless Controller への変換』内）の手順に従って手動で基本設定を行うことで、CLI を使用して AP を手動で設定できます。

その他の考慮事項は次のとおりです。

- WebUI またはシスコ ワイヤレス モビリティ アプリケーションを使用して初期設定を行う場合は、設定済みの VLAN プール（VLAN10 など）から IP アドレスが取得されるよう、Wi-Fi モジュールをリロードすることが推奨されます。

- WebUI での初期設定は、デフォルトの IP アドレス（192.168.0.1）と異なる IP アドレスを使用し、かつ、その IP アドレスが IR1800 IOS-XE の初期設定用 IP アドレスとも競合した場合には機能しない可能性があります。

# CiscoEmbeddedWirelessController（EWC）対応アクセスポイントのネットワークへの接続

展開に応じて、ルータポートに接続された Embedded Wireless Controller（EWC）対応アクセスポイントを、アクセスポートまたはトランクポートに設定できます。

アクセスポイントと WLAN がすべて同じネットワーク上にある場合、Embedded Wireless Controller（EWC）対応アクセスポイントは、次の例に示すように、アクセスモードでルータに接続できます。

```
interface Wlan-GigabitEthernet 0/1/4
switchport access vlan 10
switchport mode access
```

Embedded Wireless Controller（EWC）では、管理トラフィックはタグなしです。アクセスポイントと WLAN がすべて異なる VLAN 上にある場合、Embedded Wireless Controller（EWC）対応アクセスポイントはスイッチのトランクポートに接続し、個々の WLAN のトラフィックは個々の VLAN でローカルにスイッチングされます。次に示すのは、異なる VLAN でアクセスポイントと WLAN を使用した展開の例です。

```
interface Wlan-GigabitEthernet 0/1/4
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30
switchport mode trunk
```

# EWC モードの WebUI 管理

ここでは、WebUI を使用して EWC モードで WIM を設定する手順について説明します。

## Day 0 Over-The-Air WebUI セットアップウィザードを使用したプロビジョニング

AP が Embedded Wireless Controller（EWC）モードで再起動すると、MAC アドレスの最後の数字で終わるプロビジョニング SSID がブロードキャストされます。PSK パスワードを使用してプロビジョニング SSID に接続できます。

次に、ブラウザを開いて mywifi.cisco.com にリダイレクトすると、AP Web UI に移動します。ユーザー名に **webui**、パスワードに **cisco** と入力します。詳しい Day 0 設定手順は、次のリンクを参照してください。https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/white-paper-c11-743398.html#DeployingtheEWC

（注） Embedded Wireless Controller（EWC）設定ポータルへの Web リダイレクションは、プロビジョニング SSID に接続している場合にのみ機能します。ラップトップが別の Wi-Fi ネットワークまたは有線ネットワークに接続されている場合は機能しません。Day 0 ウィザード プロビジョニング モードのときに EWC IP アドレスを入力しても、有線ネットワークからは AP を設定できません。

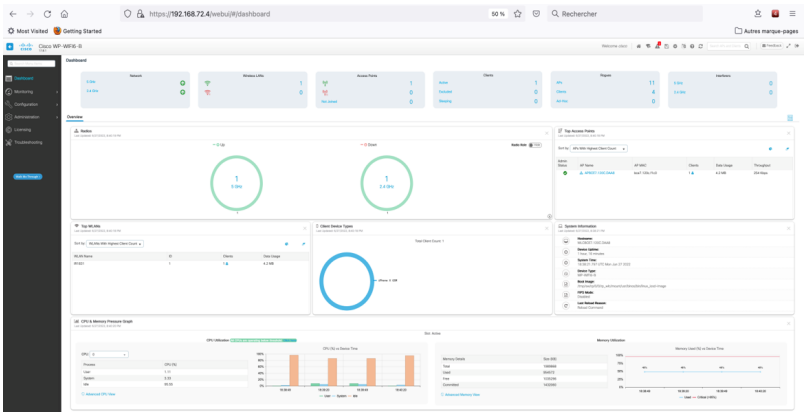
## EWC WebUI へのログイン

EWC にログインするには、次の手順を実施します。

### 手順

**ステップ 1** ブラウザから WebUI を開きます。DHCP から割り当てられた IP アドレスを使用します。

**ステップ 2** WebUI ダッシュボードが表示されます。



**ステップ 3** ワイヤレス LAN コントローラ（WLC）に接続すると、他のアクセスポイントと同様に設定が実行されます。詳細については、次のリソースを参照してください。

Overview of Cisco Embedded Wireless Controller on Catalyst Access Points [英語]

Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE [英語]

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。