



## Parallel Redundancy Protocol Over Wireless 導入ガイド

**Parallel Redundancy Protocol Over Wireless 導入ガイド 2**

Parallel Redundancy Protocol (PRP) over Wireless に関する情報 2

前提条件と使用するコンポーネント 3

デュアル WGB デュアル無線 PRP 冗長オプション 4

シングル WGB デュアル無線 PRP 冗長オプション 15

トラブルシューティング 19

関連資料 27

# Parallel Redundancy Protocol Over Wireless 導入ガイド

このドキュメントでは、Cisco IW3702 アクセスポイント上で Parallel Redundancy Protocol (PRP) over Wireless を設定する方法の詳細について説明します。

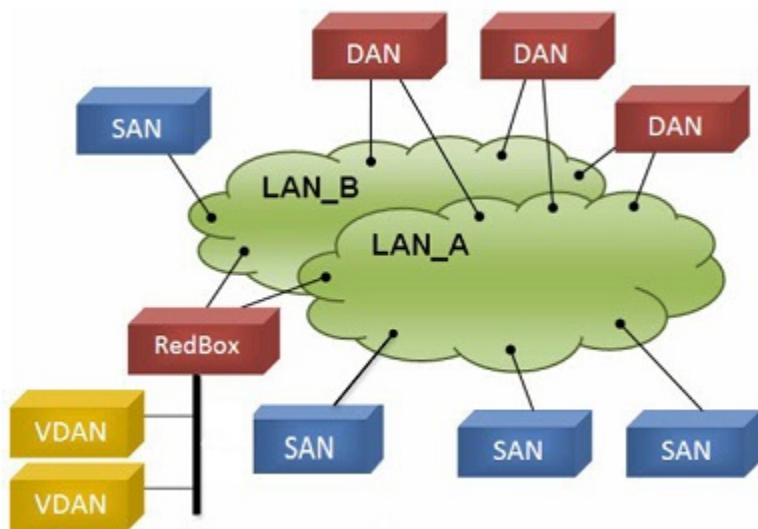
## Parallel Redundancy Protocol (PRP) over Wireless に関する情報

Parallel Redundancy Protocol (PRP) は、国際規格 IEC 62439-3 で定義されています。PRP は、イーサネットネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。

PRPを使用することで、データ通信ネットワークは、トラフィックがその宛先に到達するための2つの代替パスを提供することによって、データ伝送障害を防止できます。同様のトポロジを持つ2つのイーサネットネットワーク (LAN) は分離されています。

2つの独立したネットワーク (LAN-A および LAN-B) に接続するネットワーク全体のデータを保護する必要があるデバイスは、PRPを実装するデュアル通信ノード (DANP) と呼ばれます。DANPの送信元は、両方のLANに対して同時に2つのフレームを送信します。DANPの宛先は、両方のフレームを受信し、重複フレームを破棄します。1つのLANに障害が発生した場合でも、DANPの宛先はもう一方のLANから引き続きフレームを受信できます。

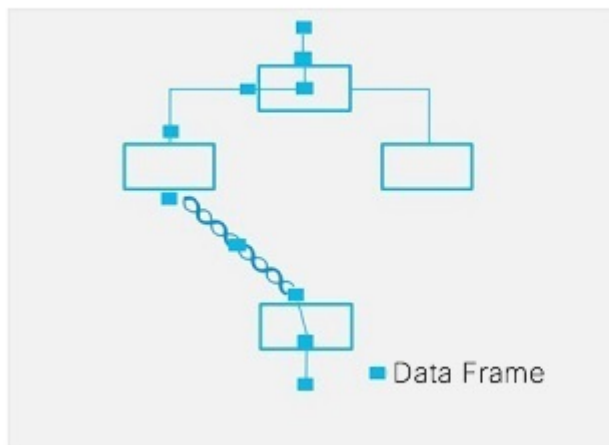
LAN-A または LAN-B のいずれかのみ接続するネットワーク内の非冗長エンドポイントは、シングル通信ノード (SAN) と呼ばれます。冗長ボックス (RedBox) は、単一のインターフェイスノードを両方のネットワークに接続する必要がある場合に使用されます。そのようなノードは、他のすべてのノードと通信することができます。



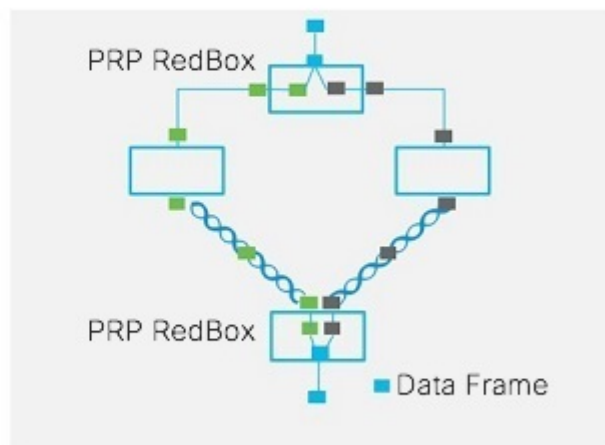
PRP機能は、シスコワイヤレスコントローラリリース8.4以降のワイヤレスで使用できます。この機能は、デュアル無線リンクを使用して (WGBの背後にある) 有線クライアントトラフィックをブリッジし、信頼性の高いワイヤレス伝送を実現するように設計されています。次の図に示すように、一般的なワイヤレスデータ伝送は単一の無線パスを経由し、ハンドオフ時にRF干渉とパケット損失を生じやすくなります。PRP over Wireless機能では、データ伝送用の

冗長無線パスが作成され、ワイヤレスネットワーク上で一貫した信頼性の高いデータ接続が可能です。これにより、2つの並列ワイヤレス接続を介したトラフィックの分散が可能となり、最高レベルの復元力と遅延変動の低減が実現します。

Wireless Network Without PRP



PRP Enabled Wireless Network



PRP over Wireless 機能は、2つの冗長オプションを備えた IW3702 WGB でサポートされています。ここでは、有線クライアントのトラフィックが2つの WGB を介したデュアル無線リンク（デュアル WGB、デュアル無線）、またはデュアル無線リンクによるシングル WGB（シングル WGB、デュアル無線）上で複製され送信されます。各冗長オプションについては、以下の項で設定例とともに詳しく説明します。

## 前提条件と使用するコンポーネント

PRP over Wireless 機能は、次のソフトウェア リリース、プラットフォーム、AP モードでサポートされています。

- デュアル WGB デュアル無線冗長オプション：ワイヤレス コントローラ ソフトウェア リリース 8.4
- シングル WGB デュアル無線冗長オプション：ワイヤレス コントローラ ソフトウェア リリース 8.5
- インフラストラクチャ側の AP：FlexConnect モード（セントラル認証、ローカル スイッチング）。次の IOS ベースのプラットフォームがサポートされています：IW3702、2700、3700、1570 シリーズ。
- モバイルクライアント側の WGB：IW3702

このマニュアルで提供されている設定例は、次のコンポーネントで構成されています。

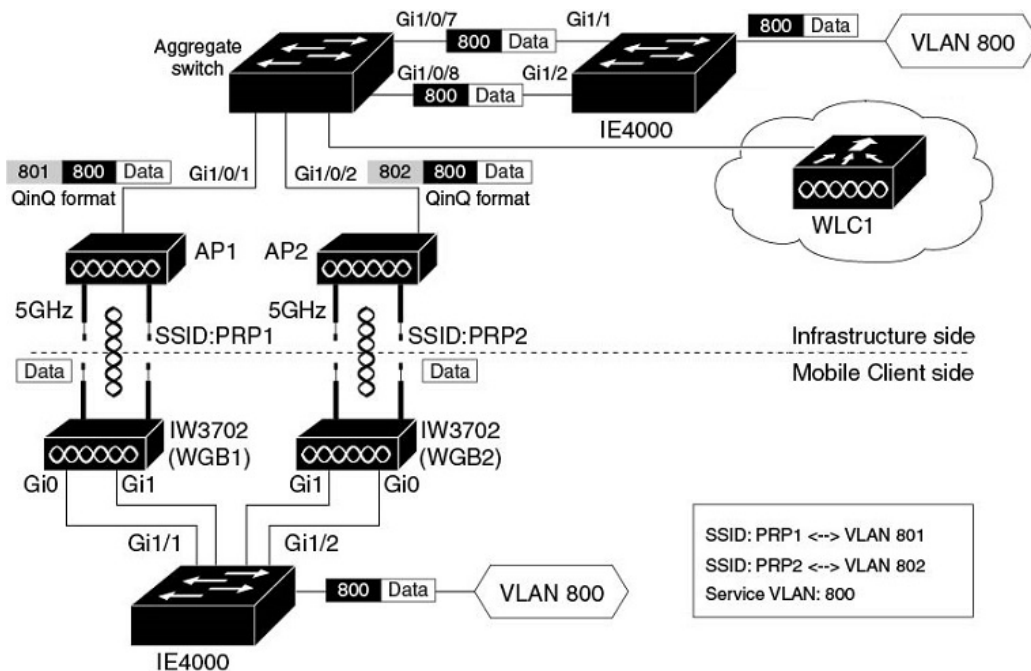
- ワイヤレス LAN コントローラ（WLC）：リリース 8.5.120.0
- インフラストラクチャ AP：FlexConnect モードの IW3702 AP（セントラル認証、ローカル スイッチング）
- WGB：リリース 15.3(3)JF の自律型イメージを実行中の IW3702 AP
- PRP スイッチ：イメージバージョンが ie4000-universal-mz.152-4.EA5 の IE 4000
- Dot1q トンネリング機能を備えた集約スイッチ：Catalyst 3750

## デュアル WGB デュアル無線 PRP 冗長オプション

これらのセクションには、デュアル WGB デュアル無線 PRP の冗長性のためのインフラストラクチャ側とモバイルクライアント側の設定が含まれています。

### ネットワーク トポロジの例

次の図に、デュアル WGB デュアル無線 PRP 冗長トポロジの例を示します。



このトポロジでは、2つの WGB で2つの 5 GHz 無線で冗長パスが提供されます。2つの PRP スイッチ（この例では Cisco IE4000）は、モバイルクライアント側とネットワークインフラストラクチャ側の両方で RedBox（冗長ボックス）として動作し、パケット重複と重複破棄を実行します。

各ネットワークコンポーネントの詳細な機能を以下で説明します。

#### インフラストラクチャ側

- インフラストラクチャ側の PRP 対応スイッチ（この例では Cisco IE4000）は、RedBox として機能し、パケット重複および重複破棄を実行します。
- インフラストラクチャ側の AP は、異なる SSID（この例では PRP1 と PRP2）を介して冗長データトラフィックを送受信し、異なる VLAN（QinQ トンネルのカプセル化またはカプセル化解除）を使用してデータにタグを付けます。
- 集約スイッチと AP 間のトラフィックは QinQ 形式であり、発信元のパスを識別します。QinQ 機能は、IE スイッチの PRP ポートに接続する集約スイッチイーサネットインターフェイス（Gi1/0/7 および Gi1/0/8）で有効になります。これらの2つのインターフェイスは、ダウンストリームトラフィックには QinQ トンネルのカプセル化を実

行し、アップストリームトラフィックにはカプセル化解除を実行して、重複したトラフィックを別の VLAN 上で伝送できるようにします。

### モバイルクライアント側

- 各 IW3702 の Gig ポート 0 (PoE IN) は、PRP スイッチの 2 つの PRP ポートに接続されます。IE4000 PRP ポートは PoE ポートではないため、IW3702 はパワーインジェクタに接続する必要があります。
- PRP 対応スイッチ IE4000 は、クライアント VLAN トラフィック (VLAN 800) に対しパケット重複および重複破棄機能を実行するために使用されます。
- 各 IW3702 は WGB として動作し、異なる SSID (この例では PRP1 と PRP2) に接続し、異なる VLAN (この例では VLAN 801 と VLAN 802) にアサインされます。冗長ワイヤレスパスは、2 つの WGB 上で 2 つの 5 GHz 無線により WGB の背後の有線クライアントに提供されます。

### ローミング調整

- 2 つの IW3702 の Gig ポート 1 (PoE OUT) を IE スイッチイーサネットインターフェイスを使用して接続することで、両方の WGB が同時にローミングしないようにするローミング調整機能を提供できます。



---

(注) 802.3at 電源入力の PoE IN ポートで電源を供給すると、IW3702 Gig ポート 1 は引き続きトラフィックを転送できます。ただし、PoE OUT 機能はサポートされません。

---

## インフラストラクチャ側の設定

ここでは、次のインフラストラクチャ側の設定について説明します。

### ワイヤレス LAN コントローラの設定

ここでは、次のワイヤレス LAN コントローラの設定について説明します。

- [WLAN の作成 \(5 ページ\)](#)
- [WLAN での PRP の有効化 \(10 ページ\)](#)
- [WGB マルチクライアント VLAN の設定 \(11 ページ\)](#)

### WLAN の作成

PRP over Wireless が機能するためには、冗長ワイヤレストラフィックを伝送する際に、2 つの異なるインターフェイス (VLAN) に 2 つの WLAN (SSID) が必要となります。インフラストラクチャ側のすべての AP に WLAN を設定します。

### 手順

---

**ステップ 1** ダイナミック インターフェイスを作成します。

Flexconnect ローカル スイッチ モードで PRP や QinQ を動作させるには、次のダイナミック インターフェイスを設定する必要があります。

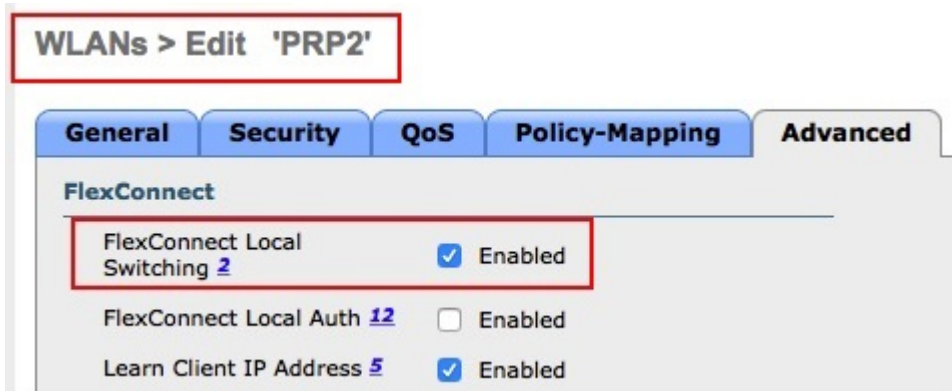
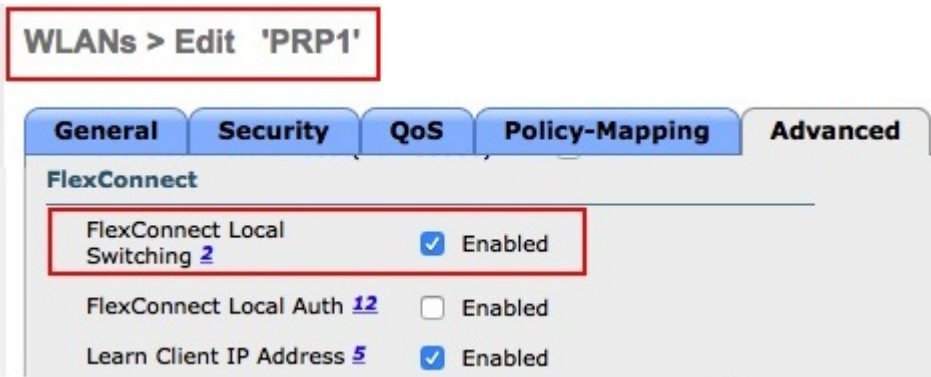
- WGB (ワイヤレス クライアント) VLAN にマッピングされる WLAN VLAN インターフェイス。この例では、VLAN 801 と VLAN 802 が、それぞれ SSID PRP1 と SSID PRP2 の VLAN になります。この VLAN は、QinQ パケットの外部タグとして使用されることになります。
- QinQ パケットの内部タグとして、Flexconnect AP によって使用される有線クライアント VLAN。この例では、VLAN 800 が有線クライアント VLAN として設定されています。

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
<a href="#">management</a>	201	172.16.201.12	Static	Enabled	2001:10:10:10::1/64
<a href="#">redundancy-management</a>	201	0.0.0.0	Static	Not Supported	
<a href="#">redundancy-port</a>	untagged	0.0.0.0	Static	Not Supported	
<a href="#">prp1_vlan</a>	801	81.1.1.254	Dynamic	Disabled	::/128
<a href="#">prp2_vlan</a>	802	82.1.1.254	Dynamic	Disabled	::/128
<a href="#">prp_client_vlan</a>	800	80.1.1.254	Dynamic	Disabled	::/128
<a href="#">service-port</a>	N/A	10.74.9.48	Static	Disabled	::/128
<a href="#">virtual</a>	N/A	1.1.1.1	Static	Not Supported	

ステップ2 SSID の WLAN を作成します (PRP1/PRP2)。

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/> 1	WLAN	PRP1	PRP1	Enabled	[WPA2][Auth(FT-PSK)]
<input type="checkbox"/> 2	WLAN	PRP2	PRP2	Enabled	[WPA2][Auth(FT-PSK)]

ステップ3 PRP over Wireless 機能は、Flexconnect モードでのみ動作します。作成された WLAN で FlexConnect ローカル スイッチング モードを有効にします。



ステップ4 AP をインフラストラクチャに接続し、Flexconnect モードで WLC に参加させます。

## All APs > Details for ROAM-AP2

General		Credentials		Interfaces		High Availability		Inventory		FlexConnect		Advanced			
<b>General</b>						<b>Versions</b>									
AP Name	ROAM-AP2					Primary Software Version	8.6.1.74								
Location	default location					Backup Software Version	3.0.51.0								
AP MAC Address	00:81:c4:ca:59:50					Predownload Status	None								
Base Radio MAC	00:81:c4:d0:26:b0					Predownloaded Version	None								
Admin Status	Enable					Predownload Next Retry Time	NA								
AP Mode	FlexConnect					Predownload Retry Count	NA								
AP Sub Mode	None					Boot Version	15.3.2.4								
Operational Status	REG					IOS Version	15.3(20170730:133551)\$								
Port Number	1					Mini IOS Version	0.0.0.0								
Venue Group	Unspecified					<b>IP Config</b>									
Venue Type	Unspecified					CAPWAP Preferred Mode	Ipv4 (Global Config)								
<b>Add New Venue</b>						Static Ipv4 Address	172.16.201.62								
<table border="1"> <thead> <tr> <th>Venue Language</th> <th>Venue Name</th> </tr> </thead> <tbody> <tr> <td>Network Spectrum Interface Key</td> <td>FOA795FD28E8CE6C3845DA80FA6E9443</td> </tr> </tbody> </table>						Venue Language	Venue Name	Network Spectrum Interface Key	FOA795FD28E8CE6C3845DA80FA6E9443	Static IP (Ipv4/Ipv6)	<input checked="" type="checkbox"/>				
Venue Language	Venue Name														
Network Spectrum Interface Key	FOA795FD28E8CE6C3845DA80FA6E9443														
						Static IP (Ipv4/Ipv6)	172.16.201.62								
						IP Mask/Prefix Length	255.255.255.0								
						Gateway (Ipv4/Ipv6)	172.16.201.15								
<b>GPS Location</b>						<b>DNS IP Address(Ipv4/Ipv6)</b>	0.0.0.0								
GPS Present	No					Domain Name									

**ステップ 5** すべての AP で VLAN マッピングを有効にし、PRP 用に作成された WLAN が VLAN に含まれていることを確認します。



All APs > Details for ROAM-AP2

General	Credentials	Interfaces	High Availability
<b>General</b>			
AP Name	ROAM-AP2		
Location	default location		
AP MAC Address	00:81:c4:ca:59:50		
Base Radio MAC	00:81:c4:d0:26:b0		
Admin Status	Enable		
AP Mode	FlexConnect		
AP Sub Mode	None		
Operational Status	REG		
Port Number	1		
Venue Group	Unspecified		
Venue Type	Unspecified		
<b>Add New Venue</b>			
	Venue Language	Venue Name	
Network Spectrum Interface Key	FOA795FD28E8CE6C3845DA80FA6E9443		
<b>GPS Location</b>			
GPS Present	No		

## All APs > Details for ROAM-AP2

**General** | Credentials | Interfaces | High Availability | Inventory | FlexConnect | **Advanced**

VLAN Support  Make VLAN AP Specific Go

Inheritance Level AP-Specific

[Native VLAN ID](#)  **VLAN Mappings**

FlexConnect Group Name dualradiopr

[WLAN AVC Mapping](#)

VLAN Template Name none

[VLAN Name Id Mappings](#)

**MONITOR** | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT

## All APs > ROAM-AP2 > VLAN Mappings

<b>AP Name</b>	ROAM-AP2
<b>Base Radio MAC</b>	00:81:c4:d0:26:b0

### WLAN VLAN Mapping

Make AP Specific Go

<input type="checkbox"/>	WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
<input type="checkbox"/>	1	PRP1	801	no	AP-specific
<input type="checkbox"/>	2	PRP2	802	no	AP-specific

(注) 高速セキュアローミング方式CCKMを使用する場合は、CCKMが動作するようにFlexConnectグループを作成する必要があります。CCKMでの高速ローミングを実現するには、AP間で同じグループ名を使用する必要があります。

## WLANでのPRPの有効化

PRP機能を必要とするWLANに対してのみPRP機能を有効にしてください。この例では、PRP機能はWLAN PRP1とWLAN PRP2に対して有効にする必要があります。

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs > Edit 'PRP1'

General Security QoS Policy-Mapping Advanced

Client user idle threshold (0-10000000)  Bytes

Radius NAI-Realm

11ac MU-MIMO

WGB PRP  Enabled

Off Channel Scanning Defer

Scan Defer Priority

0	1	2	3	4	5	6	7
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Scan Defer Time(msecs)

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs > Edit 'PRP2'

General Security QoS Policy-Mapping Advanced

11ac MU-MIMO

WGB PRP  Enabled

Off Channel Scanning Defer

Scan Defer Priority

0	1	2	3	4	5	6	7
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Scan Defer Time(msecs)

### WGB マルチクライアント VLAN の設定

WGB クライアントマルチ VLAN サポートを有効にするには、WLC と WGB の両方を設定する必要があります。

WLC で、[Controller]>[General] タブに移動し、WGB VLAN クライアントに対し [Enable] を選択します。

WGB で、次のコマンドを使用して WGB VLAN タギングを有効にします。

```
WGB (config) #workgroup-bridge unified-vlan-client
WGB (config) #workgroup-bridge unified-vlan-client
broadcast-tagging
```



- (注) WGB に複数の VLAN 設定がある場合、**encryption vlan 801 mode ciphers aes-ccm** など、特定の VLAN に対して暗号化モードとキーを設定する必要があります。次に、コマンド **encryption mode ciphers aes-ccm** を入力して、マルチキャスト/ブロードキャスト インターフェイスで暗号化モードをグローバルに設定する必要があります。

## PRP スイッチの設定

一部のシスコ産業用イーサネット スイッチは PRP 機能をサポートしています。次の例では、IE 4000 スイッチで PRP チャンネルを作成する方法を示します。

```
switch#configure terminal switch(config)#interface range GigabitEthernet1/1-2 switch(config-if)#switch port mode trunk switch(config-if)#no keepalive switch(config-if)#no cdp enable switch(config-if)#udld port disable switch(config-if)#prp-channel-group 1 switch(config-if)#no shutdown switch(config-if)#spanning-tree bpdudfilter enable
```



- (注) **spann-tree portfast edge trunk** コマンドは、**prp-channel** インターフェイスではオプションですが、強く推奨されます。これにより、PRP LAN-A および LAN-B のスパニングツリーコンバージェンス時間が改善されます。

PRP チャンネルグループの設定の詳細については、『[Parallel Redundancy Protocol \(PRP\) for IE 4000, IE 4010, and IE 5000 Switches](#)』を参照してください。

## 集約スイッチの設定

次に、集約スイッチの設定例を示します。VLAN 201 は WLC 管理インターフェイスです。

```
interface GigabitEthernet1/0/1 description ***Port to AP1*** switchport trunk encapsulation dot1q switchport trunk native vlan 201 switchport trunk allowed vlan 201,801,802 switchport mode trunk interface GigabitEthernet1/0/2 description ***Port to AP2*** switchport trunk encapsulation dot1q switchport trunk native vlan 201 switchport trunk allowed vlan 201,801,802 switchport mode trunk interface GigabitEthernet1/0/7 description ***Port to IE switch PRP port*** switchport access vlan 801 switchport mode dot1q-tunnel spanning-tree portfast trunk interface GigabitEthernet1/0/8 description ***Port to IE switch PRP port*** switchport access vlan 802 switchport mode dot1q-tunnel spanning-tree portfast trunk
```

## モバイルクライアント側の設定

ここでは、次のモバイルクライアント側の設定について説明します。

### ワークグループブリッジ構成

モバイルクライアント側の 2 つの IW3702 AP は、SSID PRP1 と SSID PRP2 に個別に接続する WGB として設定する必要があります。GigabitEthernet0 ポートは IE4000 PRP ポートに接続する必要があります。

- 次に、WGB1 でのサンプル設定を示します。SSID PRP1 に VLAN 801 と有線クライアント VLAN 800 を接続するように設定されています。



- (注) オープンセキュリティ方式が WGB 設定で使用されています。次の例では、**mobile station scan xx xx xx** および **mobile station period x threshold x** コマンドによって設定されるパラメータを、独自の展開に基づいて調整する必要があります。ローミングとセキュリティに関する WGB 設定ガイドラインについては、<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1130-ag-series/113198-wgb-roam-config.html> を参照してください。

```
hostname WGB1 dot11 ssid PRP1 vlan 801 authentication open interface Dot11Radio1 no ip address ssid PRP1
station-role workgroup-bridge mobile station scan 5745 5765 5785 mobile station period 1 threshold 70 !
interface Dot11Radio1.800 encapsulation dot1Q 800 bridge-group 2 bridge-group 2 spanning-disabled ! interface
Dot11Radio1.801 encapsulation dot1Q 801 native bridge-group 1 bridge-group 1 spanning-disabled ! interface
GigabitEthernet0.800 encapsulation dot1Q 800 bridge-group 2 ! interface GigabitEthernet0.801 encapsulation
dot1Q 801 native bridge-group 1 ! workgroup-bridge unified-vlan-client workgroup-bridge unified-vlan-client
broadcast-tagging
```

- 同様に、WGB2 は SSID PRP2 に VLAN 802 と有線クライアント VLAN 800 を接続するように設定されており、次の例のようになります。



- (注) オープンセキュリティ方式が WGB 設定で使用されています。次の例では、**mobile station scan xx xx xx** および **mobile station period x threshold x** コマンドによって設定されるパラメータを、独自の展開に基づいて調整する必要があります。ローミングとセキュリティに関する WGB 設定ガイドラインについては、<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1130-ag-series/113198-wgb-roam-config.html> を参照してください。

```
hostname WGB2 dot11 ssid PRP2 vlan 802 authentication open interface Dot11Radio1 no ip address ssid PRP2
station-role workgroup-bridge mobile station scan 5745 5765 5785 mobile station period 1 threshold 70 !
interface Dot11Radio1.800 encapsulation dot1Q 800 bridge-group 2 bridge-group 2 spanning-disabled ! interface
Dot11Radio1.802 encapsulation dot1Q 802 native bridge-group 1 bridge-group 1 spanning-disabled ! interface
GigabitEthernet0.800 encapsulation dot1Q 800 bridge-group 2 ! interface GigabitEthernet0.802 encapsulation
dot1Q 802 native bridge-group 1 ! workgroup-bridge unified-vlan-client workgroup-bridge unified-vlan-client
broadcast-tagging
```

## WGB ローミングの調整

WGB のペアは、2 番目のギガビットイーサネットインターフェイスを介して通信することにより、ローミング調整機能をサポートできます。2 つの IW3702 WGB の Gig1 ポートを、IE スイッチイーサネットポート経由で接続し、2 つの WGB 間のローミング調整機能を提供することができます。次の例には、この機能を有効にするために必要な設定が含まれています。ここでは、VLAN 51 が 2 つの WGB 間の通信チャンネルとしてローミング調整に使用されています。

### • WGB1 設定

```
dot11 coordinator uplink single Dot11Radio1 dot11 coordinator timeout roam-wait 150 interface GigabitEthernet1
no ip address duplex auto speed auto interface GigabitEthernet1.51 encapsulation dot1Q 51 ip address
51.0.0.1 255.255.255.0 ip coordinator peer-addr 51.0.0.2 workgroup-bridge service-vlan 51
```

### • WGB2 設定

```
dot11 coordinator uplink single Dot11Radio1 dot11 coordinator timeout roam-wait 150 interface GigabitEthernet1
no ip address duplex auto speed auto interface GigabitEthernet1.51 encapsulation dot1Q 51 ip address
51.0.0.2 255.255.255.0 ip coordinator peer-addr 51.0.0.1 workgroup-bridge service-vlan 51
```

### • ブリッジループを回避する設定

WGB の Gig1 ポートに直接またはスイッチ経由で接続する場合は、WGB 側の有線ネットワークにブリッジループを導入できます。次の設定例では、ブリッジループを回避できます。



---

(注) 調整トラフィックは、サービス VLAN で転送され、ブロックはされません。

---

- WGB の Gig1 ポートに直接接続する場合にブリッジループを回避するには、両方の WGB で次のように設定します。

```
WGB(config)# access-list 700 deny 0000.0000.0000 ffff.ffff.ffff WGB(config)# interface gigabitEthernet 1
WGB(config-if)# l2-filter bridge-group-acl WGB(config-if)# bridge-group 1 WGB(config-if)# bridge-group 1
output-address-list 700
```

- スイッチを介して2つの WGB を接続する場合にトラフィックループを回避するには、スイッチポートで次のように設定します。

```
interface GigabitEthernet0/3 switchport trunk allowed vlan 51 switchport mode trunk interface
GigabitEthernet0/4 switchport trunk allowed vlan 51 switchport mode trunk
```

## PRP スイッチの設定

- PRP チャネル グループを作成します。

モバイルクライアント側の PRP スイッチで PRP チャネル グループを設定するためには、次の設定が必要です。

```
switch#configure terminal switch(config)#interface range GigabitEthernet1/1-2 switch(config-if)#switch port
mode trunk switch(config-if)#no keepalive switch(config-if)#no cdp enable switch(config-if)#udld port
disable switch(config-if)#prp-channel-group 1 switch(config-if)#no shutdown switch(config-if)#spanning-tree
bpdufilter enable
```



---

(注) **spanp-tree portfast edge trunk** コマンドは、prp-channel インターフェイスではオプションですが、強く推奨されます。これにより、PRP LAN-A および LAN-B のスパンニングツリー コンバージェンス時間が改善されます。

---

- ローミング調整用の通信チャネルを作成します。

```
interface GigabitEthernet1/7 description ***To Gig1 of WGB1*** switchport trunk allowed vlan 51 switchport
mode trunk end interface GigabitEthernet 1/8 description ***To Gig1 of WGB2*** switchport trunk allowed
vlan 51 switchport mode trunk
```

## 確認

設定がすべて完了したら、次のコマンドを使用して設定を確認します。

- インフラストラクチャ側の PRP スイッチで、サービス VLAN 800 を使用して SVI インターフェイスを作成し、VLAN 800 の DHCP プールを作成します。
- モバイルクライアント側の PRP スイッチで、VLAN 800 を使用して SVI インターフェイスを作成し、DHCP クライアントとして有線クライアントをシミュレートします。DHCP アドレスは、DHCP プール VLAN 800 から割り当てる必要があります。

```
IE-SW#show ip interface brief
Interface IP-Address OK? Method Status
Protocol Vlan1 unassigned YES NVRAM administratively down down
Vlan800 10.10.80.93 YES DHCP up up
```

- 有線クライアントのステータスを確認します。

```
(WLC) >show client summary
Number of Clients..... 4 Number of PMIPv6 Clients..... 0
Number of EoGRE Clients..... 0 GLAN/ RLAN/ MAC Address AP Name Slot Status WLAN Auth Protocol Port Wired Tunnel Role -----
----- 00:10:94:00:00:07 AP1
1 Associated 8 Yes N/A 1 No No Local 4c:00:82:1a:c0:b0 AP1 1 Associated 7 Yes 802.11n(5 GHz) 1 No No Local
f4:0f:1b:f8:3b:c1 AP1 1 Associated 8 Yes N/A 1 No No Local f8:72:ea:e4:a4:d8 AP1 1 Associated 8 Yes
802.11n(5 GHz) 1 No No Local (WLC) >show client detail f4:0f:1b:f8:3b:c1 Client MAC
Address..... f4:0f:1b:f8:3b:c1 Client Username .....
N/A AP MAC Address..... d4:a0:2a:98:88:00 AP
Name..... AP1 AP radio slot Id..... 1 2nd
AP MAC Address..... d4:a0:2a:98:88:00 2nd AP
Name..... AP1 2nd AP radio slot Id..... 1 Client
State..... Associated Client User Group.....
Client NAC OOB State..... Access Workgroup Bridge Client.....
WGB: f8:72:ea:e4:a4:d8 Workgroup Bridge Client..... 2nd WGB: 4c:00:82:1a:c0:b0 Wireless
LAN Id..... 8 Wireless LAN Network Name (SSID)..... PRP2 Wireless
LAN Profile Name..... PRP2 2nd Wireless LAN Id..... 7 2nd
Wireless LAN Network Name (SSID)..... PRP1 2nd Wireless LAN Profile Name..... PRP1
```

- データパスを確認します。

モバイルクライアント側からインフラストラクチャ側に ping を実行します。

```
PRP-SW#ping 10.10.80.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.80.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```

インフラストラクチャ PRP スイッチからの出力：

```
PRP-SW#show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS: ingress pkt lan a: 6 <= LAN A receives 6 pkts ingress pkt lan b: 6 <= LAN B receives 6 pkts ingress crc lan a: 0 ingress
crc lan b: 0 ingress danp pkt acpt: 5 ingress danp pkt dscrd: 5 <= discard 5 duplicate pkts
ingress supfrm rcv a: 0 ingress supfrm rcv b: 0 ingress over pkt a: 0 ingress over pkt b: 0
ingress pri over pkt_a: 0 ingress pri over pkt_b: 0
```

- ローミング調整のステータスを確認します。

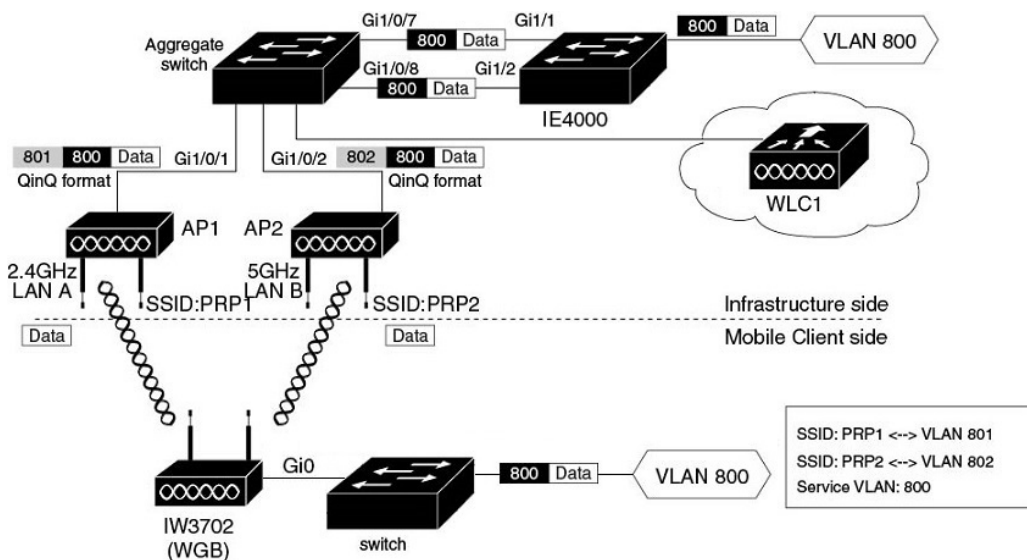
```
WGB1#show coordinator status WGB1#show dot11 coordinator statistics
```

## シングル WGB デュアル無線 PRP 冗長オプション

これらのセクションには、シングル WGB デュアル無線 PRP の冗長性のためのインフラストラクチャ側とモバイルクライアント側の設定が含まれています。

### ネットワーク トポロジの例

次の図に、シングル WGB デュアル無線 PRP 冗長性のサンプル トポロジを示します。



シングル WGB デュアル無線 PRP 冗長オプションの場合、冗長パスはシングル WGB 上の 2.4 GHz および 5 GHz 無線を介して利用できます。シングル WGB は、モバイルクライアント側で RedBox（冗長ボックス）として動作し、パケット重複と重複破棄を実行します。ネットワークインフラストラクチャ側では、PRP スイッチが RedBox として動作します。各ネットワーク コンポーネントの詳細な機能を以下に示します。

#### インフラストラクチャ側

- インフラストラクチャ側の PRP 対応スイッチ（この例では Cisco IE4000）は、RedBox として機能し、パケット重複および重複破棄機能を実行します。
- インフラストラクチャ側の AP は、異なる SSID（この例では PRP1 と PRP2）を介して冗長データトラフィックを送受信し、異なる VLAN（QinQ トンネルのカプセル化またはカプセル化解除）を使用してトラフィックにタグを付けます。
- 集約スイッチと AP 間のトラフィックは QinQ 形式であり、発信元のパスを識別します。QinQ 機能は、集約スイッチのイーサネットインターフェイス（Gi1/0/7 および Gi1/0/8）で有効になります。これらの 2 つのインターフェイスは、IE スイッチの PRP ポートに接続します。ダウンストリームトラフィックには QinQ トンネルのカプセル化を実行し、アップストリームトラフィックにはカプセル化解除を実行し、重複したトラフィックを別の VLAN 上で伝送できるようにします。

#### モバイルクライアント側

- IW3702 Gig0 ポートは、スイッチのイーサネットポートに接続します。IW3702 は PRP Redbox として機能し、クライアント VLAN トラフィック（VLAN800）に対してパケット重複および重複破棄機能を実行します。
- IW3702 は WGB として動作し、2.4 GHz および 5 GHz 無線を使用して異なる SSID（この例では PRP1 と PRP2）に接続し、異なる VLAN（この例では VLAN 801 と VLAN 802）にアサインされます。冗長ワイヤレスパスは、シングル WGB 上で 2.4 GHz および 5 GHz 無線を介して WGB の背後の有線クライアントに提供されます。

#### ローミング調整

- 2.4 GHz 無線と 5 GHz 無線の間のローミング調整は、2 つの無線が同時にローミングしないように内部通信を介して提供されます。



## インフラストラクチャ側の設定

シングル WGB デュアル無線冗長オプションの PRP over Wireless の場合、ネットワーク トポロジとインフラストラクチャ側の設定は、デュアル WGB デュアル無線冗長オプションと同じです。詳細については、「[インフラストラクチャ側の設定 \(5 ページ\)](#)」を参照してください。

## モバイルクライアント側の設定

ここでは、次のモバイルクライアント側の設定について説明します。

### ワークグループブリッジ構成

モバイルクライアント側の IW3702 の 2.4 GHz 無線と 5 GHz 無線の両方が WGB として設定され、それぞれ SSID PRP1 と SSID PRP2 に接続します。IW3702 の GigabitEthernet0 ポートは、有線クライアントトラフィックをブリッジするために通常のスイッチポートに接続されます。

次のコマンドを使用して、WGB で PRP サブモードを有効にします。

```
iw3702(config)# dot11 wgb prpiw3702(config-prp)# no shutdown
```

次の WGB の設定例では、有線クライアント vlan 800 のトラフィックが 2.4 GHz 無線の SSID PRP1 (VLAN 801) と 5 GHz 無線の SSID PRP2 (VLAN 802) の並列パスを介してブリッジされます。Bvi-vlanid は、BVI インターフェイスの VLAN ID の設定に使用され、有線クライアントの VLAN とは別である必要があります。この例では、VLAN ID 900 が設定されています。インフラストラクチャ側の WLC に、VLAN ID 900 を使用したダイナミックインターフェイスが作成されます。



(注) オープンセキュリティ方式が WGB 設定で使用されています。次の例では、**mobile station scan xx xx xx** および **mobile station period x threshold x** コマンドによって設定されるパラメータを、独自の展開に基づいて調整する必要があります。ローミングとセキュリティに関する WGB 設定ガイドラインについては、<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1130-ag-series/113198-wgb-roam-config.html> を参照してください。

```
dot11 wgb prp no shutdown bvi-vlanid 900 ! dot11 ssid PRP1 vlan 801 authentication open no ids mfp client !
dot11 ssid PRP2 vlan 802 authentication open no ids mfp client ! interface Dot11Radio0 ssid PRP1 packet retries
 32 drop-packet station-role workgroup-bridge mobile station scan 2412 2437 2462 mobile station period 1
threshold 70 rts retries 32 bridge-group 1 bridge-group 1 spanning-disabled ! interface Dot11Radio0.800
encapsulation dot1Q 800 bridge-group 50 bridge-group 50 spanning-disabled ! interface Dot11Radio0.801
encapsulation dot1Q 801 bridge-group 100 bridge-group 100 spanning-disabled ! interface Dot11Radio1 ssid PRP2
packet retries 32 drop-packet station-role workgroup-bridge mobile station scan 5745 5765 5785 mobile station
period 1 threshold 70 rts retries 32 bridge-group 1 bridge-group 1 spanning-disabled ! interface Dot11Radio1.800
encapsulation dot1Q 800 bridge-group 50 bridge-group 50 spanning-disabled ! interface Dot11Radio1.802
encapsulation dot1Q 802 bridge-group 200 bridge-group 200 spanning-disabled interface GigabitEthernet0
bridge-group 1 bridge-group 1 spanning-disabled ! interface GigabitEthernet0.800 encapsulation dot1Q 800
bridge-group 50 bridge-group 50 spanning-disabled ! workgroup-bridge unified-vlan-client workgroup-bridge
unified-vlan-client broadcast-tagging
```

シングル WGB のローミング調整機能は、両方の無線が同時にローミングするのを防ぐために、2.4 GHz 無線と 5 GHz 無線の内部通信によって動作します。ローミング調整機能は次のコマンドを使用して有効にできます。

```
dot11 coordinator uplink both dot11 coordinator timeout roam-wait 100
```

## スイッチの設定

次に、スイッチのサンプル設定を示します。

```
interface GigabitEthernet1/0/1 description ***Port to WGB*** switchport trunk encapsulation dot1q switchport
mode trunk interface GigabitEthernet1/0/2 description ***Port to wired client *** switchport access vlan 800
switchport mode access
```

## 確認

設定がすべて完了したら、次のコマンドを使用して設定を確認します。

- インフラストラクチャ側の PRP スイッチで、サービス VLAN 800 を使用して SVI インターフェイスを作成し、VLAN 800 の DHCP プールを作成します。
- モバイルクライアント側のスイッチで、VLAN 800 を使用して SVI インターフェイスを作成し、DHCP クライアントとして有線クライアントをシミュレートします。DHCP アドレスは、DHCP プール VLAN 800 から割り当てる必要があります。

```
IE-SW#show ip interface brief Interface IP-Address OK? Method Status
Protocol Vlan1 unassigned YES NVRAM administratively down down
Vlan800 10.10.80.92 YES DHCP up up
```

- 有線クライアントのステータスを確認します。

```
(WLC) >show client summary Number of Clients..... 4 Number of PMIPv6
Clients..... 0 Number of EoGRE Clients..... 0 GLAN/ RLAN/ MAC
Address AP Name Slot Status WLAN Auth Protocol Port Wired Tunnel Role -----
-----
1 Associated 8 Yes 802.11ac(5 GHz) 1 No No Local 00:81:c4:31:af:50 AP2 0 Associated 7 Yes 802.11n(2.4 GHz)
1 No No Local 00:82:c4:cc:cd:21 AP2 0 Associated 7 Yes N/A 1 No No Local (WLC) >show client detail
00:82:c4:cc:cd:21 Client MAC Address..... 00:82:c4:cc:cd:21 Client Username
..... N/A AP MAC Address..... 00:81:c4:d0:26:b0
AP Name..... AP2 AP radio slot Id.....
0 2nd AP MAC Address..... 00:81:c4:d0:26:b0 2nd AP
Name..... AP2 2nd AP radio slot Id..... 1 Client
State..... Associated Client User Group.....
Client NAC OOB State..... Access Workgroup Bridge Client.....
WGB: 00:81:c4:31:af:50 Workgroup Bridge Client..... 2nd WGB: 00:81:c4:31:7d:90 Wireless
LAN Id..... 7 Wireless LAN Network Name (SSID)..... PRP1 Wireless
LAN Profile Name..... PRP1 2nd Wireless LAN Id..... 8 2nd
Wireless LAN Network Name (SSID)..... PRP2 2nd Wireless LAN Profile Name..... PRP2
```

- データパスを確認します。

モバイルクライアント側からインフラストラクチャ側に ping を実行します。

```
PRP-SW#ping 10.10.80.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.80.1, timeout
is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```

WGB からの出力：

```
WGB#show dot11 wgb prp available uplink count: 2 Index: 0 Status: UP Name: Dot11Radio0 Virtual-Dot11Radio0
AP: cc46.d616.ad84 Index: 1 Status: UP Name: Dot11Radio1 Virtual-Dot11Radio1 AP: cc46.d616.ad8a =====
Statistic counters ===== cnt_total_sent_A: 249701 <= RADIO 0
REPLICATION cnt_total_sent_B: 249699 <= RADIO 1 REPLICATION cnt_tx_difference:
2 cnt_total_received_A: 2136458 <= RADIO 0 DISCARD cnt_total_received_B:
4123098 <= RADIO 1 DISCARD cnt_rx_difference: 1986641 cnt_total_errors_A: 0
cnt_total_errors_B: 0 cnt_total_discard: 531303 cnt_discard_table_used_items:
1024 max_duplicate_delay: 200 =====
```

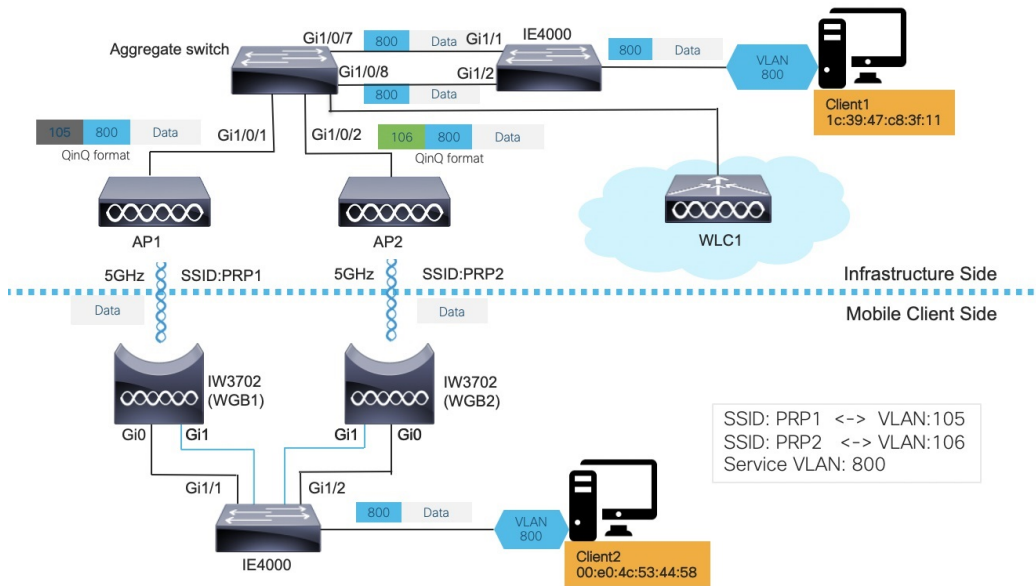
- ローミング調整のステータスを確認します。

```
WGB1#show dot11 coordinator statistics
```

## トラブルシューティング

ここでは、ワイヤレス PRP ソリューションの問題を追跡する推奨の方法について説明します。

### デュアル WGB デュアル無線 PRP 冗長オプション



上の図では、2つの有線クライアントが相互に通信しています。Client1 (1c39.47c8.3f11) はインフラストラクチャ側にあり、Client2 (00e0.4c53.4458) はモバイルクライアント側にあります。

通常、有線 Client2 は DHCP、ARP、GARP などのプロトコルを使用して通信を初期化します。ただし、有線 Client2 がパッシブクライアントである可能性があります。つまり、インフラストラクチャ側（有線 Client1 からのダウンストリーム ARP）からパケットを受信するまで通信しません。

トラブルシューティング手順については、以下の2つの項で説明します。

#### アップストリームトラフィックのトラブルシューティング

アップストリームトラフィックをトラブルシューティングするには、次の手順を使用してホップ単位でパケットを追跡します。

#### 手順

**ステップ 1** クライアント側の IE4000 で、**show mac address-table dynamic** を実行して、有線 Client2 が正しい VLAN ID を持つ MAC アドレステーブルで学習されているかどうかを確認します。

例：

```
IE4K-Switch1#show mac address-table Mac Address Table -----  
Vlan Mac Address Type Ports ----  
800 00e0.4c53.4458 DYNAMIC Gi1/24 800  
1c39.47c8.3f11 DYNAMIC PR1 1 00ee.ab49.b643 DYNAMIC PR1 1 706d.157c.1274 DYNAMIC PR1 1 d4c9.3ceb.3490  
DYNAMIC PR1 1 f80f.6fc9.2a90 DYNAMIC PR1 Total Mac Addresses for this criterion: 28
```

**ステップ2** クライアント側の IE4000 で、**show prp channel 1 detail** を実行して、PRP ポートが正しくバインドされているかどうかを確認します。

例：

```
IE4K-Switch1#show prp channel 1 detail PRP-channel: PR1 ----- Layer type = L2 Ports: 2 Maxports  
= 2 Port state = prp-channel is Inuse Protocol = Enabled Ports in the group: 1) Port: Gi1/1 Logical  
slot/port = 1/1 Port state = Inuse Protocol = Enabled 2) Port: Gi1/2 Logical slot/port = 1/2 Port  
state = Inuse Protocol = Enabled
```

**show prp statistics egressPacketStatistics** を実行して、LAN-A および LAN-B の出力カウンタを確認します。両方の PRP 無線が UP 状態の場合は、以下の送信カウンタが等しく増加します。

例：

```
IE4K-Switch1#show prp statistics egressPacketStatistics PRP channel-group 1 EGRESS STATS: duplicate  
packet: 7383179 supervision frame sent: 3113533 packet sent on lan a: 4870442 packet sent on lan  
b: 5431455 byte sent on lan a: 1105813244 byte sent on lan b: 1141294801 egress packet receive from  
switch: 7581389 overrun pkt: 0 overrun pkt drop: 0
```

**ステップ3** 両方の WGB で **show bridge** を実行して、有線クライアントの MAC が正しいブリッジグループ（ブリッジ ID）で学習されているかどうかを確認します。

例：

```
WGB1#show bridge Total of 300 station blocks, 291 free Codes: P - permanent, S - self Bridge Group  
1: Address Action Interface Age RX count TX count 1c39.47c8.3f11 forward Vi0.106 0 5168 0  
68a3.c4a0.2568 forward Vi0.106 3 2 0 00ee.ab49.bc1a forward Gi0.106 0 2385 0 00ee.ab49.b619 forward  
Vi0.106 0 20269 0 f80f.6fc9.2a90 forward Vi0.106 0 158 0 00ee.ab49.b643 forward Vi0.106 0 50 0  
Bridge Group 2: 00e0.4c53.4458 forward Gi0.800 0 3299 0 1c39.47c8.3f11 forward Vi0.800 0 1 119  
00ee.ab49.bc41 forward Gi0.800 1 6 0 WGB2#show bridge Total of 300 station blocks, 294 free Codes:  
P - permanent, S - self Bridge Group 1: Address Action Interface Age RX count TX count 1c39.47c8.3f11  
forward Vi0.105 0 5381 0 00ee.ab49.bc1a forward Gi0.105 0 1908 0 00ee.ab49.b619 forward Vi0.105 0  
3226 0 Bridge Group 2: 00e0.4c53.4458 forward Gi0.800 0 2656 0 1c39.47c8.3f11 forward Vi0.800 0 1  
81 00ee.ab49.bc41 forward Gi0.800 0 6 0
```

**ステップ4** WLC で、**show client detail <mac\_of\_client>** を実行して、クライアントが学習され、両方の WGB の詳細が WLC で学習されているかどうかを確認します。

例：

```
(Cisco Controller) >show client detail 00:e0:4c:53:44:58 Client MAC  
Address..... 00:e0:4c:53:44:58 Client Username  
..... N/A Client Webauth Username ..... N/A Hostname:  
..... Device Type: ..... Unclassified  
AP MAC Address..... 70:ea:1a:29:90:80 AP  
Name..... PRP_Root2_E984 AP radio slot  
Id..... 1 2nd AP MAC Address.....  
f8:0f:6f:c9:2a:90 2nd AP Name..... PRP_Root1_B89C 2nd AP radio slot  
Id..... 1 Client State..... Associated User  
Authenticated by ..... None Client User Group.....  
Client NAC OOB State..... Access Workgroup Bridge  
Client..... WGB: 70:6d:15:7c:12:74 Workgroup Bridge  
Client..... 2nd WGB: d4:c9:3c:eb:34:90 Wireless LAN  
Id..... 3 Wireless LAN Network Name (SSID)..... PRP2 Wireless  
LAN Profile Name..... PRP2 WLAN Profile check for roaming.....
```

```

Disabled 2nd Wireless LAN Id..... 2 2nd Wireless LAN Network Name
(SSID)..... PRP1 2nd Wireless LAN Profile Name..... PRP1 Hotspot
(802.11u)..... Not Supported Connected For
..... 56696 secs BSSID.....
70:ea:1a:29:90:8f Channel..... 36 2nd
BSSID..... f8:0f:6f:c9:2a:9f 2nd Connected For
..... 68424 secs 2nd Channel..... 108 IP
Address..... 10.80.80.58 Gateway
Address..... 10.80.80.1 Netmask.....
255.255.255.0 IPv6 Address..... fe80::5faa:5113:e3ee:1515 Association
Id..... 0 Authentication Algorithm..... Open
System Reason Code..... 1 Client
IPSK-TAG..... N/A Status Code..... 0
2nd Association Id..... 1 2nd Authentication Algorithm.....
Open System 2nd Reason Code..... 1 2nd Status
Code..... 0 Session Timeout..... 0 Client
CCX version..... No CCX support 2nd FlexConnect Data
Switching..... Local 2nd FlexConnect Dhcp Status..... Local 2nd
FlexConnect Vlan Based Central Switching.... No 2nd FlexConnect Authentication.....
Central 2nd FlexConnect Central Association..... No 2nd FlexConnect VLAN
NAME..... Unavailable 2nd Quarantine VLAN..... 0 2nd
Access VLAN..... 106 2nd Local Bridging VLAN.....
106 QoS Level..... Silver Avg data
Rate..... 0 Burst data Rate..... 0 Avg
Real time data Rate..... 0 Burst Real Time data Rate.....
0 Avg Uplink data Rate..... 0 Burst Uplink data
Rate..... 0 Avg Uplink Real time data Rate..... 0 Burst Uplink
Real Time data Rate..... 0 802.1P Priority Tag..... disabled
Security Group Tag..... Unknown(0) KTS CAC
Capability..... No Qos Map Capability ..... 非
対応

```

**ステップ5** インフラストラクチャ側の集約スイッチで、**show mac address-table** を実行して、Client2 が2つの VLAN (PRP 外部 VLAN ID) で学習されているかどうかを確認します。

例 :

```

IOTLABSWITCH#show mac address-table dynamic Mac Address Table
----- Vlan Mac Address Type Ports -----
----- 1 0077.8daa.c747 STATIC V11 77 0077.8daa.c773 STATIC V177 11 0077.8daa.c754 STATIC V111 40
0077.8daa.c764 STATIC V140 41 0077.8daa.c776 STATIC V141 47 0077.8daa.c751 STATIC V147 65
0077.8daa.c77b STATIC V165 104 0077.8daa.c769 STATIC V1104 104 d4c9.3ce3.16ec DYNAMIC Gi1/0/2 105
0077.8daa.c779 STATIC V1105 105 00ee.ab49.b619 DYNAMIC Gi1/0/9
105 00ee.ab49.b643 DYNAMIC Gi1/0/9 105 1c39.47c8.3f11 DYNAMIC Gi1/0/9 105 706d.157c.1274 DYNAMIC
Gi1/0/32 106 0077.8daa.c74d STATIC V1106 106 00ee.ab49.b619
DYNAMIC Gi1/0/5 106 00ee.ab49.b643 DYNAMIC Gi1/0/5 106 1c39.47c8.3f11 DYNAMIC Gi1/0/5 106
68a3.c4a0.2568 DYNAMIC Gi1/0/32 106 c412.f530.e10b DYNAMIC Gi1/0/48 106 d4c9.3ceb.3490 DYNAMIC
Gi1/0/32 107 0077.8daa.c75d STATIC V1107 402 0077.8daa.c77b STATIC V1402 20 0077.8daa.c756 STATIC
V120 93 0077.8daa.c774 STATIC V193 800 0077.8daa.c752 STATIC V1800 803 0077.8daa.c757 STATIC V1803

```

**ステップ6** インフラストラクチャ側の IE4000 スイッチで、**show mac address-table** を実行して、Client2 の MAC が正しい VLAN (内部 VLAN) で学習されているかどうかを確認します。

例 :

```

IE4K-Switch2#show mac address-table Mac Address Table -----
Vlan Mac Address Type Ports -----
----- 1 0077.8daa.c705 DYNAMIC PR1 1
0077.8daa.c709 DYNAMIC PR1 1 0077.8daa.c74d DYNAMIC PR1 1 0077.8daa.c779 DYNAMIC PR1 1 706d.157c.1274
DYNAMIC PR1 1 c412.f530.e10b DYNAMIC PR1 1 d4c9.3ceb.3490 DYNAMIC PR1 1 800 00e0.4c53.4458 DYNAMIC
PR1 800 1c39.47c8.3f11 DYNAMIC Gi1/11

```

## ダウンストリームトラフィックのトラブルシューティング

IoTシナリオでは、複数VLANの展開が一般的なソリューションです。お客様は、ネットワーク全体でさまざまなOT/ITデバイスに異なるVLAN IDを割り当てます。

マルチVLANネットワークの設定の詳細については、[WGBマルチクライアントVLANの設定（11ページ）](#)を参照してください。

実際の導入例では、WGB側の一部のデバイスがパッシブクライアント（静的IPアドレスを持つクライアントなど）になることがあります。ピアデバイスがクライアントと通信する場合は、セグメント内でARPをブロードキャストしません。

ブロードキャストされたARP要求は、有線ネットワーク全体にフラディングされ、最終的にインフラストラクチャAPに到達します。VLAN IDを保持するために、インフラストラクチャAPは、そのアドレスにVLAN IDを入力して、ブロードキャストアドレスを特殊なマルチキャストアドレスに変換します。

パケットがWGBに到達すると、WGBは特殊なマルチキャストをブロードキャストに変換し、VLAN IDを回復して、ブロードキャストARP REQUESTを対応するGigabitEthernetサブインターフェイスに転送します。

前述のシナリオをトラブルシューティングするには、次の手順を使用してホップ単位でパケットを追跡します。

### 手順

---

**ステップ1** インフラストラクチャAP側でキャプチャを行い、ARPがQ-in-Q形式であることを確認します。

**ステップ2** 次のデバッグログを確認します。

- a) ルートAPで、**debug dot11 d[0/1] trace print xmt**を有効にして、特殊なマルチキャストとVLANが無線で送信されるかどうかを確認します。

例：

```
ICMP ping code 0 chk D3BD, id 2591 seq 12170 9E21 665E 0000 0000 2446 0300 0000 0000 1011 1213
1415 1617 1819 1A1B 1C1D *Mar 9 16:24:35.131: 343DD786 t 18 0 - 0842 000 m01005E C92A9F 361E08
6F40 198 IP 10.80.80.255 < 10.80.80.74 f1-0-0 id 0 ttl64 sum 84C0 prot 1 len 84
```

- b) **debug dot11 forwarding** および **debug dot11 d[0/1] trace print rcv**を使用して、特殊なマルチキャストとVLANがWGBで受信されるかどうかを確認します。

例：

```
*Nov 8 21:44:53.590: C572B747 r 18 39/62/128/57 57- 0842 000 m01005E C92A9F 361E08 F150 1114 IV
AAAA0300 0000 0800 4500 0054 0000 4000 4001 84C0 0A50 504A 0A50 50FF 0800 BE39 0A1F 2DEE 0120
665E 0000 0000 D367 0800 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D 1E1F 2021 2223 2425 2627
2829 2A2B 2C2D 2E2F 3031 3233 *Nov 8 21:46:30.754: Unified WGB convert specific mcast+vlan pak
to ffff.ffff.ffff:00e0.4c36.1e08 on Virtual-Dot11Radio0 received, link 7, dest_vlan_id 0x4320
packet for ffff.ffff.ffff:00e0.4c36.1e08 on Virtual-Dot11Radio0 received, link 7 to_host 1 rc
9 smf_result 201 Virtual-Dot11Radio0.106, 0,
```

**ステップ3** WGBの背後でパケットキャプチャを実行し、ARPが正しいVLANでブロードキャストに変換されるかどうかを確認します。

```

2 0.00004606  RealtekS_36:1e:08  Broadcast  ARP  74 Who has 10.80.80.73? Tell 10.80.80.74
-----
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: RealtekS_36:1e:08 (00:e0:4c:36:1e:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 106
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 800
Address Resolution Protocol (request)

```

**次のタスク**

ダウンストリームユニキャストトラフィックの場合も同様ですが、アップストリームと方向が逆になります。PRP-WGB-SW で、**show prp statistics ingressPacketStatistics** を実行します。

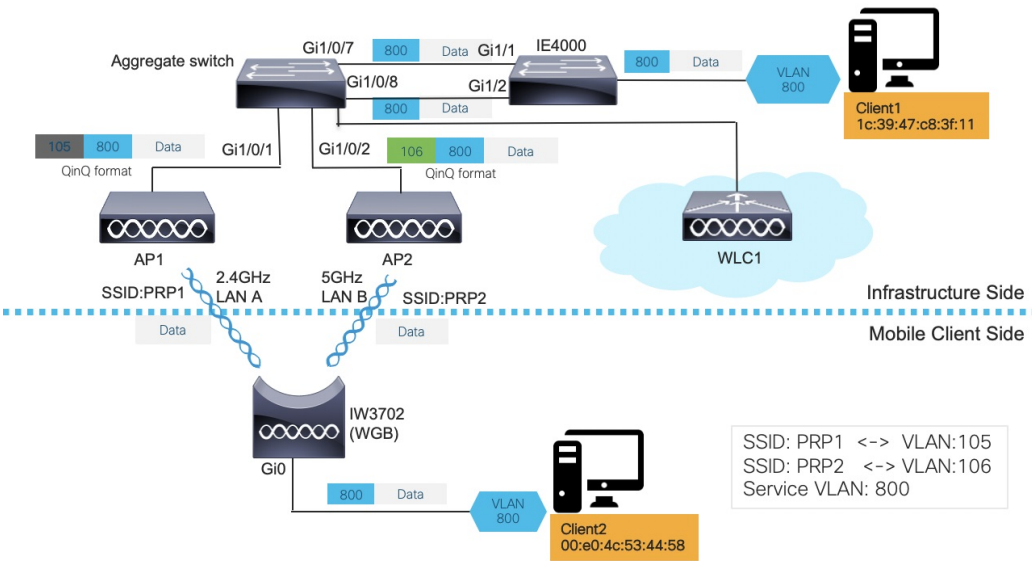
例:

```

IE4K-Switch1#show prp statistics ingressPacketStatistics PRP channel-group 1 INGRESS STATS: ingress pkt lan a:
7359054 ingress pkt lan b: 10102696 ingress crc lan a: 0 ingress crc lan b: 0 ingress danp pkt acpt: 7376949
ingress danp pkt dscrd: 1648270 ingress supfrm rcv a: 4175430 ingress supfrm rcv b: 4262230

```

**シングル WGB デュアル無線 PRP 冗長オプション**



上の図では、2つの有線クライアントが相互に通信しています。Client1 (1c:39:47:c8:3f:11) はインフラストラクチャ側にあり、Client2 (00:e0:4c:53:44:58) はモバイルクライアント側にあります。

通常、有線 Client2 は DHCP、ARP、GARP などのプロトコルを使用して通信を初期化します。ただし、有線 Client2 がパッシブクライアントである可能性があります。つまり、インフラストラクチャ側（有線 Client1 からのダウンストリーム ARP）からパケットを受信するまで通信しません。

トラブルシューティング手順については、以下の2つの項で説明します。

## アップストリームトラフィックのトラブルシューティング

アップストリームトラフィックをトラブルシューティングするには、次の手順を使用してホップ単位でパケットを追跡します。

### 手順

**ステップ 1** クライアント側の IE4000 スイッチで、**show mac address-table dynamic** を実行して、有線 Client2 が正しい VLAN ID を持つ MAC アドレステーブルで学習されているかどうかを確認します。

例：

```
IE4K-Switch1#show mac address-table Mac Address Table -----
Vlan Mac Address Type Ports ----
-----
800 00e0.4c53.4458 DYNAMIC Gi1/24 800
1c39.47c8.3f11 DYNAMIC PR1 1 00ee.ab49.b643 DYNAMIC PR1 1 706d.157c.1274 DYNAMIC PR1 1 d4c9.3ceb.3490
DYNAMIC PR1 1 f80f.6fc9.2a90 DYNAMIC PR1 Total Mac Addresses for this criterion: 28
```

**ステップ 2** WGB で **show bridge** を実行して、有線クライアントの MAC が正しいブリッジグループ（ブリッジ ID）で学習されているかどうかを確認します。

例：

```
WGB1#show bridge Total of 300 station blocks, 291 free Codes: P - permanent, S - self Bridge Group
1: Address Action Interface Age RX count TX count 1c39.47c8.3f11 forward Vi0.106 0 5168 0
68a3.c4a0.2568 forward Vi0.106 3 2 0 00ee.ab49.bc1a forward Gi0.106 0 2385 0 00ee.ab49.b619 forward
Vi0.106 0 20269 0 f80f.6fc9.2a90 forward Vi0.106 0 158 0 00ee.ab49.b643 forward Vi0.106 0 50 0
Bridge Group 2: 00e0.4c53.4458 forward Gi0.800 0 3299 0 1c39.47c8.3f11 forward Vi0.800 0 1 119
00ee.ab49.bc41 forward Gi0.800 1 6 0
```

**ステップ 3** WGB で **show dot11 wgb prp** を実行して、LAN-A および LAN-B の出力カウンタを確認します。両方の PRP 無線が UP 状態の場合は、以下の送信カウンタが等しく増加します。

例：

```
Current work mode : dual-radio Link selection mode : PRP Available uplink count: 2 Index: 0 Status:
UP Name: Dot11Radio0/Virtual-Dot11Radio0 Peer: 54a2.7474.d920 Index: 1 Status: UP Name:
Dot11Radio1/Virtual-Dot11Radio1 Peer: 54a2.7474.d92f ===== PRP STATISTICS
===== LAN-A Send : 23991 LAN-B Send : 23991 Send Difference : 0 LAN-A Rcv : 0 LAN-B
Rcv : 0 Rcv Difference : 0 LAN-A Error : 0 LAN-B Error : 0 Discard : 0 Table Usage (INTERNAL) : 0
Max Dup-Delay (INTERNAL) : 0 =====
```

**ステップ 4** WLC で、**show client detail <mac\_of\_client>** を実行して、クライアントが学習され、両方の WGB の詳細が WLC で学習されているかどうかを確認します。

例：

```
(Cisco Controller) >show client detail 00:e0:4c:53:44:58 Client MAC
Address..... 00:e0:4c:53:44:58 Client Username
..... N/A Client Webauth Username ..... N/A Hostname:
..... Device Type: ..... Unclassified
AP MAC Address..... 70:ea:1a:29:90:80 AP
Name..... PRP_Root2_E984 AP radio slot
Id..... 1 2nd AP MAC Address.....
f8:0f:6f:c9:2a:90 2nd AP Name..... PRP_Root1_B89C 2nd AP radio slot
Id..... 1 Client State..... Associated User
Authenticated by ..... None Client User Group.....
Client NAC OOB State..... Access Workgroup Bridge
Client..... WGB: 70:79:b3:87:89:b0 Workgroup Bridge
Client..... 2nd WGB: 70:79:b3:44:73:60 Wireless LAN Id
```



```

..... 3 Wireless LAN Network Name (SSID)..... PRP2 Wireless
LAN Profile Name..... PRP2 WLAN Profile check for roaming.....
Disabled 2nd Wireless LAN Id..... 2 2nd Wireless LAN Network Name
(SSID)..... PRP1 2nd Wireless LAN Profile Name..... PRP1 Hotspot
(802.11u)..... Not Supported Connected For
..... 56696 secs BSSID.....
70:ea:1a:29:90:8f Channel..... 36 2nd
BSSID..... f8:0f:6f:c9:2a:9f 2nd Connected For
..... 68424 secs 2nd Channel..... 108 IP
Address..... 10.80.80.58 Gateway
Address..... 10.80.80.1 Netmask.....
255.255.255.0 IPv6 Address..... fe80::5faa:5113:e3ee:1515 Association
Id..... 0 Authentication Algorithm..... Open
System Reason Code..... 1 Client
IPSK-TAG..... N/A Status Code..... 0
2nd Association Id..... 1 2nd Authentication Algorithm.....
Open System 2nd Reason Code..... 1 2nd Status
Code..... 0 Session Timeout..... 0 Client
CCX version..... No CCX support 2nd FlexConnect Data
Switching..... Local 2nd FlexConnect Dhcp Status..... Local 2nd
FlexConnect Vlan Based Central Switching.... No 2nd FlexConnect Authentication.....
Central 2nd FlexConnect Central Association..... No 2nd FlexConnect VLAN
NAME..... Unavailable 2nd Quarantine VLAN..... 0 2nd
Access VLAN..... 106 2nd Local Bridging VLAN.....
106 QoS Level..... Silver Avg data
Rate..... 0 Burst data Rate..... 0 Avg
Real time data Rate..... 0 Burst Real Time data Rate.....
0 Avg Uplink data Rate..... 0 Burst Uplink data
Rate..... 0 Avg Uplink Real time data Rate..... 0 Burst Uplink
Real Time data Rate..... 0 802.1P Priority Tag..... disabled
Security Group Tag..... Unknown(0) KTS CAC
Capability..... No Qos Map Capability ..... 非
対応

```

**ステップ5** インフラストラクチャ側の集約スイッチで、**show mac address-table** を実行して、Client2 が2つの VLAN (PRP 外部 VLAN ID) で学習されているかどうかを確認します。

例：

```

IOTLABSWITCH#show mac address-table dynamic Mac Address Table
----- Vlan Mac Address Type Ports -----
----- 1 0077.8daa.c747 STATIC V11 77 0077.8daa.c773 STATIC V177 11 0077.8daa.c754 STATIC V111 40
0077.8daa.c764 STATIC V140 41 0077.8daa.c776 STATIC V141 47 0077.8daa.c751 STATIC V147 65
0077.8daa.c77b STATIC V165 104 0077.8daa.c769 STATIC V1104 104 d4c9.3ce3.16ec DYNAMIC Gi1/0/2 105
0077.8daa.c779 STATIC V1105 105 00ee.ab49.b619 DYNAMIC Gi1/0/9
105 00ee.ab49.b643 DYNAMIC Gi1/0/9 105 1c39.47c8.3f11 DYNAMIC Gi1/0/9 105 706d.157c.1274 DYNAMIC
Gi1/0/32 106 0077.8daa.c74d STATIC V1106 106 00ee.ab49.b619 DYNAMIC Gi1/0/32 106 00ee.ab49.b619
DYNAMIC Gi1/0/5 106 00ee.ab49.b643 DYNAMIC Gi1/0/5 106 1c39.47c8.3f11 DYNAMIC Gi1/0/5 106
68a3.c4a0.2568 DYNAMIC Gi1/0/32 106 c412.f530.e10b DYNAMIC Gi1/0/48 106 d4c9.3ceb.3490 DYNAMIC
Gi1/0/32 107 0077.8daa.c75d STATIC V1107 402 0077.8daa.c77b STATIC V1402 20 0077.8daa.c756 STATIC
V120 93 0077.8daa.c774 STATIC V193 800 0077.8daa.c752 STATIC V1800 803 0077.8daa.c757 STATIC V1803

```

**ステップ6** インフラストラクチャ側の IE4000 スイッチで、**show mac address-table** を実行して、Client2 の MAC が正しい VLAN (内部 VLAN) で学習されているかどうかを確認します。

例：

```

IE4K-Switch2#show mac address-table Mac Address Table -----
Vlan Mac Address Type Ports ----- 1 0077.8daa.c705 DYNAMIC PR1 1
0077.8daa.c709 DYNAMIC PR1 1 0077.8daa.c74d DYNAMIC PR1 1 0077.8daa.c779 DYNAMIC PR1 1 706d.157c.1274
DYNAMIC PR1 1 c412.f530.e10b DYNAMIC PR1 1 d4c9.3ceb.3490 DYNAMIC PR1 800 00ee.04c53.4458 DYNAMIC
PR1 800 1c39.47c8.3f11 DYNAMIC Gi1/11

```

---

## ダウンストリームトラフィックのトラブルシューティング

IoTシナリオでは、複数VLANの展開が一般的なソリューションです。お客様は、ネットワーク全体でさまざまなOT/ITデバイスに異なるVLAN IDを割り当てます。

マルチVLANネットワークの設定の詳細については、[WGBマルチクライアントVLANの設定（11ページ）](#)を参照してください。

実際の導入例では、WGB側の一部のデバイスがパッシブクライアント（静的IPアドレスを持つクライアントなど）になることがあります。ピアデバイスがクライアントと通信する場合は、セグメント内でARPをブロードキャストしません。

ブロードキャストされたARP要求は、有線ネットワーク全体にフラディングされ、最終的にインフラストラクチャAPに到達します。VLAN IDを保持するために、インフラストラクチャAPは、そのアドレスにVLAN IDを入力して、ブロードキャストアドレスを特殊なマルチキャストアドレスに変換します。

パケットがWGBに到達すると、WGBは特殊なマルチキャストをブロードキャストに変換し、VLAN IDを回復して、ブロードキャストARP REQUESTを対応するGigabitEthernetサブインターフェイスに転送します。

前述のシナリオをトラブルシューティングするには、次の手順を使用してホップ単位でパケットを追跡します。

### 手順

---

**ステップ1** インフラストラクチャAP側でキャプチャを行い、ARPがQ-in-Q形式であることを確認します。

**ステップ2** 次のデバッグログを確認します。

- a) ルートAPで、**debug dot11 d[0/1] trace print xmt**を有効にして、特殊なマルチキャストとVLANが無線で送信されるかどうかを確認します。

例：

```
ICMP ping code 0 chk D3BD, id 2591 seq 12170 9E21 665E 0000 0000 2446 0300 0000 0000 1011 1213
1415 1617 1819 1A1B 1C1D *Mar 9 16:24:35.131: 343DD786 t 18 0 - 0842 000 m01005E C92A9F 361E08
6F40 198 IP 10.80.80.255 < 10.80.80.74 f1-0-0 id 0 ttl64 sum 84C0 prot 1 len 84
```

- b) **debug dot11 forwarding** および **debug dot11 d[0/1] trace print rcv** を使用して、特殊なマルチキャストとVLANがWGBで受信されるかどうかを確認します。

例：

```
*Nov 8 21:44:53.590: C572B747 r 18 39/62/128/57 57- 0842 000 m01005E C92A9F 361E08 F150 1114 IV
AAAA0300 0000 0800 4500 0054 0000 4000 4001 84C0 0A50 504A 0A50 50FF 0800 BE39 0A1F 2DEE 0120
665E 0000 0000 D367 0800 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D 1E1F 2021 2223 2425 2627
2829 2A2B 2C2D 2E2F 3031 3233 *Nov 8 21:46:30.754: Unified WGB convert specific mcast+vlan pak
to ffff.ffff.ffff:00e0.4c36.1e08 on Virtual-Dot11Radio0 received, link 7, dest_vlan_id 0x4320
packet for ffff.ffff.ffff:00e0.4c36.1e08 on Virtual-Dot11Radio0 received, link 7 to_host 1 rc
9 smf_result 201 Virtual-Dot11Radio0.106, 0,
```

**ステップ3** WGBの背後でパケットキャプチャを実行し、ARPが正しいVLANでブロードキャストに変換されるかどうかを確認します。

```
2 0.000004606 RealtekS_36:1e:08 Broadcast ARP 74 Who has 10.80.80.73? Tell 10.80.80.74
-----
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: RealtekS_36:1e:08 (00:e0:4c:36:1e:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 106
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 800
Address Resolution Protocol (request)
```

## 次のタスク

ダウンストリームユニキャストトラフィックの場合も同様ですが、アップストリームと方向が逆になります。WGBで **show dot11 wgb prp** を実行して、LAN-A および LAN-B の入力カウンタを確認します。両方の PRP 無線が UP 状態の場合は、以下の受信カウンタが等しく増加します。

例:

```
Current work mode : dual-radio Link selection mode : PRP Available uplink count : 2 Index: 0 Status: UP Name:
Dot11Radio0/Virtual-Dot11Radio0 Peer: 54a2.7474.d920 Index: 1 Status: UP Name: Dot11Radio1/Virtual-Dot11Radio1
Peer: 54a2.7474.d92f ===== PRP STATISTICS ===== LAN-A Send : 23991 LAN-B Send :
23991 Send Difference : 0 LAN-A Rcv : 53223 LAN-B Rcv : 53223 Rcv Difference : 0 LAN-A Error : 0 LAN-B Error
: 0 Discard : 0 Table Usage (INTERNAL) : 0 Max Dup Delay (INTERNAL) : 0
=====
```

## 関連資料

- [Parallel Redundancy Protocol Enhancement on AP and WGB](#)
- [Dual Radio Parallel Redundancy Protocol Enhancement on WGB](#)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017-2020 Cisco Systems, Inc. All rights reserved.

【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/](http://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。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### 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/>