WGB ローミング：内部詳細と設定

内容

概要

Cisco ワークグループ ブリッジ（WGB）は、非ワイヤレス デバイスがモビリティを取得できるようにするため、ワイヤレス ネットワークの設計と導入に非常に役に立つツールです。WGB は、必要に応じて導入シナリオに影響を与える、ローミング、セキュリティ アクセスなどに関する多くの詳細を提供します。

コード バージョン 12.4（25d）JA 以降では、高速ローミング環境での WGB の使用を最適化するために、一連のコマンドと変更が導入されました。

このドキュメントは、WGB の仕組みのさまざまな局面について説明します。それには、ローミング アルゴリズムの決定ポイントや、目的の使用モデルに合わせて WGB を設定する方法などが含まれます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ワイヤレス LAN ソリューション
- Cisco ワークグループ ブリッジ

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ワークグループ ブリッジとは何ですか。

基本的に、WGB はインフラストラクチャへのワイヤレス クライアントとして機能し、イーサネット インターフェイスに接続されたデバイスにレイヤ 2 接続を提供するように設定されたアクセスポイント（AP）です。

典型的な WGB の導入には次のコンポーネントがあります。

- WGB デバイス。通常は少なくとも 1 つの無線と 1 つのイーサネット インターフェイスを備える
- ワイヤレス インフラストラクチャ。通常はルート AP と呼ばれ、自律型または統一型のいずれか
- WGB に接続された 1 つ以上の有線クライアント デバイスこのドキュメントでは、混在したロールのシナリオ（WGB としての 1 つの無線、同じ AP のルートとしての 1 つの無線）については説明しません。

WGB の主なタイプには、以下の 3 つがあります。

- **Cisco WGB**：Cisco WGB は、WGB として設定された、Cisco IOS® ベースの AP です（1130、1240、1250 など）。 このモードは、IAPP プロトコルを使用して、WGB がイーサネット インターフェイスで学習したデバイスをネットワーク インフラストラクチャに通知します。この場合、ワイヤレス LAN コントローラ（WLC）またはルート AP は、WGB から「

接続」しているデバイスのレイヤ 2 を可視化します。
- **シスコ以外の WGB**：これは、WGB として機能するサード パーティ デバイスで、1 つ以上の有線デバイスをワイヤレス インフラストラクチャに接続します。これらは IAPP をサポートしていません。また、1 つの有線デバイスのみを許可するか、または MAC アドレス変換メカニズムを提供して、すべての有線クライアントを単一の 802.11 MAC アドレスの背後に隠します。これらのタイプのデバイスは、セキュリティ検査およびコントローラで行われるフレーム処理のためにインフラストラクチャが WLC である場合に、アドレス解決プロトコル（ARP）と DHCP フレームに対して特別な処理を必要とします。
- **「ユニバーサル WGB」として設定された Cisco AP**：これは、IAPP のメカニズムを抑制するモードであるため、WGB はシスコのインフラストラクチャまたはサード パーティのルート AP のいずれかに使用できます。この場合、WGB はイーサネット クライアントのアドレスを取得し、その背後にあるデバイスの数を 1 に制限します。

次のセクションでは、自律型または WLC インフラストラクチャ向けに使用される Cisco WGB のシナリオを中心に説明します。

使用シナリオ

典型的な WGB の使用例として、次のものがあります。

- 有線プリンタをネットワークに接続する
- ケーブルを有線デバイスに接続することが現実的でないか、実用的ではない、さまざまな製造業の導入
- WGB が車や地下鉄車両などから屋外のワイヤレス ネットワークへの接続を提供する車載導入
- 有線カメラ

それぞれの例には、次の条件に関する独自の要件があります。

- ワイヤレス インフラストラクチャ上で実行されるアプリケーションをサポートするために必要な帯域幅
- ローミング遅延耐性 - デバイスの移動中に WGB が現在の AP から次の AP に移動するのに必要な時間
- 転送時間耐性 - 各ローミングで失われるフレームの数

プリンタはあまり移動しないため、ローミングの必要性は少なくなります。一方、WGB を搭載した列車の場合、移動中に正しい動作を保証するためにローミング コンポーネントを微調整する必要があります。

ビデオ ストリームは広い帯域幅を必要とする可能性があるため、高い無線データ レートが必要です。ただし、テレメトリ アプリケーションは数個のフレームしか必要としないことがときどきあります。

要件は WGB の設定だけでなく、ワイヤレス インフラストラクチャの設計方法にも影響するため、最初から適切に定義されていることが重要です。たとえば、AP の配置、距離、電力レベル、有効な速度などはすべてローミングの特性に影響を与えます。したがって、高速ローミングが必要な場合、すべてが重要なポイントです。

一般に、次の詳細を認識している必要があります。

- アプリケーションの必要な帯域幅は何ですか。
- ローミング遅延耐性は何ですか。

- アプリケーションはネットワークの切断を適切に処理できますか。追加のバックアップ メカニズムがありますか。
- アプリケーションはパケット損失を適切に処理できますか。（最良なワイヤレス設計であっても、ある程度のパケット損失を予期する必要があります。）

このドキュメントでは、高速ローミングや屋外向けの RF 環境を設計する方法の詳細は扱っていません。屋外メッシュ導入ガイドを参照してください。

ローミング

ワイヤレス デバイスの場合、ローミングはその機能の非常に重要な部分です。

基本的に、ローミングはある AP から別の AP へ移動する機能で、両方が同じ無線インフラストラクチャに属しています。

ローミングは現在の AP から次の AP への変更を必要とするため、結果として切断やサービスのない時間が発生します。この切断は小さくてもかまいません。たとえば、音声の導入では、200 ミリ秒未満、または必要とされるセキュリティが各ローミング イベントで完全な認証を強制する場合は、さらに長い秒数です。

デバイスが可能な限り良好なシグナルで新しい親を検出し、ネットワーク インフラストラクチャに適切にアクセスを継続できるようにするにはローミングが必要です。同時に、ローミングが多すぎると、複数の切断やサービスのない時間が発生し、アクセスに影響を与えます。WGB などのモバイル デバイスでは、さまざまな RF 環境とデータのニーズに対応するのに十分な設定機能を備えた、適切なローミング アルゴリズムを使用することが重要です。

ローミングの要素

- **トリガー**：各クライアントの実装には 1 つ以上のトリガーまたはイベントがあり、これが満たされると、デバイスは別の親 AP に移動します。例:ビーコン損失（デバイスは AP からの通常のビーコンが聞こえなくなる）、パケット再試行、信号レベル、受信データなし、非認証フレームの受信、使用中の低データ レートなど。可能なトリガーは完全に標準化されているわけではないため、クライアントの実装とは異なる場合があります。簡単なデバイスのトリガー セットが不適切であると、不正なローミング（スティッキ クライアント）または不要なローミングが発生します。WGB はこれまで説明したすべての要素をサポートしています。
- **スキャン時間**：ワイヤレス デバイス（WGB）は、潜在的な親を検索するのにある程度の時間を要します。通常、これはさまざまなチャネルを使用して、アクティブなプロービングや AP の受動的なリスニングを行うことを意味します。無線がスキャンする必要があるため、WGB がデータ転送以外の実行に要する時間があることを意味します。このスキャン時間から、WGB はローミングできる有効な親のセットを作成できます。
- **親の選択**：スキャン時間後に、WGB は潜在的な親を確認し、最適な親を選択し、関連付け/認証プロセスを開始できます。ローミング イベントに重要な利点がない場合、決定ポイントが現在の親のままになることがあります（過度なローミングは悪影響を及ぼす可能性があることに注意してください）。
- **関連付け/認証**：WGB は、通常、802.11 の認証と関連付けの両方のフェーズに加え、SSID（WPA 2-PSK、CCKM、None）で設定されたセキュリティ ポリシーを実行する新しい AP に関連付けます。
- **トラフィックの転送の復元**：WGB は、ローミング後に IAPP のアップデートを実行することにより、既知の有線クライアントのネットワーク インフラストラクチャを更新します。この

時点以降、有線クライアントとネットワークの間のトラフィックが再開されます。

構成ガイド - セキュリティ ポリシー

モバイル デバイスでのローミングの重要な側面の 1 つは、インフラストラクチャに実装されるセキュリティ ポリシーです。さまざまなオプションがあり、それぞれに良い点と悪い点があります。その中でも特に重要なものは次のとおりです。

- **オープン：基本的にセキュリティはありません。**これは、すべてのポリシーの中で最速かつシンプルです。これには、インフラストラクチャへの不正アクセスを制限しない、また攻撃に対して無保護であるという大きな問題があります。そのため、この使用は非常に特殊なシナリオに限定されます。たとえば、導入の性質が純粋であるために外部攻撃が不可能な鉱山などです。
- **MAC アドレスの認証：MAC アドレスのスプーフィングは簡単な攻撃であるため、基本的にオープンなセキュリティと同じレベルです。**MAC の検証を実行する時間が余分に発生し、ローミング速度が低下するため、推奨されていません。
- **WPA2-PSK**：優れたレベルの暗号化(AES-CCMP)を提供しますが、認証セキュリティは事前共有キーの品質によって異なります。セキュリティ対策のため、12 文字以上のランダムなパスワードが推奨されます。事前共有鍵方法と同様に、鍵は複数のデバイスで使用されるため、鍵が侵害された場合、すべての機器でパスワードを変更する必要があります。ローミングは 6 回のフレーム交換で行われるため、ローミング速度は許容範囲です。また、外部機器（RADIUS サーバ など）は含まれていないため、ローミングを実行するための上限時間と下限時間を計算できます。 一般的に、問題と利点のバランスを取ると、この方法が推奨されます。
- **802.1xを使用するWPA2**：これは、個別に変更できるデバイスまたはユーザごとのクレデンシャルを使用することで、前の方法で改善されます。主な問題は、ローミングの場合、デバイスが高速で移動しているときや短いローミング時間が必要なときに、この方法が適切に機能しないことです。一般に、これは同じ 6 回のフレーム交換に加えて、4 回以上の EAP 交換を使用します。これは、選択された EAP のタイプと証明書のサイズによって異なります。通常、これには 10 ～ 20 個のフレームを使用し、RADIUS サーバの処理の遅延が追加されます。
- **WPA2+CCKM**：このメカニズムは優れた保護を提供し、802.1xを使用して初期認証を構築し、各ローミングイベントでフレームを2つだけ迅速に交換します。これはローミング時間を大幅に短縮します。主な問題は、ローミングが失敗した場合、802.1x に戻ることです。次に、認証後に CCKM の使用を再開します。問題が発生した場合に WGB の上にあるアプリケーションが偶発的な長いローミング時間を許容できる場合、PSK と比べて最適なオプションとして使用できます。

このドキュメントでは、LEAP、WPA-TKIP、WEP などのセキュリティ問題がある、推奨されないテクノロジーは対象としていません。

WPA2-PSK の設定

WGB では、これは設定が非常に簡単です。無線での SSID の定義と適切な暗号化が必要です。

```
dot11 ssid wgbpsk
vlan 32
authentication open
```

```
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

SSID 名と事前共有鍵は、ネットワーク インフラストラクチャと一致する必要があります。

802.1x を使用する WPA2 の設定

基本的に、以前の設定の上に構築されており、EAP プロファイルと認証方法が追加されています。

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

CCKM を使用する WPA2 の設定

1 つの軽微な変更を加えた WPA2 上の 1 ステップのみ：SSID 設定で CCKM フラグを使用します。これは、WLC 側でのみ WLAN が CCKM 用に設定されていることを前提としています。

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

使用される方法の検証

WGB のクイック チェックでは、CCKM などの使用中の暗号化と鍵管理を報告できます。

```
wgb-1260#sh dot11 associations al
Address            : 0024.97f2.75a0     Name              : lap1140-etsi-1
IP Address         : 192.168.40.10      Interface         : Dot11Radio 0
Device             : LWAPP-Parent      Software Version : NONE
CCX Version        : 5                  Client MFP        : Off

State              : EAP-Assoc          Parent            : -
SSID               : wlan1
VLAN               : 0
Hops to Infra      : 0                  Association Id    : 1
Tunnel Address     : 0.0.0.0
```

```
Key Mgmt type      : CCKM                Encryption        : AES-CCMP

Current Rate       : m7.-                Capability        : WMM ShortHdr ShortSlot
Supported Rates    : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates        : disabled            Bandwidth         : 20 MHz
Signal Strength    : -59  dBm            Connected for     : 72 seconds
Signal to Noise    : 41  dB             Activity Timeout : 8 seconds
Power-save         : Off                 Last Activity     : 7 seconds ago
Apsd DE AC(s)      : NONE

Packets Input      : 12064               Packets Output    : 136
Bytes Input        : 2892798             Bytes Output      : 19514
Duplicates Rcvd    : 87                  Data Retries      : 8
Decrypt Failed     : 0                   RTS Retries       : 0
MIC Failed         : 0                   MIC Missing       : 0
Packets Redirected: 0                    Redirect Filtered: 0
```

ローミングの設定

WGB では、ローミング アルゴリズムに影響を与えるいくつかのパラメータを変更できます。

パケットの再試行

デフォルトでは、WGB はフレームを 64 回再送信します。親によって正しく肯定応答（ACK）されない場合、親はもはや有効ではないとみなされ、スキャン/ローミングプロセスが開始されます。これは、送信が失敗したときにいつでも実行できるため、「非同期」ローミング トリガーと見なされます。

これを設定するコマンドは、dot11 インターフェイスの内部にあり、次のオプションがあります。

```
packet retries NUM [drop]
```

Num：1 ~ 128で、デフォルトは64です。通常、クイックローミングトリガーに適した数は32です。ほとんどのRF環境では、より低い数を使用することは推奨されません。

ドロップ：存在しない場合、WGB は最大再試行に達したときにローミング イベントを開始します。存在する場合、WGB は新しいローミングを開始せず、ビーコン損失や信号などの他のトリガーを使用します。

RSSI のモニタ

WGB は、現在の親に対して予防的な信号スキャンを実装し、信号が予期されるレベルを下回ったときに新しいローミング プロセスを開始できます。

このプロセスには 2 つのパラメータがあります。

- X 秒ごとに確認プロセスを起動するタイマー
- RSSI レベル。現在の信号がこのレベルを下回った場合にローミング処理を開始するために使用されます。

以下に、いくつかの例を示します。

```
in d0
```

```
mobile station period 4 threshold 75
```
一部の状況で「ローミング ループ」を防止するため、またはあまりにもアグレッシブなローミング動作を回避するため、WGB が認証プロセスを完了するのに要する時間より短くならないようにします。一般に、アプリケーションに必要なものを確認するためにテストする必要があります。

PSK の場合、EAP ベースの方法（非常にアグレッシブなアプリケーションの場合は通常 2 と 4）よりも低くなる可能性があります。

RSSI レベルは正の整数で表されますが、基本的には通常の -dBm の測定レベルです。データ レートを適切に維持するために必要な最小値よりも少し高い数値を使用する必要があります。たとえば、希望する最小レートが 6 mbps の場合、RSSI のしきい値である -87 で十分です。48 mbps の場合、-70 dBm などが必要です。

注：このコマンドは、「データレート変更によるローミング」をトリガーする可能性もあります。これはアグレッシブすぎます。良い結果を得るには、最小レートで使用する必要があります。

最小データ レート

12.4（25d）JA から、親への現在のデータ レートが特定の値を下回る場合、WGB が新しいローミング イベントをトリガーするタイミングを制御するための設定可能なパラメータが追加されました。

これは、ビデオ アプリケーションまたは音声アプリケーションをサポートするために、速度に関する適切な下限を維持するのに役立ちます。

このコマンドが利用可能になる前は、レートが前回よりも低いことが検出されると、WGB が頻繁にローミングをトリガーしました。基本的に時間 X + 1 で、レートが以前の X 時間よりも低い場合、WGB はローミング プロセスを開始しました。ログには次のメッセージが表示されます。

```
*Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower
data rate
```
これはあまりにもアグレッシブであるため、WGB と親 AP の両方で単一のデータ レートを設定するのが唯一の解決策でした。

ここで推奨される方法は、mobile station period コマンドが使用されるたびに、常にこのコマンドを設定することです。

```
in d0
mobile station  minimum-rate 2.0
```
これにより、新しいローミング プロセスは、現在のレートが設定された値よりも低い場合にのみトリガーされます。これにより不要なローミングが減り、予期したレート値を維持できます。

注：**この設定で**も、「Had to lower data rate」というメッセージが発生すると予想されます。WGBが設定された速度よりも低い速度で送信された場合にのみ、モバイルステーションの期間チェック時間がトリガーされたときに表示されます。

スキャン チャネル

WGB は、ローミング イベントを実行しながら、すべての「国別チャネル」をスキャンします。

つまり、無線ドメインによっては、2.4 GHz 帯のチャネル 1 ~ 11、または 1 ~ 13 をスキャンできます。

スキャンした各チャネルには時間がかかります。802.11bg では、これは約 10 ~ 13 ミリ秒です。802.11a では、チャネルが DFS 対応の場合は最大 150 ミリ秒になる可能性があります（プロービングしないで、パッシブ スキャンを行うだけです）。

適切な最適化は、スキャンされたチャネルを、インフラストラクチャによるサービス中のチャネルのみ使用するように制限することです。これは、802.11a では特に重要です。DFS が使用されている場合は、チャネル リストが大きく、チャネルごとの時間が長くなる可能性があるためです。

WGB /ローミング用のチャネル計画を作成する際には、3 つのポイントがあります。

- 2.4 GHz 帯の場合、サイド チャネルの干渉を最小限に抑えるために 1/6/11 を厳守してください。4 などの他のチャネル計画は、干渉を増加させないで、RF の観点から適切に設計することが困難になる傾向があります。
- スキャンの観点からは、すべての AP に単一のチャネル設定を使用することをお勧めします。これは、サポートするクライアントの合計数が非常に少なく、高い帯域幅要件がない場合にのみ意味を持ちます。これにより、スキャン時間からの無線変更時間がなくなります。このオプションを利用できる環境はほとんどないので、使用するには注意が必要です。
- 5.0 GHz 帯では、地方自治体の規制によって可能な場合、屋内の非 DFS チャネル（36 ～ 48）を使用すると、長時間のパッシブ リスニングを行う代わりに、WGB が各チャネルをアクティブにプローブできるため、スキャン時間が短縮されます。

導入に使用されているチャネル計画は、他の要件に対応する必要がある場合があります。一般的な RF 設計の推奨事項を使用してください。

スキャン チャネル リストを設定するには、以下のようにします。

```
in d0
mobile station scan 1 6 11
```

注：モバイルステーションは、無線でWGBロールを使用している場合にのみ表示されます。

注：WGBスキャンリストがインフラストラクチャチャネルリストと一致していることを確認してください。そうでない場合、WGB は利用可能な AP を検出しません。

タイマーの設定

12.4（25a）JA 以降、問題が見つかった場合に回復タイマーを最適化するためのいくつかの新しいコマンドがあります。これは AP が WGB モードの場合にのみ利用可能です。

```
wgb-1260(config)#workgroup-bridge timeouts ?

  assoc-response  Association Response time-out value
  auth-response   Authentication Response time-out value
  client-add      client-add time-out value
  eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

assoc-response、auth-response、client-add の場合、AP が故障したとみなして次の候補を試す前に、WGB が親 AP の応答を待機する時間を示します。デフォルト値は 5 秒ですが、アプリケ

ーションによっては長すぎることがあります。最小タイマーは 800 ミリ秒で、ほとんどのモバイル アプリケーションにこの値が推奨されます。

eap-timeout では、完全な EAP 認証プロセスが完了するまで、WGB が待機する最大時間を設定します。これは、EAP 認証者が応答していない場合にプロセスを再開するために、EAP サプリカントの観点から動作します。デフォルト値は 60 秒です。完全な 802.1x 認証を完了するのに必要な実際の時間よりも低い値を設定しないように注意してください。通常、ほとんどの導入では、2 ~ 4 秒に設定するのが適切です。

iapp-refresh の場合、WGB は、デフォルトでローミング後に親 AP への IAPP 一括更新を生成し、既知の有線クライアントに通知します。約 10 秒後、関連付けの後に 2 回目の再送信があります。このタイマーは、RF または親 AP にまだインストールされていない暗号化キーによって最初の IAPP 更新が失われた可能性がある場合にそれを解消するために、関連付けの後に IAPP 一括更新の「高速再試行」を行うことを可能にします。高速ローミングのシナリオでは、100 ミリ秒を使用できます。ただし、多数の WGB が使用されていることを確認してください。これにより、各ローミング後にインフラストラクチャに送信される IAPP の合計数が大幅に増加します。

アグレッシブな値の例：

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

これらは、モバイル WGB 導入シナリオで正常にテストされています。

その他の WGB 最適化

WGB の導入シナリオでは、他にも考慮すべき軽微な変更があります。

無線関連

- **rts retries**を減らす – **rts retries 32**。これにより、アグレッシブなシナリオのRF時間を節約できます。通常は不要です。
- アンテナの種類：単一のアンテナ（多様性なし）を使用している場合は、一般的なパフォーマンスを向上させるために無線を設定する必要があります。

```
antenna transmit right-a
antenna receive right-a
```

アンテナの多様性には価値があるものの、車両にアンテナを物理的に設置する場合には必ずしも可能とは限りません。適切なアンテナを選択することは、ローミングに重要です。一般的なローミング平均時間では、2 dB ほどでも大きな違いになる可能性があります。

ログ関連

- 数ミリ秒を節約するには、コンソールのログ レベルをエラーのみ： **logging console errors** に下げます。一部の状況ではローミング パフォーマンスに悪影響を与える可能性があるため、完全に無効にしないでください。
- 理想的には、イーサネット側から Telnet または SSH を使用して、デバッグまたはログを収

集します。これは、コンソールでのデバッグのロギング：**logging monitor debugging** と比較して、パフォーマンスへの影響がはるかに小さくなります。
- WGB のローミングの観点から発生していることを理解するためのコマンドは、**debug dot11 dot11 0 trace print uplink** です。これは CPU にはほとんど影響しませんが、それぞれが合計ローミング時間を増やす可能性があるため、指示されない限り他のデバッグ オプションは有効にしないでください。
- 可能であれば、SNTP を使用してください。これにより、WGB の時刻が同期されたままになり、トラブルシューティングに非常に役立ちます。

MFP の使用

- MFP はセキュリティ上の観点から有用です。ただし、ローミング障害のシナリオでは、何らかの理由で WGB と AP の間の暗号化キーに異常が発生した場合、WGB は新しいローミングをトリガーするために AP の親からの非認証フレームを受け入れることはありません。
- こうしたまれな障害シナリオでは、現在の親が良好な RF 信号で聞こえる場合、WGB は新しいスキャンを開始するまでに最大 5 秒かかることがあります。その間に有効なデータ フレームが受信されない場合、WGB がトリガーできる「catch-all」検出メカニズムがあります。
- デフォルトでは、SSID に WPA2 AES が使用されている場合、WGB はクライアント MFP を使用しようとします。
- 高速回復時間が必要な場合（非保護の非認証フレームに反応する WGB）、クライアント MFP を無効にすることをお勧めします。 これが、セキュリティの必要と高速回復時間との間で妥協できる部分です。この決定は、導入シナリオにとって何がより重要かによって異なります。

```
dot11 ssid wgbpsk
   no ids mfp client
```

WGB での EAP-TLS および「クロック保存間隔」

『Cisco IOS リリース 12.4(21a)JY 向け Cisco Aironet アクセス ポイントおよびブリッジ リリース ノート』の「IOS サプリカント クロックを同期して NVRAM に時刻の設定を保存する」のセクションを参照してください。

uWGB を使用する場合、uWGB は通常、接続された MAC アドレスに関連付けられており、かつ uWGB BVI にはネットワーク アクセスがないため、SNTP 同期を実行する機会がない可能性があります。したがって、uWGB の場合は、少なくとも実装時に NVRAM で適切なクロック同期をとることをお勧めします。接続された enet デバイスが NTP ソース（また、uWGB 接続を介して更新されたクライアント）になることができる場合、有効な NTP 反映ポイントとしてそこから uWGB SNTP を同期させることを検討できます。

フル構成の例

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
```

```
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
   vlan 32
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 060506324F41584B56
   no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
  packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip
```

```
sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

デバッグ分析

問題が発生した場合は、最初のステップとして **debug dot11 dot11 0 trace print uplink コマンドの出力をキャプチャすることが重要です。**これにより、ローミング プロセスで発生している事柄を理解できます。

次に、候補としての現在の親の例を示します。

```
 Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
too low
 Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

これは、低い信号が満たされた場合のトリガーです。それは、mobile station period X threshold Y コマンドに依存します。最初のメッセージは常にコンソールに送信され、2 つ目はアップリンクのデバッグ トレースの一部です。これは問題ではありません。通常の WGB プロセスの一部です。

```
 Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

アップリンク プロセスは、チャネル スキャンを開始する前に無線キューの消去を強制します。このステップは、チャネル利用率およびキューの深さに応じて、数ミリ秒から数秒かかる場合があります。データ フレームはタイムアウトしません。音声フレームでは時間の比較が行われるため、高速でドロップする必要があります。騒がしい環境では、多少の遅延が観察されることがあります。

```
 Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
 Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

以下が実際に行われるチャネル スキャンです。これは、設定されたチャネルあたり約 10 ~ 13 ミリ秒の間、無線を待機させます。

```
 Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

以下は、受信したプローブ応答のリストです。最初の番号はチャネル、2 番目は受信に要したマイクロ秒です。

```
 Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
load 0
 Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
load 0
```

これらの詳細で行われた実際の比較は次のとおりです。

```
 Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

親の選択

```
 Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
 Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0,
 Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.
```

これは、ローミングが「完了」しているポイントです。 IAPP フレームが親によって処理されると、すぐにトラフィックが再開されます。

親の比較情報

```
 Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
load 3
 Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
load 0
```

WGB が関連付けられている AP が依然として「現在の」AP である場合、compare1 は実際の関連付けカウント -1 (つまり、WGB 自体は数値を取り込まない) を出力し、次に実際のホップと負荷を出力します。

compare2 は差を出力します。負の数が表示される可能性があるのはこのためです。現在の AP よりテストの方が数が多い場合は、負の値が表示されます。

現在の関連付けカウント、負荷、信号差、モバイルしきい値に応じて、WGB は新しい親を選択するかしないか判断します。

比較は常に 2 つの AP の間で行われ、選択された AP は次の反復のために現在の AP を置き換えます。したがって、決定の一部は、あるループ上の RSSI、または次のテストでの他の要因に起因する可能性があります。

関連情報

- Cisco Unified Wireless Network における EAP-TLS 認証が設定された aIOS WGB の使用方法
- テクニカル サポートとドキュメント – Cisco Systems