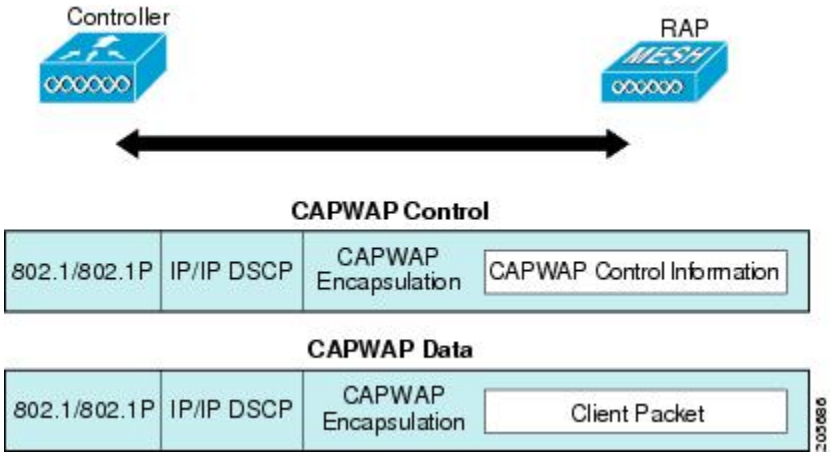
メッシュ アクセス ポイントのネットワークへの接続

概要

この章では、ネットワークに Cisco メッシュ アクセス ポイントを接続する方法について説明します。

ワイヤレス メッシュは、有線ネットワークの 2 地点で終端します。1 つ目は、RAP が有線ネットワークに接続されているロケーションで、そこではすべてのブリッジ トラフィックが有線ネットワークに接続しています。2つ目は、CAPWAP コントローラが有線ネットワークに接続するロケーションです。そのロケーションでは、メッシュ ネットワークからの WLAN クライアント トラフィックが有線ネットワークに接続しています。CAPWAP からの WLAN クライアント トラフィックはレイヤ 2 でトンネルされ、WLAN のマッチングは、コントローラがコロケーションされている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、コントローラが接続されているネットワークのセキュリティ機能によって異なります。

図 *1:* メッシュ ネットワーク トラフィックの終端



（注） HSRP 設定がメッシュ ネットワークで動作中の場合は、入出力マルチキャスト モードを設定することを推奨します。マルチキャスト設定の詳細については、「Enabling Multicast on the Network (CLI)」の項を参照してください。

新しいコントローラ ソフトウェア リリースへのアップグレードの詳細については、https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html でシスコ ワイヤレス コントローラと *Lightweight* アクセス ポイントのリリース ノート [英語] を参照してください。

メッシュとコントローラ ソフトウェアのリリースおよび互換性のあるアクセス ポイントの詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html の『*Cisco Wireless Solutions Software Compatibility Matrix*』を参照してください。

メッシュ ネットワークへのメッシュ アクセス ポイントの追加

この項では、コントローラがネットワーク内でアクティブで、レイヤ 3 モードで動作していることを前提としています。

（注） メッシュ アクセス ポイントが接続するコントローラ ポートは、タグなしでなければなりません。

メッシュ アクセス ポイントをネットワークに追加する前に、次の手順を実行します。

手順

ステップ 1 メッシュ アクセス ポイントの MAC アドレスを、コントローラの MAC フィルタに追加します。「MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加」の項を参照してください。

ステップ 2 メッシュ アクセス ポイントのロール（RAP または MAP）を定義します。「メッシュ アクセス ポイントのロールの定義」の項を参照してください。

ステップ 3 コントローラでレイヤ 3 が設定されていることを確認します。レイヤ 3 の設定の確認に関する項を参照してください。

ステップ 4 各メッシュ アクセス ポイントに、プライマリ、セカンダリ、およびターシャリのコントローラを設定します。「DHCP 43 および DHCP 60 を使用した複数のコントローラの設定」の項を参照してください。

バックアップ コントローラを設定します。「バックアップ コントローラの設定」を参照してください。

ステップ 5 外部 RADIUS サーバを使用して、MAC アドレスの外部認証を設定します。「RADIUS サーバを使用した外部認証および許可の設定」を参照してください。

ステップ 6 グローバル メッシュ パラメータを設定します。「グローバル メッシュ パラメータの設定」の項を参照してください。

ステップ 7 バックホール クライアント アクセスを設定します。「拡張機能の設定」の項を参照してください。

ステップ 8 ローカル メッシュ パラメータを設定します。「ローカル メッシュ パラメータの設定」を参照してください。

ステップ 9 アンテナ パラメータを設定します。「アンテナ利得の設定」の項を参照してください。

ステップ 10 シリアル バックホールのチャネルを設定します。この手順は、シリアル バックホール アクセス ポイントにのみ適用できます。「シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除」の項を参照してください。

ステップ 11 メッシュ アクセス ポイントの DCA チャネルを設定します。「動的チャネル割り当ての設定」の項を参照してください。

ステップ 12 （必要に応じて）モビリティ グループを設定し、コントローラを割り当てます。シスコ ワイヤレス コントローラ コンフィギュレーション ガイド [英語] の「Configuring Mobility Groups」の章を参照してください。

ステップ 13 （必要に応じて）イーサネット ブリッジを設定します。「イーサネット ブリッジングの設定」の項を参照してください。

ステップ 14 イーサネット VLAN タギング ネットワーク、ビデオ、音声などの拡張機能を設定します。「拡張機能の設定」の項を参照してください。

MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加

メッシュ ネットワーク内で使用するメッシュ アクセス ポイントは、すべての無線 MAC アドレスを適切なコントローラに入力する必要があります。コントローラは、許可リストに含まれる屋外無線からの discovery request にだけ応答します。コントローラでは、MAC フィルタリングがデフォルトで有効になっているため、MAC アドレスだけを設定する必要があります。アクセス ポイントが SSC を持ち、AP 認可リストに追加された場合は、AP の MAC アドレスを MAC フィルタリング リストに追加する必要がありません。

GUI と CLI のどちらを使用しても、メッシュ アクセス ポイントを追加できます。

（注） メッシュ アクセス ポイントの MAC アドレスのリストは、ダウンロードして、Cisco Prime Infrastructure を使用してコントローラにプッシュすることもできます。

コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（CLI）

コントローラの CLI を使用してコントローラのメッシュ アクセス ポイントの MAC フィルタ エントリを追加する手順は、次のとおりです。

手順

ステップ 1 メッシュ アクセス ポイントの MAC アドレスをコントローラ フィルタ リストに追加するには、次のコマンドを入力します。

config macfilter add *ap_mac wlan_id interface* [*description*]

wlan_id パラメータの値をゼロ（0）にすると任意の WLAN を指定し、*interface* パラメータの値をゼロ（0）にするとなしを指定します。オプションの *description* パラメータには、最大 32 文字の英数字を入力できます。

ステップ 2 変更を保存するには、次のコマンドを入力します。

save config

メッシュ アクセス ポイントのロール定義

デフォルトでは、AP1500 は MAP に設定された無線のロールで出荷されます。RAP として動作させるには、メッシュ アクセス ポイントを再設定する必要があります。

AP ロールの設定（CLI）

CLI を使用してメッシュ アクセス ポイントのロールを設定するには、次のコマンドを入力します。

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

DHCP 43 および DHCP 60 を使用した複数のコントローラの設定

組み込みの Cisco IOS DHCP サーバを使用して、メッシュ アクセス ポイント用に DHCP オプション 43 および 60 を設定する手順は、次のとおりです。

手順

ステップ 1 Cisco IOS の CLI でコンフィギュレーション モードに切り替えます。

ステップ 2 DHCP プール（デフォルトのルータやネーム サーバなどの必要なパラメータを含む）を作成します。DHCP プールの作成に使用するコマンドは次のとおりです。

```
ip dhcp pool pool name
network IP Network Netmask
default-router Default router
dns-server DNS Server
```

値は次のとおりです。

```
pool name is the name of the DHCP pool, such as AP1520
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

ステップ 3 次の構文を使用してオプション 60 の行を追加します。

```
option 60 ascii “VCI string”
```

VCI 文字列の場合は、次のいずれかの値を使用します。引用符は必ず含める必要があります。

```
For Cisco 1550 series access points, enter “Cisco AP c1550”
For Cisco 1520 series access points, enter “Cisco AP c1520”
For Cisco 1240 series access points, enter “Cisco AP c1240”
For Cisco 1130 series access points, enter “Cisco AP c1130”
```

ステップ 4 次の構文に従って、オプション 43 の行を追加します。

```
option 43 hex hex string
```

16 進文字列には、次の TLV 値を組み合わせて指定します。

型 + 長さ + 値

タイプは、常に f1（16 進数）です。長さ は、コントローラ管理 IP アドレスの個数の 4 倍の値を 16 進数で表したものです。値 は、一覧表示されるコントローラの IP アドレスを順番に 16 進数で表したものです。

たとえば、管理インターフェイスの IP アドレス 10.126.126.2 および 10.127.127.2 を持ったコントローラが 2 つあるとします。型は、f1（16 進数）です。長さは、2 X 4 = 8 = 08（16 進数）です。IP アドレスは、0a7e7e02 および 0a7f7f02 に変換されます。文字列を組み合わせると f1080a7e7e020a7f7f02 になります。

DHCP スコープに追加された結果の Cisco IOS コマンドは、次のとおりです。

```
option 43 hex f1080a7e7e020a7f7f02
```

RADIUS サーバを使用した外部認証および認可の設定

リリース 5.2 以降では、Cisco ACS（4.1 以降）などの RADIUS サーバを使用した、メッシュ アクセス ポイントの外部認証および認可がサポートされています。RADIUS サーバは、クライアント認証タイプとして、証明書を使用する EAP-FAST をサポートする必要があります。

メッシュ ネットワーク内で外部認証を使用する前に、次の変更を行う必要があります。

- AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。
- コントローラも、RADIUS サーバで設定する必要があります。
- 外部認証および認可用に設定されたメッシュ アクセス ポイントを RADIUS サーバのユーザ リストに追加します。
  - 詳細については、「RADIUS サーバへのユーザ名の追加」の項を参照してください。
- RADIUS サーバで EAP-FAST を設定し、証明書をインストールします。802.11a インターフェイスを使用してメッシュ アクセス ポイントをコントローラに接続する場合には、EAP-FAST 認証が必要です。外部 RADIUS サーバは、Cisco Root CA 2048 を信頼する必要があります。CA 証明書のインストールと信頼については、「RADIUS サーバの設定」の項を参照してください。

（注） ファスト イーサネットまたはギガビット イーサネット インターフェイスを使用してメッシュ アクセス ポイントをコントローラ接続する場合は、MAC 認可だけが必要です。

（注） また、この機能は、コントローラ上のローカル EAP および PSK 認証をサポートしています。

RADIUS サーバの設定

RADIUS サーバに CA 証明書をインストールして信頼するように設定する手順は、次のとおりです。

手順

ステップ 1 次の場所から Cisco Root CA 2048 の CA 証明書をダウンロードします。

- https://www.cisco.com/security/pki/certs/crca2048.cer
- https://www.cisco.com/security/pki/certs/cmca.cer

ステップ 2 次のように証明書をインストールします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [ACS Certification Authority Setup] をクリックします。
b) [CA certificate file] ボックスに、CA 証明書の場所（パスと名前）を入力します（たとえば、c:\Certs\crca2048.cer）。
c) [Submit] をクリックします。

ステップ 3 次のように外部 RADIUS サーバを設定して、CA 証明書を信頼するようにします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [Edit Certificate Trust List] の順に選択します。[Edit Certificate Trust List] が表示されます。
b) 証明書の名前（[Cisco Root CA 2048 (Cisco Systems)]）の横にあるチェックボックスをオンにします。
c) [Submit] をクリックします。
d) ACS を再起動するには、[System Configuration] > [Service Control] の順に選択してから、[Restart] をクリックします。

Cisco ACS サーバに関する追加の設定詳細については、次のドキュメントを参照してください。

- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html（Windows）
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/（UNIX）

メッシュ アクセス ポイントの外部認証の有効化（CLI）

CLI を使用してメッシュ アクセス ポイントの外部認証を有効にするには、次のコマンドを入力します。

手順

ステップ 1 **config mesh security eap**

ステップ 2 **config macfilter mac-delimiter colon**

ステップ 3 **config mesh security rad-mac-filter enable**

ステップ 4 **config mesh radius-server** *index***enable**

ステップ 5 **config mesh security force-ext-auth enable** （任意）

セキュリティ統計情報の表示（CLI）

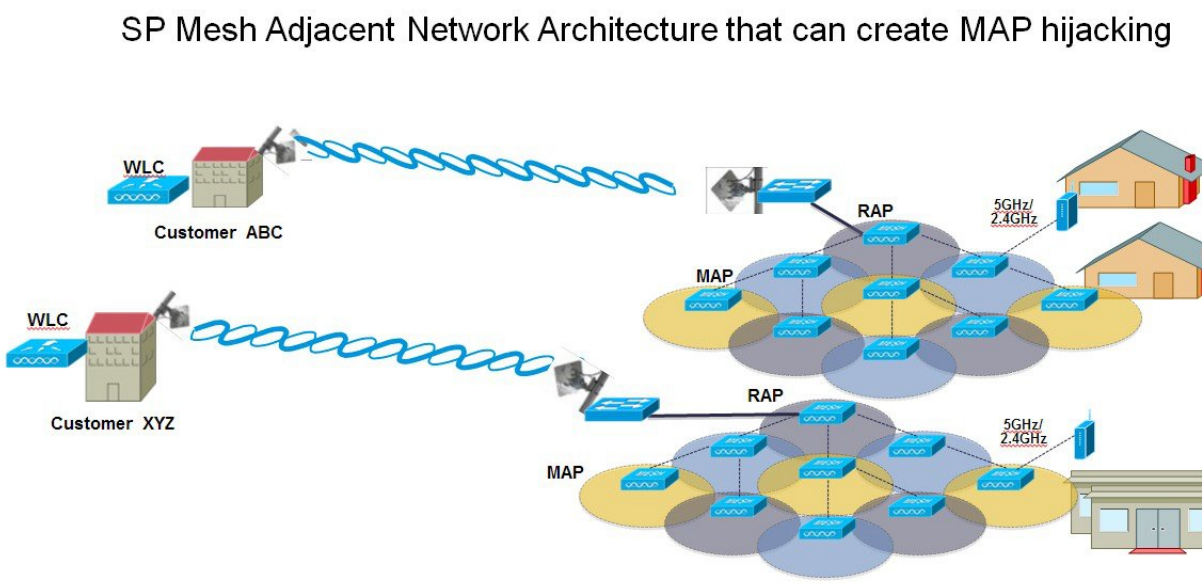
CLI を使用してメッシュ アクセス ポイントのセキュリティ統計を表示するには、次のコマンドを入力します。

show mesh security-stats *Cisco_AP*

このコマンドを使用すると、指定のアクセス ポイントとその子アクセス ポイントのパケット エラー統計、エラー数、タイムアウト数、アソシエーションと認証の成功数、再アソシエーション数、および再認証数が表示されます。

リリース8.2でのMesh PSK Keyを使ったプロビジョニング

Cisco Mesh の導入時に、いずれの導入でもワイルドカードの MAC フィルタリングで AAA を使用し MAP アソシエーションを許可する場合、メッシュ アクセス ポイント（MAP）が現在 join 中のネットワークを終了し、別のメッシュ ネットワークへ join します。メッシュ AP のセキュリティが EAP-FAST を使用する可能性があるため、この動作を制御できません。EAP セキュリティでは AP の MAC アドレスとタイプの組み合わせが使用されるため、制御設定を使用できないためです。PSK オプションでデフォルトのパスフレーズを使用すると、セキュリティ リスクとハイジャックの危険性が伴います。この問題は、MAP が移動車両（公共交通機関、フェリー、船など）に使用されるときに、2 つの異なる SP のオーバーラップ導入で顕著に現れます。この場合、MAP は SP のメッシュ ネットワークに固定される必要がなくなるため、MAP を別の SP ネットワークによってハイジャック/使用できます。このため導入環境では SP の対象顧客にサービスを提供できなくなります。



8.2 リリースで導入された新しい機能は、メッシュ導入を制御し、現在使用されているデフォルトの「**cisco**」PSK を超える MAP のセキュリティの強化に役立つ（WLC からプロビジョニングできる）PSK 機能を有効にします。この新機能によって、カスタム PSK で設定した MAP は、RAP および WLC を使用して認証を行う場合に強化されたキーを使用します。コントローラ ソフトウェア リリース 8.1 以下をアップグレードするかリリース 8.2 からダウンロードする場合は、特別な注意が必要です。管理者は MAP ソフトウェアで PSK を有効化/無効化する際の影響を理解する必要があります。

PSK 事前プロビジョニング用の CLI コマンド

- config mesh security psk provisioning enable/disable
- config mesh security psk provisioning key <pre-shared-key>
- config mesh security psk provision window enable/disable
- config mesh security psk provisioning delete_psk <ap|wlc> <ap_name|psk_index>”

グローバル メッシュ パラメータの設定

この項では、メッシュ アクセス ポイントがコントローラとの接続を確立するよう設定する手順について説明します。内容は次のとおりです。

- RAP と MAP 間の最大レンジの設定（屋内 MAP には非適用）
- クライアント トラフィックを伝送するバックホールの有効化
- VLAN タグが転送されるかどうかの指定

- セキュリティ設定（ローカルおよび外部認証）を含むメッシュ アクセス ポイントの認証モード（EAP または PSK）および認証方式（ローカルまたは外部）の定義

必要なメッシュ パラメータを設定するには、GUI と CLI のいずれかを使用できます。パラメータはすべてグローバルに適用されます。

グローバル メッシュ パラメータの設定（CLI）

コントローラの CLI を使用して認証方式を含むグローバル メッシュ パラメータを設定する手順は、次のとおりです。

（注） CLI コマンドで使用されるパラメータの説明、有効範囲およびデフォルト値については、「グローバル メッシュ パラメータの設定（GUI）」の項を参照してください。

手順

ステップ 1 ネットワークの全メッシュ アクセス ポイントの最大レンジをフィート単位で指定するには、次のコマンドを入力します。

config mesh range *feet*

現在のレンジを確認するには、**show mesh range** コマンドを入力します。

ステップ 2 バックホールのすべてのトラフィックに関して IDS レポートをイネーブルまたはディセーブルにするには、次のコマンドを入力します。

config mesh ids-state {**enable** | **disable**}

ステップ 3 バックホール インターフェイスでのアクセス ポイント間のデータ共有レート（Mbps 単位）を指定するには、次のコマンドを入力します。

config ap bhrate {*rate* | **auto**} *Cisco_AP*

ステップ 4 メッシュ アクセス ポイントのプライマリ バックホール（802.11a）でクライアント アソシエーションを有効または無効にするには、次のコマンドを入力します。

config mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {**add** | **delete**} **802.11a** *wlan_id Cisco_AP*

ステップ 5 VLAN トランスペアレントをイネーブルまたはディセーブルにするには、次のコマンドを入力します。

config mesh ethernet-bridging VLAN-transparent {**enable** | **disable**}

ステップ 6 メッシュ アクセス ポイントのセキュリティ モードを定義するには、次のいずれかのコマンドを入力します。

a) コントローラによるメッシュ アクセス ポイントのローカル認証を提供するには、次のコマンドを入力します。

config mesh security {**eap** | **psk**}

b) 認証用にコントローラ（ローカル）の代わりに外部 RADIUS サーバに MAC アドレス フィルタを格納するには、次のコマンドを入力します。

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

c) RADIUS サーバで外部認証を提供し、コントローラでローカル MAC フィルタを定義するには、次のコマンドを入力します。

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

d) RADIUS サーバで MAC ユーザ名（c1520-123456 など）を使用し、RADIUS サーバで外部認証を提供するには、次のコマンドを入力します。

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

ステップ 7 変更を保存するには、次のコマンドを入力します。

save config

グローバル メッシュ パラメータ設定の表示（CLI）

グローバル メッシュ設定の情報を取得するには、次のコマンドを入力します。

- **show mesh client-access**：バックホール クライアント アクセスが有効な場合は、無線バックホールを介したワイヤレス クライアント アソシエーションが許可されます。無線バックホールには、大部分のメッシュ アクセス ポイントで 5 GHz 帯が使用されます。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

  バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみが無線バックホールを介して送信され、クライアント アソシエーションは 2 番目の無線のみを介して送信されます。

```
(Cisco Controller)> show mesh client-access
Backhaul with client access status: enabled
```

- **show mesh ids-state**：バックホールの IDS レポートの状態が有効か無効かを示します。

```
(Cisco Controller)> show mesh ids-state
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

- **show mesh config**：グローバル設定を表示します。

```
(Cisco Controller)> show mesh config
Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. disabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... disabled

Mesh Security
Security Mode.................................. EAP
External-Auth.................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled

Mesh Alarm Criteria
Max Hop Count.................................. 4
Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20
Low Link SNR................................... 12
High Link SNR.................................. 60
Max Association Number......................... 10
Association Interval........................... 60 minutes
Parent Change Numbers.......................... 3
Parent Change Interval......................... 60 minutes

Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

バックホール クライアント アクセス

バックホール クライアント アクセスが有効な場合は、無線バックホールを介したワイヤレス クライアント アソシエーションが許可されます。バックホール無線は 5 GHz 無線です。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみが無線バックホールを介して送信され、クライアントアソシエーションは2番目の無線のみを介して送信されます。

（注） バックホール クライアント アクセスはデフォルトで無効になります。この機能を有効にすると、デイジーチェーン導入のスレーブ AP と子 AP を除くすべてのメッシュ アクセス ポイントは再起動します。

この機能は、2 つの無線を使用するメッシュ アクセス ポイント（1552、1532、1540、1560、1572、およびブリッジ モードの屋内 AP）に適用されます。

バックホール クライアント アクセスの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Mesh]** の順に選択して、[Mesh] ページを開きます。

ステップ 2 [General] セクションで、[Backhaul Client Access] チェックボックスをオンにします。

ステップ 3 設定を保存します。

次のタスク

Flex + ブリッジの導入環境では、バックホール クライアント アクセスをグローバルに有効にした後、ビーコンに対して 5 GHz 無線を想定している場合は、Flex + ブリッジ モードで動作しているルート AP の [Install mapping on radio backhaul] オプションを有効にする必要があります。

[Install mapping on radio backhaul] オプションの有効化の詳細については、「Flex+ ブリッジ モードの設定（GUI）」の項を参照してください。

関連トピック

Flex + ブリッジ モードの設定（GUI）

バックホール クライアント アクセスの設定（CLI）

次のコマンドを使用して、バックホール クライアント アクセスを有効にします。

```
(Cisco Controller)> config mesh client-access enable
```

次のメッセージが表示されます。

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

次のタスク

Flex + ブリッジの導入環境では、バックホール クライアント アクセスをグローバルに有効にした後、ビーコンに対して 5 GHz 無線を想定している場合は、Flex + ブリッジ モードで動作しているルート AP の [Install mapping on radio backhaul] オプションを有効にする必要があります。

[Install mapping on radio backhaul] オプションの有効化の詳細については、「Flex+ ブリッジ モードの設定（CLI）」の項を参照してください。

関連トピック

Flex + ブリッジ モードの設定（CLI）

ローカル メッシュ パラメータの設定

グローバル メッシュ パラメータを設定したら、ネットワークで使用中の機能について次のローカル メッシュ パラメータを設定する必要があります。

- バックホール データ レート。
- イーサネット ブリッジング。
- ブリッジ グループ名。
- ワークグループ ブリッジ。
- 電源およびチャネル設定。
- アンテナ ゲイン設定。
- 動的チャネル割り当て。

無線バックホールのデータ レートの設定

バックホールは、アクセス ポイント間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは、アクセス ポイントによって、802.11a/n/ac レートが異なります。利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。また、レートはクライアント デバイスのスループットにも影響を与えることがあり、スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです。

Dynamic Rate Adaptation（DRA）には、パケット伝送のために最適な伝送レートを推測するプロセスが含まれます。レートを正しく選択することが重要です。レートが高すぎると、パケット伝送が失敗し、通信障害が発生します。レートが低すぎると、利用可能なチャネル帯域幅が使用されず、品質が低下し、深刻なネットワーク輻輳および障害が発生する可能性があります。

データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。低データ レート（6 Mbps など）が、高データ レート（1300 Mbps など）よりもアクセス ポイントからの距離を延長できます。結果として、データ レートはセル カバレッジと必要なアクセス ポイントの数に影響を与えます。異なるデータ レートは、ワイヤレス リンクで冗長度の高い信

号を送信することにより（これにより、データをノイズから簡単に復元できます）、実現されます。1 Mbps のデータ レートでパケットに対して送信されるシンボル数は、11 Mbps で同じパケットに使用されたシンボル数より多くなります。したがって、低ビット レートでのデータの送信には、高ビット レートでの同じデータの送信よりも時間がかり、スループットが低下します。

コントローラ リリース 5.2 では、メッシュ 5 GHz バックホールのデフォルト データ レートは 24 Mbps です。これは、6.0 および 7.0 コントローラ リリースでも同じです。

6.0 コントローラ リリースでは、メッシュ バックホールに「Auto」データ レートを設定できます。設定後に、アクセス ポイントは、最も高いレートを選択します（より高いレートは、すべてのレートに影響を与える状況のためではなくそのレートに適切でない状況のため、使用できません）。つまり、設定後は、各リンクが、そのリンク品質に最適なレートに自動的に設定されます。

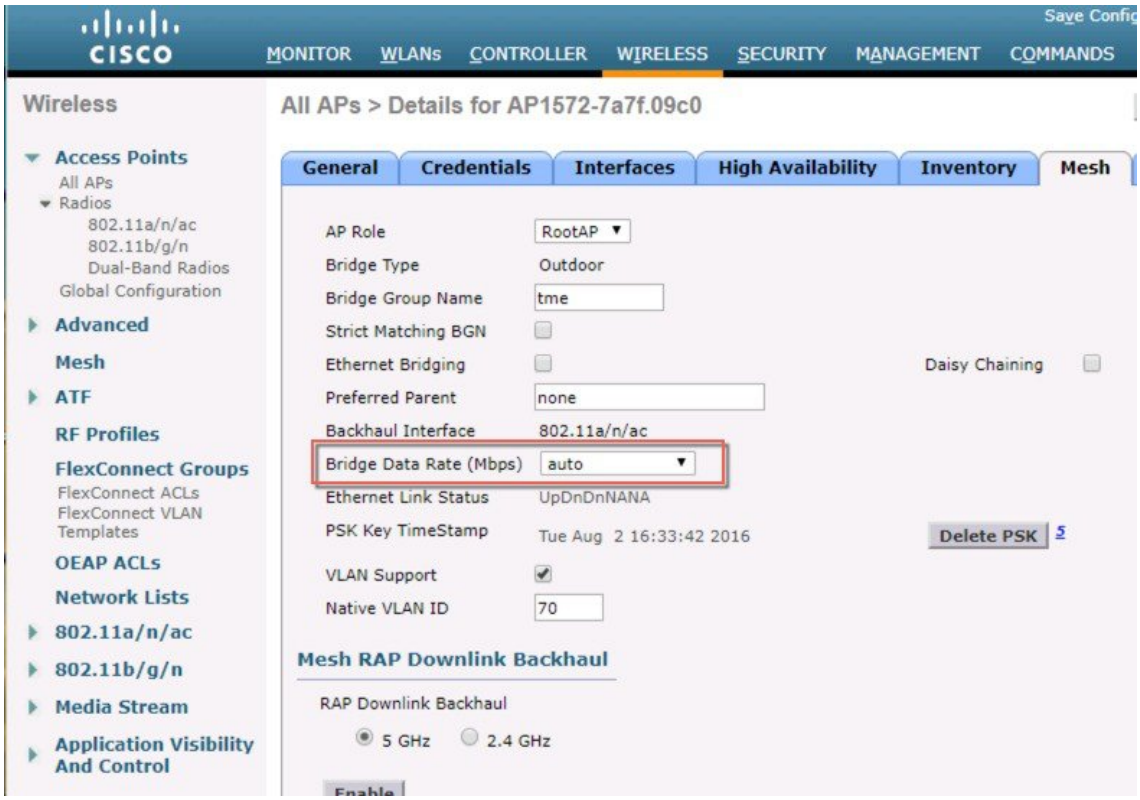
メッシュ バックホールを「Auto」に設定することをお勧めします。

たとえば、メッシュ バックホールが 48 Mbps を選択した場合、この決定は、誰かが電子レンジを使用したためではなく（これによりすべてのレートが影響を受けます）、54 に対して十分な SNR がないため、54 Mbps を使用できないことが確認された後に行われます。

低ビット レートでは、MAP 間の距離を長くすることが可能になりますが、WLAN クライアント カバレッジにギャップが生じる可能性が高く、バックホール ネットワークのキャパシティが低下します。バックホール ネットワークのビット レートを増加させる場合は、より多くの MAP が必要となるか、MAP 間の SNR が低下し、メッシュの信頼性と相互接続性が制限されます。

この図では、RAP が「Auto」バックホール データ レートを使用しており、子 MAP との間では 54 Mbps を使用していることを示しています。

図 *2:* 自動設定されたブリッジ レート



（注） データ レートは、AP ごとにバックホールで設定できます。これはグローバル コマンドではありません。

関連コマンド

以下のコマンドを使用してバックホールに関する情報を取得します。

- **config ap bhrate**：Cisco ブリッジ バックホール送信レートを設定します。

  構文は次のようになります。

```
(controller) > config ap bhrate backhaul-rate ap-name
```

（注） 各 AP に対して設定済みのデータ レート（RAP=18 Mbps、MAP1=36 Mbps）は、6.0 以降のソフトウェア リリースへのアップグレード後も保持されます。6.0 リリースにアップグレードする前に、データ レートに設定されるバックホールデータ レートがある場合は、その設定が保持されます。

次の例は、RAP でバックホール レートを 36000 Kbps に設定する方法を示しています。

```
(controller) > config ap bhrate 36000 HPRAP1
```

- **show ap bhrate**：Cisco ブリッジ バックホール レートを表示します。

  構文は次のようになります。

  ```
  (controller) > show ap bhrate ap-name
  ```

- **show mesh neigh summary**：バックホールで現在使用されているレートを含むリンク レート概要を表示します。

  例：

  ```
  (controller) > show mesh neigh summary HPRAP1

  AP Name/Radio    Channel     Rate     Link-Snr     Flags      State
  ---------------- --------   --------   -------     -----      -----
  00:0B:85:5C:B9:20 0          auto        4       0x10e8fcb8   BEACON
  00:0B:85:5F:FF:60 0          auto        4       0x10e8fcb8   BEACON DEFAULT
  00:0B:85:62:1E:00 165        auto        4       0x10e8fcb8   BEACON
  OO:0B:85:70:8C:A0 0          auto        1       0x10e8fcb8   BEACON
  HPMAP1            165        54          40      0x36         CHILD BEACON
  HJMAP2            0          auto        4       0x10e8fcb8   BEACON
  ```

バックホールのキャパシティとスループットは AP のタイプ（つまり、802.11a/n であるかや、802.11a のみであるかや、バックホール無線の数など）によって異なります。

イーサネット ブリッジングの設定

セキュリティ上の理由により、デフォルトではすべての MAP でイーサネット ポートが無効になっています。有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定します。

イーサネット ブリッジングが有効な場合：

- VLAN ID 0 は、ネイティブ VLAN とアクセス VLAN として設定できます。ただし、ネイティブでない VLAN としては設定できません。

- すべてのネイティブ VLAN は、ネイティブでない VLAN として設定できます。またその逆も設定できます。
- 許可 VLAN リストからネイティブ VLAN を削除しても、ネイティブ VLAN には干渉しません。
- 古いネイティブ VLAN は、許可 VLAN リストに自動的には追加されません。

（注） イーサネットブリッジングが無効な場合であっても、いくつかのプロトコルで例外が許可されます。たとえば、次のプロトコルが許可されます。

- スパニング ツリー プロトコル（STP）
- アドレス解決プロトコル（ARP）
- Control and Provisioning of Wireless Access Points（CAPWAP）[ControlandProvisioningofWirelessAccessPointsCAPWAP]
- ブートストラップ プロトコル（BOOTP）パケット

レイヤ2のループの発生を防止するために、接続されているすべてのスイッチ ポート上でスパニング ツリー プロトコル（STP）を有効にします。

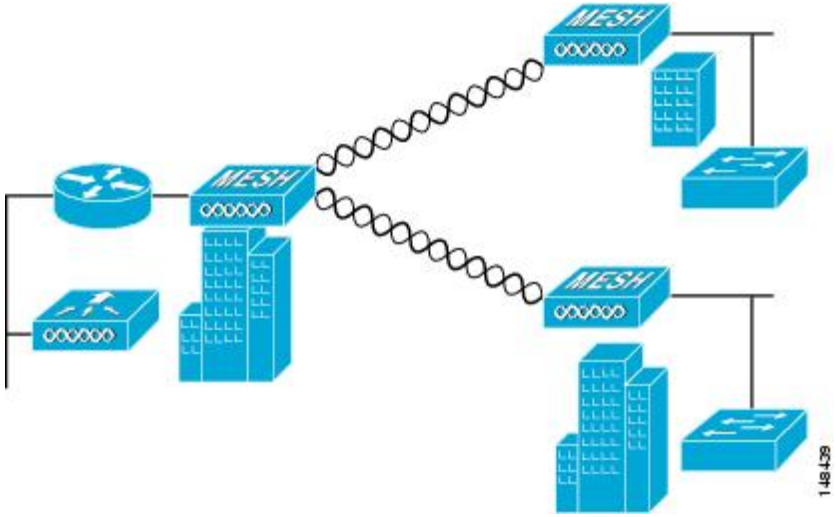
イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

1. メッシュ ノードをブリッジとして使用する場合。

（注） ポイントツーポイントおよびポイントツーマルチポイント ブリッジング導入でイーサネット ブリッジングを使用するのに、VLAN タギングを設定する必要はありません。

2. MAP でイーサネット ポートを使用して任意のイーサネット デバイス（ビデオ カメラなど）を接続する場合。VLAN タギングを有効にするときの最初の手順です。

図 *3*: ポイントツーマルチポイント ブリッジング



ネイティブ VLAN の設定（CLI）

（注） 8.0 以前は、有線バックホールのネイティブ VLAN は VLAN 1 に設定されていました。8.0 リリース以降では、ネイティブ VLAN を設定できます。

1. コマンド **config ap vlan-trunking native** ***vlan-id ap-name*** を使用して有線バックホール ポートにネイティブ VLAN を設定します。

   これは、アクセス ポイントにネイティブ VLAN 設定を適用します。

ブリッジ グループ名の設定

ブリッジ グループ名（BGN）は、メッシュ アクセス ポイントのアソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておくと、同じチャネルにある 2 つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター（領域）のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字までの文字列です。

NULL VALUE という BGN は、工場で設定されているデフォルトです。装置自体にブリッジ グループ名は表示されていませんが、このグループ名を使用することで、ネットワーク固有の BGN を割り当てる前に、メッシュ アクセス ポイントをネットワークに参加させることができます。

同一セクターのネットワーク内に（より大きなキャパシティを得るために）RAP が 2 つある場合は、別々のチャネルで 2 つの RAP に同じ BGN を設定することをお勧めします。

完全一致BGNをメッシュAPで有効にすると、一致するBGN親を見つけるために10回スキャンします。10回スキャンした後、APが一致するBGN親を見つけられない場合は、一致しないBGNに接続し、15分間接続を維持します。15分後にAPが再び10回スキャンを行い、このサイクルが継続されます。デフォルトのBGNの機能は完全一致BGNが有効な場合も同じです。

ブリッジ グループ名の設定（CLI）

手順

ステップ 1 ブリッジ グループ名（BGN）を設定するには、次のコマンドを入力します。

config ap bridgegroupname set *group-name ap-name*

（注） BGNの設定後に、メッシュ アクセス ポイントがリブートします。

注意 稼働中のネットワークでBGNを設定する場合は、注意してください。BGNの割り当ては、必ずRAPから最も遠い距離にあるノード（メッシュ ツリーの一番下にある終端ノード）から開始し、RAPに向かって設定して、同じネットワーク内に混在するBGN（古いBGNと新しいBGN）のため、メッシュ アクセス ポイントがドロップしないようにします。

ステップ 2 BGNを確認するには、次のコマンドを入力します。

show ap config general *ap-name*

アンテナ利得の設定

コントローラのGUIまたはCLIを使用して、取り付けられているアンテナのアンテナ ゲインと一致するように、メッシュアクセスポイントのアンテナゲインを設定する必要があります。

アンテナ ゲインの設定（CLI）

コントローラのCLIを使用して802.11aバックホール無線のアンテナ ゲインを設定するには、次のコマンドを入力します。

config 802.11a antenna extAntGain *antenna_gain AP_name*

ここで、ゲインは0.5 dBm単位で入力します（たとえば、2.5 dBmの場合は5になります）。

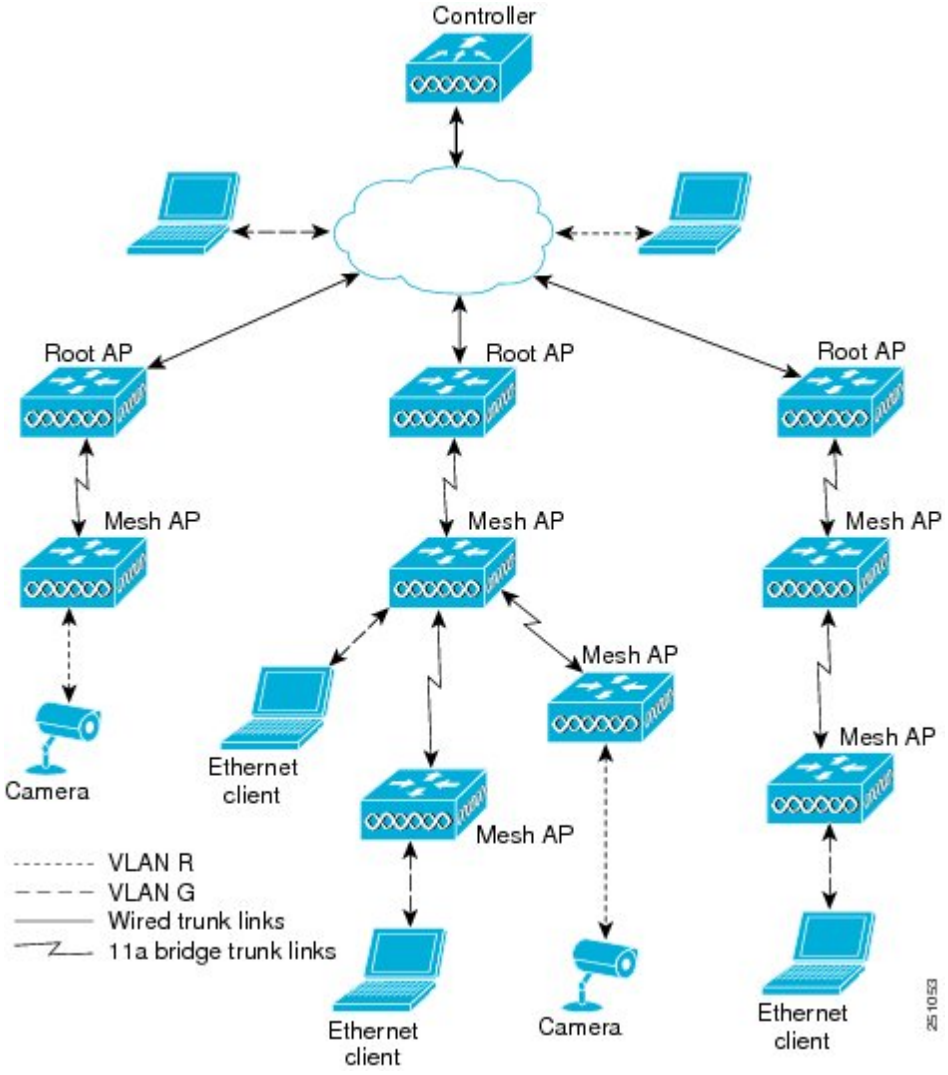
拡張機能の設定

イーサネット VLAN タギングの設定

イーサネットVLANタギングを使用すると、無線メッシュ ネットワーク内で特定のアプリケーション トラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセス モード）、別の無線メッシュ ネットワークにブリッジングすることができます（トランク モード）。

イーサネットVLANタギングを使用した一般的なPublic Safetyアクセス アプリケーションは、市内のさまざまな屋外の場所へのビデオ監視カメラの設置を前提にしたものです。これらのビデオ カメラはすべて MAP に有線で接続されています。また、これらのカメラのビデオはすべてワイヤレス バックホールを介して有線ネットワークにある中央の指令本部にストリーミングされます。

図 *4:* イーサネット ***VLAN*** タギング



イーサネット ポートに関する注意

イーサネット VLAN タギングを使用すると、屋内と屋外の両方の実装で、イーサネット ポートをノーマル、アクセス、またはトランクとして設定できます。

（注） VLAN 透過が無効な場合、デフォルトのイーサネット ポート モードはノーマルです。VLAN タギングを使用し、イーサネット ポートの設定を許可するには、VLAN 透過を無効にする必要があります。グローバル パラメータである VLAN トランスペアレント モードを無効にするには、「グローバル メッシュ パラメータの設定」の項を参照してください。

- アクセス モード：このモードでは、タグなしパケットだけを許可します。すべての着信パケットに、アクセス VLAN と呼ばれるユーザ設定 VLAN のタグが付けられます。

  MAP に接続され、RAP に転送される装置（カメラや PC）から情報を収集するアプリケーションでは、アクセス モードを使用します。次に、RAP はタグを適用し、トラフィックを有線ネットワーク上のスイッチに転送します。

- トランク モード：このモードでは、ユーザがネイティブ VLAN および許可された VLAN リストを設定する必要があります（デフォルトではありません）。このモードではタグ付きのパケットとタグなしパケットの両方が許可されます。タグなしパケットは許可され、ユーザ指定のネイティブ VLAN のタグが付けられます。許可された VLAN リスト内の VLAN のタグが付けられたタグ付きパケットは許可されます。

- キャンパス内の別々の建物に存在している 2 つの MAP 間でトラフィックを転送するようなブリッジング アプリケーションでは、トランク モードを使用します。

イーサネット VLAN タギングは、バックホールとして使用されていないイーサネット ポートで動作します。

（注） コントローラの 7.2 よりも前のリリースでは、ルート アクセス ポイント（RAP）のネイティブ VLAN は、メッシュ イーサネット ブリッジングと VLAN トランスペアレントを有効にしたメッシュ アクセス ポイント（MAP）のイーサネット ポートから転送されます。

7.2 および 7.4 リリースでは、ルート アクセス ポイント（RAP）のネイティブ VLAN は、メッシュ イーサネット ブリッジングと VLAN トランスペアレントを有効にしたメッシュ アクセス ポイント（MAP）のイーサネット ポートから転送されません。この動作は 7.6 から変更されます。ネイティブ VLAN は、VLAN トランスペアレントが有効になると MAP により転送されます。

この動作の変更は信頼性を向上し、メッシュ バックホールの転送ループの発生を最小限に抑えます。

VLAN 登録

メッシュ アクセス ポイントで VLAN をサポートするには、すべてのアップリンク メッシュ アクセス ポイントが、異なる VLAN に属するトラフィックを分離できるよう同じ VLAN をサポートする必要があります。メッシュ アクセス ポイントが VLAN 要件を通信して親からの応答を得る処理は、VLAN 登録と呼ばれます。

（注） VLAN 登録は自動的に行われます。ユーザの操作は必要ありません。

VLAN 登録の概要は次のとおりです。

1. メッシュ アクセス ポイントのイーサネット ポートが VLAN で設定されている場合は、ポートから親へその VLAN をサポートすることを要求します。
2. 親は、要求をサポートできる場合、その VLAN のブリッジ グループを作成し、要求をさらにその親へ伝搬します。この伝搬は RAP に達するまで続きます。
3. 要求が RAP に達すると、RAP は VLAN 要求をサポートできるかどうかを確認します。サポートできる場合、RAP は VLAN 要求をサポートするために、ブリッジ グループとサブインターフェイスをアップリンク イーサネット インターフェイスで作成します。
4. メッシュ アクセス ポイントのいずれかの子で VLAN 要求をサポートできない場合、メッシュアクセスポイントはネガティブ応答を返します。この応答は、VLANを要求したメッシュ アクセス ポイントに達するまでダウンストリーム メッシュ アクセス ポイントに伝搬されます。
5. 親からのネガティブ応答を受信した要求元メッシュ アクセス ポイントは、VLAN の設定を延期します。ただし、将来試みるときのために設定は保存されます。メッシュの動的な特性を考慮すると、ローミング時やCAPWAP再接続時に、別の親とそのアップリンク メッシュ アクセス ポイントがその設定をサポートできることがあります。

イーサネット VLAN タギングのガイドライン

イーサネット タギングの以下のガイドラインに従います。

- 安全上の理由により、メッシュ アクセス ポイント（RAP および MAP）にあるイーサネット ポートはデフォルトで無効になっています。このイーサネット ポートは、メッシュ アクセス ポイント ポートでイーサネット ブリッジングを設定することにより、有効になります。
- イーサネット VLAN タギングが動作するには、メッシュ ネットワーク内の全メッシュ アクセス ポイントでイーサネット ブリッジングが有効である必要があります。
- VLAN モードは、非 VLAN トランスペアレントに設定する必要があります（グローバル メッシュ パラメータ）。「グローバル メッシュ パラメータの設定（CLI）」の項を参照してください。VLANトランスペアレントは、デフォルトで有効になっています。非VLANトランスペアレントとして設定するには、[Wireless] > [Mesh] ページで [VLAN transparent] オプションをオフにする必要があります。
- VLAN タギングは、次のようにイーサネット インターフェイスでだけ設定できます。
  - AP1500 では、4 つのポートのうちポート 0（PoE 入力）、ポート 1（PoE 出力）、およびポート 3（光ファイバ）の 3 つをセカンダリ イーサネット インターフェイスとして使用できます。ポート 2- ケーブルは、セカンダリ イーサネット インターフェイスとして設定できません。

- イーサネット VLAN タギングでは、RAP のポート 0-PoE 入力は、有線ネットワークのスイッチのトランク ポートへの接続に使用します。MAP のポート 1-PoE 出力は、ビデオ カメラなどの外部デバイスへの接続に使用します。

- バックホール インターフェイス（802.11a 無線）は、プライマリ イーサネット インターフェイスとして機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべてのVLANトラフィックを伝送します。プライマリ イーサネット インターフェイスに必要な設定はありません。
- 屋内メッシュ ネットワークの場合、VLAN タギング機能は、屋外メッシュ ネットワークの場合と同様に機能します。バックホールとして動作しないアクセス ポートはすべてセカンダリであり、VLAN タギングに使用できます。
- RAP にはセカンダリ イーサネット ポートがないため、VLAN タギングを RAP 上で実装できず、プライマリ ポートがバックホールとして使用されます。ただし、イーサネット ポートが 1 つの MAP では VLAN タギングを有効にすることができます。これは、MAP のイーサネット ポートがバックホールとして機能せず、結果としてセカンダリ ポートになるためです。
- 設定の変更は、バックホールとして動作するイーサネットインターフェイスに適用されません。バックホールの設定を変更しようとすると警告が表示されます。設定は、インターフェイスがバックホールとして動作しなくなった後に適用されます。
- メッシュ ネットワーク内の任意の 802.11a バックホール イーサネット インターフェイスで VLAN タギングをサポートするために設定は必要ありません。
  - これには RAP アップリンク イーサネット ポートが含まれます。登録メカニズムを使用して、必要な設定が自動的に行われます。
  - バックホールとして動作する 802.11a イーサネット リンクへの設定の変更はすべて無視され、警告が表示されます。イーサネット リンクがバックホールとして動作しなくなると、変更した設定が適用されます。
- AP1500 のポート 02（ケーブル モデム ポート）では、VLAN を設定できません（該当する場合）。ポート 0（PoE 入力）、1（PoE 出力）、および 3（光ファイバ）では VLAN を設定できます。
- 各セクターでは、最大 16 個の VLAN がサポートされています。したがって、RAP の子（MAP）によってサポートされている VLAN の累積的な数は最大 16 です。
- RAP に接続されるスイッチ ポートはトランクである必要があります。
  - スイッチのトランク ポートと RAP トランク ポートは一致している必要があります。
  - RAP は常にスイッチのネイティブ VLAN ID 1 に接続する必要があります。RAP のプライマリ イーサネット インターフェイスは、デフォルトではネイティブ VLAN 1 です。
  - RAP に接続されている有線ネットワークのスイッチ ポート（ポート 0–PoE 入力）は、トランク ポートでタグ付きパケットを許可するように設定する必要があります。RAP

は、メッシュ ネットワークから受信したすべてのタグ付きパケットを有線ネットワークに転送します。

- メッシュ セクター宛以外の VLAN をスイッチのトランク ポートに設定しないでください。

- MAP イーサネット ポートで設定した VLAN は、管理 VLAN として機能できません。
- メッシュ アクセス ポイントが CAPWAP RUN 状態であり、VLAN 透過モードが無効な場合にのみ、設定は有効です。
- ローミングする場合、または CAPWAP が再び開始される場合は、必ず設定の適用が再び試行されます。

イーサネット VLAN タギングの設定（CLI）

MAP アクセス ポートを設定するには、次のコマンドを入力します。

config ap ethernet 1 mode access enable *AP1500-MAP 50*

ここで、*AP1500-MAP* は可変の *AP* 名であり、*50* は可変のアクセス *VLAN ID* です。

RAP または MAP のトランク ポートを設定するには、次のコマンドを入力します。

config ap ethernet 0 mode trunk enable *AP1500-MAP 60*

ここで、*AP1500-MAP* は可変の *AP* 名であり、*60* は可変のネイティブ *VLAN ID* です。

VLAN をネイティブ VLAN の VLAN 許可リストに追加するには、次のコマンドを入力します。

config ap ethernet 0 mode trunk add *AP1500-MAP3 65*

ここで、*AP1500-MAP 3* は可変の *AP* 名であり、*65* は可変の *VLAN ID* です。

イーサネット VLAN タギング設定詳細の表示（CLI）

手順

- 特定のメッシュ アクセス ポイント（*AP Name*）またはすべてのメッシュ アクセス ポイント（*summary*）のイーサネットインターフェイスの VLAN 設定の詳細を表示するには、次のコマンドを入力します。

  show ap config ethernet *ap-name*

- VLAN トランスペアレント モードが有効と無効のどちらであるかを確認するには、次のコマンドを入力します。

  show mesh config

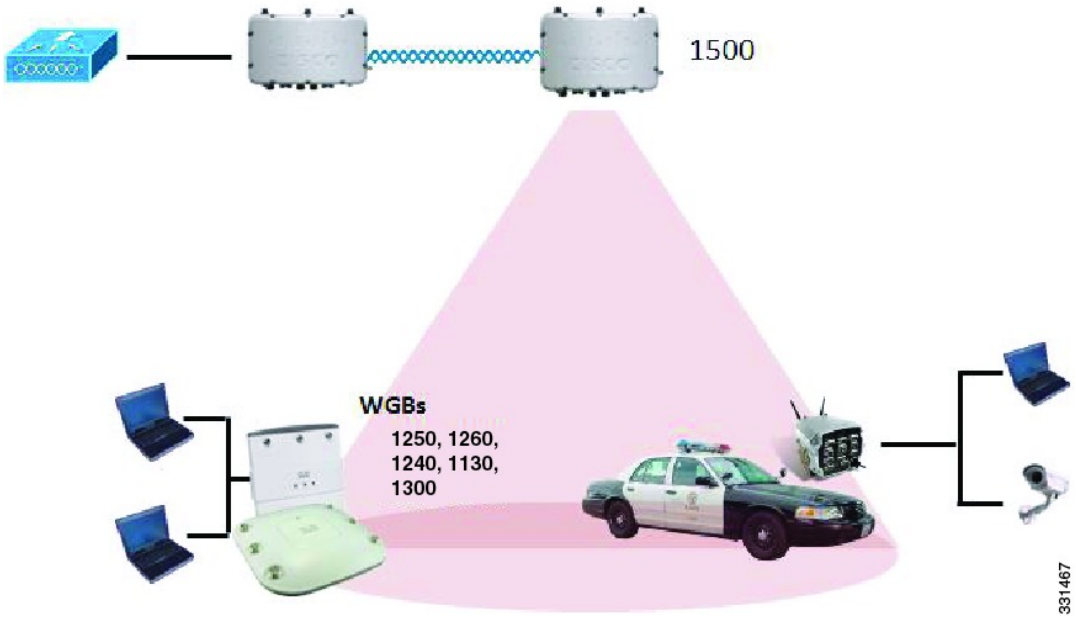
ワークグループ ブリッジとメッシュ インフラストラクチャとの相互運用性

ワークグループ ブリッジ（WGB）は、イーサネット対応デバイスにワイヤレス インフラストラクチャ接続を提供できる小さいスタンドアロンユニットです。無線ネットワークに接続するためにワイヤレス クライアント アダプタを備えていないデバイスは、イーサネット ポート経由で WGB に接続できます。WGB は、ワイヤレス インターフェイスを介してルート AP にアソシエートされます。つまり、有線クライアントはワイヤレス ネットワークにアクセスできます。

WGB は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。WGB クライアントのデータ パケットでは、802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。ヘッダー内の追加 MAC は、WGB 自体のアドレスです。この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするために使用されます。

WGB アソシエーションは、各メッシュ アクセス ポイントの AP 全機でサポートされます。

図 *5 : WGB* の例



現在のアーキテクチャでは、Autonomous AP がワークグループ ブリッジとして機能しますが、1 つの無線インターフェイスだけがコントローラ接続、有線クライアント接続用イーサネット インターフェイス、およびワイヤレス クライアント接続の他の無線インターフェイスに使用されます。コントローラ（メッシュ インフラストラクチャを使用）および有線クライアントのイーサネット インターフェイスに接続するには、dot11radio 1（5 GHz）を使用できます。dot11radio 0（2.4 GHz）はワイヤレス クライアント接続に使用できます。要件に応じて、クライアント アソシエーションまたはコントローラ接続に dot11radio 1 または dot11radio 0 を使用できます。

7.0 リリースでは、ワイヤレス インフラストラクチャへのアップリンクを失ったとき、またはローミング シナリオの場合、WGB の 2 番目の無線のワイヤレス クライアントが、WGB によってアソシエート解除されません。

2 つの無線を使用する場合、1 つの無線をクライアント アクセスに使用し、もう 1 つの無線をアクセス ポイントにアクセスするために使用できます。2 つの独立した無線が 2 つの独立した機能を実行するため、遅延の制御が向上し、遅延が低下します。また、アップリンクが失われたとき、またはローミング シナリオの場合、WGB の 2 番目の無線のワイヤレス クライアントはアソシエーション解除されません。一方の無線はルート AP（無線の役割）として設定し、もう一方の無線は WGB（無線の役割）として設定する必要があります。

（注） 一方の無線が WGB として設定された場合、もう一方の無線は WGB またはリピータとして設定できません。

次の機能を WGB と使用することはサポートされていません。

- アイドル タイムアウト
- Web 認証：WGB が Web 認証 WLAN にアソシエートする場合、WGB は除外リストに追加され、すべての WGB 有線クライアントが削除されます（Web 認証 WLAN はゲスト WLAN の別名です）。
- WGB 背後の有線クライアントでの MAC フィルタリング、リンク テスト、およびアイドル タイムアウト

ワークグループ ブリッジの設定

ワークグループ ブリッジ（WGB）は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。IAPP 制御メッセージの他にも、WGB クライアントのデータ パケットでは 802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。ヘッダー内の追加 MAC は、ワークグループ ブリッジ自体のアドレスです。この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするときに使用されます。

WGB アソシエーションは、すべての Cisco AP で 2.4 GHz 帯（802.11b/g）および 5 GHz 帯（802.11a）の両方でサポートされます。

WGB はメッシュ アクセス ポイントに関連付けることができるため、設定されたサポートされるプラットフォームは自律 1600、1700、2600、2700、3600、3700、1530、1550、および 1570 です。設定手順については、https://www.cisco.com/c/en/us/support/wireless/8500-series-wireless-controllers/products-installation-and-configuration-guides-list.html の『*Cisco Wireless LAN Controller Configuration Guide*』の「Cisco Workgroup Bridges」の項を参照してください。

サポートされる WGB モードおよび機能は次のとおりです。

- WGB として設定された自律アクセス ポイントでは Cisco IOS リリース 12.4.25d-JA 以降が実行されている必要があります。

（注） メッシュ アクセス ポイントに 2 つの無線がある場合、いずれかの無線でだけワークグループ ブリッジ モードを設定できます。2 番目の無線を無効にすることをお勧めします。3 チャネルの同時使用に対応するアクセス ポイントは、ワークグループ ブリッジ モードをサポートしません。

- クライアント モード WGB（BSS）はサポートされていますが、インフラストラクチャ WGB はサポートされていません。クライアント モード WGB では VLAN をトランクできませんが、インフラストラクチャ WGB ではトランクできます。
- ACK がクライアントから返されないため、マルチキャスト トラフィックは WGB に確実に転送されるわけではありません。マルチキャスト トラフィックがインフラストラクチャ WGB にユニキャストされると、ACK が返されます。
- Cisco IOS アクセス ポイントで一方の無線が WGB として設定された場合、もう一方の無線を WGB やリピータにすることができません。
- メッシュ アクセス ポイントでは、アソシエートされた WGB の背後で、ワイヤレス クライアント、WGB、および有線クライアントを含む、最大 200 のクライアントをサポートできます。
- WLAN が WPA1（TKIP）+WPA2（AES）で設定され、対応する WGB インターフェイスがこれらの暗号化の 1 つ（WPA1 または WPA2）で設定された場合、WGB はメッシュ アクセス ポイントとアソシエートできません。

図 *6 : WGB* の *WPA* セキュリティ設定

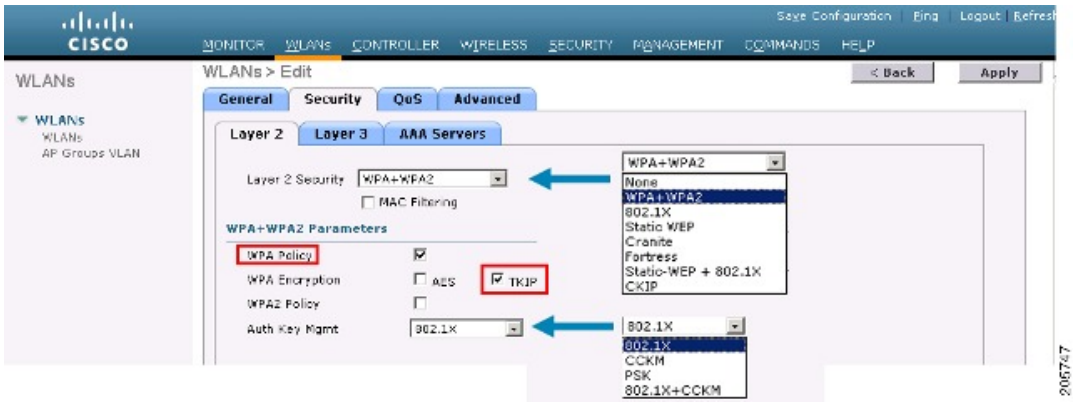
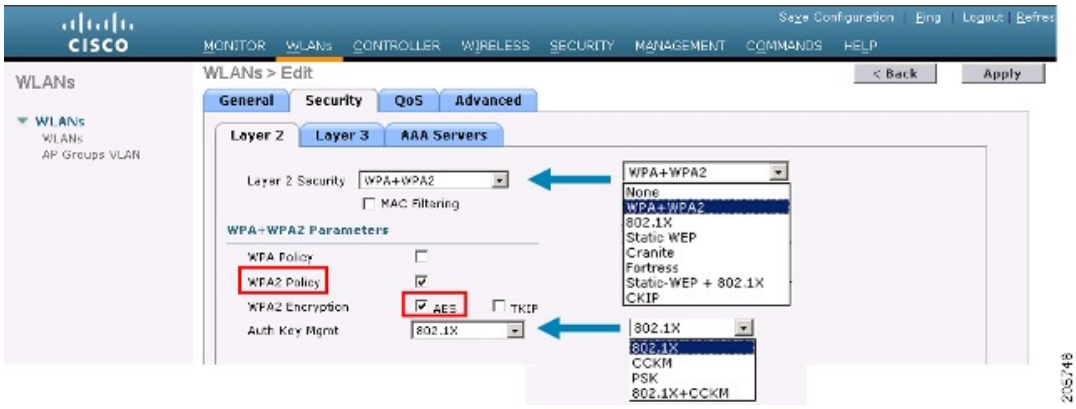


図 *7: WGB* の *WPA-2* セキュリティ設定



WGB クライアントのステータスを表示する手順は、次のとおりです。

手順

ステップ 1 [Monitor] > [Clients] を選択します。

ステップ 2 クライアント サマリー ページで、クライアントの MAC アドレスをクリックするか、その MAC アドレスを使用してクライアントを検索します。

ステップ 3 表示されるページで、クライアントの種類が *WGB* として認識されていることを確認します（右端）。

図 *8:* クライアントが *WGB* であると認識されている

ステップ 4 クライアントの MAC アドレスをクリックすると、設定の詳細が表示されます。

- ワイヤレス クライアントの場合は、**[Monitor]** > **[Clients]** > **[Detail Page (Wireless WGB Client)]** で表示されるページが表示されます。
- 有線クライアントの場合は、**[Monitor]** > **[Clients]** > **[Detail Page (Wireless WGB Client)]** で表示されるページが表示されます。

図 *9 : [Monitor] > [Clients] > [Detail]* ページ（無線 *WGB* クライアントの場合）

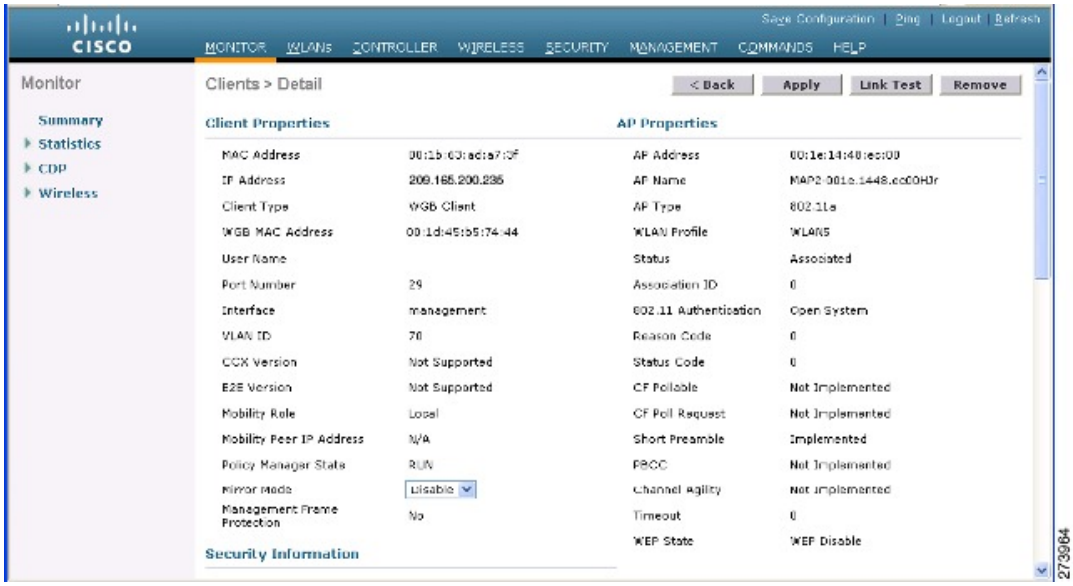
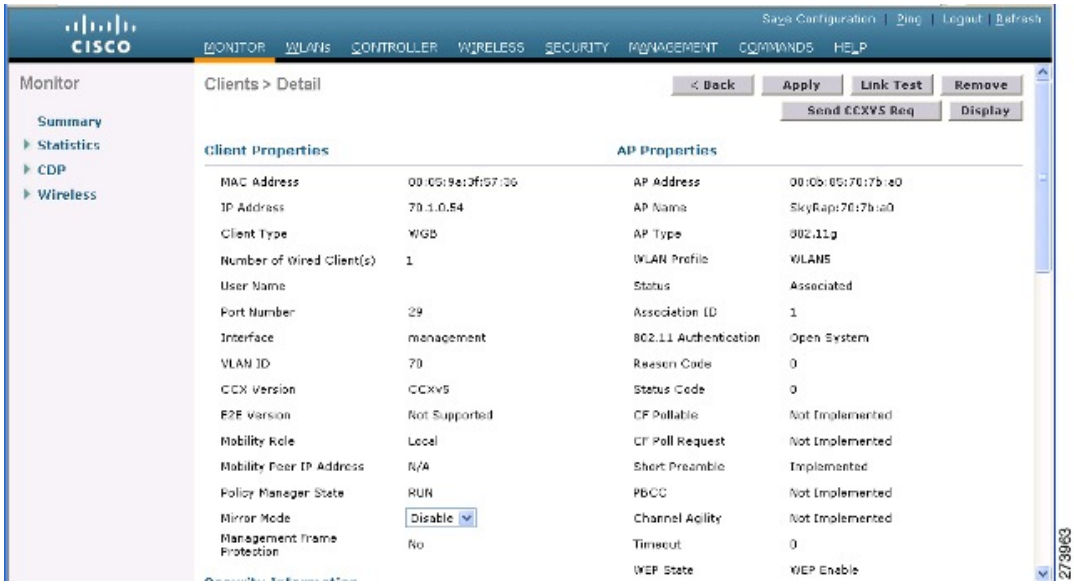


図 *10 : [Monitor] > [Clients] > [Detail]* ページ（有線 *WGB* クライアントの場合）



設定のガイドライン

設定時は、次のガイドラインに従います。

- メッシュ アクセス ポイントで利用可能な 2 つの 5 GHz 無線で強力なクライアント アクセスを利用できるよう、メッシュ AP インフラストラクチャへのアップリンクには 5 GHz 無線を使用することをお勧めします。5 GHz 帯域を使用すると、より大きい Effective Isotropic Radiated Power（EIRP）が許可され、品質が劣化しにくくなります。2 つの無線がある WGB では、5 GHz 無線（無線 1）モードを WGB として設定します。この無線は、メッシュ イ

ンフラストラクチャにアクセスするために使用されます。2 番目の無線 2.4 GHz（無線 0）モードをクライアント アクセスのルートとして設定します。

- 自律アクセス ポイントでは、SSID を 1 つだけネイティブ VLAN に割り当てることができます。自律側では、1 つの SSID で複数の VLAN を使用できません。SSID と VLAN のマッピングは、異なる VLAN でトラフィックを分離するために一意である必要があります。Unified アーキテクチャでは、複数の VLAN を 1 つの WLAN（SSID）に割り当てることができます。
- アクセス ポイント インフラストラクチャへの WGB のワイヤレス アソシエーションには 1 つの WLAN（SSID）だけがサポートされます。この SSID はインフラストラクチャ SSID として設定し、ネイティブ VLAN にマッピングする必要があります。
- 動的インターフェイスは、WGB で設定された各 VLAN のコントローラで作成する必要があります。
- アクセス ポイントの 2 番目の無線（2.4 GHz）でクライアント アクセスを設定する必要があります。両方の無線で同じ SSID を使用し、ネイティブ VLAN にマッピングする必要があります。異なる SSID を作成した場合は、一意な VLAN と SSID のマッピングの要件のため、その SSID をネイティブ VLAN にマッピングすることはできません。SSID を別の VLAN にマッピングしようとしても、ワイヤレス クライアントの複数 VLAN サポートはありません。
- WGB でのワイヤレス クライアント アソシエーションでは、WLAN（SSID）に対してすべてのレイヤ 2 セキュリティ タイプがサポートされます。
- この機能は AP プラットフォームに依存しません。コントローラ側では、メッシュ AP および非メッシュ AP の両方がサポートされます。
- WGB では、20 クライアントの制限があります。20 クライアントの制限には、有線クライアントとワイヤレス クライアントの両方が含まれます。WGB が自律アクセス ポイントと対話する場合、クライアントの制限は非常に高くなります。
- コントローラは、WGB の背後にあるワイヤレス クライアントと有線クライアントを同様に扱います。コントローラからワイヤレス WGB クライアントに対する MAC フィルタリングやリンク テストなどの機能は、サポートされません。
- 必要な場合、WGB ワイヤレス クライアントに対するリンク テストは自律 AP から実行できます。
- WGB にアソシエートされたワイヤレス クライアントに対する複数の VLAN はサポートされません。
- 7.0 リリース以降、WGB の背後にある有線クライアントに対して最大 16 の複数 VLAN がサポートされます。
- WGB の背後にあるワイヤレス クライアントおよび有線クライアントに対してローミングがサポートされます。アップリンクが失われたとき、またはローミング シナリオの場合、他の無線のワイヤレス クライアントは WGB によってアソシエート解除されません。

無線 0（2.4 GHz）をルート（自律 AP の 1 つの動作モード）として設定し、無線 1（5 GHz）を WGB として設定することをお勧めします。

設定例

CLI で設定する場合に必須な項目は次のとおりです。

- dot11 SSID（WLAN のセキュリティは要件に基づいて決定できます）。
- 単一ブリッジ グループに両方の無線のサブインターフェイスをマッピングすること。

（注） ネイティブ VLAN は、デフォルトで常にブリッジ グループ 1 にマッピングされます。他の VLAN の場合、ブリッジ グループ番号は VLAN 番号に一致します。たとえば、VLAN 46 の場合、ブリッジ グループは 46 です。

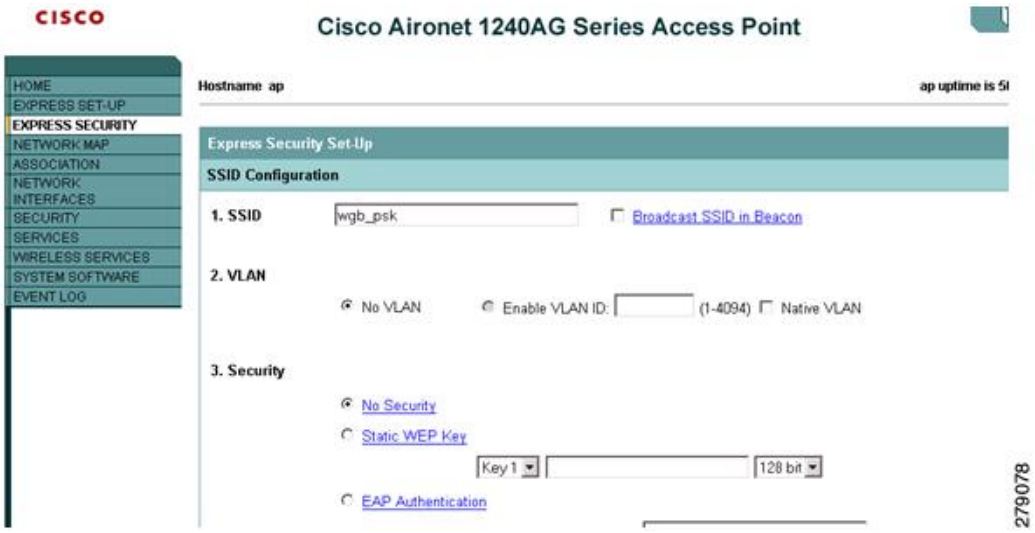
- SSID を無線インターフェイスにマッピングし、無線インターフェイスの役割を定義します。

次の例では、両方の無線で 1 つの SSID（WGBTEST）が使用され、SSID は NATIVE VLAN 51 にマッピングされたインフラストラクチャ SSID です。すべての無線インターフェイスは、ブリッジ グループ -1 にマッピングされます。

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

また、自律 AP の GUI を使用して設定を行うこともできます。この GUI から VLAN が定義された後に、サブインターフェイスは自動的に作成されます。

図 *11 : [SSID Configuration]* ページ



WGB アソシエーションの確認

コントローラと WGB のアソシエーションおよび WGB とワイヤレス クライアントのアソシエーションはどちらも、自律 AP で **show dot11 associations client** コマンドを入力して確認できます。

```
WGB#show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :
```

MAC Address	IP Address	Device	Name	Parent	State
0024.130f.920e	209.165.200.225	LWAPP-Parent	RAPSB	-	Assoc

コントローラで、[Monitor]>[Clients] を選択します。WGB と、WGB の背後にあるワイヤレス/有線クライアントは更新され、ワイヤレス/有線クライアントが WGB クライアントとして表示されます。

図 *12* : 更新された *WGB* クライアント

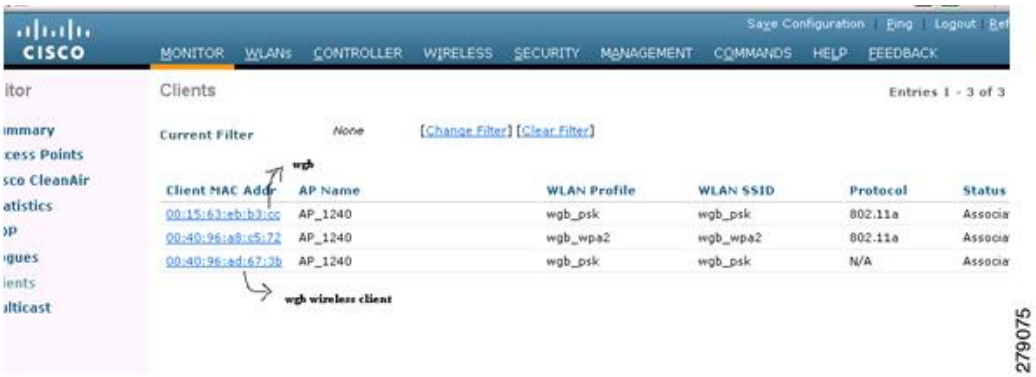
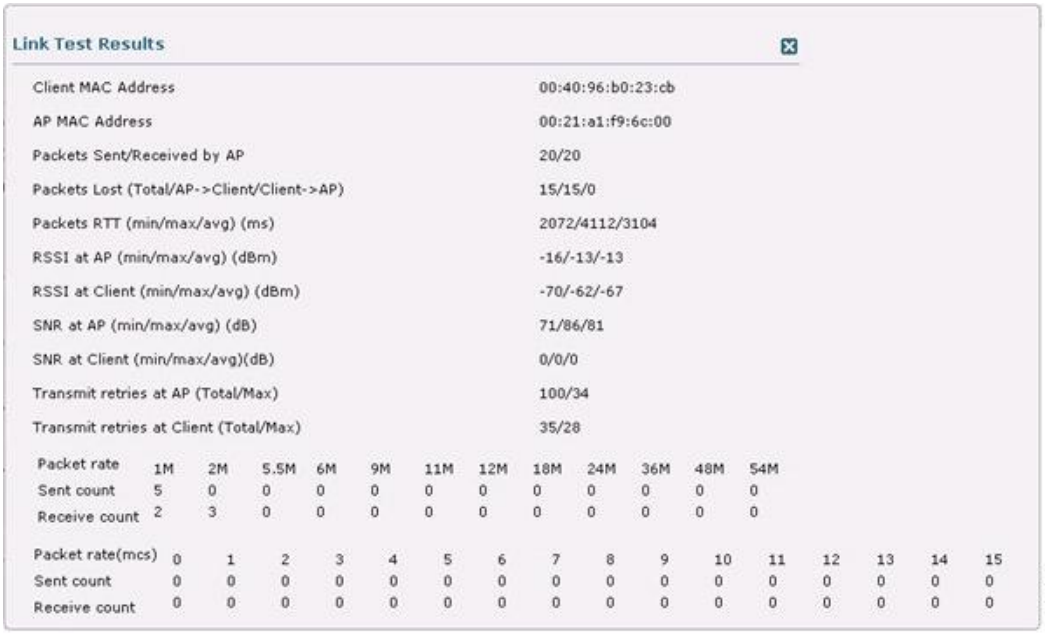


図 *13* : 更新された *WGB* クライアント

図 *14* : 更新された *WGB* クライアント

リンク テストの結果

図 *15:* リンク テストの結果



リンク テストは、コントローラのCLIから次のコマンドを使用して実行することもできます。

```
(Cisco Controller) > linktest client mac-address
```

コントローラからのリンク テストはWGBにのみ制限され、コントローラから、WGBに接続された有線またはワイヤレス クライアントに対してWGB外部で実行することはできません。WGB自体からWGBに接続されたワイヤレス クライアントのリンク テストを実行するには、次のコマンドを使用します。

```
ap#dot11 dot11Radio 0 linktest target client-mac-address
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
```

POOR (4% lost)	Time (msec)	Strength (dBm)		SNR Quality		Retries	
		In	Out	In	Out	In	Out
Sent: 100	Avg. 22	-37	-83	48	3	Tot. 34	35
Lost to Tgt: 4	Max. 112	-34	-78	61	10	Max. 10	5
Lost to Src: 4	Min. 0	-40	-87	15	3		

```
Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB 有線/ワイヤレス クライアント

また、次のコマンドを使用して、WGB と、Cisco Lightweight アクセス ポイントにアソシエートされたクライアントの概要を確認することもできます。

```
(Cisco Controller) > show wgb summary
Number of WGBs..................................... 2
```

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

```
(Cisco Controller) > show client summary

Number of Clients.................................. 7
```

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:d2	R14	Associated	1	Yes	802.11a	29	No

```
(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2

Number of wired client(s): 5
```

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth

00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No
00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes
00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

クライアント ローミング

Cisco Compatible Extension（CX）バージョン4（v4）クライアントによる高速ローミングでは、屋外メッシュ展開において最大70 mphの速度がサポートされます。適用例としては、メッシュ パブリック ネットワーク内を移動する緊急車両の端末との通信を維持する場合があります。

3 つの Cisco CX v4 レイヤ 2 クライアント ローミング拡張機能がサポートされています。

- アクセス ポイント経由ローミング：クライアントによるスキャン時間が短縮されます。Cisco CX v4 クライアントがアクセス ポイントにアソシエートする際、新しいアクセス ポイントに以前のアクセスポイントの特徴を含む情報パケットを送信します。各クライアントがアソシエートされていた以前のアクセスポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセスポイントをすべてまとめて作成したアクセスポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセスポイントのリストには、チャネル、クライアントの現在の SSID をサポートするネイバー アクセス ポイントの BSSID、およびアソシエーション解除からの経過時間が含まれます。
- 拡張ネイバー リスト：音声アプリケーションを中心に、Cisco CX v4 クライアントのローミング能力とネットワーク エッジのパフォーマンスを向上させます。アクセス ポイントは、ネイバーリストのユニキャスト更新メッセージを使用して、アソシエートされたクライアントのネイバーに関する情報を提供します。
- ローミング理由レポート：Cisco CX v4 クライアントが新しいアクセス ポイントにローミングした理由を報告できます。また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。

（注） クライアントローミングはデフォルトでは有効です。詳細については、『Enterprise Mobility Design Guide』（http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf）を参照してください。

WGB ローミングのガイドライン

WGB ローミングのガイドラインは次のとおりです。

- WGB でのローミングの設定：WGB がモバイルである場合は、親アクセス ポイントまたはブリッジへのより良好な無線接続をスキャンするよう設定できます。ワークグループ ブリッジをモバイル ステーションとして設定するには、 ap(config-if)#**mobile station period 3 threshold 50** コマンドを使用します。

  この設定を有効にすると、受信信号強度表示（RSSI）の数値が低いこと、電波干渉が多いこと、またはフレーム損失率が高いことが検出された場合に、WGBは新しい親アソシエーションをスキャンします。これらの基準を使用して、モバイル ステーションとして設定された WGB は新しい親アソシエーションを検索し、現在のアソシエーションが失われる前に新しい親にローミングします。モバイル ステーションの設定が無効な場合（デフォルト設定）、WGB は現在のアソシエーションが失われるまで新しいアソシエーションを検索しません。

- WGB での限定チャネル スキャンの設定：鉄道などのモバイル環境では、WGB はすべてのチャネルをスキャンする代わりに、限定チャネルのセットのみをスキャンするよう制限され、WGB のローミングが 1 つのアクセス ポイントから別のアクセス ポイントに切り替わるときにハンドオフによる遅延が減少します。チャネル数を制限することにより、WGB は必要なチャネルのみをスキャンします。モバイル WGB では、高速かつスムーズなローミングとともに継続的なワイヤレス LAN 接続が実現され、維持されます。この限定チャネル セットは、ap(config-if)#**mobile station scan** *set of channels* を使用して設定されます。

  このコマンドにより、すべてのチャネルまたは指定されたチャネルに対するスキャンが実行されます。設定できるチャネルの最大数に制限はありません。設定できるチャネルの最大数は、無線がサポートできるチャネル数に制限されます。実行時に、WGB はこの限定チャネル セットのみをスキャンします。この限定チャネルの機能は、WGB が現在アソシエートされているアクセス ポイントから受け取る既知のチャネル リストにも影響します。チャネルは、チャネルが限定チャネル セットに含まれる場合にのみ、既知のチャネル リストに追加されます。

設定例

次に、ローミング設定を設定する例を示します。

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

no mobile station scan コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

トラブルシューティングのヒント

ワイヤレス クライアントがWGBにアソシエートされていない場合は、次の手順を実行して問題をトラブルシューティングします。

1. クライアントの設定を確認し、クライアントの設定が正しいことを確認します。
2. 自律 AP で **show bridge** コマンドの出力を確認し、AP が適切なインターフェイスからクライアント MAC アドレスを参照していることを確認します。
3. 異なるインターフェイスの特定のVLANに対応するサブインターフェイスが同じブリッジグループにマッピングされていることを確認します。
4. 必要に応じて、**clear bridge** コマンドを使用してブリッジ エントリをクリアします（このコマンドは、WGB 内の関連付けられているすべての有線およびワイヤレス クライアントを削除し、それらのクライアントを再度関連付けます）。
5. **show dot11 association** コマンドの出力を確認し、WGB がコントローラに関連付けられていることを確認します。
6. WGB で 20 クライアントの制限が超えていないことを確認します。

通常のシナリオでは、**show bridge** コマンドと **show dot11 association** コマンドの出力が期待されたものである場合、ワイヤレス クライアントの関連付けは成功です。

屋内メッシュ ネットワークの音声パラメータの設定

メッシュ ネットワークにおける音声およびビデオの品質を管理するために、コントローラでコール アドミッション制御（CAC）および QoS を設定できます。

屋内メッシュ アクセス ポイントは 802.11e 対応であり、QOS は、2.4 および 5 GHz のローカル AP、2.4 および 5 GHz の AP、2.4 および 5 GHz の無線バックホールでサポートされます。CAC は、バックホールおよびCCXv4 クライアントでサポートされています（メッシュ アクセス ポイントとクライアント間の CAC を提供）。

（注） 音声は、屋内メッシュ ネットワークだけでサポートされます。音声は、メッシュ ネットワークの屋外においてベストエフォート方式でサポートされます。

Call Admission Control（コール アドミッション制御）

コール アドミッション制御（CAC）を使用すると、ワイヤレス LAN で輻輳が発生した際でも、メッシュ アクセス ポイントで定義された QoS を維持できます。CCX v3 で展開される Wi-Fi Multimedia（WMM）プロトコルにより、無線 LAN に輻輳が発生しない限り十分な QoS が保証されます。ただし、さまざまなネットワーク負荷で QoS を維持するには、CCXv4 以降の CAC が必要です。

（注） CAC は Cisco Compatible Extensions（CCX）v4 以降でサポートされています。『*Cisco Wireless LAN Controller Configuration Guide, Release 7.0*』（http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html）の第 6 章を参照してください。

アクセスポイントには、帯域幅ベースの CAC と load-based の CAC という 2 種類の CAC が利用できます。メッシュ ネットワーク上のコールはすべて帯域幅ベースであるため、メッシュ アクセス ポイントは帯域幅ベースの CAC だけを使用します。

帯域幅に基づく、静的な CAC を使用すると、クライアントで新しいコールを受信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセスポイントは、使用可能な帯域幅を確認して特定のコールに対応できるかどうかを判断し、そのコールに必要な帯域幅と比較します。品質を許容できる最大可能コール数を維持するために十分な帯域幅が使用できない場合、メッシュ アクセス ポイントはコールを拒否します。

QoS および DiffServ コード ポイントのマーキング

ローカル アクセスとバックホールでは、802.11e がサポートされています。メッシュ アクセス ポイントでは、分類に基づいて、ユーザ トラフィックの優先順位が付けられるため、すべてのユーザ トラフィックがベストエフォートの原則で処理されます。

メッシュのユーザが使用可能なリソースは、メッシュ内の位置によって異なり、ネットワークの 1 箇所に帯域幅制限を適用する設定では、ネットワークの他の部分でオーバーサブスクリプションが発生することがあります。

同様に、クライアントの RF の割合を制限することは、メッシュ クライアントに適していません。制限するリソースはクライアント WLAN ではなく、メッシュ バックホールで使用可能なリソースです。

有線イーサネット ネットワークと同様に、802.11 WLAN では、キャリア検知多重アクセス（CSMA）が導入されます。ただし、WLAN は、衝突検出（CD）を使用する代わりに衝突回避（CA）を使用します。つまり、メディアが空いたらすぐに各ステーションが伝送を行う代わりに、WLAN デバイスは衝突回避メカニズムを使用して複数のステーションが同時に伝送を行うのを防ぎます。

衝突回避メカニズムでは、CWmin と CWmax という 2 つの値が使用されます。CW はコンテンション ウィンドウ（Contention Window）を表します。CW は、インターフレーム スペース（IFS）の後、パケットの転送に参加するまで、エンドポイントが待機する必要がある追加の時間を指定します。Enhanced Distributed Coordination Function（EDCF）は、遅延に影響を受けるマルチメディア トラフィックのあるエンドデバイスが、CWmin 値と CWmax 値を変更して、メディアに統計的に大きい（および頻繁な）アクセスを行えるようにするモデルです。

シスコのアクセス ポイントは EDCF に似た QoS をサポートします。これは最大 8 つの QoS のキューを提供します。

これらのキューは、次のようにいくつかの方法で割り当てることができます。

- パケットの TOS / DiffServ 設定に基づく

- レイヤ 2 またはレイヤ 3 アクセス リストに基づく
- VLAN に基づく
- デバイス（IP 電話）の動的登録に基づく

AP1500 は Cisco コントローラとともに、コントローラで最小の統合サービス機能（クライアント ストリームに最大帯域幅の制限がある）と、IP DSCP 値と QoS WLAN 上書きに基づいたより堅牢なディファレンシエーテッド サービス（diffServ）機能を提供します。

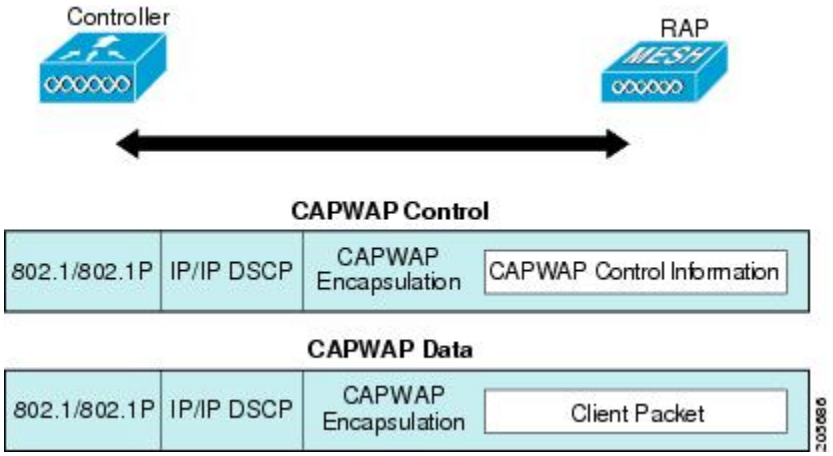
キュー容量に達すると、追加のフレームがドロップされます（テール ドロップ）。

カプセル化

メッシュ システムでは複数のカプセル化が使用されます。これらのカプセル化には、コントローラと RAP 間、メッシュ バックホール経由、メッシュ アクセス ポイントとそのクライアント間の CAPWAP 制御とデータが含まれます。バックホール経由のブリッジ トラフィック（LAN からの非コントローラ トラフィック）のカプセル化は CAPWAP データのカプセル化と同じです。

コントローラと RAP 間には 2 つのカプセル化があります。1 つは CAPWAP 制御のカプセル化であり、もう 1 つは CAPWAP データのカプセル化です。制御インスタンスでは、CAPWAP は制御情報とディレクティブのコンテナとして使用されます。CAPWAP データのインスタンスでは、イーサネットと IP ヘッダーを含むパケット全体が CAPWAP コンテナ内で送信されます

図 *16* : カプセル化

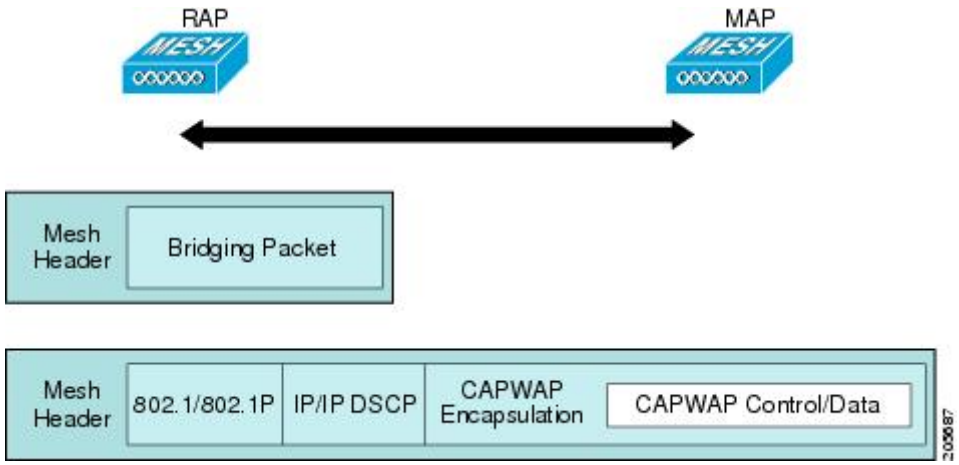


バックホールの場合、メッシュ トラフィックのカプセル化のタイプは1つだけです。ただし、2つのタイプのトラフィック（ブリッジ トラフィックと CAPWAP 制御およびデータ トラフィック）がカプセル化されます。どちらのタイプのトラフィックもプロプライエタリ メッシュ ヘッダーにカプセル化されます。

ブリッジ トラフィックの場合、パケットのイーサネット フレーム全体がメッシュ ヘッダーにカプセル化されます。

すべてのバックホール フレームが MAP から MAP、RAP から MAP、または MAP から RAP でも関係なく適切に処理されます。

図 *17* : メッシュ トラフィックのカプセル化



（注） メッシュ データ DTLS 暗号化は、1540 および 1560 モデルなどの Wave 2 メッシュ AP でのみサポートされます。

メッシュ アクセス ポイントでのキューイング

メッシュ アクセス ポイントは高速の CPU を使用して、入力フレーム、イーサネット、およびワイヤレスを先着順に処理します。これらのフレームは、適切な出力デバイス（イーサネットまたはワイヤレスのいずれか）への伝送のためにキューに格納されます。出力フレームは、802.11 クライアント ネットワーク、802.11 バックホール ネットワーク、イーサネットのいずれかを宛先にすることができます。

AP1500 は、ワイヤレス クライアント伝送用に 4 つの FIFO をサポートします。これらの FIFO は 802.11e Platinum、Gold、Sliver、Bronze キューに対応し、これらのキューの 802.11e 伝送ルールに従います。FIFO では、キューの深さをユーザが設定できます。

バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Siliver、および Bronze に制限されます。Platinum キューは、CAPWAP 制御トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

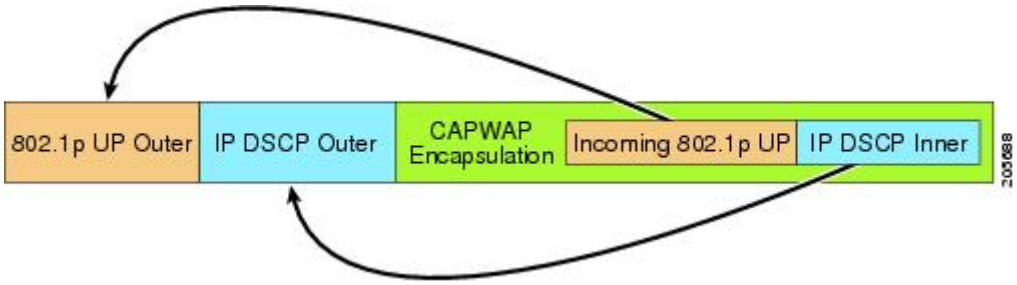
Gold キューの CWmin や CWmax などの 802.11e パラメータは、遅延が少なくなるように変更されています。ただし、エラー レートとアグレッシブが若干増加します。これらの変更の目的は、ビデオ アプリケーションから使いやすいチャネルを提供することです。

イーサネット宛のフレームは FIFO として、使用可能な最大伝送バッファ プール（256 フレーム）までキューに格納されます。レイヤ 3 IP Differentiated Services Code Point（DSCP）がサポートされ、パケットのマーキングもサポートされます。

データ トラフィックのコントローラから RAP へのパスでは、外部 DSCP 値が着信 IP フレームの DSCP 値に設定されます。インターフェイスがタグ付きモードである場合、コントローラ

は、802.1Q VLAN ID を設定し、802.1p UP 着信と WLAN のデフォルトの優先度上限から 802.1p UP（外部）を派生させます。VLAN ID 0 のフレームはタグ付けされません。

図 *18 :* コントローラから *RAP* へのパス



CAPWAP 制御トラフィックの場合、IP DSCP 値は 46 に設定され、802.1p ユーザ優先度（UP）は7に設定されます。バックホール経由のワイヤレス フレームの伝送の前に、ノードのペア化（RAP/MAP）や方向に関係なく、外部ヘッダーの DSCP 値を使用して、バックホール優先度が判断されます。次の項で、メッシュ アクセス ポイントで使用される 4 つのバックホール キューとバックホール パス QoS に示される DSCP 値のマッピングについて説明します。

表 *1 :* バックホール パス *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze
26、32 ～ 63	Gold
46 ～ 56	Platinum
その他すべての値（0 を含む）	Silver

（注） Platinum バックホール キューは CAPWAP 制御トラフィック、IP 制御トラフィック、音声パケット用に予約されています。DHCP、DNS、および ARP 要求も Platinum QoS レベルで伝送されます。メッシュ ソフトウェアは、各フレームを調査し、それが CAPWAP 制御フレームであるか、IP 制御フレームであるかを判断して、Platinum キューが CAPWAP 以外のアプリケーションに使用されないようにします。

MAP からクライアントへのパスの場合、クライアントが WMM クライアントか通常のクライアントかに応じて、2 つの異なる手順が実行されます。クライアントが WMM クライアントの場合、外部フレームの DSCP 値が調査され、802.11e プライオリティ キューが使用されます。

表 *2 : MAP* からクライアントへのパスの *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze

DSCP 値	バックホール キュー
26、32 ～ 45、47	Gold
46、48 ～ 63	Platinum
その他すべての値（0 を含む）	Silver

クライアントが WMM クライアントでない場合、WLAN の上書き（コントローラで設定された）によって、パケットが伝送される 802.11e キュー（Bronze、Gold、Platinum、または Silver）が決定されます。

メッシュ アクセス ポイントのクライアントの場合、メッシュ バックホールまたはイーサネットでの伝送に備えて、着信クライアント フレームが変更されます。WMM クライアントの場合、MAP が着信 WMM クライアント フレームから外部 DSCP 値を設定する方法を示します。

図 *19 : MAP* から *RAP* へのパス

着信 802.11e ユーザ優先度および WLAN の上書き優先度の最小値が、表 3 : DSCP とバックホール キューのマッピング （45 ページ） に示された情報を使用して変換され、IP フレームの DSCP 値が決定されます。たとえば、着信フレームの優先度の値が Gold 優先度を示しているが、WLAN が Silver 優先度に設定されている場合は、最小優先度の Silver を使用して DSCP 値が決定されます。

表 *3 : DSCP* とバックホール キューのマッピング

DSCP 値	802.11e UP	バックホール キュー	パケット タイプ
2、4、6、8 ～ 23	1、2	Bronze	最小の優先度のパケット（存在する場合）
26、32 ～ 34	4、5	Gold	ビデオ パケット
46 ～ 56	6、7	Platinum	CAPWAP 制御、AWPP、DHCP/DNS、ARP パケット、音声パケット
その他すべての値（0 を含む）	0、3	Silver	ベスト エフォート、CAPWAP データ パケット

着信WMM優先度がない場合、デフォルトのWLAN優先度を使用して、外部ヘッダーのDSCP値が生成されます。フレームが（APで）生成された CAPWAP 制御フレームの場合は、46 の DSCP 値が外部ヘッダーに配置されます。

5.2 コード拡張では、DSCP 情報が AWPP ヘッダーに保持されます。

Platinum キューを経由する DHCP/DNS パケットと ARP パケットを除き、すべての有線クライアント トラフィックは 5 の最大 802.1p UP 値に制限されます。

WMM 以外のワイヤレス クライアント トラフィックは、その WLAN のデフォルトの QoS 優先度を取得します。WMM ワイヤレス クライアント トラフィックには 802.11e の最大値の 6 を設定することができますが、それらはその WLAN に設定された QoS プロファイル未満である必要があります。アドミッション制御を設定した場合、WMM クライアントは TSPEC シグナリングを使用し、CAC によって許可されている必要があります。

CAPWAPP データ トラフィックはワイヤレス クライアント トラフィックを伝送し、ワイヤレス クライアント トラフィックと同じ優先度を持ち、同じように扱われます。

DSCP 値が決定されたので、さらに、RAP から MAP へのバックホール パスの先述したルールを使用して、フレームを伝送するバックホール キューが決定されます。RAP からコントローラに伝送されるフレームはタグ付けされません。外部DSCP値は最初に作成されているため、そのままになります。

ブリッジ バックホール パケット

ブリッジサービスの処理は通常のコントローラベースのサービスと少し異なります。ブリッジパケットは、CAPWAPカプセル化されないため、外部DSCP値がありません。そのため、メッシュ アクセス ポイントによって受信された IP ヘッダーの DSCP 値を使用して、メッシュ アクセス ポイントからメッシュ アクセス ポイント（バックホール）までのパスに示されたようにテーブルがインデックス化されます。

LAN 間のブリッジ パケット

LAN 上のステーションから受信されたパケットは、決して変更されません。LAN 優先度の上書き値はありません。したがって、LAN では、ブリッジ モードで適切に保護されている必要があります。メッシュ バックホールに提供されている唯一の保護は、Platinum キューにマップされる CAPWAP 以外の制御フレームは Gold キューに降格されます。

パケットはメッシュへの着信時にイーサネット入口で受信されるため、LAN に正確に伝送されます。

AP1500 上のイーサネット ポートと 802.11a 間の QoS を統合する唯一の方法は、DSCP によってイーサネット パケットをタグ付けすることです。AP1500 は DSCP を含むイーサネット パケットを取得し、それを適切な 802.11e キューに格納します。

AP1500 では、DSCP 自体をタグ付けしません。

- AP1500 は、入力ポートで DSCP タグを確認し、イーサネット フレームをカプセル化して、対応する 802.11e 優先度を適用します。

- AP1500 は、出力ポートでイーサネット フレームのカプセル化を解除し、DSCP フィールドをそのままにして、そのフレームを回線上に配置します。

ビデオ カメラなどのイーサネット デバイスは、QoS を使用するために、DSCP 値でビットをマークする機能を持つ必要があります。

（注） QoS は、ネットワーク上で輻輳が発生したときにだけ関連します。

メッシュ ネットワークでの音声使用のガイドライン

メッシュ ネットワークで音声を使用する場合は、次のガイドラインに従います。

- 音声は、屋内メッシュ ネットワークだけでサポートされます。屋外の場合、音声は、メッシュ インフラストラクチャにおいてベストエフォート方式でサポートされます。
- 音声がメッシュ ネットワークで動作している場合、コールは3ホップ以上を通過してはいけません。音声で3ホップ以上を必要としないように、各セクターを設定する必要があります。
- 音声ネットワークの RF の考慮事項は次のとおりです。
  - 2 ～ 10 % のカバレッジ ホール
  - 15 ～ 20 % のセル カバレッジ オーバーラップ
  - 音声がデータ要件より 15 dB 以上高い RSSI 値および SNR 値を必要とする
  - すべてのデータ レートの -67 dBm の RSSI が 11b/g/n および 11a/n の目標である
  - AP に接続するクライアントにより使用されるデータ レートの SNR は 25 dB である必要がある
  - パケット エラー レートの値が 1 % 以下の値になるように設定する必要がある
  - 最小使用率のチャネル（CU）を使用する必要がある
- [802.11a/n/ac] または [802.11b/g/n] > [Global] パラメータ ページで、次のことを行う必要があります。
  - Dynamic Transmit Power Control（DTPC）を有効にする
  - 11 Mbps 未満のすべてのデータ レートを無効にする
- [802.11a/n/ac] または [802.11b/g/n] > [Voice] パラメータ ページで、次のことを行う必要があります。
  - 負荷に基づく CAC を無効にする

- WMM が有効化されている CCXv4 または v5 クライアントに対してアドミッション コントロール（ACM）を有効にする。そうしない場合、帯域幅ベースの CAC は適切に動作しません。
- 最大 RF 帯域幅を 50 % に設定する
- 予約済みローミング帯域幅を 6 % に設定する
- トラフィック ストリーム メトリックを有効にする

- [802.11a/n/ac] または [802.11b/g/n] > [EDCA] パラメータ ページで、次のことを行う必要があります。
  - インターフェイスの EDCA プロファイルを [Voice Optimized] に設定する
  - 低遅延 MAC を無効にする

- [QoS > *Profile*] ページで、次の手順を実行する必要があります。
  - 音声プロファイルを作成して有線 QoS プロトコル タイプとして 802.1Q を選択する

- [WLANs > *Edit* > *QoS*] ページで、次の手順を実行する必要があります。
  - バックホールの QoS として [Platinum]（音声）および [Gold]（ビデオ）を選択する
  - WMM ポリシーとして [Allowed] を選択する

- [WLANs > *Edit* > *QoS*] ページで、次の手順を実行する必要があります。
  - 高速ローミングをサポートする場合、認可（*auth*）キー管理（*mgmt*）で [CCKM] を選択します。

- [x > *y*] ページで、次の手順を実行する必要があります。
  - Voice Active Detection（VAD）を無効にする

メッシュ ネットワークでの音声コールのサポート

表 4 : 802.11a/n 無線および 802.11b/g/n 無線で可能な 1550 シリーズのコール （48 ページ） に、クリーンで理想的な環境での実際のコールを示します。

表 *4 : 802.11a/n* 無線および *802.11b/g/n* 無線で可能な *1550* シリーズのコール

コール数 [1]	802.11a/n 無線 20 MHz	802.11a/n 無線 40 MHz	802.11b/g/n バックホール無線 20 MHz	802.11b/g/n バックホール無線 40 MHz
RAP	20	35	20	20

コール数 [1]	802.11a/n 無線 20 MHz	802.11a/n 無線 40 MHz	802.11b/g/n バックホール無線 20 MHz	802.11b/g/n バックホール無線 40 MHz
MAP1（最初のホップ）	10	20	15	20
MAP2（2 番目のホップ）	8	15	10	15

[1] トラフィックは双方向 64K 音声フローです。VoCoder タイプ：G.711、PER <= 1%。ネットワークのセットアップはデイジーチェーン接続され、コールは 2 ホップを超えて伝送しません。外部干渉はありません。

コールを発信する間、7921 電話のコールの MOS スコアを観察します。3.5 ～ 4 の MOS スコアが許容可能です。

表 *5 : MOS* 評価

MOS 評価	ユーザ満足度
> 4.3	たいへん満足している
4.0	満足している
3.6	一部のユーザが満足していない
3.1	多くのユーザが満足していない
< 2.58	—

ビデオのメッシュ マルチキャストの抑制の有効化

コントローラ CLI を使用して 3 種類のメッシュ マルチキャスト モードを設定し、すべてのメッシュ アクセス ポイントでビデオ カメラ ブロードキャストを管理できます。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは、ブリッジング対応アクセス ポイント MAP および RAP が、メッシュ ネットワーク内のイーサネット LAN 間でマルチキャストを送信する方法を決定します。メッシュ マルチキャスト モードは非 CAPWAP マルチキャスト トラフィックのみを管理します。CAPWAP マルチキャスト トラフィックは異なるメカニズムで管理されます。

次の 3 つのメッシュ マルチキャスト モードがあります。

- **regular モード**：データは、ブリッジ対応の RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにマルチキャストされます。
- **in-only モード**：MAP がイーサネットから受信するマルチキャスト パケットは RAP のイーサネット ネットワークに転送されます。追加の転送は行われず、これにより、RAP によっ

て受信された CAPWAP 以外のマルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワーク（それらの発信ポイント）に返送されず、MAP から MAP へのマルチキャストはフィルタで除去されるため発生しません。

（注） HSRP 設定がメッシュ ネットワークで動作中の場合は、in-out マルチキャスト モードを設定することをお勧めします。

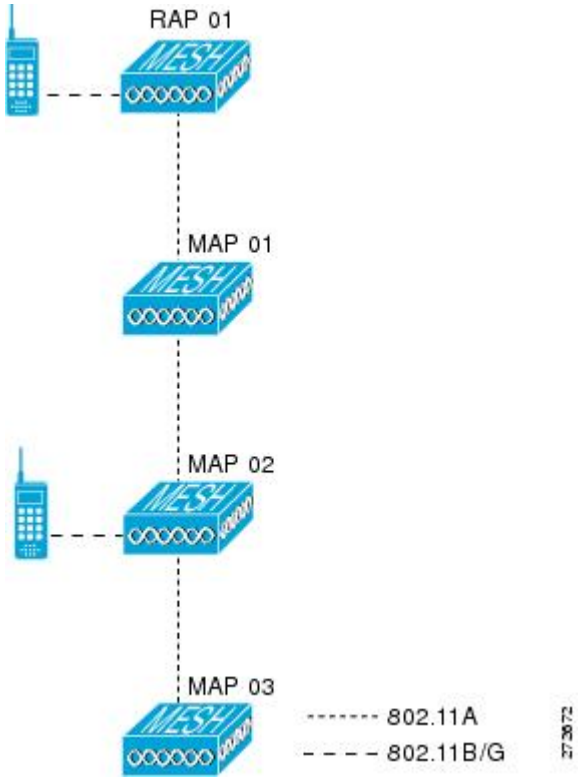
- **in-out モード**：RAP と MAP は別々の方法でマルチキャストを行います。
  - in-out モードはデフォルトのモードです。
  - マルチキャスト パケットが、イーサネット経由で MAP で受信されると、それらは RAP に送信されますが、それらはイーサネット経由で他の MAP に送信されず、MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。
  - マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

（注） 802.11b クライアントで CAPWAP マルチキャストを受信する必要がある場合、マルチキャストは、コントローラおよびメッシュ ネットワークでグローバルに有効にする必要があります（**config network multicast global enable** CLI コマンドを使用）。マルチキャストをメッシュ ネットワーク外の 802.11b クライアントまで拡張する必要がない場合は、グローバル マルチキャスト パラメータを無効にする必要があります（**config network multicast global disable** CLI コマンドを使用）。

メッシュ ネットワークの音声詳細の表示（CLI）

この項のコマンドを使用して、メッシュ ネットワークの音声およびビデオ コールの詳細を表示します。

図 *20* : メッシュ ネットワークの例



- 各 RAP での音声コールの合計数と音声コールに使用された帯域幅を表示するには、次のコマンドを入力します。

  show mesh cac summary

  以下に類似した情報が表示されます。

```
AP Name          Slot#   Radio  BW Used/Max  Calls
------------    -------  -----  -----------  -----
SB_RAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    2
SB_MAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP2              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP3              0   11b/g     0/23437    0
                     1   11a      0/23437    0?
```

- ネットワークのメッシュ ツリー トポロジおよび各メッシュ アクセス ポイントと無線の音声コールとビデオ リンクの帯域幅使用率（使用/最大）を表示するには、次のコマンドを入力します。

  show mesh cac bwused {**voice** | **video**} *AP_name*

  以下に類似した情報が表示されます。

```
AP Name       Slot#    Radio      BW Used/Max
```

```
-------------- -------  -----      -----------
SB_RAP1          0      11b/g       1016/23437
                 1      11a         3048/23437
|SB_MAP1         0      11b/g       0/23437
                 1      11a         3048/23437
||  SB_MAP2      0      11b/g       2032/23437
                 1      11a         3048/23437
||| SB_MAP3      0      11b/g       0/23437
                 1      11a         0/23437
```

（注） [AP Name] フィールドの左側の縦棒（|）は、MAP のその RAP からのホップ カウントを示します。

（注） 無線タイプが同じ場合、各ホップでのバックホール帯域幅使用率（bw使用/最大）は同じです。たとえば、メッシュ アクセス ポイント *map1*、*map2*、*map3*、および *rap1* はすべて同じ無線バックホール（802.11a）上にあるので、同じ帯域幅（3048）を使用しています。コールはすべて同じ干渉ドメインにあります。そのドメインのどの場所から発信されたコールも、他のコールに影響を与えます。

- ネットワークのメッシュ ツリー トポロジを表示し、メッシュ アクセス ポイント無線によって処理中の音声コール数を表示するには、次のコマンドを入力します。

  show mesh cac access *AP_name*

```
Information similar to the following appears:

AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） メッシュ アクセス ポイント無線で受信された各コールによって、該当のコール サマリー カラムが 1 つずつ増加されます。たとえば、map2 の 802.11b/g がコールを受信すると、802.11b/g の *calls* カラムにある既存の値が 1 増加します。上記の例では、map2 の 802.11b/g でアクティブなコールは、新しいコールだけです。新しいコールが受信されるときに 1 つのコールがアクティブである場合、値は 2 になります。

- ネットワークのメッシュ ツリートポロジを表示し、動作中の音声コールを表示するには、次のコマンドを入力します。

  show mesh cac callpath *AP_name*

```
Information similar to the following appears:

AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コール パス内にある各メッシュ アクセス ポイント無線の *Calls* カラムは 1 ずつ増加します。たとえば、map2 (**show mesh cac call path** *SB_MAP2*) で発信され、map1 を経由して rap1 で終端するコールの場合、1 つのコールが map2 802.11b/g および 802.11a 無線の [calls] カラムに追加され、1 つのコールが map1 802.11a バックホール 無線の [calls] カラムに追加され、1 つのコールが rap1 802.11a バックホール無線の [calls] カラムに追加されます。

- ネットワークのメッシュ ツリートポロジ、帯域幅の不足のためメッシュ アクセス ポイント無線で拒否される音声コール、拒否が発生した対応するメッシュ アクセス ポイント無線を表示するには、次のコマンドを入力します。

  show mesh cac rejected *AP_name*

  以下に類似した情報が表示されます。

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コールが map2 802.11b/g で拒否された場合、*calls* カラムは 1 ずつ増加します。

- 指定のアクセス ポイントでアクティブな Bronze、Silver、Gold、Platinum、および管理キューの数を表示するには、次のコマンドを入力します。各キューのピークおよび平均長と、オーバーフロー数が表示されます。

  show mesh queue-stats *AP_name*

  以下に類似した情報が表示されます。

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows：キュー オーバーフローによって破棄されたパケットの総数。

  Peak Length：定義された統計期間中にキューで待機していたパケットの最大数。

  Average Length：定義された統計期間中にキューで待機していたパケットの平均数。

メッシュ ネットワークにおけるマルチキャストの有効化（CLI）

（注）
- Cisco Aironet 1540 および 1560 シリーズの屋外アクセス ポイントは in-out モードのみサポートします。
- Cisco Aironet 1530、1550、および 1570 シリーズの屋外アクセス ポイントはすべてのモードをサポートします。

手順

- メッシュ ネットワークでマルチキャスト モードを有効にしてメッシュ ネットワーク外からのマルチキャストを受信するには、次のコマンドを入力します。

  config network multicast global enable

  config mesh multicast {**regular** | **in-only** | **in-out**}

- メッシュ ネットワークのみでマルチキャスト モードを有効にする（マルチキャストはメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない）には、次のコマンドを入力します。

  config network multicast global disable

  config mesh multicast {**regular** | **in-only** | **in-out**}

（注）コントローラ GUI を使用してメッシュ ネットワークのマルチキャストをイネーブルにすることはできません。

IGMP スヌーピング

IGMP スヌーピングを使用すると、特別なマルチキャスト転送により、RF 使用率が向上し、音声およびビデオ アプリケーションでのパケット転送が最適化されます。

メッシュ アクセス ポイントは、クライアントがマルチキャスト グループに登録されているメッシュ アクセス ポイントに関連付けられている場合にだけ、マルチキャスト パケットを伝送します。そのため、IGMP スヌーピングが有効な場合、指定したホストに関連するマルチキャスト トラフィックだけが転送されます。

コントローラ上で IGMP スヌーピングをイネーブルにするには、次のコマンドを入力します。

configure network multicast igmp snooping enable

クライアントは、メッシュ アクセス ポイントを経由してコントローラに転送される IGMP *join* を送信します。コントローラは、*join* を代行受信し、マルチキャスト グループ内のクライアントのテーブル エントリを作成します。次にコントローラはアップストリーム スイッチまたはルータを経由して、IGMP *join* をプロキシします。

次のコマンドを入力して、ルータで IGMP グループのステータスをクエリーできます。

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address    Interface   Uptime  Expires    Last Reporter
233.0.0.1        Vlan119     3w1d    00:01:52   10.1.1.130
```

レイヤ 3 ローミングの場合、IGMP クエリーはクライアントの WLAN に送信されます。コントローラはクライアントの応答を転送する前に変更し、ソース IP アドレスをコントローラの動的インターフェイス IP アドレスに変更します。

ネットワークは、コントローラのマルチキャスト グループの要求をリッスンし、マルチキャストを新しいコントローラに転送します。

音声の詳細については、次のマニュアルを参照してください。

- メッシュ上のビデオ サーベイランスの導入ガイド [英語]：http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080b02511.shtml
- *Cisco Unified Wireless Network* ソリューション：*VideoStream* 導入ガイド [英語]：http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b6e11e.shtml

メッシュ AP のローカルで有効な証明書

7.0 リリースまでは、メッシュ AP は、コントローラを認証したり、コントローラに join するためにコントローラにより認証を受けたりするために、製造元がインストールした証明書（MIC）しかサポートしていませんでした。CA の制御、ポリシーの定義、有効な期間の定義、生成された証明書の制限および使用方法の定義、および AP とコントローラでインストールされたこれらの証明書の取得を行うために、独自の公開鍵インフラストラクチャ（PKI）を用意する必要がある場合がありました。これらのユーザ生成証明書またはローカルで有効な証明書

（LSC）が AP とコントローラにある場合、デバイスはこれらの LSC を使用して join、認証、およびセッション キーの派生を行います。5.2 リリース以降では通常の AP がサポートされ、7.0 リリース以降ではメッシュ AP もサポートされるようになりました。

- AP が LSC 証明書を使用してコントローラに join できない場合の MIC へのグレースフル フォールバック：ローカル AP は、コントローラで設定された回数（デフォルト値は 3）、コントローラに join しようとします。これらの試行後に、AP は LSC を削除し、MIC を使用してコントローラに join しようとします。

  メッシュ AP は、孤立タイマーが切れ、AP がリブートされるまで LSC を使用してコントローラに join しようとします。孤立タイマーは 40 分に設定されます。リブート後に、AP は MIC を使用してコントローラに join しようとします。40 分後に AP が MIC を使用して再びコントローラに join できない場合は、AP がリブートされ、LSC を使用してコントローラに join しようとします。

  （注） メッシュ AP の LSC は削除されません。LSC は、コントローラで無効な場合にのみメッシュ AP で削除され、その結果、AP がリブートされます。

- MAP の無線プロビジョニング

設定のガイドライン

メッシュ AP に LSC を使用する場合は、次のガイドラインに従います。

- この機能により、AP からどの既存の証明書も削除されません。AP では LSC 証明書と MIC 証明書の両方を使用できます。
- AP が LSC を使用してプロビジョニングされると、AP は起動時に MIC 証明書を読み取りません。LSC から MIC に変更するには、AP をリブートする必要があります。AP は、LSC を使用して join できない場合に、フォールバックのためにこの変更を行います。
- AP で LSC をプロビジョニングするために、AP で無線をオフにする必要はありません。このことは、無線でプロビジョニングを行うことができるメッシュ AP にとって重要です。
- メッシュ AP には dot1x 認証が必要なため、CA および ID 証明書をコントローラ内のサーバにインストールする必要があります。
- LSC プロビジョニングは、MAP の場合、イーサネットと OTA を介して実行できます。その場合は、イーサネットを介してコントローラにメッシュ AP を接続し、LSC 証明書をプロビジョニングする必要があります。LSC がデフォルトになると、AP は LSC 証明書を使用して無線でコントローラに接続できます。

メッシュ AP の LSC と通常の AP の LSC の違い

CAPWAP AP は、AP モードに関係なく、join 時に LSC を使用して DTLS のセットアップを行います。メッシュ AP でもメッシュ セキュリティに証明書が使用されます。これには、親 AP を介したコントローラの dot1x 認証が含まれます。LSC を使用してメッシュ AP がプロビジョニングされたら、この目的のために LSC を使用する必要があります。これは、MIC が読み込まれないためです。

メッシュ AP は、静的に設定された dot1x プロファイルを使用して認証します。

このプロファイルは、証明書の発行元として「cisco」を使用するようハードコーディングされています。このプロファイルは、メッシュ認証にベンダー証明書を使用できるように設定可能にする必要があります（**config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** コマンドを入力）。

メッシュ AP の LSC を有効または無効にするには、**config mesh lsc enable/disable** コマンドを入力する必要があります。このコマンドを実行すると、すべてのメッシュ AP がリブートされます。

（注） 7.0 リリースでは、メッシュの LSC は、非常に限定された石油およびガス業界のお客様向けに提供されています。これは、隠し機能です。**config mesh lsc enable/disable** は隠しコマンドです。また、**config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** コマンドは通常のコマンドですが、「prfMaP1500LlEAuth93」プロファイルは隠しプロファイルであり、コントローラには保存されず、コントローラのリブート後に失われます。

LSC AP での証明書検証プロセス

LSC でプロビジョニングされた AP には LSC 証明書と MIC 証明書の両方がありますが、LSC 証明書がデフォルトの証明書になります。検証プロセスは次の 2 つの手順から構成されます。

1. コントローラが AP に MIC デバイス証明書を送信し、AP が MIC CA を使用してその証明書を検証します。
2. AP は LSC デバイス証明書をコントローラに送信し、コントローラは LSC CA を使用してその証明書を検証します。

LSC 機能の証明書の取得

LSC を設定するには、まず適切な証明書を収集してコントローラにインストールする必要があります。Microsoft 2003 Server を CA サーバとして使用して、この設定を行う手順を次に示します。

LSC の証明書を取得する手順は、次のとおりです。

手順

ステップ 1 CA サーバ（http://<ip address of caserver/crtsrv）にアクセスしてログインします。

ステップ 2 次の手順で、CA 証明書を取得します。

a) [Download a CA certificate link, certificate chain, or CRF] をクリックします。
b) 暗号化方式に [DER] を選択します。
c) [Download CA certificate] リンクをクリックし、[Save] オプションを使用して、CA 証明書をローカル マシンにダウンロードします。

ステップ 3 コントローラで証明書を使用するには、ダウンロードした証明書を PEM 形式に変換します。次のコマンドを使用して、Linux マシンでこれを変換することができます。

```
# openssl x509 -in <input.cer> -inform DER -out <output.cer> -outform PEM
```

ステップ 4 次の手順で、コントローラに CA 証明書を設定します。

a) [COMMANDS] > [Download File] を選択します。
b) [File Type] ドロップダウン リストから、ファイル タイプ [Vendor CA Certificate] を選択します。
c) 証明書が保存されている TFTP サーバの情報を使用して、残りのフィールドを更新します。
d) [Download] をクリックします。

ステップ 5 WLC にデバイス証明書をインストールするには、手順 1 に従い CA サーバにログインして、次の手順を実行します。

a) [Request a certificate] リンクをクリックします。
b) [advanced certificate request] リンクをクリックします。
c) [Create and submit a request to this CA] リンクをクリックします。
d) 次の画面に移動し、[Certificate Template] ドロップダウン リストから [Server Authentication Certificate] を選択します。
e) 有効な名前、電子メール、会社、部門、市、州、および国/地域を入力します。（CAP 方式を使用して、ユーザ クレデンシャルのデータベースでユーザ名を確認する場合は忘れないでください）。

（注） 電子メールは使用されません。

f) [Mark keys as exportable] をイネーブルにします。
g) [Submit] をクリックします。
h) ラップトップに証明書をインストールします。

ステップ 6 ステップ 5 で取得したデバイス証明書を変換します。証明書を取得するには、インターネット ブラウザのオプションを使用して、ファイルにエクスポートします。使用しているブラウザのオプションに従い、実行します。ここで設定するパスワードは覚えておく必要があります。

証明書を変換するには、Linux マシンで次のコマンドを使用します。

```
# openssl pkcs12 -in <input.pfx> -out <output.cer>
```

ステップ 7 コントローラの GUI で、[Command] > [Download File] を選択します。[File Type] ドロップダウン リストから [Vendor Device Certificate] を選択します。証明書が保存されている TFTP サーバの情報および前の手順で設定したパスワードを使用して残りのフィールドを更新し、[Download] をクリックします。

ステップ 8 コントローラをリブートして、証明書が使用できるようにします。

ステップ 9 次のコマンドを使用して、コントローラに証明書が正常にインストールされていることを確認できます。

show local-auth certificates

ローカルで有効な証明書の設定（CLI）

ローカルで有効な証明書（LSC）を設定するには、次の手順に従ってください。

手順

ステップ 1 LSC を有効にし、コントローラで LSC CA 証明書をプロビジョニングします。

ステップ 2 次のコマンドを入力します。

config local-auth eap-profile cert-issuer vendor *prfMaP1500LlEAuth93*

ステップ 3 次のコマンドを入力して、機能をオンにします。

config mesh lsc {**enable** | **disable**}

ステップ 4 イーサネットを介してメッシュ AP に接続し、LSC 証明書のためにプロビジョニングします。

ステップ 5 メッシュ AP で証明書を取得し、LSC 証明書を使用してコントローラに join します。

図 *21 :* ローカルで有効な証明書ページ

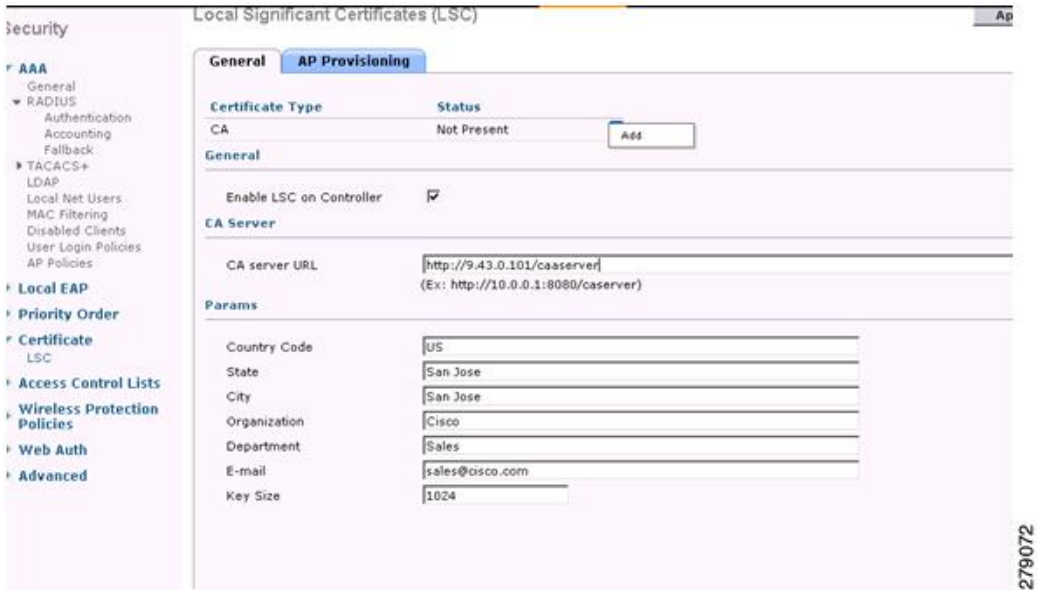


図 *22 : AP* ポリシーの設定

ワイルドカード MAC を使用した LSC 専用 MAP 認証

ワイルドカード MAC を使用した LSC 専用 MAP 認証に関する情報

8.0 リリースは、ワイルドカードの MAC アドレスを使用し、MAC フィルタを無効にして LSC 専用認証をサポートします。承認済みアクセス ポイントだけを認証するには、Cisco WLC が LSC 認証を EAP に強制できる必要があります。

この表は、LSC 認証のさまざまな方式を示しています。

表 *6 : MAP* 認証方式

動作	MAC フィルタ	LSC 専用認証
LSC 専用 MAP 認証有効	disabled	enabled
LSC 専用 MAP 認証無効	enabled	disabled
セキュリティ モード：EAP および PSK	EAP または PSK が使用可能	LSC 搭載の EAP のみを使用する必要がある
証明書：MIC および LSC	MIC または LSC が使用可能	LSC 搭載の EAP のみを使用する必要がある

WLC には、MAC フィルタ リストにワイルドカードの MAC アドレスが含まれ、すべての AP が WLC に join できるようになります。MAC 認証は自動的に無効になります。EAP セキュリティ モードは LSC で有効なセキュリティを提供します。EAP-FAST では、AP は LSC を使用して認証され、WLC から MSK キーを取得します。すべての不正な AP がフィルタで除去されます。これらのキーを使用してメッセージ ハンドシェイクが行われ、PTK キーが生成されます。メッシュ AP は LSC のみを使用して WLC に join します。

PSK セキュリティ モードには脆弱性が伴います。MSK キーがメッシュ AP のコード内でハードコード化されているため、AP は、不正 AP であっても WLC に join できます。これらのキーを使用して、メッセージのハンドシェイクが行われ、PTK キーが生成されます。メッシュ AP は LSC のみを使用して WLC に join します。PSK のワイルドカードはデバッグ目的でのみ使用する必要があります。

メッシュ アクセス ポイントの LSC 専用認証の設定（GUI）

メッシュ アクセス ポイントは Cisco WLC に関連付ける前に認証を行う必要があります。すべての Cisco WLC のフィルタ リストに AP 全機の MAC アドレスを入力するのは現実的ではありません。サービス プロバイダーにはローカルで有効な証明書（LSC）があり、これを使用して MAC 認証をバイパスし LSC のみ使用できます。

手順

ステップ 1 [Security] > [Certificate] > [LSC] の順に選択します。

[Locally Significant Certificates] ページが表示されます。

ステップ 2 [AP Provisioning] タブを選択します。

ステップ 3 [Enable LSC on Controller] チェックボックスをオンにします。

ステップ 4 [General] タブを選択します。

ステップ 5 [AP Provisioning] グループの [Enable] チェックボックスをオンにします。

ステップ 6 **[Wireless]** > **[Mesh]** の順に選択します。

[Mesh] ページが表示されます。

ステップ 7 [LSC Only MAP Authentication] チェックボックスをオンまたはオフにします。

ステップ 8 [Apply] をクリックします。

ステップ 9 [Save Configuration] をクリックします。

メッシュ アクセス ポイントの LSC 専用認証の設定（CLI）

メッシュ アクセス ポイントは Cisco WLC に関連付ける前に認証を行う必要があります。すべての Cisco WLC のフィルタ リストに AP 全機の MAC アドレスを入力するのは現実的ではありません。サービス プロバイダーにはローカルで有効な証明書（LSC）があり、これを使用して MAC 認証をバイパスし LSC のみ使用できます。

手順

- 次のコマンドを入力して、メッシュ アクセス ポイントの LSC 専用認証を設定します。
  config mesh security lsc-only-auth {**enable** | **disable**}

LSC 関連のコマンド

LSC に関連するコマンドは次のとおりです。

- **config certificate lsc** {**enable** | **disable**}
  - **enable**：システムで LSC を有効にします。
  - **disable**：システムで LSC を無効にします。LSC デバイス証明書を削除する場合や、AP にメッセージを送信して LSC デバイス証明書を削除し、LSC を無効にする場合は、このキーワードを使用します。その結果、以降の join を MIC/SSC を使用して行えるようになります。MIC/SSC に切り替わっていない AP を使用できるようにするために、WLC での LSC CA 証明書の削除は、CLI を使用して明示的に行う必要があります。

- **config certificate lsc ca-server url-path** *ip-address*

  次に、Microsoft 2003 Server 使用時の URL の例を示します。

  http:<ip address of CA>/sertsrv/mscep/mscep.dll

  このコマンドは、証明書を取得するために CA サーバへの URL を設定します。URL には、ドメイン名または IP アドレスのいずれか、ポート番号（通常は 80）、および CGI-PATH が含まれます。

  http://ipaddr:port/cgi-path

  CA サーバは 1 つだけ設定できます。CA サーバは LSC をプロビジョニングするよう設定する必要があります。

- **config certificate lsc ca-server delete**

  このコマンドは、コントローラで設定された CA サーバを削除します。

- **config certificate lsc ca-cert** {**add** | **delete**}

  このコマンドは、コントローラの CA 証明書データベースに対して LSC CA 証明書を次のように追加/削除します。

  - **add**：SSCEP getca 操作を使用して、設定された CA サーバで CA 証明書を問い合わせ、WLC にログインし、WLC データベースに証明書を永久的にインストールします。インストールされたら、この CA 証明書は AP から受信された LSC デバイス証明書を検証するために使用されます。
  - **delete**：WLC データベースから LSC CA 証明書を削除します。

- **config certificate lsc subject-params** *Country State City Orgn Dept Email*

  このコマンドは、コントローラと AP で作成およびインストールされるデバイス証明書のパラメータを設定します。

  これらすべての文字列は、最大3バイトを使用する国を除き64バイトです。Common Name は、イーサネット MAC アドレスを使用して自動的に生成されます。Common Name は、コントローラ デバイス証明書要求を作成する前に提供する必要があります。

  上記のパラメータは LWAPP ペイロードとして AP に送信されるため、AP はこれらのパラメータを使用して certReq を生成できます。CN は、現在の MIC/SSC の「Cxxxx-MacAddr」形式を使用して AP で自動的に生成されます。ここで、xxxx は製品番号です。

- **config certificate lsc other-params** *keysize*

  デフォルトのキーサイズ値は 2048 ビットです。

- **config certificate lsc ap-provision** {**enable** | **disable**}

  このコマンドは、AP が SSC/MIC を使用して join した場合に、AP で LSC のプロビジョニングを有効または無効にします。有効な場合は、join し、LSC があるすべての AP がプロビジョニングされます。

  無効な場合は、自動的なプロビジョニングが行われません。このコマンドは、LSC がすでにある AP に影響を与えます。

- **config certificate lsc ra-cert** {**add** | **delete**}

  このコマンドの使用は、CA サーバが Cisco IOS CA サーバである場合にお勧めします。コントローラで RA を使用して証明書要求を暗号化すれば、通信をセキュアにできます。RA 証明書は現在、MSFT などの他の外部 CA サーバによりサポートされていません。

  - **add**：SCEP オペレーションを使用して、設定された CA サーバで RA 証明書を照会し、その証明書をコントローラ データベースにインストールします。このキーワードは、CA により署名された certReq を取得するために使用されます。
  - **delete**：WLC データベースから LSC RA 証明書を削除します。

- **config auth-list ap-policy lsc** {**enable** | **disable**}

  LSC の取得後に、AP はコントローラに join を試みます。AP がコントローラに join を試みるには、その前にコントローラ コンソールで次のコマンドを入力する必要があります。デ

フォルトでは、**config auth-list ap-policy lsc** コマンドは無効な状態にあり、AP は LSC を使用してコントローラに join できません。

- **config auth-list ap-policy mic** {**enable** | **disable**}

  MIC の取得後に、AP はコントローラに join を試みます。AP がコントローラに join を試みるには、その前にコントローラ コンソールで次のコマンドを入力する必要があります。デフォルトでは、**config auth-list ap-policy mic** コマンドは有効な状態になっています。AP が有効なため join できない場合は、コントローラ側に「LSC/MIC AP is not allowed to join」というログ メッセージが表示されます。

- **show certificate lsc summary**

  このコマンドは、WLC にインストールされた LSC 証明書を表示します。RA 証明書もすでにインストールされている場合は、CA 証明書、デバイス証明書、および RA 証明書（オプション）を表示します。また、LSC が有効であるか有効でないかも示されます。

- **show certificate lsc ap-provision**

  このコマンドは、AP のプロビジョニングのステータス、プロビジョニングが有効であるか無効であるか、プロビジョニング リストが存在するか存在しないかを表示します。

- **show certificate lsc ap-provision details**

  このコマンドは、AP プロビジョニング リストに存在する MAC アドレスのリストを表示します。

コントローラ GUI セキュリティ設定

この設定は機能に直接関連しませんが、LSC を使用してプロビジョニングされた AP で必要な設定をするのに役立つことがあります。

- ケース 1：ローカル MAC 認可とローカル EAP 認証

  RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加します。

  例：

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- ケース 2：外部 MAC 認可とローカル EAP 認証

  WLC で次のコマンドを入力します。

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

  または

  GUI ページで外部 MAC フィルタ認可のみをオンにし、次のガイドラインに従います。

  - RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加しません。

- WLC で、外部 RADIUS サーバの詳細を設定します。
- WLC で **config macfilter mac-delimiter colon** 設定コマンドを入力します。
- 外部 RADIUS サーバで、RAP/MAP の MAC アドレスを次の形式で追加します。

  User name: 11:22:33:44:55:66 Password: 11:22:33:44:55:66

- ケース 3：LSC 専用 MAP 認証

  WLC で次のコマンドを入力します。

```
(Cisco Controller) > config mesh security lsc-only-auth enable
```

  または

  GUI ページ内の LSC 専用 MAP 認証を確認します。次のメッセージが表示されます。

```
Warning: Enabling LSC Only MAP Authentication will provision LSC Certificate into MAP (if MAP are being provisioned for first time). Please make sure MAP is connected to WLC using Ethernet cable to avoid security risk. Are you sure you want to continue? (Y/N)
```

展開ガイドライン

- ローカル認証を使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラをインストールする必要があります。
- 外部 AAA サーバを使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラをインストールする必要があります。
- メッシュ セキュリティが証明書発行元として「vendor」を使用するよう設定する必要があります。
- MAP は、バックアップ コントローラにフォール バックするときに LSC から MIC に切り替わることができません。

メッシュ AP に対して LSC を有効または無効にするには、**config mesh lsc** {**enable** | **disable**} コマンドが必要です。このコマンドを実行すると、すべてのメッシュ AP がリブートされます。

Antenna Band Mode の設定

Antenna Band Mode 設定に関する情報

次のいずれかとしてメッシュ アクセス ポイントの Antenna Band Mode を設定できます。

- Dual Antenna Band Mode：下部の 2 つのポート、ポート 1 およびポート 2 は、デュアル バンド 2.4 GHz および 5 GHz の二重放射素子（DRE）アンテナ用に使用されます。

- Single Antenna Band Mode：上部の 2 つのポート、ポート 3 およびポート 4 は、5 GHz の単一放射素子（SRE）アンテナ用に使用され、下部の 2 ポート、ポート 1 およびポート 2 は、2.4 GHz の SRE アンテナ用に使用されます。

Antenna Band Mode 設定の制約事項

Antenna Band Mode 設定は Cisco Aironet 1532E および 1572EC/EAC アクセス ポイントのモデルで使用できます。

（注） Cisco Aironet 1532I アクセス ポイントのモデルは、内部アンテナがあり、追加のアンテナを必要としません。

Antenna Band Mode の設定（CLI）

始める前に

Antenna Band Mode を変更する前に、物理アンテナが正しく設定されていることを確認してください。Antenna Band Mode を誤って設定すると、メッシュ AP が孤立状態になります。

手順

- Cisco WLC CLI で次のコマンドを入力して、メッシュ AP の Antenna Band Mode を設定します。
  config ap antenna-band-mode {**single** | **dual**} *mesh-ap-name*
- 次のコマンドを入力して、Antenna Band Mode のステータスを表示します。
  show ap config general *mesh-ap-name*

Antenna Band Mode の設定（AP CLI）

手順

- AP コンソールで次のコマンドを入力して、メッシュ AP CLI の Antenna Band Mode を設定します。
  capwap ap ant-band-mode {**dual** | **single**}

Cisco Aironet 1530 シリーズ アクセス ポイントでのデイジーチェーンの設定

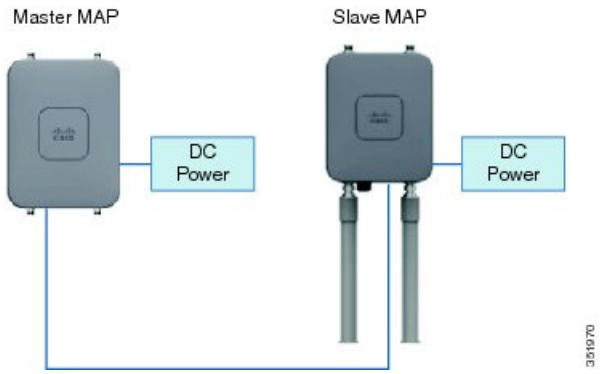
Cisco Aironet 1530 シリーズ アクセス ポイントのデイジーチェーン接続に関する情報

Cisco Aironet 1530 シリーズ アクセス ポイントをメッシュ AP（MAP）として使用すれば、アクセス ポイントをデイジーチェーン接続できます。MAP をデイジーチェーン接続することによって、アップリンク アクセスとダウンリンク アクセスに別々のチャネルを使用できるため、

バックホール幅の向上やユニバーサル アクセスの拡張が可能となり、AP をシリアル バックホールとして運用できます。ユニバーサル アクセスの拡張により、ローカル モードまたは FlexConnect モードの Cisco AP1530 を MAP のイーサネット ポートに接続できるため、ネットワークが拡張され、より適切なクライアント アクセスを提供できます。

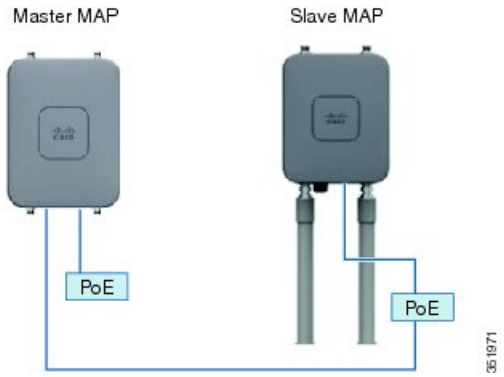
デイジーチェーン接続されたアクセス ポイントは、AP の電源供給方法によって異なる方法でケーブルを取り付ける必要があります。アクセス ポイントへの電力が DC 電源を使用して供給されている場合は、イーサネット ケーブルはマスター AP の LAN ポートからスレーブ AP の PoE 入力ポートに直接接続する必要があります。

図 *23 : DC* 電源を使用してデイジーチェーン接続された *AP*



アクセス ポイントへ PoE で電力供給する場合、イーサネット ケーブルは、マスター AP の LAN ポートから出発し、スレーブ AP に給電する PoE インジェクタへと接続する必要があります。

図 *24 : PoE* インジェクタを使用してデイジーチェーン接続された *AP*



1572 とのデイジーチェーン接続

1572 アクセス ポイント（AP）の重要な機能の 1 つが、メッシュ AP（MAP）として動作中に、AP をデイジーチェーン接続できる機能です。MAP をデイジーチェーン接続することによって、アップリンク アクセスとダウンリンク アクセスに別々のチャネルを使用できるため、バックホール帯域幅の向上やユニバーサル アクセスの拡張が可能となり、AP をシリアル バックホールとして運用できます。ユニバーサル アクセスの拡張により、ローカル モードまたは flexconnect モードの 1572 AP を MAP のイーサネット ポートに接続できるため、ネットワーク

が拡張され、より適切なクライアントアクセスを提供できます。これらの機能について、以降の項で詳しく説明します。

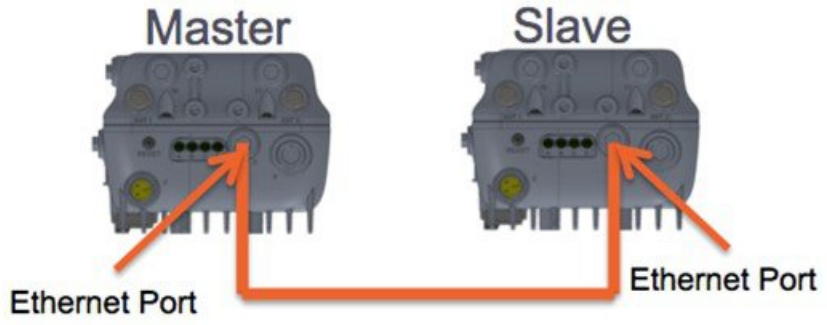
8.0MR リリースでは、1572 がマスター AP として設定されている場合に、次の AP がスレーブ AP としてサポートされます。

- 1572EAC
- 1572EC
- 1572IC
- 1552
- 1532E/I
- 3700P

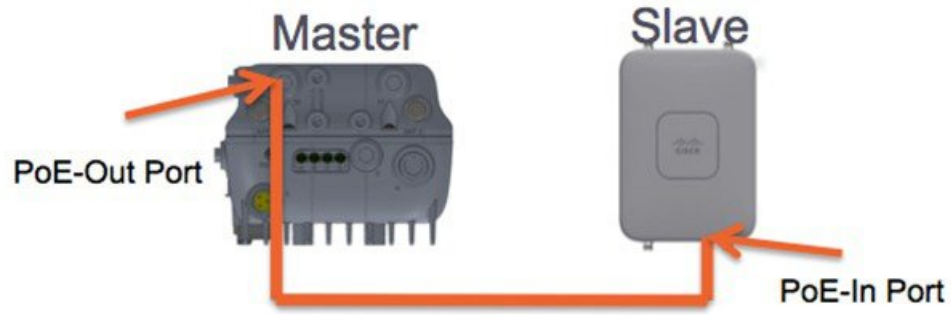
デイジーチェーン接続されたアクセス ポイントは、終端のスレーブ AP の AP タイプに応じて配線を変更する必要があります。

マスター AP とスレーブ AP の両方が 1572 の場合は、マスター AP のイーサネット ポートとスレーブ AP のイーサネット ポートをイーサネット ケーブルで接続する必要があります。両方の AP でデイジーチェーン接続を有効にする必要があります。

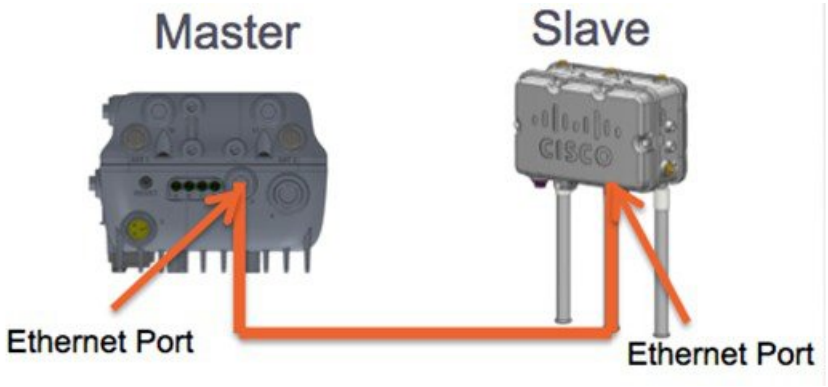
注意 イーサネット ブリッジ接続された有線クライアントまたはデイジーチェーン接続された AP は、イーサネット ポートか PoE-Out ポートのいずれかにのみ接続することをお勧めします。イーサネット ブリッジ接続された有線クライアントは PoE-In ポートには絶対に接続しないでください。



マスター AP が 1570 で、スレーブ AP が 1532 または 3700P の場合は、マスター AP の PoE-Out ポートとスレーブ AP の PoE-In ポートをイーサネット ケーブルで接続します。



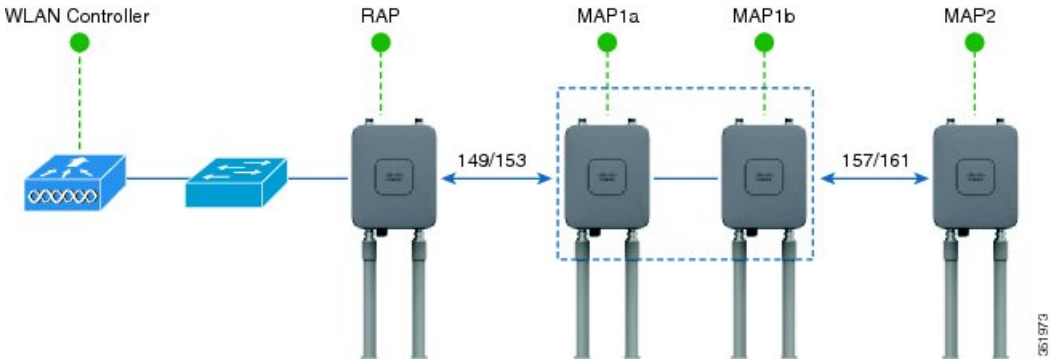
マスター AP が 1570 で、スレーブ AP が 1520 または 1550 の場合は、1572 のイーサネット ポートと 1552 の任意のイーサネット ポートをイーサネット ケーブルで接続します。



Cisco Aironet 1530/1572 シリーズ アクセス ポイントのシリアル バックホール

Cisco Aironet アクセス ポイントのデイジーチェーン接続はシリアル バックホール メッシュを供給するために使用できます。MAP1a はマスター MAP で、優先される親が RAP として選択されています。MAP1b は、スレーブ MAP で、優先される親が選択されていません。MAP1b は「RootAP」ロールのある「ブリッジ」 AP モードで設定されます。デイジーチェーン接続は MAP1b で有効です。MAP2 には、MAP1b として選択された優先される親があります。

図 *25 :* シリアルバックホール メッシュのあるデイジーチェーン



高利得方向性アンテナは、一般的なシリアルバックホール展開で使用する必要があります。また、シリアルバックホール メッシュ ネットワークを作成するには、優先される親設定を使用する必要があります。

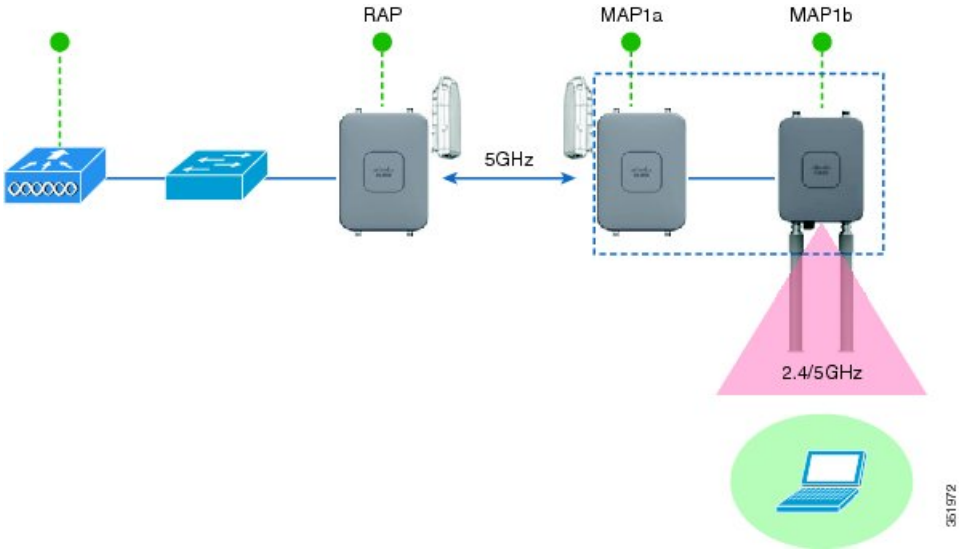
子 AP は、次の基準に基づいて優先される親を選択します：

- 優先される親は最適な親である。
- 優先される親に、少なくとも 20 dB のリンク SNR がある。
- 優先される親には 12 dB ～ 20 dB の範囲内の リンク SNR があるが、その他にこれよりも優れた親がない（SNR は 20 % 以上が理想的）。SNR が 12 dB 未満の場合、設定は無視されます。
- 優先される親はブラックリストに掲載されていない。
- 優先される親は、動的周波数選択（DFS）のため、サイレント モードではない。
- 優先される親は同じブリッジ グループ名（BGN）に属する。設定された優先される親が同じ BGN に属さず、他の親が利用可能でない場合、子はデフォルトの BGN を使用して親 AP に関連付けられます。

拡張ユニバーサル アクセス

Cisco Aironet 1530 シリーズ アクセス ポイントのデイジーチェーン接続は、メッシュ ネットワーク全体にユニバーサル アクセスを拡張する場合でも使用できます。この例では、MAP1a はマスター MAP で、RAP と無線バックホールされます。MAP1b はスレーブ MAP で、ローカル/フレックス接続モードで動作し、2.4 GHz 帯と 5 GHz 帯でクライアント アクセスを提供しています。

図 *26 :* ユニバーサル アクセスを拡張するデイジーチェーン接続



Cisco Aironet 1530/1570 シリーズ アクセス ポイントをデイジーチェーン接続設定するときに注意すべき重要ポイント

- デイジーチェーン接続されたAPとして動作できるのはメッシュアクセスポイント（MAP）だけです。
- アップリンクでデイジーチェーン接続されている AP がマスター AP となり、接続された AP がスレーブ AP として見なされます。
- 接続するイーサネット ケーブルは、マスター AP の LAN ポートからスレーブ AP の PoE 入力ポートに接続される必要があります。
- それぞれのデイジーチェーン接続されたメッシュ ホップに、優先される親が設定されている必要があります。マスター MAP には優先される親が必要です。
- デイジーチェーン接続は、Cisco WLC の GUI または CLI を介したブリッジ モードのスレーブ AP で、または AP コンソールで有効にする必要があります。
- 指向性アンテナはデイジーチェーンの作成時に使用する必要があります。アンテナは、必要に応じて、メッシュ ツリーを形成するために使用する必要があります。
- 指向性アンテナは、物理的に 3 m 離す必要があります。
- イーサネット ブリッジングはブリッジ モードのすべての AP で有効にする必要があります。

デイジーチェーンの設定（CLI）

手順

- 次のコマンドを入力して、デイジーチェーンを設定します。
  config ap daisy-chaining {**enable** | **disable**} *cisco-mesh-ap*
- 次のコマンドを入力して、各シリアル バックホール AP の優先される親を設定します。
  config mesh parent preferred *cisco-ap parent-mac-address*
- 次のコマンドを入力して、デイジーチェーンおよび設定された優先される親のステータスを表示します。
  show ap config general *cisco-ap*

デイジーチェーンの設定（AP CLI）

手順

- AP コンソールで次のコマンドを入力して、AP のデイジーチェーンを設定します。
  capwap ap daisy-chaining {**enable** | **disable**}

デイジーチェーンの設定

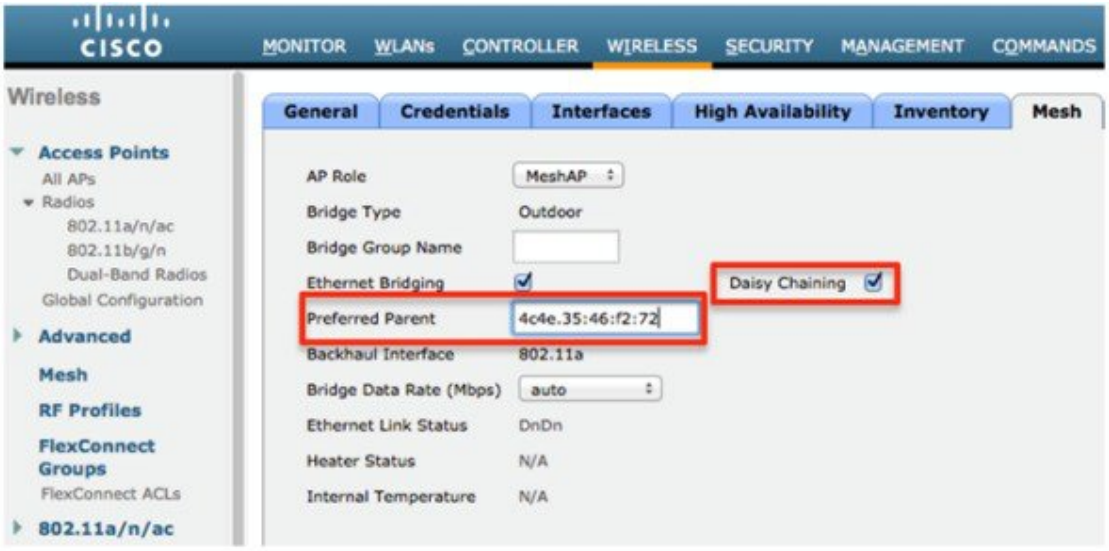
デイジーチェーン接続展開を設定する場合に解決すべきいくつかの主要な要素があります。

- デイジーチェーン接続されたAPとして動作できるのはメッシュアクセスポイント（MAP）だけです。
- アップリンク デイジーチェーン接続された AP がマスター AP と見なされ、接続先の AP がスレーブ AP と見なされます。
- デイジーチェーン接続されたメッシュ ホップごとに優先される親を設定する必要があります。マスター MAP に、優先される親を割り当てる必要があります。
- デイジーチェーン接続は、WLC GUI、WLC CLI、AP CLI のいずれかを使用して AP 上で有効にする必要があります。
- 顧客ニーズに合わせてメッシュ ツリー情報を調整するデイジーチェーンを構築する場合は、指向性アンテナを使用する必要があります。

WLC GUI を使用したデイジーチェーン接続の有効化

WLC GUI からデイジーチェーン接続を有効にするには、[Wireless] > [Access Point] > [(AP_NAME)] > [Mesh] に移動してから、[Daisy-Chaining] チェックボックスをオンにします。AP がシリアル バックホール ソリューションで使用されている場合は、[Preferred Parent] を選択する必要があります。

（注） デイジーチェーンはスレーブ RAP でのみ有効にする必要があります。マスター MAP はデイジーチェーンを無効にする必要があります。



WLC CLI を使用したデイジーチェーン接続の有効化

WLC CLI からデイジーチェーン接続を有効にするには、次のコマンドを発行します。

```
(Cisco Controller) >config ap daisy-chaining [enable/disable] <ap_name>
```

デイジーチェーン機能はアクセス ポイント単位で有効にする必要があります。

```
(Cisco Controller) >show ap config general <ap_name>
```

その後で、Daisy Chaining エントリまでスクロール ダウンします。

```
Daisy Chaining ................................. Disabled
```

AP CLI を使用したデイジーチェーン接続の有効化

AP CLI からデイジーチェーン接続を有効にするには、次のコマンドを発行します。

```
AP#capwap ap daisy-chaining <enable/disable>
```

シリアルバックホール AP ごとの優先される親の設定

優先される親をシリアルバックホール AP ごとにセットアップするには、次のコマンドを発行します。

```
(Cisco Controller) >config mesh parent preferred <ap_name> <PARENT_MAC_ADDRESS>
```

アクセス ポイントの優先される親は、次のコマンドを発行することによって確認できます。

```
(Cisco Controller) >show ap config general <ap_name>
```

その後で、Mesh preferred parent エントリまでスクロール ダウンします。

```
Mesh preferred parent ......................... 00:24:13:0f:92:00
```

メッシュ コンバージェンスの設定

メッシュ コンバージェンスに関する情報

Cisco WLC を使用して、メッシュ AP（MAP）ごとに、またはすべてのメッシュ AP 用にメッシュ コンバージェンス メソッドを設定できます。これにより、既存のコンバージェンス メカニズムに影響を与えることなく、配置に基づいてコンバージェンス メソッドを選択できます。デフォルト設定は、既存のコンバージェンス メカニズムです。

メッシュ コンバージェンス	親の損失の検出 / キープ アライブ タイマー	チャネル スキャン / シーク	DHCP / CAPWAP 情報
規格	21 / 3 秒	すべての 5 GHz チャネルのスキャン/シーク	CAPWAP の更新/再起動
速い	7 / 3 秒	プリセットされたチャネルのみのスキャン/シーク	DHCP および CAPWAP の維持
非常に高速	4 / 1.5 秒	プリセットされたチャネルのみのスキャン/シーク	DHCP および CAPWAP の維持

メッシュ コンバージェンスに関する制約事項

Cisco Wave 2 AP でのコンバージェンスの設定は次のとおりです。

表 *7:* 親を検索する頻度

コンバージェンス設定	親を検索する頻度
Very Fast	500 ミリ秒ごと
Fast	750 ミリ秒ごと
Standard	1 秒ごと

ネイバーを検索する頻度は、すべてのコンバージェンス設定で 15 秒です。

AP が 8 回を応答しなかった場合、親やネイバーは失われたと見なされます。

表 *8:* 親の損失の計算にかかる合計時間

コンバージェンス設定	計算の合計時間
Very Fast	4 秒
Fast	6 秒
Standard	8 秒

ネイバー（親以外）、損失時間は 2 分です。

Fast および Very Fast コンバージェンスでは、サブセット チャネル検索が実行されます。AP はネイバーの親でサポートされているチャネルのリストを維持し、チャネル スキャンを行う代わりに、それらのチャネルを直接検索します。Standard コンバージェンスの場合、親が失われたときにチャネル スキャンが実行されます。

メッシュ コンバージェンスの設定（CLI）

手順

- 次のコマンドを入力して、Cisco WLC CLI のメッシュ コンバージェンスを設定します。
  config mesh convergence {**fast** | **standard** | **very-fast**} **all**

（注） **all** キーワードはすべての MAP ノードを意味します。

- AP コンソールの Mesh convergence コマンド：
  a) チャネルの現在のサブセットのリストを表示するには：
  show mesh convergence

b) メッシュ コンバージェンスをデバッグするには：
debug mesh convergence

c) AP でコンバージェンス メソッドを設定するには：
test mesh convergence {fast | standard | very_fast}

LWAPP と Autonomous イメージの切り替え（AP CLI）

デフォルトでは、Cisco AP1532 および AP1572 は統合モードに設定されています。

手順

- AP コンソールで次のコマンドを入力して、LWAPP モードから自律モード（aIOS）にアクセス ポイントを切り替えます。
capwap ap autonomous

（注） このコマンドは、アクセスポイントの最初のプライミング時に一度のみ使用する必要があります。自律モードから LWAPP モードにスイッチバックする方法については、https://supportforums.cisco.com/docs/DOC-14960 を参照してください。

RAP の DHCP について

この機能は、ルート AP（RAP）にある内部 DHCP IPv4 サーバを有効にします。このサーバは、メッシュ AP（MAP）とその関連付けられたクライアント（有線およびワイヤレス）に IPv4 アドレスを提供します。この DHCP サーバに使用可能な範囲は、単一範囲の IP アドレスに限定されています。使用可能な範囲は 10.1.1.1 ～ 10.1.200.200 です。

RAP が物理的に異なるメッシュ ネットワークに存在する場合にのみ、1 台のコントローラで複数の RAP をサポートできます。異なるメッシュ ネットワークでのメッシュ AP のローミングはサポートされていません。

この機能は、シスコの屋外用 AP（Flex + ブリッジ モード専用の 1540 AP と 1560 AP）でサポートされています。

RAP の DHCP の制約事項

- 1 つのサブネットでは、1 つのルート AP のみ DHCP サーバを実行できます。
- メッシュ ネットワークでは、1 つのネイティブ VLAN のみサポートされます。
- GUI の設定はありません。

コントローラでの RAP の DHCP の設定（CLI）

コントローラの CLI で次のコマンドを使用して、RAP の DHCP を設定します。

手順

- 次のコマンドを入力して、内部の AP メッシュ DHCP サーバを設定します。

  config ap mesh-internal-dhcp {**enable | disable**}*ap-name*

- 次のコマンドを入力して、メッシュ DHCP のステータスを表示します。

  show mesh dhcp status

メッシュ AP での RAP の DHCP の設定（CLI）

AP CLI で次のコマンドを使用して、RAP の DHCP を設定します。

手順

- 次のコマンドを入力して、メッシュ DHCP の管理を設定します。

  config mesh dhcp mgmt start-ip *start-addr end-addr mask*

  開始 IP は RAP に割り当てられます。これは、ゲートウェイ IP アドレスです。

- 次のコマンドを入力して、メッシュ DHCP DNS サーバを設定します。

  config mesh dhcp mgmt dns-server *IP-addr*

  1 つの IP アドレスのみに制限されます。

- 次のコマンドを入力して、メッシュ DHCP オプション 43 を設定します。

  config mesh dhcp mgmt option-43 *IP-addr*

  1 つの IP アドレスのみに制限されます。

- 次のコマンドを入力して、メッシュ DHCP ドメインを設定します。

  config mesh dhcp mgmt domain *domain-name*

- 次のコマンドを入力して、メッシュ DHCP のリース時間を設定します。

  config mesh dhcp mgmt lease *lease-time in seconds*

  有効な範囲は 600 ～ 86,400 秒です。

- 次のコマンドを入力して、メッシュ DHCP サーバの状態を設定します。

  config mesh dhcp {**start-server** | **stop-server**}

- 次のコマンドを入力して、メッシュ DHCP IP アドレスのリースをクリアします。

  config mesh dhcp clear-lease {**all** | *IP-addr*}

- 次のコマンドを入力して、現在の DHCP の設定を表示します。

show mesh dhcp config

- 次のコマンドを入力して、すべてのアクティブなリース IP アドレスを表示します。

  show mesh dhcp lease

- 次のコマンドを入力して、RAP アクティビティ ログで DHCP を確認します。

  show mesh dhcp log

メッシュ AP での RAP の DHCP のデバッグ（CLI）

手順

- 次のコマンドを入力して、メッシュ DHCP をデバッグします。

  debug mesh dhcp

RAP の NAT-PAT について

Flex メッシュ ルート AP（RAP）のネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）は、内部 DHCP サーバによって異なります。この機能は、内部 DHCP サーバが有効または無効になっている場合に有効または無効になります。

RAP のローカル DHCP サーバが有効になっている場合、定義済みの IP アドレス範囲の最初の IP アドレスがデフォルト ゲートウェイの IP アドレスとして割り当てられます。

メッシュ AP または関連付けられているクライアントからのトラフィックがある場合、プライベート IPv4 アドレスが RAP で NAT されます。ただし、それらの IP アドレスはコントローラに送信され、コントローラの GUI でそれらの IPv4 アドレスが表示されます。

（注） メッシュ ネットワークにパブリック IP アドレスを持てるのは RAP だけです。

RAP の NAT-PAT の制約事項

- コントローラで AP LAG が有効になっている場合、Cisco Mesh AP を使用したデイジーチェーンの作成は失敗します。これは、NAT-PAT の背後にある AP ではサポートされていないためです。

メッシュ AP での RAP の NAT-PAT の表示（CLI）

AP CLI で次のコマンドを使用して、RAP の NAT-PAT を表示します。

手順

- 次のコマンドを入力して、クライアント IP MAC マッピングを表示します。

  show mesh nat client

- 次のコマンドを入力して、クライアント ダウンリンク IP MAC マッピングを表示します。

  show mesh nat dl-map

- 次のコマンドを入力して、ICMP マッピングを表示します。

  show mesh nat icmp

- 次のコマンドを入力して、TCP マッピングを表示します。

  show mesh nat tcp

- 次のコマンドを入力して、UDP マッピングを表示します。

  show mesh nat udp

メッシュ AP での RAP の NAT-PAT のデバッグ（CLI）

手順

- 次のコマンドを入力して、メッシュの NAT をデバッグします。

  debug mesh nat