メッシュ ネットワーク コンポーネント

この章では、メッシュ ネットワーク コンポーネントについて説明します。

Cisco ワイヤレス メッシュ ネットワークには、次の 4 つのコア コンポーネントがあります。

- Cisco Aironet シリーズ アクセス ポイント

（注） Cisco Aironet 1520 シリーズのメッシュ アクセス ポイントは、生産終了のためサポートされていません。

- シスコ ワイヤレス LAN コントローラ（以下、**コントローラ**）
- Cisco Prime Infrastructure
- メッシュ ソフトウェア アーキテクチャ

この章の内容は、次のとおりです。

メッシュ アクセス ポイント

5508、5520、および8540シリーズCiscoコントローラにおけるメッシュ アクセス ポイントのライセンス

Cisco 5500 および 8500 シリーズ コントローラでメッシュ アクセス ポイントと非メッシュ アクセス ポイントの両方を使用する場合、7.0 リリース以降、必要なライセンスは基本ライセンスだけになりました。ライセンスの取得とインストールの詳細については、http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html の『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

アクセス ポイントのロール

メッシュ ネットワーク内のアクセス ポイントは、次の 2 つの方法のいずれかで動作します。

1. ルート アクセス ポイント（RAP）
2. メッシュ アクセス ポイント（MAP）

（注） すべてのアクセス ポイントは、メッシュ アクセス ポイントとして設定され、出荷されます。アクセス ポイントをルート アクセス ポイントとして使用するには、メッシュ アクセス ポイントをルート アクセス ポイントに再設定する必要があります。すべてのメッシュ ネットワークで、少なくとも 1 つのルート アクセス ポイントがあることを確認します。

RAP はコントローラへ有線で接続されますが、MAP はコントローラへ無線で接続されます。

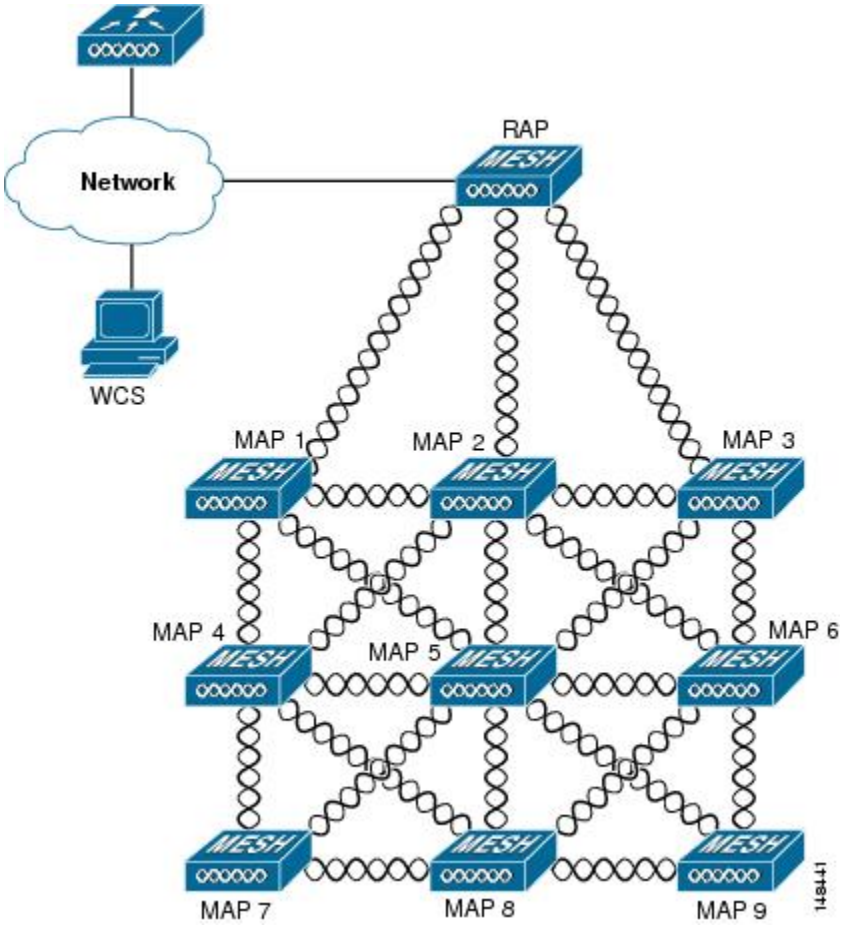
MAP は MAP 間および RAP への通信に 802.11a/n/g 無線バックホールを使用して無線接続を行います。MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。

ブリッジモードのアクセスポイントでは、CleanAirによってメッシュバックホールがサポートされ、干渉デバイス レポート（IDR）および電波品質の指標（AQI）レポートのみが生成されます。

（注） RAP または MAP は、ブリッジ プロトコル データ ユニット（BPDU）自体は生成しません。ただし、RAP または MAP がネットワーク全体で接続された有線またはワイヤレスのインターフェイスから BPDU を受信した場合、RAP または MAP はアップストリーム デバイスに BPDU を転送します。

この図は、メッシュ ネットワーク内の RAP と MAP の間にある関係を示しています。

図 *1*：単純なメッシュ ネットワーク階層



ネットワークアクセス

ワイヤレス メッシュ ネットワークでは、異なる 2 つのトラフィック タイプを同時に伝送できます。伝送できるトラフィック タイプは次のとおりです。

- 無線 LAN クライアント トラフィック
- MAP イーサネット ポート トラフィック

無線LANクライアントトラフィックはコントローラで終端し、イーサネットトラフィックはメッシュ アクセス ポイントのイーサネット ポートで終端します。

メッシュ アクセス ポイントによる無線 LAN メッシュへのアクセスは次の認証方式で管理されます。

- MAC 認証：メッシュ アクセス ポイントが参照可能データベースに追加され、特定のコントローラおよびメッシュ ネットワークに確実にアクセスできるようにします。

- 外部 RADIUS 認証：メッシュ アクセス ポイントは、証明書付きの拡張認証プロトコル（EAP-FAST）のクライアント認証タイプをサポートする Cisco ACS（4.1 以上）などの RADIUS サーバを使用して、外部から認証できます。

ネットワークのセグメント化

メッシュ アクセス ポイント用のワイヤレス LAN メッシュ ネットワークへのメンバーシップは、ブリッジ グループ名（BGN）によって制御されます。メッシュ アクセス ポイントは、類似のブリッジグループに配置して、メンバーシップを管理したり、ネットワーク セグメンテーションを提供したりすることができます。

Cisco 屋内メッシュ アクセス ポイント

このリリースでサポートされているアクセス ポイント プラットフォームは以下のとおりです。

- Cisco Aironet 1600 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 2600 シリーズ アクセス ポイント
- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 3500 シリーズ アクセス ポイント
- Cisco Aironet 3600 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Aironet 1530 シリーズ アクセス ポイント
- Cisco Aironet 1550 シリーズ アクセス ポイント
- Cisco Aironet 1560 シリーズ アクセス ポイント
- Cisco Aironet 1570 シリーズ アクセス ポイント
- Cisco Industrial Wireless 3700 シリーズ アクセス ポイント

（注） 8.4 リリースでは次の AP がサポートされます。

（注） アクセス ポイントのコントローラ ソフトウェアのサポートの詳細については、『*Cisco Wireless Solutions Software Compatibility Matrix*』を参照してください。URL は次のとおりです。http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html

エンタープライズ 11n/ac メッシュは、802.11n/ac アクセス ポイントで動作するために CUWN 機能に追加される拡張機能です。エンタープライズ 11ac メッシュ機能は 802.11ac 以外のメッシュと互換性がありますが、バックホールとクライアントのアクセス速度が向上します。802.11ac 屋内アクセス ポイントは、特定の屋内展開用のデュアル無線 Wi-Fi インフラストラクチャ デバイスです。一方の無線をアクセス ポイントのローカル（クライアント）アクセスに使用でき、もう一方の無線をワイヤレス バックホールに対して設定できます。ユニバーサル バックホール アクセスが有効な場合、リリース 8.2 の 5 GHz および 2.4 GHz 無線はローカル（クライアント）アクセス、バックホールの両方に使用できます。エンタープライズ 11ac メッシュは、P2P、P2MP、およびアーキテクチャのメッシュ タイプをサポートします。

屋内アクセス ポイントをブリッジモードに直接設定して、これらのアクセス ポイントをメッシュ アクセス ポイントとして直接使用できます。これらのアクセス ポイントがローカル モード（非メッシュ）である場合は、これらのアクセス ポイントをコントローラに接続し、AP モードをブリッジ モード（メッシュ）に変更する必要があります。このシナリオは、特に、展開されるアクセス ポイント量が大きく、アクセス ポイントが従来の非メッシュ ワイヤレス カバレッジに対してローカル モードですでに展開されている場合に、煩雑になります。

Cisco 屋内メッシュ アクセス ポイントでは、次の 2 つの無線が同時に動作します。

- リリース 8.2 以降、UBA が有効な場合に 2.4 GHz 無線はデータ バックホールとクライアント アクセスに使用されてきました。
- ユニバーサル バックホール アクセスが有効である場合、データ バックホールおよびクライアント アクセスに使用される 5 GHz の無線

5 GHz の無線は、5.15 GHz、5.25 GHz、5.47 GHz、および 5.8 GHz の帯域をサポートします。

Cisco 屋外メッシュ アクセス ポイント

Cisco 屋外メッシュ アクセス ポイントは、Cisco Aironet 1500 シリーズ アクセス ポイントから構成されます。1500 シリーズには、1572 11ac 屋外アクセス ポイント、1552 および 1532 11n 屋外メッシュ アクセス ポイント、および 1560 11ac Wave 2 シリーズが含まれます。

Cisco 1500 シリーズ メッシュ アクセス ポイントは、ワイヤレス メッシュ展開の中核的なコンポーネントです。AP1500 は、コントローラ（GUI および CLI）と Cisco Prime Infrastructure の両方により設定されます。屋外メッシュ アクセス ポイント（MAP および RAP）間の通信は、802.11a/n/ac 無線バックホールを介します。クライアント トラフィックは、一般に 802.11b/g/n 無線を介して送信されます（クライアント トラフィックを受け入れるように 802.11a/n/ac も設定できます）。

メッシュ アクセス ポイントは、有線ネットワークに直接接続されていない他のアクセス ポイントの中継ノードとしても動作します。インテリジェントな無線ルーティングは Adaptive Wireless Path Protocol（AWPP）によって提供されます。このシスコのプロトコルを使用することで、各メッシュ アクセス ポイントはネイバー アクセス ポイントを識別し、パスごとに信号の強度とコントローラへのアクセスに必要なホップ カウントについてコストを計算して、有線ネットワークまでの最適なパスをインテリジェントに選択できるようになります。

アップリンク サポートには、ギガビット イーサネット（1000BASE-T）と、ファイバまたはケーブル モデム インターフェイスに接続できる小型フォーム ファクタ（SFP）スロットが含まれます。1000BASE-BX までのシングルモード SFP とマルチモード SFP の両方がサポートされます。

メッシュ アクセス ポイントのタイプに基づき、ケーブル モデムは DOCSIS 2.0 または DOCSIS/EuroDOCSIS 3.0 になります。

AP1550 は、厳しい環境向けハードウェア格納ラックに設置します。危険場所対応の AP1500 は、Class I、Division 2、Zone 2 の危険場所での安全基準を満たしています。

メッシュ アクセス ポイントは、メッシュ モード以外では、以下のモードで動作できます。

- ローカル モード：このモードでは、AP は割り当てられたチャネル上のクライアントを処理できます。180 秒周期で帯域上のすべてのチャネルをモニタ中にも、クライアントの処理が可能です。この間に、AP は 50 ミリ秒周期で各チャネルをリッスンし、不正なクライアントのビーコン、ノイズ フロアの測定値、干渉、および IDS イベントを検出します。また AP は、チャネル上の CleanAir 干渉もスキャンします。
- FlexConnect モード：FlexConnect は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。FlexConnect モードを使用すると、各オフィスにコントローラを展開しなくても、会社のオフィスから WAN リンクを介して支社や離れた場所にあるオフィスのアクセス ポイントを設定および制御できます。コントローラとの接続が失われたときは、FlexConnect AP でクライアント データ トラフィックをローカルでスイッチして、クライアント認証をローカルで実行することができます。コントローラに接続されている場合、FlexConnect モードではコントローラにトラフィックをトンネリングで戻すこともできます。
- Flex+Bridge モード：このモードでは、FlexConnect とブリッジ モードの設定オプションの両方をアクセス ポイントで使用できます。
- モニタ モード：このモードでは、AP 無線は受信状態にあります。AP は、12 秒ごとにすべてのチャネルをスキャンし、不正なクライアントのビーコン、ノイズ フロアの測定値、干渉、IDS イベント、および CleanAir 侵入者を検出します。
- Rogue Detector モード：このモードでは、AP 無線がオフになり、AP は有線トラフィックのみをリッスンします。コントローラは Rogue Detector として設定されている AP と、疑わしい不正クライアントおよび AP の MAC アドレスのリストを渡します。Rogue Detector は ARP パケットを監視します。Rogue Detector はトランク リンクを介して、すべてのブロードキャスト ドメインに接続できます。
- スニファ モード：AP はチャネル上のすべてのパケットをキャプチャし、Wireshark などのパケット アナライザ ソフトウェアを使用してパケットを復号するリモート デバイスに転送します。
- ブリッジ モード：このモードでは、有線ネットワークのケーブル接続が利用できない無線メッシュ ネットワークを作成するために、AP が設定されます。

（注） GUI および CLI の両方を使用してこれらのモードを設定できます。手順については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

（注） MAP は、有線と無線のバックホールに関係なく、ブリッジ/Flex+Bridge モードでだけ設定できます。有線バックホールを持つ MAP の場合は、AP モードを変更する前に、AP ロールを RAP に変更する必要があります。

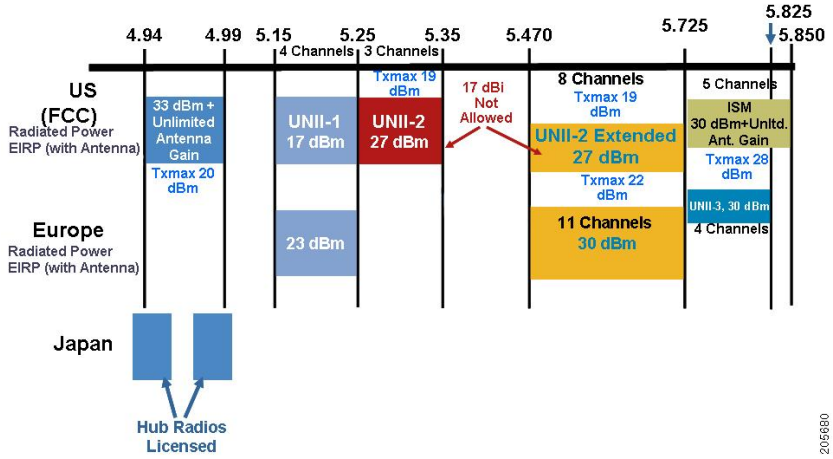
（注） 屋外メッシュ AP のすべてのモデルの詳細と仕様については、以下のリンクを参照してください。

- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data_sheet_c78-728356.html
- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1550-series/data_sheet_c78-641373.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://wwwin.cisco.com/c/cec/prods-industry/selling-en/products/wireless/ap.html
- http://www.cisco.com/c/en/us/support/wireless/aironet-1572eac-outdoor-access-point/model.html
- http://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-1570-series/datasheet-c78-732348.pdf

周波数帯域

2.4 GHz および 5 GHz の両方の周波数帯域が屋内および屋外アクセス ポイントでサポートされます。

図 *2*：*AP1500* の *802.11a* 無線でサポートする周波数帯域



米国では、5 GHz 帯域は、5.150 ～ 5.250（UNII-1）、5.250 ～ 5.350（UNII-2）、5.470 ～ 5.725（UNII-2 拡張）、および 5.725 ～ 5.850（ISM）の 3 つの帯域で構成されています。UNII-1 と UNII-2 の帯域は隣接しており、802.11a では 2.4 GHz の 2 倍以上の大きさの 200 MHz 幅のスペクトルの連続 Swath として処理されます（表 1：周波数帯域，（8 ページ）を参照）。

インドの国ドメインである –D のドメインは次をサポートします。

- 20 MHz チャネル：169（5.845 GHz）および 173（5.865 GHz）
- 40 MHz チャネル：チャネル ペア 169/173（5.855 GHz）

（注） 周波数はアクセス ポイントが設定されている規制ドメインにより異なります。詳細については、http://www.cisco.com/en/US/docs/wireless/access_point/channels/lwapp/reference/guide/lw_chp2.html のドキュメント『Channels and Power Levels』を参照してください。

表 *1*：周波数帯域

周波数帯域用語	説明	サポート モデル
UNII-1[1]	5.15 ～ 5.25 GHz 周波数帯域で稼働する UNII デバイスに関する規制。-B reg のドメインを使用した屋内動作および屋外 AP。	すべての 11n/ac 屋内 AP および 1572

周波数帯域用語	説明	サポート モデル
UNII-2	5.25 ～ 5.35 GHz 周波数帯で稼働する UNII デバイスに関する規制。この帯域では、DFS と TPC が必須です。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。
UNII-2 拡張帯域	5.470 ～ 5.725 GHz の周波数帯域で動作する UNII-2 デバイスの規則。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。
ISM[2]	5.725 ～ 5.850 GHz の周波数帯域で動作する UNII デバイスの規則。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。

1 UNII は、Unlicensed National Information Infrastructure を意味しています。
2 ISM は産業、科学、および医療を意味しています。

（注） 規制に関する情報については、http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html を参照してください。

動的周波数選択

以前は、レーダーを搭載するデバイスは、他の競合サービスがなく周波数サブバンドで動作していました。しかし、規制当局の管理により、これらの帯域をワイヤレス メッシュ LAN（IEEE 802.11）などの新しいサービスに開放して共有できるようにしようとしています。

既存のレーダー サービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要のあるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFS では、無線デバイスがレーダー信号の存在を検出できる機能の採用を義務付けています。無線でレーダー信号が検出されると、最低30分間は伝送を停止して、そのサービスを保護する必要があります。その後、その無線は伝送のための別のチャネルを選択しますが、伝送前にこのチャネルをモニタリングする必要があります。使用する予定のチャネルで少なくとも 1 分間レーダーが検出されなかった場合には、新しい無線サービス デバイスはそのチャネルで伝送を開始できます。

AP は新たな DFS チャネルで、DFS スキャンを 60 秒間実行します。ただし、この新規 DFS チャネルが隣接 AP にすでに使用されている場合は、AP は DFS スキャンを実行しません。

無線がレーダー信号を検出して識別するプロセスは複雑なタスクであり、ときどきは誤った検出が起こります。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャネル レーダーを確実に検出するためのアクセス ポイントの機能など、非常に多くの要因が考えられます。

802.11h 規格では、DFS および Transmit Power Control（TPC）について、5 GHz 帯域に関連するものと指定しています。DFS を使用してレーダーの干渉を回避し、TPC を使用して Satellite Feeder Link の干渉を回避します。

（注） DFS は、米国では 5250 ～ 5350 および 5470 ～ 5725 周波数帯域に義務付けられています。ヨーロッパでは、DFS と TPC が上記帯域に義務付けられています

図 *3*：*DFS* および *TPC* 帯域の要件

アンテナ

概要

アンテナは、すべてのワイヤレス ネットワークの設置に重要なコンポーネントです。アンテナには次の 2 つの大きな種類があります。

- 指向性
- 全方向性

アンテナの種類それぞれには特定の用途があり、特定の設置タイプのときに最大に効果を発揮します。アンテナは、アンテナの設計によって決まる、ローブのあるカバレッジ エリアに RF 信号を配信するため、カバレッジが成功するかどうかは、アンテナの選択に重度に依存します。

アンテナによって、メッシュ アクセス ポイントに、ゲイン、指向性、偏波の 3 つの基本的な特性が与えられます。

- ゲイン：電力の増加の度合いを表します。ゲインは、アンテナが RF 信号に追加するエネルギーの増加量です。
- 指向性：伝送パターンの形状を表します。アンテナのゲインが増加すると、カバレッジエリアは減少します。カバレッジエリアや放射パターンは、度数で測ります。これらの角度は、度数で測定され、ビーム幅と呼ばれます。

（注） ビーム幅は、空間の特定の方向に向けて無線信号エネルギーを集中させるアンテナの能力の大きさとして定義されます。ビーム幅は通常、HB（水平ビーム幅）の度数で表現されます。通常、最も重要なビーム幅はVB（垂直ビーム幅）（上下）放射パターンで表現されます。アンテナのプロットまたはパターンを見るとき、角度は通常、メイン ローブの最大効果放射電力を基準とした場合の、メイン ローブの半電波強度（3 dB）ポイントで測定されます。

（注） 8 dBi アンテナは 360 度の水平ビーム幅で伝送するため、電波は全方位に電力を分散します。それにより、8 dBi アンテナからの電波は、ビーム幅がこれより狭い（360 度より小さい）14 dBi パッチアンテナ（またはサードパーティのディッシュ アンテナ）から送信された電波ほど遠くまではほとんど届きません。

- 偏波：空間を通る電磁波の電界の方向。アンテナは、水平方向または垂直方向のいずれかに偏向される可能性がありますが、他の種類の偏波が可能です。1 つのリンク内にあるアンテナは、それ以上無用な信号損失を避けるため、両方が同じ偏波を持つ必要があります。性能を向上させるため、アンテナを時々回転させると、偏波を変更し干渉を減少できます。RF 波を送信してコンクリートの谷間を下らせるときには垂直方向の偏波が、広範囲に伝搬させるときには水平方向の偏波の方が適しています。偏波は、RF エネルギーを隣接ストラクチャのレベルにまで減らすのが重要であるときに、RF Bleed-over を最適化するのにも利用できます。ほとんどの全方向性アンテナは、デフォルトとして垂直偏波を設定して出荷されています。

アンテナ オプション

幅広いアンテナが利用でき、さまざまな地形にメッシュ アクセス ポイントを展開する際の柔軟性を提供します。サポートされるアンテナのリストについては、該当するアクセス ポイント データシートまたは発注ガイドを参照してください。

シスコのアンテナおよびアクセサリについては、次の URL にある『*Cisco Aironet Antenna and Accessories Reference Guide*』を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

配置および設計、制限事項および機能、さらにアンテナの基礎理論や取り付け手順、規制に関する情報、技術仕様についても記載されています。

クライアント アクセス認定アンテナ（サードパーティ製アンテナ）

AP1500 は、サードパーティ製のアンテナと一緒に使用できます。ただし、次のことに注意してください。

- シスコは、未認定のアンテナやケーブルの品質、性能、信頼性についての情報を追跡したり保持したりしません。

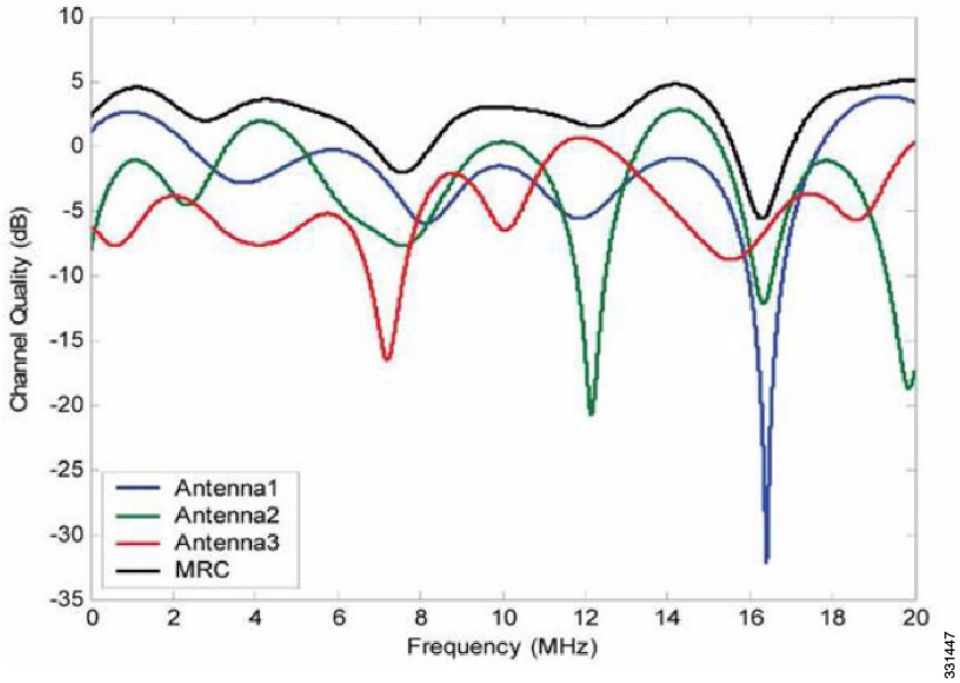
- RF 接続性および準拠性については、お客様の責任で使用してください。
- 準拠性を保証するのは、シスコ製のアンテナもしくは、シスコ製のアンテナと同一の設計およびゲインのアンテナの場合だけです。
- シスコ社以外のアンテナおよびケーブルについて、Cisco Technical Assistance Center（TAC）にトレーニングやカスタマー履歴の情報はありません。

最大比合成

この機能を理解するために、1 つのトランスミッタを装備した 802.11a/g クライアントが、複数のトランシーバを装備した 802.11n アクセスポイントにアップリンク パケットを送信する場合について考えてみます。アクセス ポイントは 3 本の受信アンテナそれぞれで信号を受信します。

受信した各信号の位相と振幅は、アンテナとクライアントの間隔の特性によって異なります。アクセス ポイントは、最適な信号を形成するために位相と振幅を調整することで、受信した 3 つの信号を処理して 1 つの強化された信号にします。使用されるアルゴリズムは最大比合成（MRC）と呼ばれ、通常すべての 802.11n アクセス ポイントで使用されます。MRC はアップリンク方向にだけ有用で、アクセス ポイントがクライアントをより適切に「ヒアリング」できるようにします。

図 *4*：*MRC* アルゴリズムによる受信信号の強化



Cisco ワイヤレス LAN コントローラ

ワイヤレス メッシュ ソリューションは、Cisco 2500、5500、および 8500 シリーズ ワイヤレス LAN コントローラでサポートされます。

Cisco 2500、5500、および 8500 シリーズ ワイヤレス LAN コントローラの詳細については、http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html を参照してください。

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、ワイヤレス メッシュの計画、設定、管理のためのグラフィカルなプラットフォームを提供します。Prime Infrastructure を使用すると、ネットワーク管理者は、ワイヤレス メッシュ ネットワークの設計、コントロール、モニタリングを中央の場所から行えます。

Prime Infrastructure はネットワーク管理者に、RF 予測、ポリシー プロビジョニング、ネットワーク最適化、トラブルシューティング、ユーザ トラッキング、セキュリティ モニタリング、およびワイヤレス LAN システム管理のソリューションを提供します。グラフィカル インターフェイスを使用したワイヤレス LAN の配置と操作は、簡単で費用有効です。詳細なトレンド分析および分析レポートにより、Prime Infrastructure は現行のネットワーク操作に不可欠なものになります。

Prime Infrastructure は、組み込みデータベースと共に、サーバ プラットフォームで実行されます。これにより、何百ものコントローラや何千もの Cisco メッシュ アクセス ポイントを管理可能にするスケーラビリティが提供されます。コントローラは、Prime Infrastructure と同じ LAN 上、別の経路選択済みサブネット上、または広域接続全体にわたって配置できます。

アーキテクチャ

アーキテクチャ

Control and Provisioning of Wireless Access Points

Control And Provisioning of Wireless Access Points（CAPWAP）は、ネットワークのアクセス ポイント（メッシュおよび非メッシュ）を管理するためにコントローラが使用するプロビジョニングと制御プロトコルです。リリース 5.2 で、Lightweight AP Protocol（LWAPP）が CAPWAP に置き換えられました。

（注） CAPWAP を使用すると、資本的支出（CapEx）と運用維持費（OpEx）が著しく減少し、シスコ ワイヤレス メッシュ ネットワーキング ソリューションが、企業、キャンパス、メトロポリタンのネットワークにおける費用有効でセキュアな配置オプションになります。

メッシュ ネットワークの CAPWAP ディスカバリ

メッシュ ネットワークの CAPWAP ディスカバリ プロセスは次のとおりです。

1. CAPWAP ディスカバリの開始の前に、メッシュ アクセス ポイントがリンクを確立します。その一方で、非メッシュ アクセス ポイントが、そのメッシュ アクセス ポイント用の静的 IP（ある場合）を使用して、CAPWAP ディスカバリを開始します。
2. メッシュ アクセス ポイントは、レイヤ 3 ネットワークのメッシュ アクセス ポイントの静的 IP を使用して CAPWAP ディスカバリを開始するか、割り当てられたプライマリ、セカンダリ、ターシャリのコントローラ用のネットワークを探します。接続するまで最大 10 回試行されます。

（注） メッシュ アクセス ポイントは、セットアップ中に、そのアクセス ポイントで設定されている（準備のできている）コントローラのリストを探します。

3. 手順 2 が 10 回の試行の後に失敗した場合、メッシュ アクセス ポイントは DHCP にフォールバックし、接続を 10 回試行します。
4. 手順 2 と 3 の両方に失敗し、コントローラに対して成功した CAPWAP 接続がない場合、メッシュ アクセス ポイントは LWAPP にフォール バックします。
5. 手順 2、3、4 の試行後にディスカバリがなかった場合、メッシュ アクセス ポイントは次のリンクを試みます。

ダイナミック MTU 検出

ネットワークで MTU が変更された場合、アクセス ポイントは、新しい MTU の値を検出し、それをコントローラに転送して、新しい MTU に調整できるようにします。新しい MTU でアクセス ポイントとコントローラの両方がセットされると、それらのパス内にあるすべてのデータは、新しい MTU 内で断片化されます。変更されるまで、その新しい MTU のサイズが使用されます。スイッチおよびルータでのデフォルトの MTU は、1500 バイトです。

XML 設定ファイル

コントローラのブート設定ファイル内のメッシュの機能は、XML ファイルに ASCII 形式で保存されます。XML 設定ファイルは、コントローラのフラッシュ メモリに保存されます。

（注） 現行リリースは、バイナリの設定ファイルをサポートしませんが、設定ファイルはメッシュ リリースからコントローラ ソフトウェア リリース 7.0 へのアップグレード後すぐにバイナリ状態になります。XML 構成ファイルは、リセット後に選択されます。

注意 XMLファイルを編集しないでください。修正された設定ファイルをコントローラにダウンロードすると、ブート時に巡回冗長検査（CRC）エラーが発生し、設定がデフォルト値にリセットされます。

XML設定ファイルは、CLI形式に変換すると、容易に読み込みや修正ができます。XMLからCLI形式に変換するには、設定ファイルを TFTP または FTP のサーバにアップロードします。コントローラはアップロード中に、XML から CLI への変換を開始します。

サーバ上では、CLI 形式で設定ファイルを読み取りまたは編集できます。その後、そのファイルをダウンロードして、コントローラに戻すことができます。コントローラでは、設定ファイルが再度 XML 形式に変換されて、フラッシュ メモリに保存され、新しい設定を使用してリブートされます。

コントローラは、ポート設定 CLI コマンドのアップロードおよびダウンロードをサポートしません。コントローラ ポートを設定したい場合は、次にまとめた関連コマンドを入力します。

（注） 次のコマンドは、ソフトウェアをリリース 7.0 にアップグレードすると、手動で入力できます。

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートでアップ リンク トラップおよびダウン リンク トラップを有効または無効にします。
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートで管理モードを有効または無効にします。
- **config port multicast appliance** *port* {**enable** | **disable**}：特定のコントローラ ポートに対し、マルチキャスト アプライアンス サービスを有効または無効にします。
- **config port power** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートで Power-over-Ethernet（PoE）を有効または無効にします。

既知のキーワードおよび正しい構文を持つCLIコマンドはXMLに変換されますが、不適切なCLIコマンドは無視されてフラッシュ メモリに保存されます。無効な値を持つフィールドは、XML 検証エンジンにより、フィルタ アウトされ、デフォルト値にセットされます。検証は、ブート中に実行されます。

無視されたコマンドおよび無効な設定値を確認するには、次のコマンドを入力します。

show invalid-config

（注） このコマンドは、**clear config** コマンドまたは **save config** コマンドの前にしか実行できません。ダウンロードした設定に多数の無効なCLIコマンドが含まれている場合、分析のため、無効な設定を TFTP または FTP サーバにアップロードできます。

アクセスパスワードは、設定ファイルの中に隠されて（難読化されて）います。アクセスポイントまたはコントローラのパスワード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 switchconfig secret-obfuscation {**enable** | **disable**}

Adaptive Wireless Path Protocol

Adaptive Wireless Path Protocol（AWPP）は、ワイヤレス メッシュ ネットワーキング用に設計されたもので、これを使用すると、配置が容易になり、コンバージェンスが高速になり、リソースの消費が最小限に抑えられます。

AWPP は、クライアント トラフィックがコントローラにトンネルされているために AWPP プロセスから見えないという CAPWAP WLAN の特性を利用します。また、CAPWAP WLAN ソリューションの拡張無線管理機能はワイヤレス メッシュ ネットワークに利用できるため、AWPP に組み込む必要はありません。

AWPP を使用すると、リモート アクセス ポイントは、RAP のブリッジ グループ（BGN）の一部である各 MAP 用の RAP に戻る最適なパスを動的に見つけられるようになります。従来のルーティング プロトコルとは異なり、AWPP は RF の詳細を考慮に入れています。

ルートを最適化するため、MAP はネイバー MAP をアクティブに送信要求します。要請メッセージのやり取りの際に、MAP は RAP への接続に使用可能なネイバーをすべて学習し、最適なパスを提供するネイバーを決定して、そのネイバーと同期します。AWPP では、リンクの品質とホップ数に基づいてパスが決定されます。

AWPP は、パスごとに信号の強度とホップ カウントについてコストを計算して、CAPWAP コントローラへ戻る最適なパスを自動で判別します。パスが確立されると、AWPP は継続的に条件をモニタし、条件の変化に応じてルートを変更します。また、AWPP は、条件情報を知らせるスムージング機能を実行して、RF 環境のエフェメラルな性質に、ネットワークの安定性が影響を受けないようにします。

トラフィック フロー

ワイヤレス メッシュ内のトラフィック フローは、次の 3 つのコンポーネントに分けられます。

1. オーバーレイ CAPWAP トラフィック：標準の CAPWAP アクセス ポイントの配置内のフローで、CAPWAP アクセス ポイントと CAPWAP コントローラの間の CAPWAP トラフィックのことです。
2. ワイヤレス メッシュ データ フレーム フロー
3. AWPP 交換

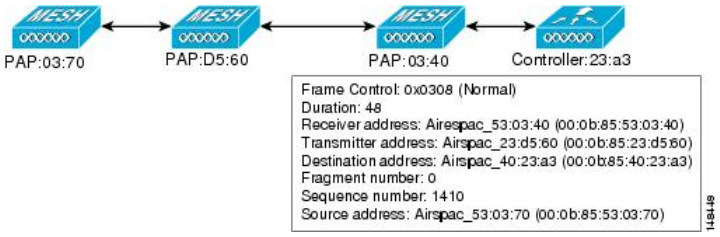
CAPWAP モデルはよく知られており、AWPP は専用プロトコルのため、ワイヤレス メッシュ データ フローについてだけ説明します。ワイヤレス メッシュ データ フローのキーは、メッシュ アクセス ポイント間で送信される 802.11 フレームのアドレス フィールドです。

802.11 データ フレームは、レシーバ、トランスミッタ、送信先、発信元の 4 つまでのアドレス フィールドを使用できます。WLAN クライアントから AP までの標準フレームでは、トランスミッ

タ アドレスと発信元アドレスが同じため、これらのアドレス フィールドのうち 3 つしか使用されません。しかし、WLANブリッジング ネットワークでは、フレームが、トランスミッタの背後にあるデバイスによって生成された可能性があるため、フレームの発信元がフレームのトランスミッタであるとは限らず、4 つのすべてのアドレス フィールドが使用されます。

図 5：ワイヤレス メッシュ フレーム，（17 ページ） は、このタイプのフレーム構成の例を示しています。フレームの発信元アドレスはMAP:03:70、このフレームの送信先アドレスはコントローラ（メッシュ ネットワークはレイヤ 2 モードで動作しています）、トランスミッタ アドレスはMAP:D5:60、レシーバ アドレスは RAP:03:40 です。

図 *5*：ワイヤレス メッシュ フレーム



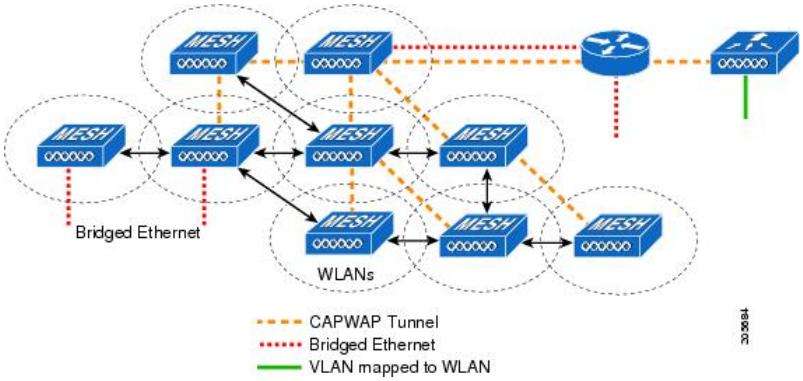
このフレームの送信により、トランスミッタとレシーバのアドレスは、ホップごとに変わります。各ホップでレシーバ アドレスを判別するために AWPP が使用されます。トランスミッタ アドレスは、現在のメッシュ アクセス ポイントのアドレスです。パス全体を通して、発信元アドレスと送信先アドレスは同一です。

RAP のコントローラ接続がレイヤ 3 の場合、MAP はすでに CAPWAP を IP パケット内にカプセル化してコントローラに送信済みのため、そのフレームの送信先アドレスはデフォルト ゲートウェイ MAC アドレスになり、ARP を使用する標準の IP 動作を使用してデフォルト ゲートウェイの MAC アドレスを検出します。

メッシュ内の各メッシュ アクセス ポイントは、コントローラと共に、CAPWAP セッションを形成します。WLAN トラフィックはCAPWAP 内にカプセル化されるため、コントローラ上の VLAN インターフェイスにマップされます。ブリッジされたイーサネット トラフィックは、メッシュ ネットワーク上の各イーサネット インターフェイスから渡される可能性があり、コントローラの

インターフェイスにマップされる必要はありません（図 6：論理ブリッジと WLAN マッピング, （18 ページ） を参照）。

図 *6*：論理ブリッジと *WLAN* マッピング

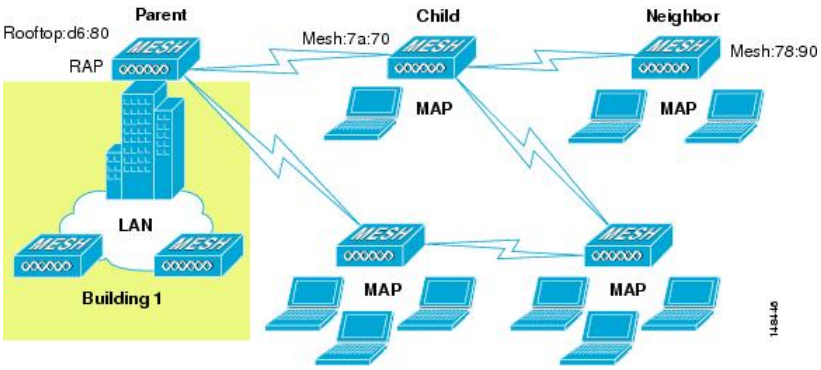


メッシュ ネイバー、親、および子

メッシュ アクセス ポイント間の関係は、親、子、ネイバーです（図 7：親、子、およびネイバー アクセス ポイント, （18 ページ） を参照）。

- 親アクセス ポイントは、容易度の値（ease value）に基づいて RAP への最適なルートを提供します。親は RAP 自身または別の MAP のいずれかです。
  - 容易度の値（ease value）は各ネイバーの SNR およびリンク ホップ値を用いて計算されます。複数の選択肢がある場合、通常は緩和値の高いアクセス ポイントが選択されます。
- 子アクセスポイントは、RAPに戻る最適なルートとして親アクセスポイントを選択します。
- ネイバーアクセスポイントは、他のアクセスポイントのRF範囲内にありますが、その容易度の値は親よりも低いため、親や子としては選択されません。

図 *7*：親、子、およびネイバー アクセス ポイント



最適な親を選択するための基準

AWPP は、次のプロセスに従って、無線バックホールを使用して RAP または MAP 用に親を選択します。

- *scan* ステートでは、パッシブ スキャニングによって、ネイバーのあるチャネルのリストが生成され、それが、すべてのバックホール チャネルのサブセットになります。
- *seek* ステートでは、アクティブ スキャニングによって、ネイバーを持つチャネルが探され、バックホール チャネルは最適なネイバーを持つチャネルに変更されます。
- *seek* ステートでは、親は最適なネイバーとしてセットされ、親子のハンドシェイクが完了します。
- *maintain* ステートでは、親のメンテナンスと最適化が実行されます。

このアルゴリズムは、起動時、および親が消失して他に親になりそうなものがない場合に実行され、通常は、CAPWAP ネットワークとコントローラのディスカバリが続けて実行されます。すべてのネイバー プロトコル フレームは、チャネル情報を運びます。

親メンテナンスは、誘導 NEIGHBOR_REQUEST を親に送信している子ノードおよび NEIGHBOR_RESPONSE で応答している親によって実行されます。

親の最適化とリフレッシュは、親が常駐しているチャネル上で NEIGHBOR_REQUEST ブロードキャストを送信している子ノードによって、そのチャネル上のネイバリング ノードからのすべての応答の評価によって発生し実行されます。

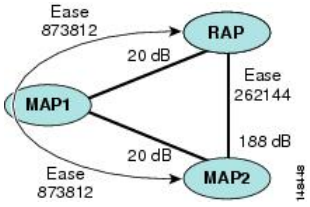
親メッシュ アクセス ポイントは、RAP に戻る最適なパスを提供します。AWPP は、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

容易度の計算

容易度は、各ネイバーの SNR とホップの値を使用し、さまざまな SNR しきい値に基づく乗数を適用して計算します。この乗数には、Spreading 機能を、さまざまなリンクの質に影響する SNR に適用するという意味があります。

図 8：親パスの選択，（19 ページ） では、親パスの選択で、MAP2 は MAP1 を通るパスを選択します。このパスを通る調整された容易度の値（436906）が、MAP2 から RAP に直接進むパスの容易度の値（262144）より大きいためです。

図 *8*：親パスの選択



親の決定

親メッシュ アクセス ポイントは、各ネイバーの容易度を RAP までのホップ カウントで割り算した、調整された容易度を使用して選択されます。

調整された容易度 = 最小値（各ホップでの容易度）ホップ カウント

SNR スムージング

WLANルーティングの難しいところは、RFのエフェメラルな性質です。最適なパスを分析して、パス内で変更がいつ必要かを決めるときに、この点を考慮しなければなりません。特定の RF リンクのSNRは、刻一刻と大幅に変化する可能性があり、これらの変動に基づいてルートパスを変更すると、ネットワークが不安定になり、パフォーマンスが深刻に低下します。基本的なSNRを効果的にキャプチャしながらも経時変動を除去するため、調整されたSNRを提供するスムージング機能が適用されます。

現在の親に対する潜在的なネイバーを評価するとき、親間のピンポン効果を減少させるため、親の計算された容易度に加えて、親に20%のボーナス容易度が与えられます。子がスイッチを作成するには、潜在的な親の方が著しくよくなければなりません。親スイッチングはCAPWAPおよびその他の高レイヤの機能に透過的です。

ループの防止

ルーティングループが作成されないようにするため、AWPPは、自分のMACアドレスを含むルートをすべて破棄します。つまり、ホップ情報とは別に、ルーティング情報がRAPへの各ホップのMAC アドレスを含むため、メッシュ アクセス ポイントはループするルートを容易に検出して破棄できます。