CHAPTER 2

Cisco Unified Wireless のテクノロジーおよびアーキテクチャ

この章では、企業の Cisco Unified Wireless Network を展開する場合の、設計上および運用上の主な考慮事項について説明します。

この章では、次の内容について説明します。

- CAPWAP
- コア コンポーネント
- コンポーネントの機能グループ
- ローミング
- ブロードキャストとマルチキャストの処理
- 設計上の考慮事項
- 運用および保守

この章で扱う内容のほとんどは、この文書の後の章でさらに詳しく説明されます。Cisco Unified Wireless テクノロジーの詳細については、次の Web サイトにある Cisco 5500 シリーズ ワイヤレス LAN コントローラに関連する展開戦略を説明したシスコのホワイト ペーパーを参照してください。

http://www.cisco.com/en/US/products/ps10315/prod_white_papers_list.html

CAPWAP の概要

ワイヤレス アクセス ポイント（CAPWAP）の制御およびプロビジョニングは、シスコの *中央集中型 WLAN アーキテクチャ*（Cisco Unified Wireless Network ソリューションの機能アーキテクチャ）で使用される基盤となるプロトコルです。CAPWAP は、中央集中型 WLAN コントローラ（WLC）への WLAN クライアントによる双方向トンネリング トラフィックの管理に加えて、WLAN の設定および管理を行います。図 2-1 は、基本的な中央集中型 WLAN 展開のハイレベルの概略図を示します。この図では、CAPWAP AP は CAPWAP 経由で WLC に接続されます。

CAPWAP コントローラおよび LWAPP コントローラは、同じネットワークで展開が可能です。CAPWAP 対応ソフトウェアでは、AP は CAPWAP と LWAPP のいずれが稼働するコントローラに join できます。唯一の例外は Cisco Aironet 1140 シリーズの AP で、ここでは CAPWAP だけがサポートされているため、CAPWAP が稼働するコントローラにだけ join できます。たとえば、1130 シリーズの AP では、CAPWAP と LWAPP のいずれが稼働するコントローラにも join できますが、Aironet 1140 シリーズの AP が join できるのは、CAPWAP が稼働するコントローラだけです。

シスコでは、CAPWAP を使用するときは、次のガイドラインに従うことを推奨します。

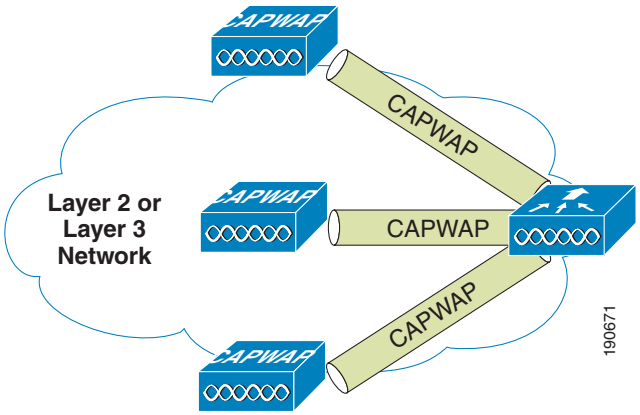
- LWAPP を使用する AP からのトラフィックのみを許容するようにファイアウォールが設定されている場合、CAPWAP を使用する AP からのトラフィックを許容するようにファイアウォールのルールを変更する必要があります。
- CAPWAP UDP ポート 5246 および 5247（LWAPP UDP ポート 12222 および 12223 と同等のポート）が有効になっており、AP がコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト（ACL）がコントローラと AP の間の制御パスにある場合は、新しいプロトコル ポートを開いて AP が孤立しないようにする必要があります。

CAPWAP AP では、ランダムな UDP 送信元ポートを使用し、コントローラ上のそれら宛先ポートに到達します。Cisco WLC リリース 5.2 では、LWAPP が削除され、CAPWAP に置き換えられています。ただし、新しく開封したばかりの AP があれば、コントローラから CAPWAP イメージをダウンロードする前に、LWAPP を使用してコントローラへのアクセスを試行することもできます。AP は、コントローラから CAPWAP イメージをダウンロードしたら、CAPWAP のみを使用して、コントローラとやり取りします。

（注）　CAPWAP を使用してコントローラへの join を 60 秒間試行した後、AP は LWAPP の使用にフォールバックします。AP は、LWAPP を使用してコントローラを 60 秒以内に検出できないと、CAPWAP を使用してコントローラへの join を再度試行します。AP は、コントローラに join できるまで、CAPWAP と LWAPP を 60 秒ごとに切り替えるこのサイクルを繰り返します。

LWAPP リカバリ イメージを持つ AP（自律またはスタンドアロン モードまたは新しく開封したばかりの AP から移行した AP）は、コントローラから CAPWAP イメージをダウンロードする前に、LWAPP のみを使用してコントローラに join しようとします。

図 2-1　　WLC に接続された CAPWAP AP



（注）　CAPWAP プロトコルは多数の機能コンポーネントから構成されますが、このデザイン ガイドでは、中央集中型 WLAN ネットワークの設計および運用に影響を与えるものについてのみ説明します。

CAPWAP の主な機能は、以下のとおりです。

- スプリット MAC トンネル

- L3 ベースのトンネル
- WLC ディスカバリ プロセス

スプリット MAC

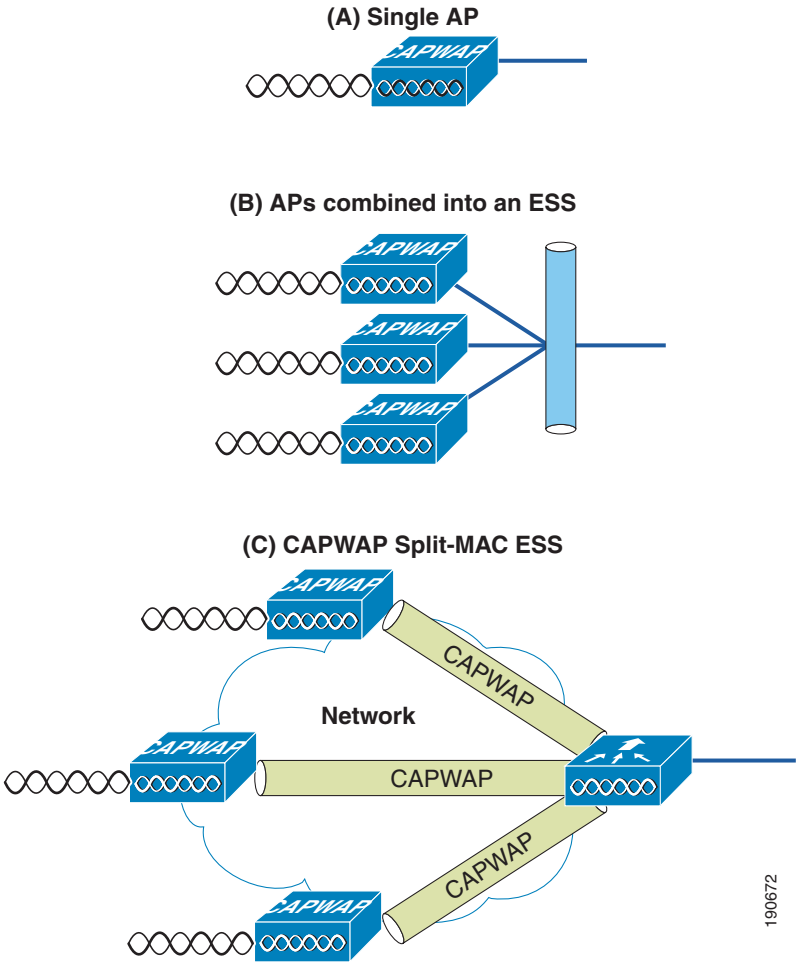
CAPWAP の主要なコンポーネントの 1 つに、*スプリット MAC* という概念があります。これは、802.11 プロトコルでの動作の一部を CAPWAP AP が管理し、残りの部分を WLC が管理するというものです。図 2-2 は、スプリット MAC の概念を図に表したものです。

図 2-2（A）に示す最も単純な汎用 802.11 AP は、Basic Service Set Identifier（BSSID）へのアソシエーションに基づいて有線ネットワークに WLAN クライアントをブリッジする 802.11 MAC レイヤ無線にすぎません。802.11 規格では、図 2-2（B）に示すように、AP を 1 台だけ使用するという概念（前述）が拡張され、複数の AP に対して同じ Extended Service Set 識別子（ESSID、通常 SSID と呼ばれます）を割り当てることで、WLAN クライアントが複数の AP を経由して共通のネットワークに接続できるようになります。

CAPWAP スプリット MAC の概念では、通常は個々の AP によって実行されるすべての機能を、CAPWAP AP と WLC の 2 つの機能コンポーネントに割り振ります。この 2 つのコンポーネントは、ネットワーク経由で CAPWAP プロトコルを使用してリンクされ、個々の AP を使用する場合と同等の無線/ブリッジ サービスを、展開や管理がより容易な方法で提供します。

（注） *スプリット MAC* により、WLAN クライアントと WLC の有線インターフェイスとの間のレイヤ 2 接続はスムーズになりますが、すべてのトラフィックが CAPWAP トンネルを通過できるわけではありません。WLC は、IP Ethertype フレームだけを転送します。デフォルトの動作では、ブロードキャストやマルチキャスト トラフィックは転送されません。WLAN の展開時にマルチキャストやブロードキャストの要件を検討するときには、このことが重要になりますので、覚えておいてください。

図 2-2　CAPWAP スプリット MAC の概念



単純で時間に依存した処理は、通常 CAPWAP AP によってローカルで管理され、より複雑で時間への依存が少ない処理は WLC によって管理されます。

たとえば、CAPWAP AP は次のような操作を扱います。

- クライアントと AP 間のフレーム交換ハンドシェイク
- ビーコン フレームの転送
- 省電力モードでのクライアントに対するフレームのバッファリングおよび転送
- クライアントからのプローブ要求フレームへの応答（プローブ要求は WLC にも送信され、そこで処理されます）
- 受信したプローブ要求の通知の WLC への転送
- 受信したすべてのフレームを持つスイッチへのリアルタイムでの信号品質情報のプロビジョニング
- 各無線チャネルにおけるノイズ、干渉、およびその他の WLAN の監視
- 他の AP の存在の監視
- 802.11 フレームの暗号化および復号化

その他の機能は WLC により処理されます。WLC が提供する MAC レイヤ機能には、次のようなものが含まれます。

- 802.11 認証
- 802.11 アソシエーションおよび再アソシエーション（モビリティ）
- 802.11 フレームの変換およびブリッジ
- 802.1X/EAP/RADIUS 処理
- 有線インターフェイス上の 802.11 トラフィックの終端、ただし、このデザイン ガイドの後半で説明する REAP 機能および H-REAP 機能が設定された AP は除きます。

CAPWAP トンネルは、次の 2 つのカテゴリのトラフィックをサポートしています。

- CAPWAP 制御メッセージ：WLC と AP の間で制御、設定、および管理に関する情報を伝達するために使用されます。
- 無線クライアント データのカプセル化：レイヤ 2 無線クライアント トラフィックをカプセル化された IP EtherType パケットで AP から WLC に転送します。

カプセル化されたクライアント トラフィックは、WLC に到達すると、対応する WLC の VLAN インターフェイスおよびポートにマッピングされます。このインターフェイスのマッピングは、WLC で WLAN の設定の一部として定義されます。通常、インターフェイス マッピングは静的に実行されますが、EAP 認証が正常に終了した場合、アップストリーム AAA サーバにより送信されるパラメータに基づいて、WLAN クライアントを特定の VLAN に動的にマッピングできます。WLAN の設定パラメータには、VLAN の割り当てのほか、次のものがあります。

- SSID
- 動作状態
- 認証およびセキュリティ方式
- QoS

レイヤ 3 トンネル

レイヤ 3 CAPWAP は、推奨されるトンネル タイプです。この方式では、CAPWAP AP と WLC 間の通信をスムーズにするために、IP UDP パケットが使用されます。レイヤ 3 CAPWAP は、トンネル パケットのフラグメンテーションおよび再アセンブリを実行できます。これにより、クライアント トラフィックは 1500 バイトの MTU を使用できるようになり、トンネル オーバーヘッドの調整は不要になります。

（注） フラグメンテーションおよび再アセンブリの処理を最適化するため、WLC または AP が受信するフラグメントの数は制限されます。Cisco Unified Wireless Network を展開する上でサポートされる理想的な MTU のサイズは 1500 バイトですが、MTU が 500 バイト程度のネットワークであれば、ソリューションは問題なく動作します。

以下は、CAPWAP 操作を示すためのレイヤ 3 CAPWAP パケット キャプチャです。サンプル デコードは、Wireshark パケット アナライザを使用してキャプチャしたものです。

（注） Wireshark のデフォルト設定では、Cisco CAPWAP パケットを正しくデコードすることはできません。この問題は、Wireshark の設定ウィンドウの [Protocol Preferences] タブで [SWAP Frame Control] オプションを選択することで解決できます。

図 2-3 は、CAPWAP コントロール パケットのデコードを示しています。WLC からのすべての CAPWAP コントロール パケットと同様、このパケットも WLC から送信元 UDP ポート 5246 を使用して送られてきたものです。Control Type 12 は、AP 設定情報を CAPWAP AP に渡すために WLC により使用される設定コマンドを表します。コントロール パケットのペイロードは AES で暗号化されています。この暗号化では、CAPWAP AP が WLC との接続を最初に確立したときに実行される PKI 認証プロセスで生成されたキーが使用されます。

図 2-3　CAPWAP コントロール パケット

```
⊞ Frame 456: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0
⊞ Ethernet II, Src: Cisco_a9:91:94 (00:3a:9a:a9:91:94), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 172.20.227.125 (172.20.227.125), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: 39195 (39195), Dst Port: capwap-control (5246)
    Source port: 39195 (39195)
    Destination port: capwap-control (5246)
    Length: 131
  ⊞ Checksum: 0x0000 (none)
⊟ Control And Provisioning of Wireless Access Points
  ⊞ Preamble
  ⊟ Header
      Header Length: 4
      Radio ID: 0
      Wireless Binding ID: IEEE 802.11 (1)
    ⊞ Header flags
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      MAC length: 6
      MAC address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
      Padding for 4 Byte Alignement: 00
  ⊟ Control Header
    ⊞ Message Type: 1
      Sequence Number: 0
      Message Element Length: 102
      Flags: 0
```

図 2-4 は、802.11 プローブ要求を含む CAPWAP パケットのデコードを示しています。すべての CAPWAP でカプセル化される 802.11 フレームと同様、このパケットも UDP ポート 5246 を使用して CAPWAP AP から WLC に送られるパケットです。この例では、RF 情報を WLC に提供するために、CAPWAP パケットには、受信信号強度インジケータ（RSSI）の値と信号対雑音比（SNR）の値も含まれています。

図 2-4　CAPWAP の 802.11 プローブ要求

```
⊞ Frame 668: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
⊞ Ethernet II, Src: Cisco_42:57:5c (44:d3:ca:42:57:5c), Dst: Cisco_da:78:20 (64:d8:14:da:78:20)
⊞ Internet Protocol Version 4, Src: 172.20.227.123 (172.20.227.123), Dst: 172.20.227.99 (172.20.227.99)
⊟ User Datagram Protocol, Src Port: 9590 (9590), Dst Port: capwap-data (5247)
    Source port: 9590 (9590)
    Destination port: capwap-data (5247)
    Length: 117
  ⊞ Checksum: 0x0000 (none)
⊟ Control And Provisioning of Wireless Access Points
  ⊞ Preamble
  ⊟ Header
      Header Length: 4
      Radio ID: 0
      Wireless Binding ID: IEEE 802.11 (1)
    ⊟ Header flags
        1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
        .0.. .... . = Fragment: Don't Fragment
        ..0. .... . = Last Fragment: More fragments follow
        ...1 .... . = Wireless header: Wireless Specific Information is present
        .... 0... . = Radio MAC header: No Radio MAC Address
        .... .0.. . = Keep-Alive: No Keep-Alive
        .... ..00 0 = Reserved: Not set
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      Wireless length: 4
      Wireless data: 00000000
    ⊟ Wireless data ieee80211 Frame Info: 00000000
        Wireless data ieee80211 RSSI (dBm): 0
        Wireless data ieee80211 SNR (dB): 0
        Wireless data ieee80211 Data Rate (Mbps): 0
      Padding for 4 Byte Alignement: 000000
⊞ IEEE 802.11 Probe Request, Flags: ........
```

図 2-5 は、別の CAPWAP で暗号化された 802.11 フレームを示していますが、この場合は、図 2-4 に示すような 802.11 データ フレームです。これには、完全な 802.11 フレームのほかに、WLC に対する RSSI と SNR の情報が含まれます。このキャプチャは、CAPWAP で、802.11 のデータ フレームがその他の 802.11 のフレームと同様に扱われることを示しています。図 2-5 は、CAPWAP AP と WLC の間の CAPWAP パケットで、最小 MTU サイズに合わせたフラグメンテーションがサポートされていることを示しています。Wireshark デコードでは、フレーム コントロール デコード バイトがスワップされていることに注意してください。これは、一部の CAPWAP AP がこれらのバイトをスワップすることを考慮して、CAPWAP パケットの Wireshark プロトコルの解析中に実行されます。

図 2-5　CAPWAP の 802.11 データ フレーム

```
Internet Protocol Version 4, Src: 172.20.227.100 (172.20.227.100), Dst: 172.20.227.125 (172.20.227.125)
User Datagram Protocol, Src Port: capwap-data (5247), Dst Port: 39195 (39195)
  Source port: capwap-data (5247)
  Destination port: 39195 (39195)
  Length: 42
⊞ Checksum: 0x0000 (none)
Control And Provisioning of Wireless Access Points
⊞ Preamble
⊟ Header
    Header Length: 2
    Radio ID: 1
    Wireless Binding ID: IEEE 802.11 (1)
  ⊟ Header flags
      1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
      .0.. .... . = Fragment: Don't Fragment
      ..0. .... . = Last Fragment: More fragments follow
      ...0 .... . = Wireless header: No Wireless Specific Information
      .... 0... . = Radio MAC header: No Radio MAC Address
      .... .0.. . = Keep-Alive: No Keep-Alive
      .... ..00 0 = Reserved: Not set
    Fragment ID: 0
    Fragment Offset: 0
    Reserved: 0
IEEE 802.11 Disassociate, Flags: ........
  Type/Subtype: Disassociate (0x0a)
⊞ Frame Control: 0x00A0 (Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Destination address: Apple_d1:22:39 (18:20:32:d1:22:39)
  Source address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  BSS Id: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  Fragment number: 0
  Sequence number: 0
```

WLC ディスカバリおよび選択

この項では、リセット時のレイヤ 3 CAPWAP AP の典型的な動作について説明します。

ディスカバリ / join プロセスの詳細については、次の Web サイトにある『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_cg73.html

CAPWAP AP のリセット

レイヤ 3 CAPWAP AP をリセットすると、次のような一連の処理が実行されます。

ステップ 1　AP がローカル IP サブネット上でレイヤ 3 CAPWAP ディスカバリ メッセージをブロードキャストします。同一の IP サブネットに接続されている、レイヤ 3 CAPWAP モード用に設定された WLC はすべて、ディスカバリ メッセージを受信します。その後、CAPWAP ディスカバリ メッセージを受信した各 WLC は、AP に対してユニキャストされる CAPWAP ディスカバリ応答メッセージで応答します。

ステップ 2　AP は以前に確認した WLC IP アドレスをローカルの NVRAM に保持します。AP はこれらの WLC IP アドレスのそれぞれにユニキャスト CAPWAP ディスカバリ要求を送信します。CAPWAP ディスカバリ要求を受信する WLC は、AP に CAPWAP ディスカバリ応答を送信することで応答します。前述のとおり、WLC の IP アドレスは、すでに WLC に接続している既存の AP から送信される OTAP メッセージによって確認できます。NVRAM に保存される情報には、別のモビリティ グループのメンバとして以前に接続していた WLC のアドレス情報も含まれます（詳細については、「モビリティ グルー

プ、AP グループ、および RF グループ」（P.2-13）を参照してください）。

ステップ 3　ベンダー固有の DHCP オプションを使用して WLC の IP アドレスを返すように、DHCP サーバをプログラムできます。プログラムする場合、CAPWAP AP に WLC のアドレスを *アドバタイズ*するために、*DHCP オファーでオプション 43* を使用します。AP が DHCP 経由で IP アドレスを受信する場合、DHCP *オファー*のオプション 43 フィールドで WLC の IP アドレスの情報を確認します。AP は、DHCP オプション 43 に含まれる各 WLC にユニキャスト CAPWAP ディスカバリ メッセージを送信します。CAPWAP ディスカバリ要求メッセージを受信する WLC は、AP に対して CAPWAP ディスカバリ応答をユニキャストします。

ステップ 4　AP は、オプション 43 の情報なしで DNS 名 `CISCO-LWAPP-CONTROLLER.localdomain` を解決しようとします。この名前を解決できた場合、AP は、DNS 応答で返された個々の IP アドレスに対して、ユニキャスト CAPWAP ディスカバリ メッセージを送信します。前述のとおり、CAPWAP ディスカバリ要求メッセージを受信した各 WLC は、AP に対してユニキャスト CAPWAP ディスカバリ応答で応答します。

ステップ 5　ステップ 1 ～ 4 の後、CAPWAP ディスカバリ応答が受信されない場合、AP は検索アルゴリズムをリセットしてから、再開します。

通常、1 つまたは複数のシード WLC アドレスを提供するには、DHCP または DNS ディスカバリ メカニズムが使用されます。また、その後の WLC ディスカバリ応答では、WLC モビリティ グループの全メンバの一覧が提供されます。

CAPWAP AP は通常、推奨 WLC を表す、最大 3 つまでの WLC の一覧を使用して設定されています。これらの WLC が使用できないか、オーバーサブスクライブされている場合、AP はディスカバリ応答で確認された WLC の一覧から最も負荷の少ない別の WLC を選択します。

コア コンポーネント

Cisco Unified Wireless Network ソリューションを構成する主要コンポーネントは、正式にはワイヤレス制御システム（WCS）、ネットワーク制御システム（NCS）、ワイヤレス LAN コントローラ（WLC）、および Cisco Mobility Services Engine（MSE）として知られる Cisco Prime Infrastructure です。この項では、Cisco Prime Infrastructure、WLC、および AP 製品のオプションについて説明します（MSE の詳細については、第 11 章「Cisco モビリティ サービス エンジン」を参照してください）。

Cisco ワイヤレス LAN コントローラ

Cisco Unified Wireless Network コントローラの機能はすべての Cisco WLC プラットフォームで同一かつ共通しているため、便宜上、このドキュメントでは、これらのコントローラをすべて WLC と呼びます。

各種 Cisco WLC とその機能を簡単にまとめると、次のようになります。

- Cisco 2504 WLC：2504 コントローラは、Cisco AP および Cisco Prime Infrastructure と連携して動作して、システム全体にワイヤレス LAN 機能を提供します。2504 コントローラは、Cisco Unified Wireless Network のコンポーネントであり、ワイヤレス AP と他のデバイスとの間でリアルタイムの通信を行い、中央集中型セキュリティ ポリシー、ゲスト アクセス、ワイヤレス侵入防御システム（WIPS）、Context Aware（ロケーション）、受賞歴のある RF 管理、音声やビデオなどのモビリティ サービスの QoS、およびテレワーカー ソリューションに対する OEAP のサポートなどの機能を備えています。

  Cisco 2504 WLC は、最低 5 台から最大 50 台まで（5 台単位）の AP をサポートし、小売業、大企業の支社、および中小企業向けにコスト パフォーマンスに優れたソリューションを提供します。2504 WLC には 4 個のギガビット イーサネット ポートが搭載されています。

- Cisco 5508 WLC：5508 コントローラは Cisco Aironet AP、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間でリアルタイムの通信を行います。また、中央集中型セキュリティ ポリシー、ワイヤレス侵入防御システム（wIPS）機能、RF 管理、および Quality of Service (QoS) を備えています。ワイヤレス ネットワークの例外的なエンドユーザ エクスペリエンスに対応するために、Cisco 5500 シリーズには、さまざまな機能が用意されています。
  - 統合された CleanAir テクノロジーは、自己回復、自己最適化が可能なワイヤレス ネットワークを有効にすることで 802.11n のパフォーマンスを保護します。
  - シスコの ClientLink テクノロジーは、802.11a/g および 802.11n クライアントが最適なレートで動作できるようにすることで、クライアントが混在するネットワークのキャパシティを最適化します。
  - Cisco Identity Services Engine は、有線およびワイヤレス ネットワーク全体にわたり、単一の中央集中化型管理ポイントを提供します。企業は、従業員、ゲスト、および請負業者にセキュアで、適切なアクセスを提供することにより、モバイル スマート フォン、タブレット、ラップトップの急激な増加に対応できます。
- Cisco Wireless Services Module 2（WiSM-2）: Cisco Catalyst 6500 スイッチ シリーズ専用に設計された WLC モジュール。1 モジュールあたり最大 1000 台の AP をサポートします。6500 プラットフォームによっては、複数の WISM-2 をインストールして、拡張性を大幅に向上できます。WISM-2 は、6500 バックプレーンへの接続を提供する dot1 トランクとして設定可能な、6500 上の単一の集約されたリンク インターフェイスです。大規模なビルディングまたはキャンパスに適しています。
- Cisco Virtual Wireless Controller（vWLC）: Virtual Wireless Controller は、Cisco Aironet アクセス ポイント、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間で、中央集中化されたリアルタイムの通信を行います。仮想化イニシアチブに対応した組織や中小企業での展開用に設計された Virtual Wireless Controller は、以下の機能を提供します。
  - 最大 200 カ所のブランチ ロケーションに対応する中央集中型ワイヤレス ネットワークの可視性と制御
  - IT マネージャが FlexConnect を介して最大 200 台のアクセス ポイントと 3000 のクライアントを設定、管理、およびトラブルシューティングする機能
  - セキュアなゲスト アクセス、Payment Card Industry（PCI）コンプライアンスのための不正検出、およびブランチ内部（ローカル スイッチング）での Wi-Fi の音声とビデオ
  - ブランチ ネットワーク用の Cisco FlexConnect ソリューションを備えた信頼性の高い接続
  - ブランチの WAN 障害のためリモート コントローラに接続されたアクセス ポイントの保護。ワイヤレス クライアントは、ローカル リソースへのアクセスとの接続が保持されます
- Cisco Flex 7500 WLC：7500 シリーズ コントローラは、単一のロケーションから何千ものワイヤレス ブランチを管理するために必要な可視性と制御を提供します。このコントローラには、次の機能が用意されています。
  - ブランチ ロケーションごとにローカル コントローラを必要としない、費用対効果の高いソリューションを提供します。
  - 統合リモート管理により、何千ものブランチの拡張された、一貫性のある制御を行うことができます。
  - 分散されたゲストと従業員のアクセスに対するセキュアな中央集中型ポリシー管理を提供します。
  - WAN 障害に対する復元力によって各ローカル ブランチの事業継続性を確保します。
  - データ トラフィックのローカル スイッチングによる効率的なネットワーキングにより、WAN 最適化および QoS ポリシーを実現できます。WAN を介したトンネリングは必要はありません。

- Cisco 8500 WLC : 8500 シリーズ コントローラは、Cisco Aironet アクセス ポイント、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間でリアルタイムの通信を行います。サービス プロバイダーおよび大規模キャンパスへの展開向けに設計された 8500 シリーズ コントローラは、以下の機能を提供します。
  - 最大 6000 のアクセス ポイント、64,000 のクライアント、および 6000 のブランチ ロケーション用の中央集中型タッチポイントに対応する、単一のラック ユニット スペース（1RU）における業界最大の拡張性
  - 10 ギガビット イーサネット接続のサポートによる高速化 : 冗長性のために 2 つの 10 ギガビット イーサネット ポートを装備
  - SSID の高可用性とワイヤレス クライアントへの影響の最小化を保証する 1 秒未満のアクセス ポイントのステートフル フェールオーバーによる高可用性
  - 冗長性のためのデュアル電源装置による高い復元力

表 2-1 に、利用可能な Cisco WLC を要約して示します。

表 2-1　Cisco WLC の要約

	Cisco 2500 Wireless LAN Controller 	Cisco 5508 Wireless LAN Controller 	Cisco Flex 7500 Wireless LAN Controller 	Cisco 8500 Wireless LAN Controller 	Cisco WLAN Controller Module for Cisco Integrated Services Router 	Cisco Catalyst 6500 Series Wireless Services Module 2 (WISM-2) 
Controller Type	Standalone	Standalone	Standalone	Standalone	Module	Module
Platform Integration	N/A	N/A	N/A	N/A	2900 and 3900 Series Integrated Services Routers	Series Switches
Number of Lightweight Access Points Supported	5, 15, 25 or 50	12, 25, 50, 100, 250 or 500	250, 300, 500, 1000, 2000 or 3000	300-6,000	25 and 50	1,000
Number of clients Supported	500	7000	30,000	64,000	1000	15,000
	Remote location, branch office or campus	Remote location, branch office or campus	Branch/Remote location from the corporate location through a WAN link	SP Wi-Fi and Large Enterprise Campus	Remote location, branch office, or small office	Large campus
Uplink Interfaces	Four 1-Gbps ports	Eight 1-Gbps ports	2 x 10 Gigabit Ethernet interfaces	2 x 10 Gigabit Ethernet interfaces	One 10-/1--- Mbps port	Eight 1-Gbps ports

Cisco アクセス ポイント

Cisco Unified Wireless Network では、Autonomous と CAPWAP の 2 種類の AP が使用されます。この項では、利用可能な CAPWAP AP のさまざまなモデルについて説明します。

（注）　Cisco 1500 シリーズ MESH AP については、後で簡単に説明しますが、ワイヤレス MESH アプリケーションや MESH 展開のガイドラインについては、この設計ガイドでは扱っていません。Cisco MESH ソリューションの詳細については、『*Cisco Mesh Networking Solution Deployment Guide*』（http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh.html）参照してください。

CAPWAP AP

表 2-2 に、利用可能な Cisco CAPWAP AP を要約して示します。

表 2-2　CAPWAP AP の要約

	3600 Series	3500 Series	2600 Series	1260 Series	1140 Series	1040 Series	600 Series
Data Rate	450 Mbps	300 Mbps	450 Mbps	300 Mbps	300 Mbps	300 Mbps	300 Mbps
Radio Design	4X4:3	2X3:2	3x4:3	2x3:2	2x3:2	2X2:2	2X2:2
CleanAir	☑	☑	☑				
ClientLink	ClientLink 2.0	☑	ClientLink 2.0	☑	☑		
BandSelect	☑	☑	☑	☑	☑	☑	
VideoStream	☑	☑		☑	☑	☑	
Rogue AP Detection	☑	☑	☑	☑	☑	☑	
Adaptive wIPS	☑	☑	☑	☑	☑	☑	
OfficeExtend	☑		☑				☑
FlexConnect	☑	☑	☑	☑	☑	☑	☑*
WirelessMesh	☑*	☑		☑	☑	☑	
Future-proof Modularity	☑						
Data Uplink (Mbps)	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100
Power	802.3af	802.3af	802.3af	802.3af	802.3af	802.3af	100 to 240 VAC, 50-60 Hz
Temperature Range in Celsius	(i) -0 to 40° C (e) -20 to 55°C	(i) -0 to 40° C (e) -20 to 55°C	(i) -0 to 40° C (e) -20 to 55°C	-20 to 55°C	-0 to 40°C	-0 to 40°C	0 to 40°C
Wi-Fi Standards	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、有線 / ワイヤレス アクセス、キャンパス、ブランチ ネットワークの包括的なライフ サイクル管理、エンドユーザの接続性に対する豊富な可視性、およびアプリケーション パフォーマンスの保証問題のための単一の統合ソリューションを提供します。Cisco Prime Infrastructure は、新しいサービスのロールアウト、モバイル デバイスのセキュアなアクセスと管理、企業 IT への「個人所有デバイスの持ち込み」（BYOD）の実現を加速します。アプリケーション パフォーマンスの

可視性とネットワーク制御と緊密に結びつ蹴られたクライアントの認識によって、Cisco Prime Infrastructure は、経験に基づいた妥協のないエンドユーザの品質を保証します。Cisco Identity Services Engine（ISE）とのさらなる統合の深化により、セキュリティおよびポリシー関連の問題に関する可視性が拡張され、これらを解決するための明確な手順を含むクライアントのアクセス問題の全体像が示されます。

Cisco Prime Infrastructure は、次のような高レベルのタスク領域を含むライフ サイクル ワークフローに整理されます。

- デザイン：デザイン フェーズは、機能またはデバイス パターン、あるいはテンプレートの全体のデザインに焦点を当てます。デザイン領域は、設定テンプレートなどの再利用可能なデザイン パターンを作成する場所です。Cisco Prime Infrastructure では、事前定義されたテンプレートが提供されますが、独自のテンプレートを作成することもできます。これらのパターンおよびテンプレートは、ライフサイクルの展開フェーズでの使用を目的としています。
- 導入：導入フェーズは、以前に定義されたデザインまたはテンプレートをネットワークに導入することに焦点を当てます。導入領域は、デザイン フェーズで作成されたテンプレートを使用して、機能の導入方法を指定する場所です。展開段階では、テンプレートに定義した設定を 1 つまたは複数のデバイスにプッシュできます。
- 操作：操作領域は、毎日ネットワークをモニタし、ネットワーク デバイス インベントリと設定管理に関連する他の日常の操作またはアドホックの操作を実行する場所です。[Operate] タブには、毎日のモニタリング、トラブルシューティング、保守、および操作に必要なダッシュボード、Device Work Center、およびツールが含まれています。
- レポート：Cisco Prime Infrastructure では、システムおよびネットワーク ヘルスを監視し、問題をトラブルシューティングするために使用できるレポートを提供します。Cisco Prime Infrastructure の Report Launchpad では、レポートへのアクセスとすべてのタイプのレポート機能のスケジューリングを行います。
- 管理：管理領域は、システム設定を指定し、アクセス コントロールを管理し、データ収集設定を指定する場所です。

モビリティ グループ、AP グループ、および RF グループ

Cisco Unified Wireless Network における重要な*グループ*の概念には、次の 3 種類があります。

- モビリティ グループ
- AP グループ
- RF グループ

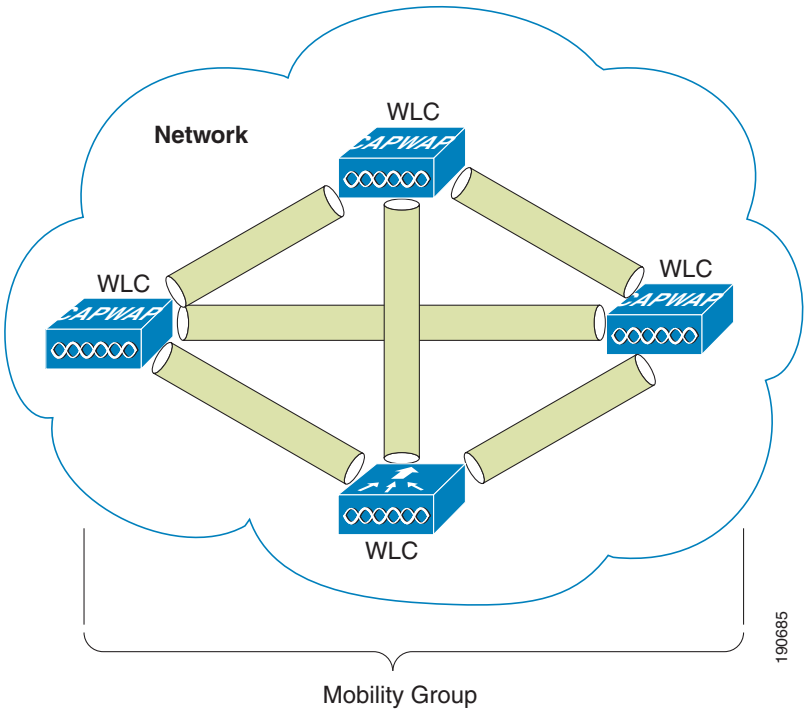
この項では、Cisco Unified Wireless Network におけるこれらのグループの目的と用途について説明します。

モビリティ グループ

モビリティ グループとは、エンド クライアント、AP、および RF といった重要な情報を共有することで 1 つの仮想 WLC として機能する WLC のグループのことです。モビリティ ドメイン内の特定の WLC は、その WLC が直接接続されている AP やクライアントから得た情報だけではなく、モビリティ グループ全体の他のメンバから受け取ったデータにも基づいた判断を下すことができます。

モビリティ グループは、図 2-6 に示すように、メンバ WLC 間にメッシュ状の認証トンネルを形成し、WLC がグループ内のほかの WLC に直接問い合わせることができるようにします。

図 2-6　WLC モビリティ グループ



モビリティ グループの定義

モビリティ グループは簡単に作成できて、これについては詳しく文書化されています。ただし、以下に示すいくつかの重要な留意事項があります。

- 1 つのモビリティ グループには、最大 24 台の標準 WLC（Cisco 2500、5508、WiSM-2、7500、8500、仮想 WLC、WLCM2 シリーズ）を含めることができます。1 つのモビリティ グループには、最大 24 基の Wireless Services Module（WISM-2）ブレードを設定できます。したがって、1 つのモビリティ グループでは、最大 24000 の AP がサポートされます。企業で、複数の WLC および AP が構成されていることがありますが、これらは別のモビリティ グループのメンバとして設定する必要があります。
- WLC リリース 5.1 では、最大 72000 の AP を持つ 1 つのモビリティ グループに最大 72 の WLC（WLC あたり 1000 AP）を設定することができます。
- WLC は、同一のモデルやタイプでなくても、モビリティ グループのメンバにできます。Cisco 2500 シリーズ コントローラ、Cisco Flex 7500、Cisco 5500 シリーズ コントローラ、仮想コントローラ、8500 シリーズ、WiSM-2、SRE 向け Cisco ワイヤレス コントローラ ソフトウェア、または Cisco ワイヤレス LAN コントローラ モジュールを自由に組み合わせてグループを構成できますが、実行されているソフトウェアのバージョンは同じでなければなりません。デバイス間でソフトウェアが異なっていてもモビリティ グループは機能しますが、統合ワイヤレス展開全体で機能の同一性を保証するために、共通のソフトウェア バージョンの使用を強く推奨します。
- モビリティ グループでは、グループ内のすべての WLC が同じ仮想 IP アドレスを使用する必要があります。
- 各 WLC には同一の *モビリティ ドメイン名*（グループ名）を使用します。また、WLC は、それぞれの [Static Mobility Members] リストでピアとして定義する必要があります。

- モビリティ グループ メンバ（WLC）の間でワイヤレス クライアントがシームレスにローミングできるようにするには、モビリティ グループを構成するすべての WLC で、特定の WLAN SSID とセキュリティ設定を同一に設定する必要があります。

モビリティ グループの用途

モビリティ グループは、別の WLC に接続している AP 間でのシームレスなクライアント ローミングを実現するために使用されます。モビリティ グループの主な目的は、無線カバレッジ エリアの包括的なビューを提供するために、複数の WLC 間に仮想 WLAN ドメインを作成することです。モビリティ グループの使用は、異なる WLC に接続された複数の AP が、カバレッジが*重複するように*展開されている場合にだけ効果的です。たとえば、キャンパスやブランチ、キャンパス内の複数のビル間など、それぞれ異なる WLC にアソシエートされている 2 つの AP が、物理的にまったく別の場所にあり、これらのカバレッジが重複（接触）していない場合には、モビリティ グループは有効ではありません。

モビリティ グループの例外

Cisco Unified Wireless Network ソリューションにより、ネットワーク管理者は、ネットワーク内のアンカー WLC とその他の WLC の間の静的なモビリティ トンネル（*自動アンカー*）を定義できるようになります。このオプションは、特に、ワイヤレス ゲスト アクセス サービスの展開時に使用します。

自動アンカー機能を使用した場合、指定されたアンカー WLC にマッピングできる WLC の数は、71 個未満です。外部 WLC は自動アンカーに接続されているため、外部 WLC どうしがモビリティ関係を確立することはありません。アンカー WLC では、静的モビリティ トンネルを必要とする外部 WLC ごとに*静的モビリティ グループ メンバ*エントリを定義する必要があります。同様に、静的モビリティ トンネルが設定されている外部 WLC のそれぞれについて、アンカー WLC を外部 WLC の*静的モビリティ グループ メンバ*として定義する必要があります。

動的なコントローラ間クライアント ローミングのサポートを目的とした場合、WLC は 1 つのモビリティ グループのメンバにしかなれません。自動アンカーとして設定されている WLC は、外部 WLC と同じモビリティ グループに属する必要はありません。WLC は、あるモビリティ グループのメンバであると同時に、別のモビリティ グループのメンバである外部 WLC を起点とする WLAN の自動アンカーとして機能するようにできます。

モビリティ アンカーの設定の詳細は、第 10 章「Cisco Unified Wireless Network ゲスト アクセス サービス」を参照してください。

AP グループ

典型的な展開シナリオでは、各 WLAN は WLC ごとに単一の動的なインターフェイスにマッピングされます。しかし、ここで、最大 500 台までの AP をサポートする 5508 WLC が使用される展開シナリオを考えてみてください。各 AP に 25 ユーザがアソシエートされているとします。その結果、125,000 人のユーザが 1 つの VLAN を共有することになります。お客様の設計によっては、サブネットのサイズを非常に小さくすることが要求される場合もあります。このような要求に対処するには、WLAN を複数のセグメントに分割するのも 1 つの方法です。Cisco AP グループ機能により、WLC 上の複数の動的インターフェイス（VLAN）で 1 つの WLAN をサポートできるようになります。そのためには、AP のグループを特定の動的インターフェイスにマッピングします。AP は、従業員のワークグループごとに論理的にグループ化するか、ロケーションごとに物理的にグループ化できます。図 2-7 は、サイト固有の VLAN に基づく AP グループの使用を示しています。

（注） AP グループでは、グループの境界を越えたマルチキャスト ローミングは許可されていません。詳細については、第 6 章「Cisco Unified Wireless のマルチキャスト設計」を参照してください。

図 2-7　AP グループとサイト固有の VLAN

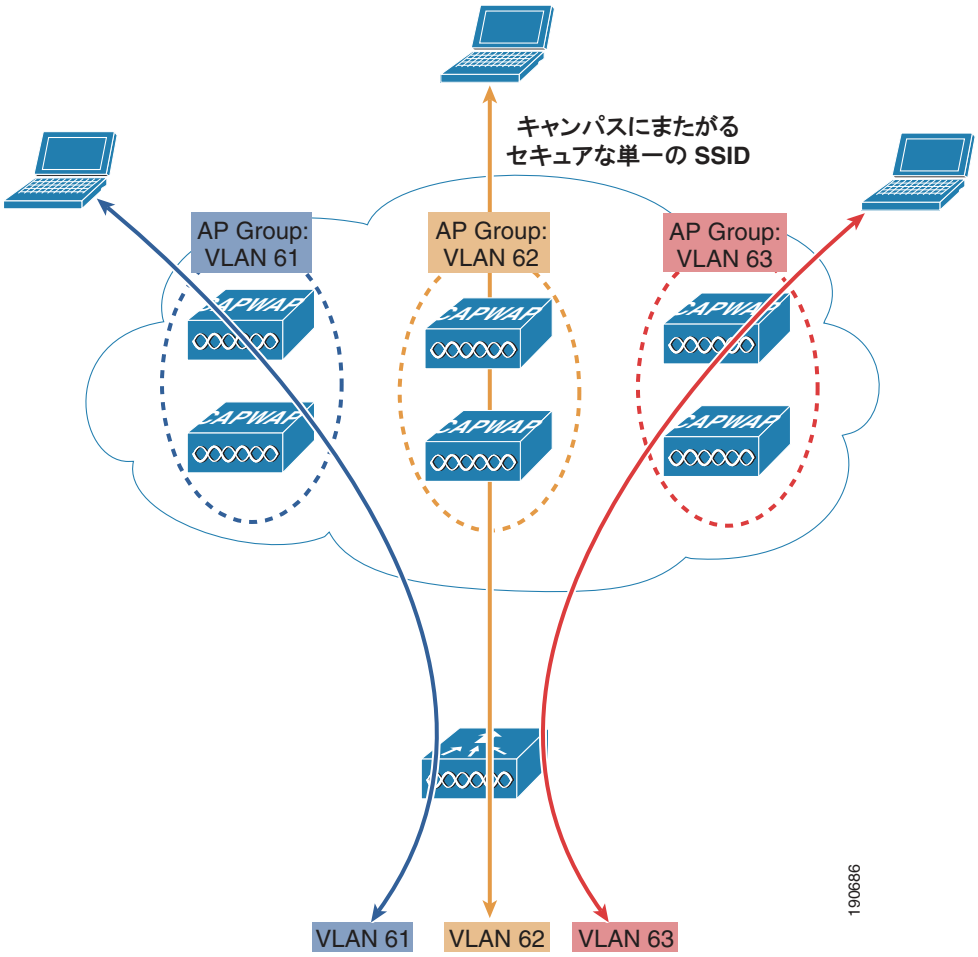


図 2-7 では、3 つの動的インターフェイスが設定され、それぞれがサイト固有の VLAN（61、62、および 63）にマッピングされています。サイト固有の VLAN およびアソシエートされた AP は、それぞれ AP グループ機能を使用して同一の WLAN SSID にマッピングされます。VLAN 61 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 61 IP サブネットで IP アドレスを取得します。同様に、VLAN 62 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 62 IP サブネットなどで IP アドレスを取得します。サイト固有 VLAN 間のローミングは、レイヤ 3 ローミング イベントとして WLC により内部的に処理されます。したがって、ワイヤレス LAN クライアントでは元の IP アドレスが維持されます。

RF グループ

RF グループ（*RF ドメイン*とも呼ばれる）も、展開にあたり考慮しなければならない重要な事項の 1 つです。RF グループとは、802.11b/g や 802.11a などの 802.11 PHY のタイプに基づいて、動的な無線リソース管理（RRM）の設定を一括して調整および計算する WLC のクラスタです。

802.11 PHY タイプごとに RF グループが存在します。WLC を RF ドメインにグループ化すると、ソリューションの動的な RRM アルゴリズムが複数の WLC で使用され、特定の RF ドメインの RRM がフロア、ビルディング、さらにキャンパス間で使用されるようになります。RF グループおよび RRM については、第 3 章「WLAN RF の設計に関する考慮事項」でさらに詳しく説明しますが、概要をまとめると次のようになります。

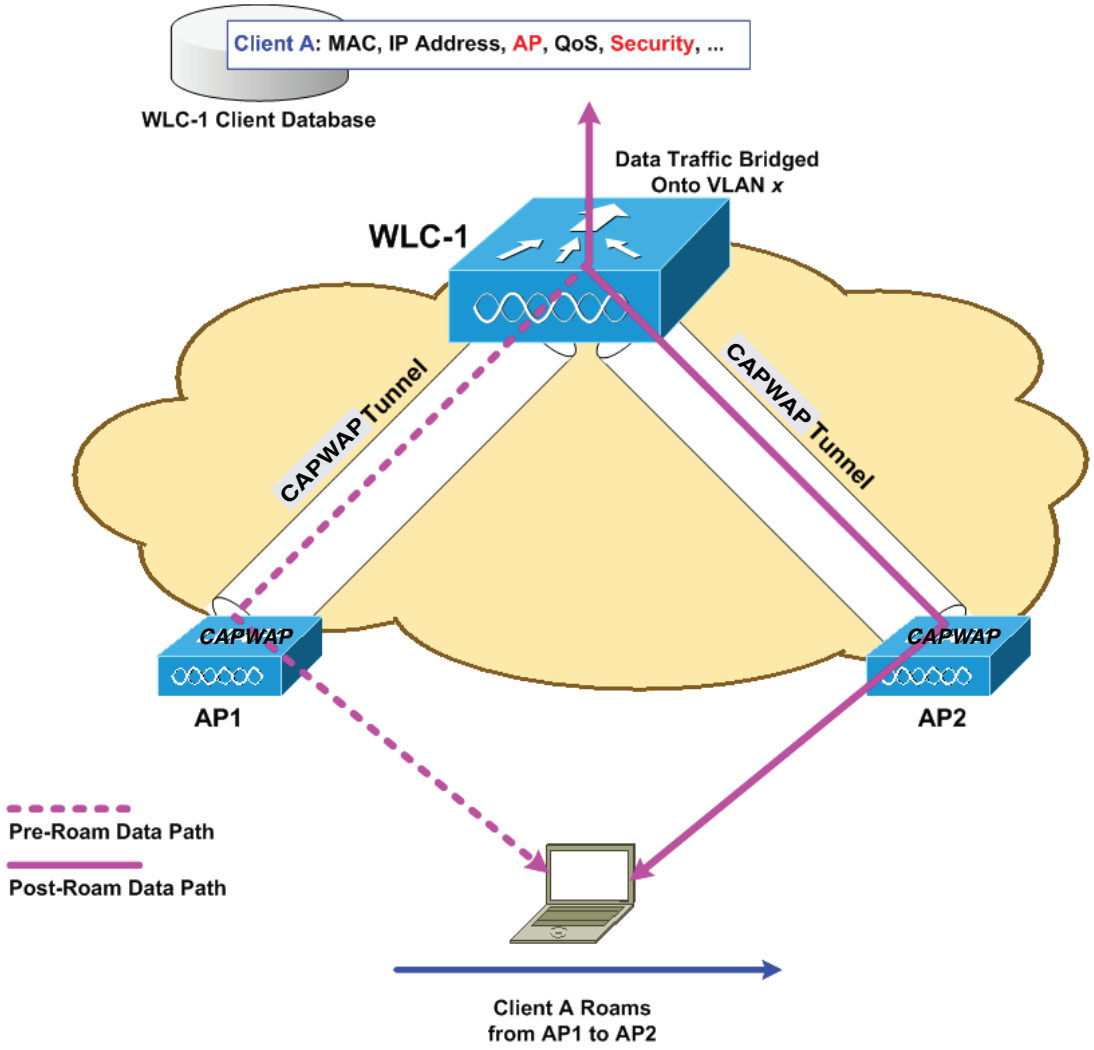
- CAPWAP AP は、定期的にネイバー メッセージを無線で送信します。これには、WLC の IP アドレスと、AP のタイムスタンプおよび BSSID からハッシュされた Message Integrity Check（MIC）が含まれています。
- ハッシュ アルゴリズムでは、共有秘密（RF グループ名）が使用されます。共有秘密は、WLC で設定され、各 AP にプッシュされます。同じ秘密を共有する AP は、MIC を使用して、互いに送信されたメッセージを検証できます。他の WLC に属する AP が、検証されたネイバー メッセージを -80 dBm 以上の信号強度で受信すると、その WLC は動的に RF グループのメンバになります。
- RF グループのメンバによって、RF グループの マスター電力およびチャネル スキームを管理する RF ドメイン リーダーが選ばれます。
- RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析し、マスター電力とチャネル計画が割り出されます。
- RRM アルゴリズム：
  - すべての AP 間の信号強度を -65 dBm に均一化（最適化）しようとします。
  - 802.11 相互チャネルの干渉およびコンテンションを回避しようとします。
  - 802.11 以外の干渉を回避しようとします。
- RRM アルゴリズムでは、ダンプニング計算を使用してシステム全体の動的な変更を最小限に抑えます。最終的には、絶えず変動する RF 環境に対応する、最適に近い電力とチャネル計画が動的に割り出されます。
- RF グループ リーダーおよびメンバは、指定された更新間隔（デフォルトでは 600 秒）で RRM メッセージを交換します。更新間隔の合間に、RF グループ リーダーは各 RF グループ メンバにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。1 つの RF グループあたりの最大コントローラ数は 20 です。

ローミング

モビリティ（ローミング）は、できるだけ遅れることなく、確実かつスムーズに、ある AP から別の AP へアソシエーションをシームレスに維持するワイヤレス LAN クライアントの機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントが AP にアソシエートして認証すると、コントローラは、クライアント データベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC および IP アドレス、セキュリティ コンテキストおよびアソシエーション、QoS コンテキスト、WLAN、SSID、およびアソシエートされた AP が含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。図 2-8 は、両方の AP が同じコントローラに接続されたときにある AP から別の AP にローミングするワイヤレス クライアントを示します。

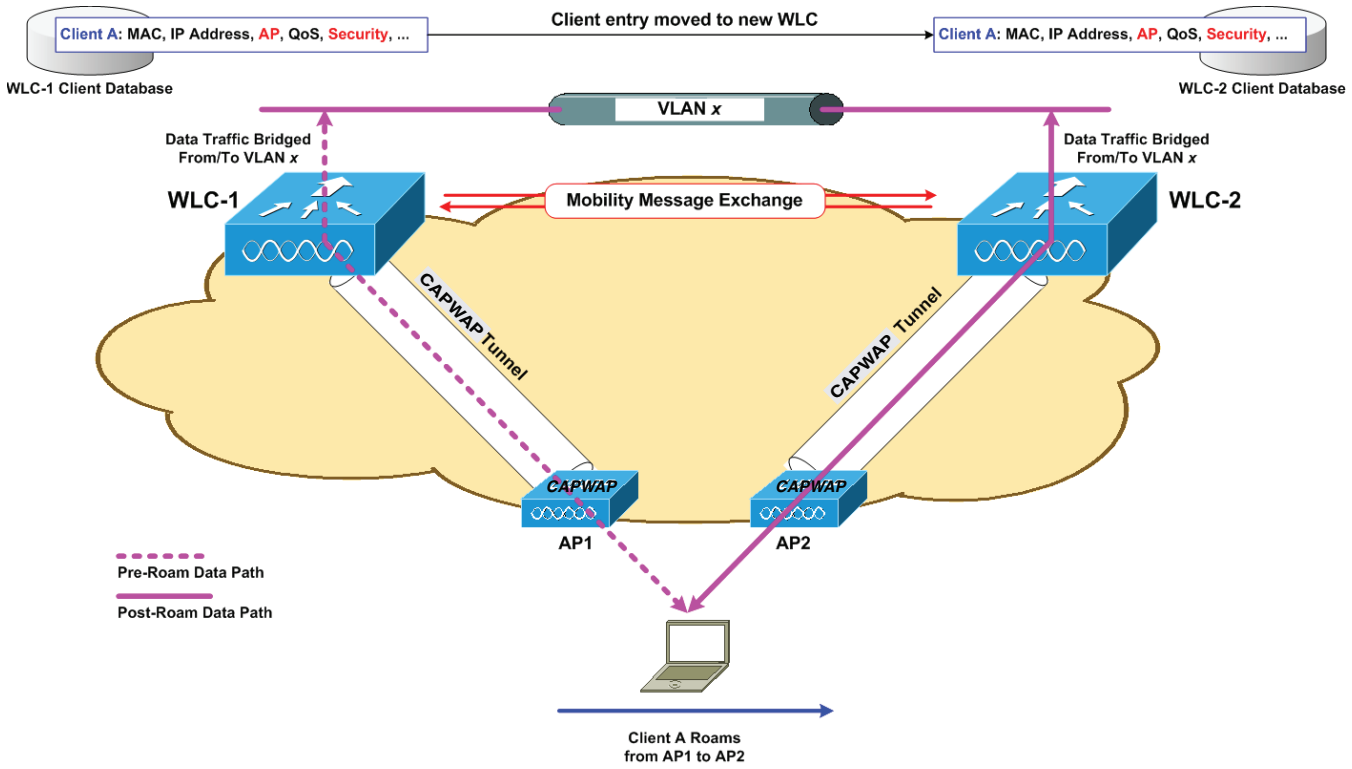
図 2-8　コントローラ内ローミング



ワイヤレス クライアントがそのアソシエーションをある AP から別の AP に移動するときには、コントローラは新規にアソシエートされた AP を含むクライアント データベースをアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

しかし、クライアントが 1 つのコントローラに接続された AP から別のコントローラに接続された AP にローミングする際には、プロセスはより複雑になります。また、同一のサブネット上でこれらのコントローラが動作しているかどうかによっても異なります。図 2-9 は、コントローラのワイヤレス LAN インターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを示します。

図 2-9　コントローラ間ローミング

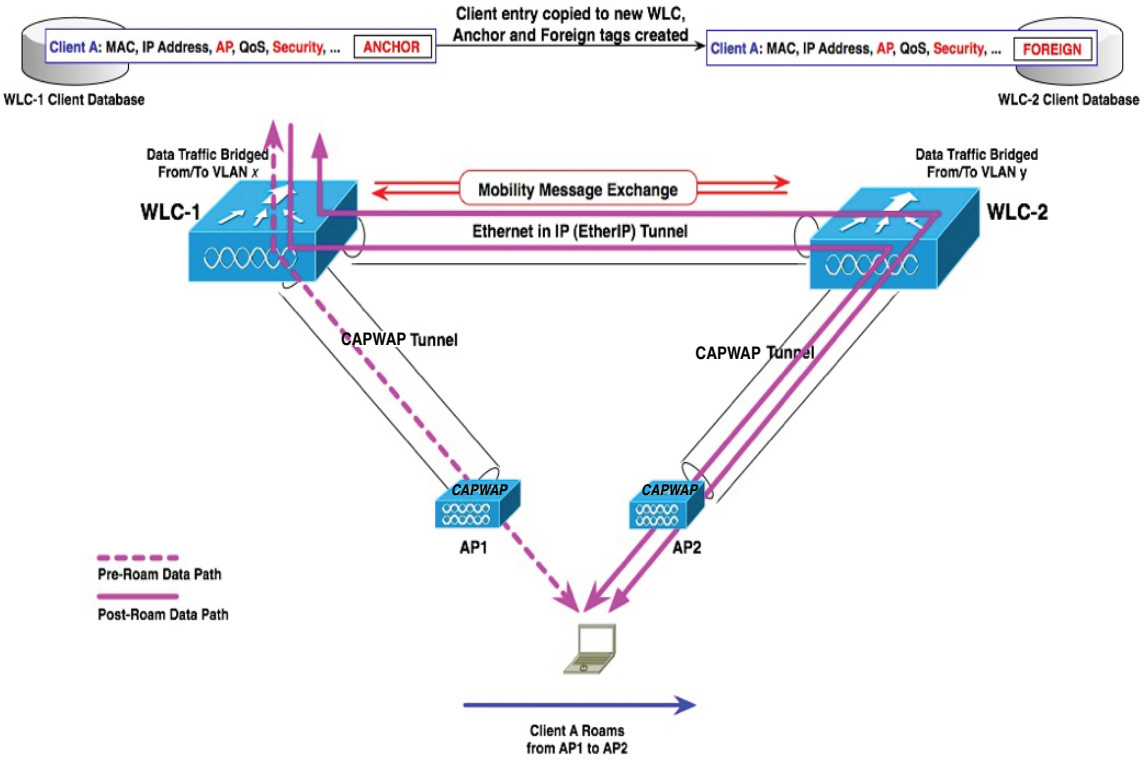


クライアントが新たなコントローラに接続された AP へアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たな AP に対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

（注）　802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 2-10 は、コントローラのワイヤレス LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを示します。

図 2-10　サブネット間ローミング



サブネット間ローミングは、コントローラがクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しいコントローラに移動するのではなく、元のコントローラのクライアント データベース内で該当クライアントに*アンカー*エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しいコントローラ内で*外部*エントリのマークが付けられます。ローミングはワイヤレス クライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両コントローラの WLAN に同一のネットワーク アクセス権限を設定し、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

（注）　クライアントが Web 認証状態でローミングする場合、クライアントはモバイル クライアントして見なされるのではなく、別のコントローラ上の新しいクライアントとして見なされます。

（注）　インターフェイスがタグなしの場合、ネイティブ IPv6 クライアントではシームレスなモビリティはサポートされません。

WLC でのブロードキャストおよびマルチキャスト

この項では、WLC によるブロードキャストおよびマルチキャスト トラフィックの処理および WLC が設計に与える影響について説明します。

図 2-11 は、基本的な 802.11 のブロードキャスト動作またはマルチキャスト動作を図示したものです。この例のクライアント 1 が 802.11 のブロードキャスト フレームを送信すると、そのフレームは AP にユニキャストされます。その後、AP は、そのフレームを、ワイヤレス インターフェイスと有線インターフェイスの両方にブロードキャストとして送信します。

図 2-11 802.11 ブロードキャスト / マルチキャスト

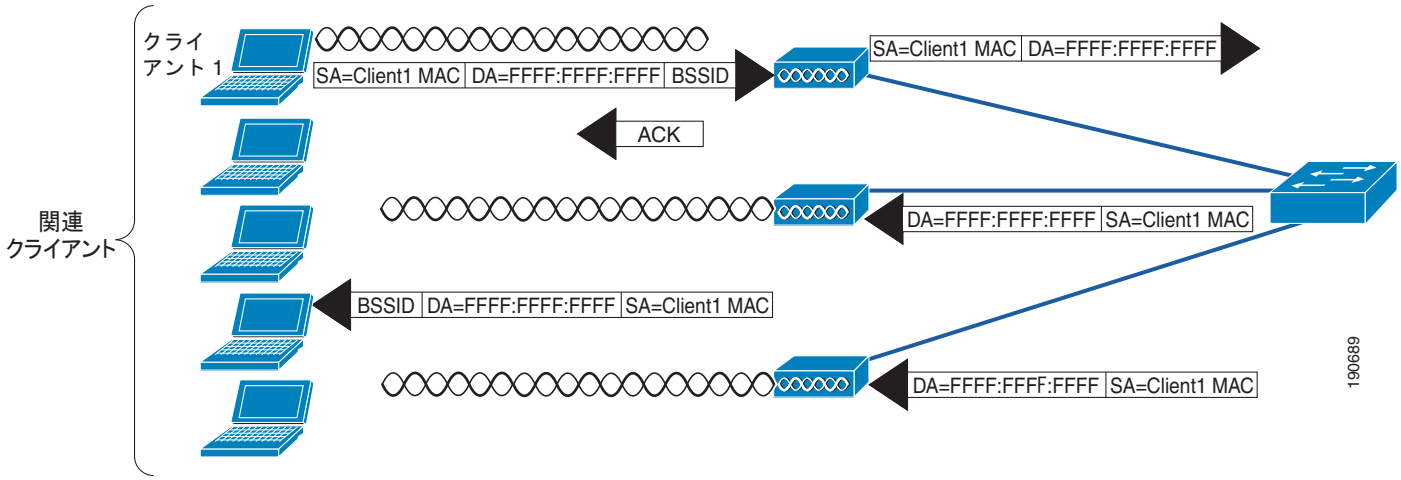
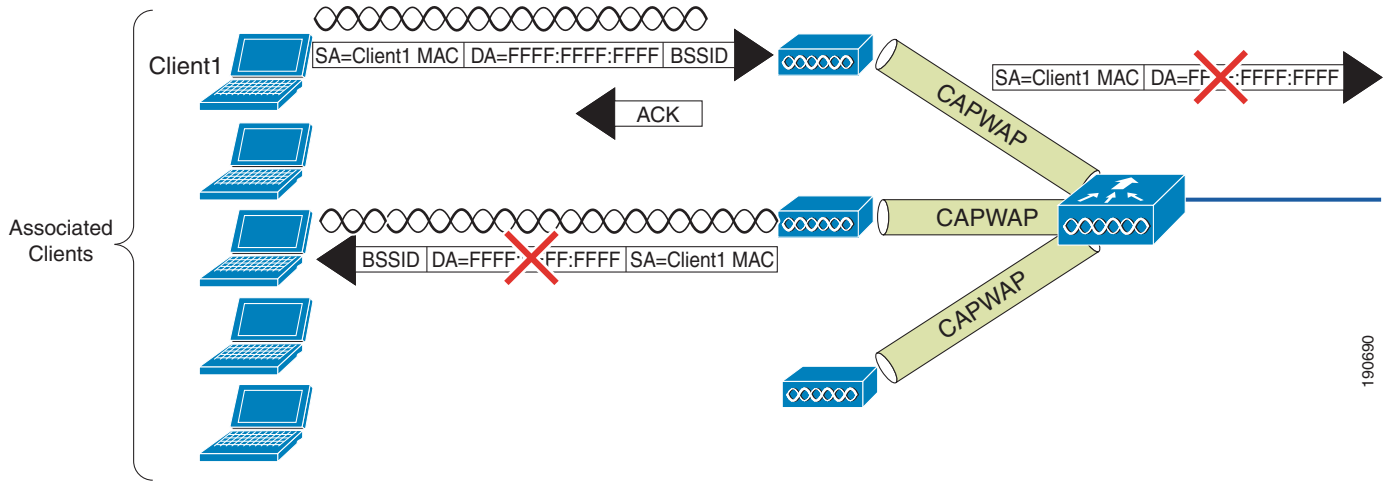


図 2-11 に示されているように、AP と同じ有線 VLAN 上に別の AP がある場合、それらの AP は、有線ブロードキャスト パケットをワイヤレス インターフェイスに転送します。

WLC の CAPWAP *スプリット MAC* 方式では、図 2-14 に示すように、別の方法でブロードキャスト トラフィックを処理します。この場合、クライアントからブロードキャスト パケットが送信されると、AP または WLC は、そのパケットを WLAN に転送せず、ブロードキャスト メッセージと考えられるすべてのメッセージのサブセットのみを、WLC で指定された WLAN の有線インターフェイスに転送します。

図 2-12WLC ブロードキャストのデフォルトの動作



（注）　どのような状況でどのようなプロトコルが転送されるかについては、次の項で説明します。

WLC ブロードキャストおよびマルチキャストの詳細

ブロードキャストおよびマルチキャスト トラフィックは、通常、WLAN ネットワーク内で特別に処理する必要があります。このトラフィックは最小限の共通ビットレートで送信しなければならないので、WLAN に余計な負荷がかかるからです。これによって、アソシエートされているすべてのワイヤレス デバイスで、ブロードキャストまたはマルチキャスト情報を確実に受信できるようになります。

WLC のデフォルトの動作では、ブロードキャストおよびマルチキャスト トラフィックは、WLAN からその他のワイヤレス クライアント デバイスに送信されないようにブロックされます。WLC は、クライアントの動作に影響を与えずにこの処理を実行できます。これは、ほとんどの IP クライアントは、ネットワーク情報を取得する（DHCP）以外の理由では、ブロードキャストまたはマルチキャスト タイプのトラフィックを送信しないからです。

DHCP

WLC は、アソシエートされている WLAN クライアントの DHCP リレー エージェントとして機能します。L3 クライアント ローミング中を除き、この WLC は、クライアント DHCP 要求を、ローカルに設定された DHCP サーバ、またはアップストリーム DHCP にユニキャストします（詳細については後述します）。DHCP サーバの定義は動的インターフェイスごとに設定されます。その後、このインターフェイスは、1 つまたは複数の WLAN にアソシエートされます。DHCP リレー要求は、指定された動的インターフェイスのソース IP アドレスを使用して、このインターフェイス経由で転送されます。WLC は、特定のインターフェイスまたは WLAN に対してどの DHCP サーバを使用するかがわかっているため、有線またはワイヤレス インターフェイスにクライアント DHCP 要求をブロードキャストする必要はありません。

この方法により、次のことが実現されます。

- DHCP 要求を WLC の外にブロードキャストする必要がなくなります。
- WLC は DHCP プロセスの一部となり、その結果、接続されている WLAN クライアントの MAC アドレスや IP アドレスの関係がわかるようになります。その後、WLC は DHCP ポリシーを施行し、IP スプーフィングやサービス拒絶（DoS）攻撃を軽減できるようになります。

VideoStream

VideoStream 機能では、無線でブロードキャスト フレームをユニキャスト ストリームに変換することで、IP マルチキャスト ストリームの無線配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。VideoStream はすべての Cisco AP でサポートされています。

次に、コントローラ上で VideoStream を設定するための推奨ガイドラインを示します。

- AP1100 および AP1200 は信頼できるマルチキャスト機能をサポートしていません。
- マルチキャスト機能が有効であることを確認します。コントローラ上の IP マルチキャストは multicast-multicast モードで設定することを推奨します。
- クライアント マシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。
- AP がコントローラに接続されていることを確認します。
- クライアントが 802.11a/n の速度で設定された WLAN に関連づけられることを確認します。

その他のブロードキャストおよびマルチキャスト トラフィック

前述のとおり、WLC は、デフォルトでワイヤレス ユーザに対してブロードキャストやマルチキャストを転送しません。第 6 章「Cisco Unified Wireless のマルチキャスト設計」で説明したとおり、マルチキャスト転送が有効になっている場合は、WLC の接続先インターフェイスで生成されるマルチキャスト トラフィックを最小限に抑えるための処理を実行する必要があります。

WLAN により明示的にサポートされるマルチキャスト アドレス グループを制限するために、標準的な対策をすべて講じる必要があります。マルチキャストが有効になっている場合、これは事実上グローバルな設定です。つまり、WLAN がマルチキャストを必要としているかどうかに関係なく、設定されているすべての WLAN で有効になっていることを意味します。Cisco Unified Wireless Network ソリューションでは、データ リンク レイヤとネットワーク レイヤのマルチキャスト トラフィックは区別されません。どちらも、特定のマルチキャスト トラフィックをフィルタできる能力は WLC にはありません。したがって、次の手順の追加を考慮する必要があります。

- WLC に接続しているインターフェイスで CDP を無効にします。
- WLC に接続されている VLAN で、受信した CDP および HSRP トラフィックをポート フィルタします。
- マルチキャストは、ゲスト WLAN を含む WLC のすべての WLAN で有効になるため、リンク レイヤのマルチキャスト セキュリティを含むマルチキャスト セキュリティを考慮する必要があることを覚えておいてください。

設計上の考慮事項

Cisco Unified Wireless Network 展開の設計における主な考慮事項は、AP 接続と WLC のロケーションおよび接続です。この項では、これらのトピックについて簡単にまとめ、必要に応じて標準的な推奨事項について説明します。

WLC のロケーション

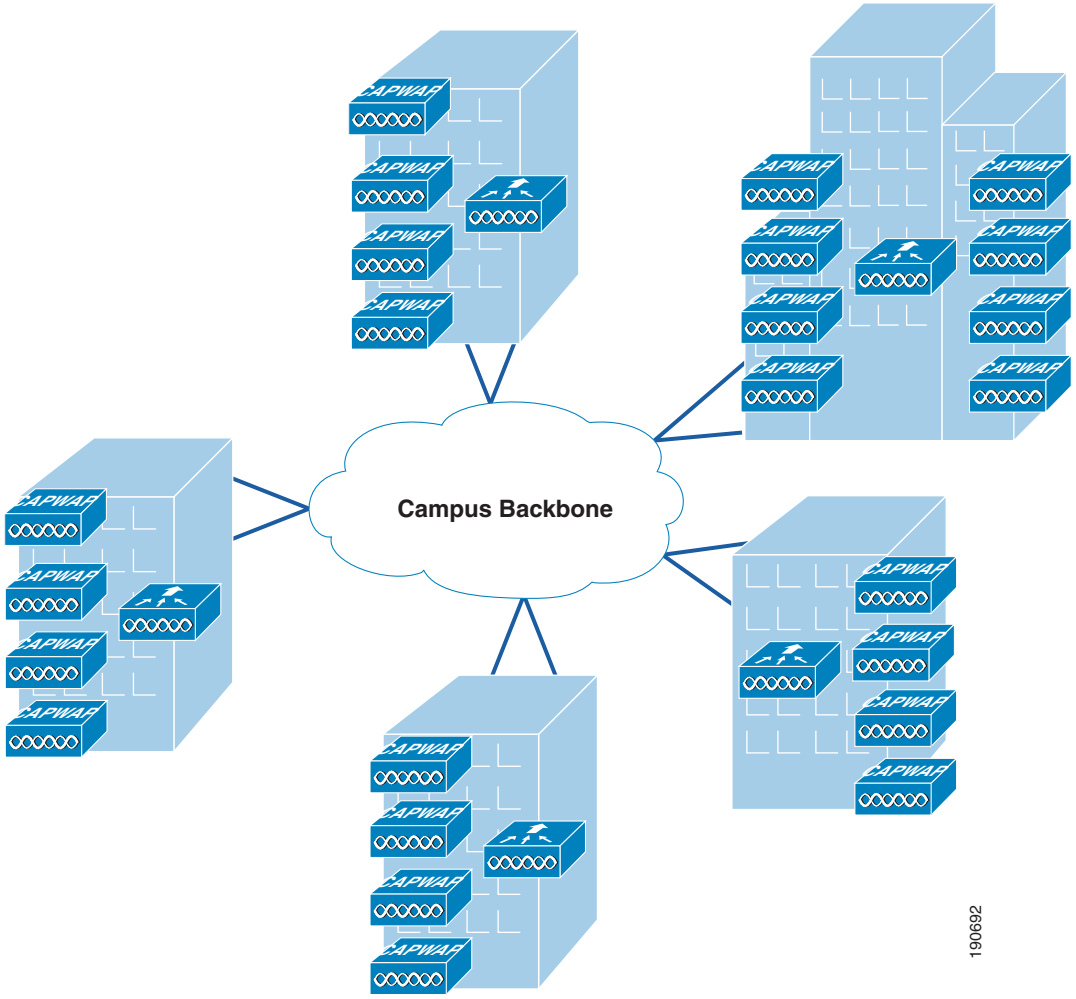
Cisco Unified Wireless Network ソリューションでは、次の項で説明するように、分散型または中央集中型により WLC を展開することができます。

分散型の WLC 展開

図 2-13 は分散型の WLC 展開を示しています。このモデルでは、WLC はキャンパス ネットワーク全体、通常はビルディングごとに配置され、そのビルディングに存在する AP を管理します。WLC をキャンパス ネットワークに接続するために、ビルディング内の分散ルータが使用されます。このシナリオでは、AP と WLC の間の CAPWAP トンネルは通常ビルディング内にとどまります。

WLAN カバレッジがビルディング間で重複しない限り、分散型の WLC をそれぞれ、別々の RF グループおよびモビリティ グループに設定できます。

図 2-13　　分散型の WLC 展開

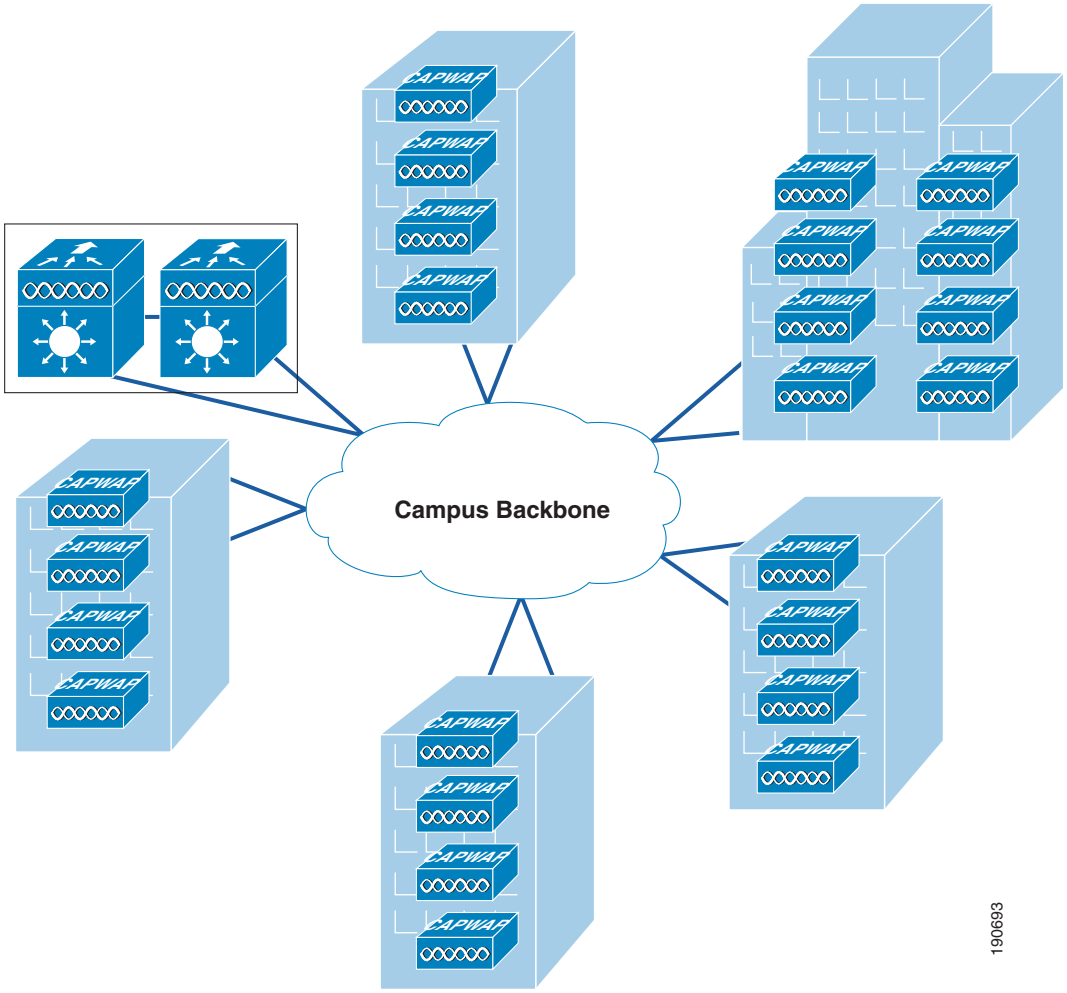


中央集中型の WLC 展開

図 2-14 は中央集中型の WLC 展開を示しています。このモデルでは、WLC は企業ネットワークの集中化された場所に配置されます。この展開モデルでは、キャンパス バックボーン ネットワークを経由するために AP/WLC CAPWAP トンネルが必要です。下図の例では、中央集中型の WLC が特定のビルディング内には示されていないことに注意してください。中央集中型の WLC クラスタは専用スイッチ

ブロック経由でキャンパス コアに接続されます。キャンパス コアは、通常、データセンターと同じビルディングにあります。データセンターと WLC クラスタでは、通常、ネットワークおよびセキュリティ要件が異なるので、WLC をデータセンターのスイッチ ブロックに直接接続してはいけません。

図 2-14　　中央集中型の WLC 展開



WLC の中央集中化

シスコでは、一般的に、キャンパス環境全体の中心的な位置に WLC を展開することを推奨しています。モビリティ グループとレイヤ 3 ローミングを必要とする分散展開モデルは十分に証明されていますが、レイヤ 3 ローミングに関連するマルチキャスト サポートに現在不十分な点があるため、推奨されていません。これらへの対策が行われた場合、分散展開モデルの検討を妨げる障壁の大半は解消されます。

レイヤ 3 ローミングに対応する最善策は、レイヤ 3 ローミングを使用せざるを得ないような展開シナリオを避けることです。現時点では、WISM モデルの持つ拡張性、および WLC の提供するブロードキャストまたはマルチキャスト抑制機能のため、大きなモビリティ サブネットの方が実現性が高くなっています。

WLC インフラストラクチャを中央集中化することにより、容量管理はさらに簡単になり、費用対効果も向上します。また、WLAN はよりミッション クリティカルになるため、中央集中型の実装により、可用性の高い WLC トポロジを作成しやすくなります。中央集中化により、容量管理や高可用性の問題に対応しなければならない場所が減少します。

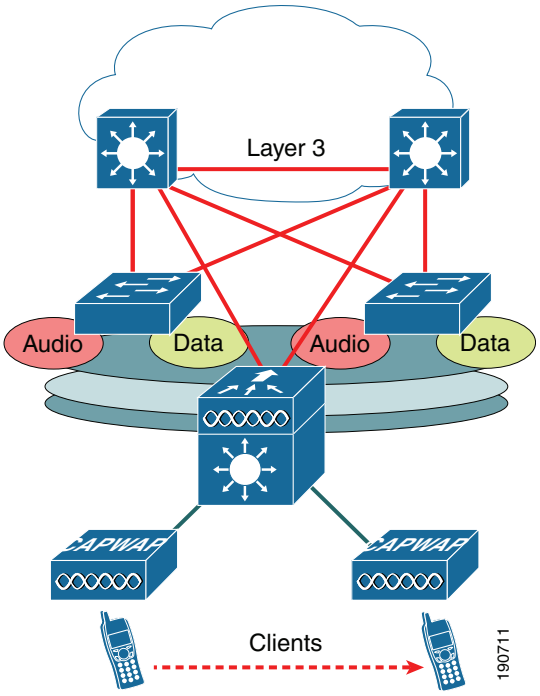
WLC を他のインフラストラクチャ コンポーネントと統合する場合にも同様の原理が当てはまります。中央集中型の WLC により、統合ポイントおよび統合デバイスの数を最小限に抑えられます。たとえば、NAC アプライアンスのようなインライン セキュリティ デバイスの実装を決定したとき、集中化された WLC の場合は統合ポイントが 1 か所ですが、分散ソリューションの場合は統合ポイントが *n* か所になります（この場合、*n* は、WLC の展開箇所の数を示します）。

要約すると、中央集中型の WLC 展開の使用が推奨されるということです。中央集中型の WLC 展開を計画する場合、WLC に直接接続される有線ネットワーク インフラストラクチャの保護を考慮する必要があります。これは、WLC は基本的に、接続さえしていなければ*ネットワーク アクセス*およびこれに伴う脆弱性にさらされることのないような企業トポロジ内の場所にある*アクセス* ネットワークを接続するからです。したがって、アクセス レイヤ ネットワーク デバイスに関連する一般的なセキュリティ上の配慮事項をすべて検討する必要があります。たとえば、WISM-2 をベースとする展開では、DoS 攻撃やトラフィック ストームに対する保護などの機能を検討する必要があります。これは、多数のエンド ユーザに対してさまざまな WLAN サービスを提供すると同時に、複数レイヤにわたるマルチファンクション Catalyst 6500 スイッチ プラットフォームのバックプレーンに直接接続されている WISM-2 が果たす役割は大変大きいからです。

分散型の WLC ネットワーク接続

図 2-15 レイヤ 3 に接続された WLC（この場合は 3750G）では、WLAN 関連のソフトウェアおよび設定を 1 つのデバイスに分離し、他のアクセス レイヤ ルーティング デバイスと同じルーティング設定を使用してディストリビューション レイヤに接続できます。

図 2-15　　レイヤ 3 に接続された WLC



トラフィックの負荷と有線ネットワークのパフォーマンス

Cisco Unified Wireless Network ソリューションを展開する場合に、次のような疑問が生じることがよくあります。

- 有線バックボーンに対する CAPWAP トラフィックの影響または負荷
- Unified Wireless 展開をサポートするために必要な最低限のパフォーマンス要件
- ネットワークのトラフィック負荷に関連して、分散型の WLC 展開と中央集中型の WLC 展開の相対的な利点

ネットワークのトラフィック ボリューム全体に対して CAPWAP トラフィックが与える影響を検証するうえで、考慮する点は主に 3 つあります。

- CAPWAP コントロール トラフィックのボリューム
- トンネリングによって生じるオーバーヘッド
- トラフィック処理

CAPWAP コントロール トラフィックのボリューム

CAPWAP コントロールに関連するトラフィックのボリュームは、ネットワークの実際の状態によって異なります。たとえば、通常ソフトウェアのアップグレード中や WLC のリブート中は多くなります。しかし、トラフィックの調査では、CAPWAP コントロール トラフィックがネットワークにかける平均的な負荷は約 0.35 Kb/sec であることが判明しています。このトラフィックは、ほとんどのキャンパスで無視できる量であり、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

トンネリングによって生じるオーバーヘッド

CAPWAP トンネルによって、WLAN クライアントとの間で送受信される通常の IP パケットに 44 バイトが追加されます。標準的な企業で見られる平均パケット サイズが約 300 バイトであることを考えると、約 15% のオーバーヘッドとなります。このオーバーヘッドは、ほとんどのキャンパスで無視できる量であり、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

トラフィック エンジニアリング

中央集中型の WLC にトンネルされた WLAN トラフィックはすべて、WLC のロケーションからネットワークでのデスティネーションにルーティングされます。トンネルの距離と WLC のロケーションによっては、これ以外の方法では、WLAN クライアント トラフィックは指定された宛先への最適なパスをたどって進まない可能性があります。従来のアクセス トポロジや分散型の WLC 展開の場合、クライアント トラフィックはエッジから入り、宛先アドレスに基づいてそのポイントから適切にルーティングされます。

しかし、中央集中型の展開モデルに関連する長いトンネルや潜在的に効率の悪いトラフィック フローは、クライアント トラフィックの大半が宛先としているネットワークの部分（データセンターなど）に WLC を配置することで、ある程度、緩和できます。企業のクライアント トラフィックのほとんどがデータセンターのサーバに向かうことと、企業のバックボーン ネットワークが低遅延であることを考えると、効率の悪いトラフィック フローに関連するオーバーヘッドは無視できますし、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

ほとんどの企業において、WLAN の導入によって、新しいアプリケーションがすぐに必要になることはありません。したがって、Cisco Unified Wireless Network を追加するだけで、キャンパスのバックボーン トラフィックの量に深刻な影響が出ることはありません。

AP 接続

AP は、エンド ユーザ（802.11 クライアント）とは別のネットワーク上になければなりません。これは、インフラストラクチャ管理インターフェイスはエンド ユーザとは別のサブネット上にあるべきであると定義している一般的なベスト プラクティスのガイドラインと一致しています。さらに、Catalyst Integrated Security Features（CISF）を CAPWAP AP スイッチ ポートで有効にして、WLAN インフラストラクチャの保護を強化することを推奨します （FlexConnect AP 接続については、第 7 章「FlexConnect」を参照）。

展開を容易にするために、最新の WLC アドレス情報を提供する簡単なメカニズムを備えていることから、AP アドレス割り当て方法としては、一般に DHCP が推奨されています。AP に静的 IP アドレスを割り当てることができますが、詳細な計画および個々の設定が必要になります。静的 IP アドレスを設定できるのは、コンソール ポートを備えた AP だけです。

Cisco Unified Wireless Network に WLAN QoS 機能を効率的に提供するには、CAPWAP AP と WLC の間の接続を提供する有線ネットワーク全体で QoS も有効にしておく必要があります。

運用および保守

ここでは、Cisco Unified Wireless Network 開の運用および保守を簡単にするための展開上の一般的な考慮事項と推奨事項について説明します。

WLC ディスカバリ

AP のための、次のようなさまざまな WLC ディスカバリ メカニズム（前述）により、CAPWAP AP の初期展開は非常に簡単になります。次のオプションがあります。

- 制御された環境での WLC を使用して前もって行われる CAPWAP AP のステージング（プライミング）
- 自動ディスカバリ メカニズムの 1 つ（DHCP または DNS）を使用し、難しい設定なしに行われる展開

自動ディスカバリは非常に便利ですが、ネットワークへの接続後は、AP の接続先 WLC の制御は通常、ネットワーク管理者により行われます。その後、管理者により、通常動作中の特定の AP の *プライマリ* WLC の定義や、バックアップのためのセカンダリ WLC およびターシャリ WLC の設定が行われます。

AP 分散

典型的な初期 WLAN 展開では、AP は、各 WLC の負荷に応じて、使用可能な WLC 全体に AP 自体を自動的に分散します。このプロセスにより展開は簡単になりますが、いくつかの運用上の理由から、自動分散の使用はお勧めしません。

物理的に同じ場所にある AP は、同じ WLC に接続する必要があります。これにより、一般的な管理、運用、および保守が簡単になり、担当者はさまざまな運用上の作業がその場所に与える影響を抑えることができるようになるほか、WLC 内でのローミングと WLC 間でのローミングのいずれにかかわる WLAN の問題を特定の WLC とすばやく関連付けることができるようになります。

複数の WLC にわたる AP 分散を制御するために使用される要素は、次のとおりです。

- プライマリ、セカンダリ、ターシャリ WLC 名：各 AP は、プライマリ、セカンダリ、およびターシャリ WLC 名で設定できます。これにより、モビリティ グループの WLC 間の負荷の変化に関係なく、AP が接続するモビリティ グループ内の最初の 3 つの WLC が決まります。
- マスター WLC：初めて AP がモビリティ グループの WLC に接続するときには、AP にはプライマリ、セカンダリ、およびターシャリ WLC は設定されていません。したがって、既知の WLC 負荷に応じて、どの WLC（モビリティ グループ内にある）ともパートナーになることができます。WLC がマスター WLC として設定されている場合、プライマリ、セカンダリ、およびターシャリ WLC 定義を持たない AP はすべて、マスター WLC に接続されます。これにより、運用担当者は、新しく接続された AP を簡単に見つけられるようになります。また、プライマリ、セカンダリ、およびターシャリ WLC 名前パラメータを定義して、AP が稼働状態になるタイミングを制御できます。