



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、企業で Cisco Unified Wireless 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。

- LWAPP
- ローミング
- ブロードキャストおよびマルチキャストの処理
- 製品の選択
- 展開に関する考慮事項

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 テクノロジーについて詳しく説明した資料としては、『*Deploying Cisco 440X Series Wireless LAN Controller*』

(<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>) をお勧めします。

LWAPP の概要

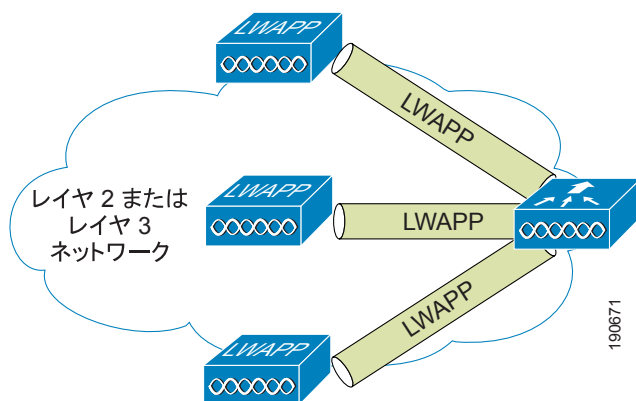
Lightweight Access Point Protocol (LWAPP; Lightweight アクセス ポイント プロトコル) は、シスコの中央集中型 WLAN アーキテクチャの基盤となるプロトコルです。このプロトコルは、WLAN の設定や管理のほか、中央集中型 WLAN コントローラ (WLC) と WLAN クライアントの間のトラフィックのトンネリングの機能を提供します。図 2-1 は、基本的な中央集中型 WLAN アーキテクチャの概略図です。この図では、LWAPP AP は LWAPP 経由で WLC に接続されています。



(注)

WLAN の基本機能は同じであるため、WLC という用語は、一般的にすべての Cisco WLAN コントローラを表すために使用されています。コントローラがスタンドアロン アプライアンス、WLC モジュールを持つ ISR、サービス モジュールまたは統合 WLC を持つ Catalyst スイッチのいずれであっても関係ありません。

図 2-1 WLC に接続された LWAPP AP



LWAPP 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、この文書では、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。

LWAPP の主な機能は、以下のとおりです。

- スプリット MAC トンネル
- L2 または 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

LWAPP プロトコル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 LWAPP 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 2-2c は、スプリット MAC の概念を図に表したものです。

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。図 2-2a を参照してください。802.11 規格では、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 1 つの Extended Service Set (ESS) を割り当てることができます。そして、そのように複数の AP が同じ ESS 識別子 (ESSID; 通常は「SSID」と言う) を使用することで、WLAN クライアントがそれら複数の 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。図 2-2b を参照してください。

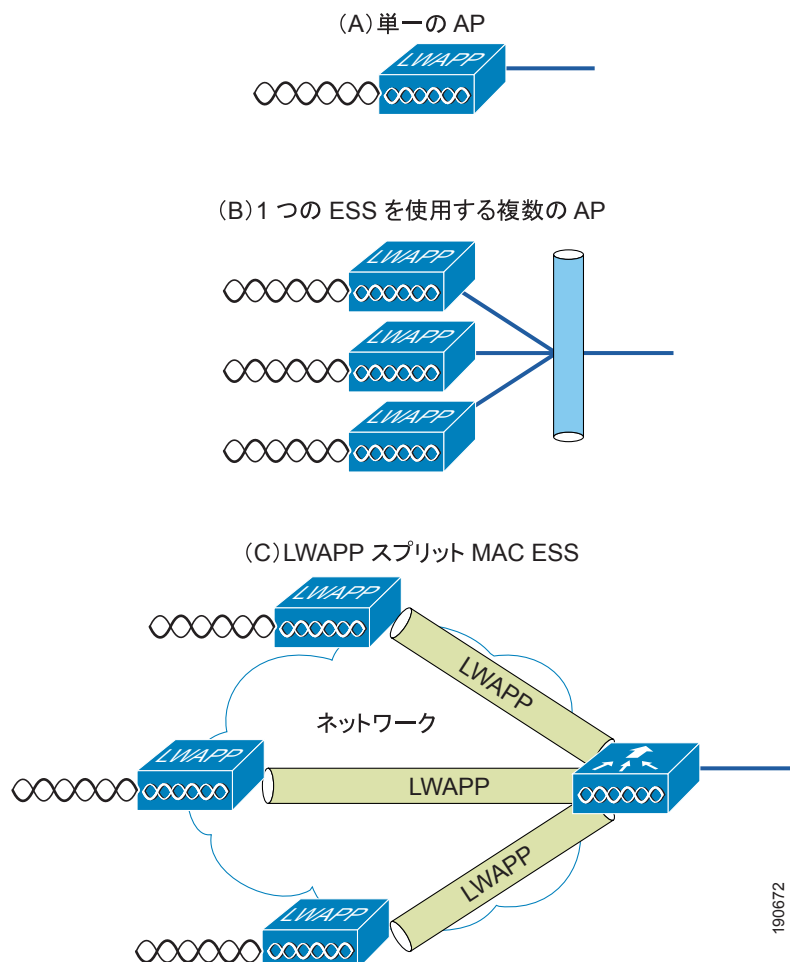
LWAPP スプリット MAC の概念では、通常は個々の AP によって実行されるすべての機能を、LWAPP AP と WLC の 2 つの機能コンポーネントに割り振ります。この 2 つのコンポーネントは、ネットワーク経由で LWAPP プロトコルを使用してリンクされ、個々の AP を使用する場合と同等の無線/ブリッジサービスを、展開や管理がより容易な方法で提供します。



(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 LWAPP 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 スプリット MAC の概念



単純で時間に依存した処理は、通常 LWAPP 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、LWAPP 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 フレームの転送およびブリッジ
- 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。

LWAPP 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。

- LWAPP 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プされます。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 に動的にマップできます。WLAN の設定パラメータには、VLAN の割り当てのほか、SSID、動作状態、認証およびセキュリティの手段、および QoS に関するものがあります。

レイヤ 2 およびレイヤ 3 のトンネル

LWAPP では、イーサネットフレーム内（レイヤ 2）または UDP パケット内（レイヤ 3）でのトンネリングが可能です。これは、WLC 上で設定可能です。一度にサポートされる方式は 1 つだけです。また、すべての WLC でレイヤ 2 方式がサポートされているわけではありません。

レイヤ 2 トンネル

レイヤ 2 LWAPP を展開する場合、LWAPP トンネルで WLC と LWAPP AP の間のトラフィックをカプセル化するために Ethertype 0xB BBBB が使用されているとしても、WLC と LWAPP AP では IP アドレスが必要になります。LWAPP AP と WLC の間の通信はすべて、Ethertype 0xB BBBB を使用してカプセル化されます。

レイヤ 2 LWAPP は、AP の接続を確立したり、AP の設定を行ったりするための単純な方法の 1 つですが、一般に企業での展開ではこの方法は勧められません。したがって、本書ではこれ以上詳しくは説明しません。

現在、シスコがレイヤ 2 方式をベスト プラクティスとして推奨していない主な理由は、次のとおりです。

- LWAPP AP と WLC の間のレイヤ 2 接続により、ネットワーク内で AP や WLC を配置できる場所が制限される可能性があります。この制限を回避するために企業ネットワーク全体にレイヤ 2 転送を拡張することは、現在、ベスト プラクティスとして推奨されていません。
- レイヤ 2 LWAPP は、一部の LWAPP AP および WLC プラットフォームではサポートされていません。
- クライアント トラフィックの DSCP 値はトンネル内で保持されますが、レイヤ 2 LWAPP は、Ethernet フレームに対して対応する CoS マーキングを提供しないため、トンネルされたトラフィックに透過的なエンドツーエンドの QoS を提供することはできません。

レイヤ 3 トンネル

レイヤ 3 LWAPP は、推奨されるトンネルタイプです。この方式では、LWAPP 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。L3 LWAPP 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 Maximum Transmission Unit (MTU; 最大転送単位) 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、LWAPP 操作を示すためのレイヤ 3 LWAPP パケット キャプチャです。サンプルデコードは、Wireshark Network Analyzer 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 LWAPP 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、プロトコルの設定で SWAP Frame Control オプションを使用することで解決できます。

LWAPP コントロール パケット は、LWAPP 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 LWAPP 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 12223 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 LWAPP 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、LWAPP 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 LWAPP コントロール パケット

```

# Frame 27 (803 bytes on wire, 803 bytes captured)
# Ethernet II, Src: Cisco 6a:fd:4b (00:14:6a:6a:fd:4b), Dst: Airespac 52:40:d0 (00:0b:85:52:40:d0)
# Internet Protocol, Src: 192.168.63.2 (192.168.63.2), Dst: 192.168.60.14 (192.168.60.14)
# User Datagram Protocol, Src Port: 12223 (12223), Dst Port: 9229 (9229)
  Source port: 12223 (12223)
  Destination port: 9229 (9229)
  Length: 769
  Checksum: 0x0000 (none)
# LWAPP Encapsulated Packet
  Version: 0
  slotId: 0
  .... .1.. = Type: LWAPP Control Packet
  .... ..0. = Fragment: Set
  .... ...0 = Fragment Type: Set
  Fragment Id: 0x72
  Length: 755
  RSSI: 0x00
  SNR: 0x00
# LWAPP Control Message
  Control Type: 12
  Control Sequence Number: 1
  Control Length: 747
  Data (751 bytes)

```

190673

LWAPP の 802.11 プロブ要求 は、802.11 プロブ要求を含む LWAPP パケットのデコードを示しています。すべての LWAPP 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 12222 を使用して LWAPP 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、LWAPP パケットには RSSI 値と SNR 値も含まれています。

図 2-4 LWAPP の 802.11 プロブ要求

```

# Frame 18 (72 bytes on wire, 72 bytes captured)
# Ethernet II, Src: Airespac 52:40:d0 (00:0b:85:52:40:d0), Dst: Cisco 6a:fd:4b (00:14:6a:6a:fd:4b)
# Internet Protocol, Src: 192.168.60.14 (192.168.60.14), Dst: 192.168.63.2 (192.168.63.2)
# User Datagram Protocol, Src Port: 9229 (9229), Dst Port: 12222 (12222)
  Source port: 9229 (9229)
  Destination port: 12222 (12222)
  Length: 38
  Checksum: 0x0000 (none)
# LWAPP Encapsulated Packet
  Version: 0
  slotId: 1
  .... .0.. = Type: Encapsulated 80211
  .... ..0. = Fragment: Set
  .... ...0 = Fragment Type: Set
  Fragment Id: 0xd7
  Length: 24
  RSSI: 0xc5
  SNR: 0x27
# IEEE 802.11
  Type/Subtype: Probe Request (4)
  # Frame Control: 0x0040 (Swapped)
    Version: 0
    Type: Management frame (0)
    Subtype: 4
    # Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = order flag: Not strictly ordered
    Duration: 0
    Destination address: Airespac_52:40:d0 (00:0b:85:52:40:d0)
    Source address: Aironet_aa:22:20 (00:40:96:aa:22:20)
    BSS Id: Airespac_52:40:d0 (00:0b:85:52:40:d0)
    Fragment number: 10
    Sequence number: 1551
  # IEEE 802.11 wireless LAN management frame
    Tagged parameters (0 bytes)

```

190674

図 2-5 は、別の LWAPP 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、LWAPP 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、LWAPP AP と WLC の間の LWAPP 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 LWAPP AP がこれらのバイトをスワップすることを考慮して、LWAPP 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 LWAPP の 802.11 データ フレーム

```

Ethernet II, Src: Airespac_52:40:d0 (00:0b:85:52:40:d0), Dst: Cisco_6a:fd:4b (00:14:6a:6a:fd:4b)
Internet Protocol, Src: 192.168.60.14 (192.168.60.14), Dst: 192.168.63.2 (192.168.63.2)
User Datagram Protocol, Src Port: 9229 (9229), Dst Port: 12222 (12222)
  Source port: 9229 (9229)
  Destination port: 12222 (12222)
  Length: 106
  Checksum: 0x0000 (none)
LWAPP Encapsulated Packet
  Version: 0
  slotId: 1
  ... 0... = Type: Encapsulated 80211
  ... ..0. = Fragment: Set
  ... ..0. = Fragment Type: Set
  Fragment Id: 0xf7
  Length: 92
  RSSI: 0xde
  SNR: 0x40
IEEE 802.11
  Type/Subtype: Data (32)
  Frame Control: 0x0108 (Swapped)
  Version: 0
  Type: Data frame (2)
  Subtype: 0
  Flags: 0x1
    DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)
    ... ..0.. = More Fragments: This is the last fragment
    ... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0... .... = WEP flag: WEP is disabled
    0... .... = order flag: Not strictly ordered
  Duration: 29952
  BSS Id: Airespac_52:40:d0 (00:0b:85:52:40:d0)
  Source address: 192.168.50.11 (00:02:8a:a3:22:7e)
  Destination address: 192.168.50.1 (00:14:6a:6a:fd:4a)
  Fragment number: 9
  Sequence number: 3840
Logical-Link Control
  DSAP: SNAP (0xaa)
  IG Bit: Individual
  SSAP: SNAP (0xaa)
  CR Bit: Command
  Control field: u, func=UI (0x03)
  organization Code: Encapsulated Ethernet (0x000000)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.50.11 (192.168.50.11), Dst: 192.169.123.1 (192.169.123.1)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 60
  Identification: 0x0361 (865)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (0x01)
  Header checksum: 0x0902 [correct]
  Source: 192.168.50.11 (192.168.50.11)
  Destination: 192.169.123.1 (192.169.123.1)
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x375c [correct]
  Identifier: 0x0200
  Sequence number: 0x1400
  Data (32 bytes)

```

190684

WLC ディスカバリおよび選択

次の項では、リセット時のレイヤ 3 LWAPP AP の典型的な動作について説明します。検出 / 接続プロセスの詳細については、『*Deploying Cisco 440X Series Wireless LAN Controller*』 (<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>) を参照してください。

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 LWAPP 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 LWAPP 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、LWAPP 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 LWAPP ディスカバリ 応答メッセージで応答します。
- ステップ 2** Over-the-Air Provisioning (OTAP) と呼ばれる機能が WLC で有効になっている場合、WLC にすでに接続している AP は、既知の WLC を、無線で他の AP に送信されるネイバー メッセージでアドバタイズします。初めて WLC の「検出」を試みている新しい AP は、これらのメッセージを受信し、OTAP メッセージでアドバタイズされた各 WLC に LWAPP ディスカバリ 要求をユニキャストします (初期状態では、OTAP は IOS AP によりサポートされていません。つまり、IOS を使用する新しい AP は、OTAP を使用して WLC を検出できません)。LWAPP ディスカバリ 要求メッセージを受信する WLC は、AP に LWAPP ディスカバリ 応答をユニキャストします。
- ステップ 3** AP は以前に学習した 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 LWAPP ディスカバリ 要求を送信します。LWAPP ディスカバリ 要求を受信する WLC は、AP に LWAPP 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、既に 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 グループのメンバー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 (モビリティ グループの概念は、この文書の後半で詳しく説明します)。
- ステップ 4** OTAP を使用しない場合は、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。この場合、LWAPP 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 は 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 LWAPP ディスカバリ メッセージを送信します。LWAPP 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 LWAPP ディスカバリ 応答をユニキャストします。
- ステップ 5** オプション 43 の情報の代わりに、AP は DNS 名 CISCO-LWAPP-CONTROLLER.localdomain を解決しようとしています。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 LWAPP ディスカバリ メッセージを送信します。前述のとおり、LWAPP 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 LWAPP ディスカバリ 応答で応答します。
- ステップ 6** 手順 1 ~ 5 の後、LWAPP ディスカバリ 応答を受信されない場合、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ーの一覧が提供されます。

LWAPP 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提供された WLC の一覧から最も負荷の少ない別の WLC を選択します。

コンポーネント

Cisco Unified Wireless のアーキテクチャを構成する主要コンポーネントは、Lightweight AP、WLC、および WCS の 3 つです。この項では、AP および WLC 製品のオプションについて説明します。

Cisco WCS はオプションのネットワーク コンポーネントで、Cisco Aironet Lightweight AP、Cisco 無線 LAN コントローラ、および Cisco Wireless Location Appliance と共に動作します。Cisco WCS を使用すると、ネットワーク管理者は、単一のソリューションを通じて、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、および無線 LAN システムの管理が可能になります。また、堅牢なグラフィック インターフェイスにより、無線 LAN を簡単かつコスト効率の優れた方法で展開し、運用できるようになります。詳細な傾向レポートや分析レポートの機能を備えた Cisco WCS は、ネットワークを継続的に運用するためには欠かせません。Cisco WCS の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

WLC

Cisco Unified Wireless 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で共通しているため、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 Unified Wireless WLC とその機能を簡単にまとめると、次のようになります。

- 2106 : 8 個のファスト イーサネット インターフェイスを持ち、最高 6 個の AP をサポートするスタンドアロン WLC。2 個のファスト イーサネット インターフェイスは、直接接続された AP への電力供給 (802.3af 準拠) に使用できます。また、このインターフェイスを dot1q トランクとして設定し、有線ネットワークへの接続を提供することもできます。2106 は、ユーザ数、WAN 要件、クライアント ローミング要件などのために H-REAP が不向きな、小規模から中規模のオフィスに適しています。
- 4402 : 12 台、25 台、または 50 台の AP をサポートするスタンドアロンの WLC です。有線ネットワークへの接続を提供する dot1q トランクとして設定可能な SFP ベースのギガビットイーサネット ポートを 2 つ備えています。また、スイッチド ネットワークへの EtherChannel 接続を提供するために、ギガビット ポートをリンク集約することもできます。中規模のオフィスまたはビルディングに適しています。
- 4404 : 100 台の AP をサポートするスタンドアロンの WLC です。有線ネットワークへの接続を提供する dot1q トランクとして設定可能な SFP ベースのギガビットイーサネット ポートを 4 つ備えています。ギガビット ポートをリンク集約して、スイッチド ネットワークへの EtherChannel 接続を提供することもできます。大規模なオフィス、ビルディング、および小規模キャンパスに適しています。
- WLCM : WLC モジュールは、シスコの Integrated Service Router (ISR) シリーズ用に設計されたものです。現在は、6 台、8 台、または 12 台の AP をサポートしています。WLCM は、有線ネットワークへのルーテッド接続を提供する dot1q トランクとして設定可能な、ISR ルータ上のインターフェイスです。統合ソリューションを必要としている小規模から中規模のオフィスに適しています。

- WS-C3750G : Catalyst 3750 スイッチに統合されている WLC で、25 台または 50 台の AP をサポートしています。この WLC は、バックプレーン接続用に 2 つのギガビット イーサネットポートを備えており、それぞれのポートを dot1q トランクとして設定して、3750 への接続を提供できます。また、3750 への単一の EtherChannel 接続を提供するために、ギガビットポートをリンク集約することもできます。WLC は直接統合されているので、スタック可能な 3750 スイッチの高度なルーティング機能やスイッチング機能をすべて使用できます。中規模のオフィスまたはビルディングに適しています。仮想スイッチとして、50 台の AP をサポートする 4 台の 3750 をスタックした場合、最高 200 台の AP をサポートするように拡張できます。
- WiSM : シスコの Catalyst 6500 スイッチ シリーズ用に設計された WLC モジュール。1 モジュールあたり最大 300 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 をインストールして、拡張性を大幅に向上できます。WiSM 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。

表 2-1 は Cisco Unified Wireless コントローラをまとめたものです。

表 2-1 Cisco Unified Wireless コントローラの要約

製品	AP の数	インターフェイス	備考
2106	6	ファスト イーサネット 8 個	モビリティ アンカーにはできません。また、レイヤ 2 LWAPP はサポートしておらず、ファスト イーサネット インターフェイスのうち 2 つは 802.3af の PoE をサポートしています。
4402	12 または 25	ギガビット イーサネット 2 個	
4404	50 または 100	ギガビット イーサネット 4 個	
WLCM	6、8、または 12	ISR バックプレーン	モビリティ アンカーにはできず、レイヤ 2 LWAPP はサポートしていません。静的および動的 WLC インターフェイスだけのレイヤ 3 サブインターフェイス終端であり、dot1q トランクはサポートしていません。
WS-C3750G	25 または 50	3750 バックプレーン	統合 WLC により 3750 のスタック可能スイッチを完全装備
WiSM	300	6500 バックプレーン	モジュールは 6500 バックプレーンに直接接続

AP

Cisco Unified Wireless アーキテクチャでは、スタンドアロンと LWAPP の 2 種類の AP が使用されます。ここでは、各カテゴリで利用可能なさまざまな AP 製品モデルについて簡単に説明し、特性、機能、およびアプリケーションを比較します。Cisco 1500 シリーズ Mesh AP については、後で簡単に説明しますが、無線メッシュの活用方法や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、以下のガイドを参照してください。

Cisco Mesh Networking Solution Deployment Guide :

http://www.cisco.com/en/US/partner/products/ps6548/products_technical_reference_book09186a008062b50e.html

Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide :

<http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP.html>

シスコのスタンドアロン AP

このカテゴリの AP は、従来の Aironet 製品ラインで構成されます。以下のモデルは、LWAPP 動作モードで入手するか、LWAPP モードにフィールドアップグレードできます。この機能を使用すると、企業では、混合無線トポロジに展開可能な共通の AP プラットフォーム上での標準化が可能になります。

第 1 世代のスタンドアロン AP は、次のとおりです。

- AP 1100 : このシングル バンド 802.11b/g AP。一体型アンテナを持つ、エンタープライズ展開向けのエン트리 レベル AP です。LWAPP AP の製品番号は AIR-LAP1121G-x-K9 です。x は地域コードになります。
- AP 1200 : エンタープライズ展開をターゲットとした、単一帯域の 802.11b/g AP。1100 シリーズとは異なり、1200 は、外部アンテナへの接続をサポートしており、より柔軟性に優れています。802.11a 無線をサポートするようにフィールドアップグレードしたり、Lightweight (LWAPP) 動作用にアップグレードしたりできます。LWAPP AP の製品番号は AIR-LAP1231G-x-K9 です。x は地域コードになります。
- AP 1230AG : 両方の帯域にアンテナ用の外部コネクタを備えたデュアルバンド 802.11a/b/g AP。これは、1240AG のすべての機能（特に 802.3af PoE 規格）および RF パフォーマンスを備えているわけではありません。また、Lightweight (LWAPP) バージョンでも提供されますが、後から Lightweight 操作モードにアップグレードすることもできます。LWAPP AP の製品番号は AIR-LAP1232G-x-K9 です。x は地域コードになります。

第 2 世代のスタンドアロン AP は、次のとおりです。

- AP 1130AG : AG バージョンは一体型アンテナを備えたデュアルバンド (a/b/g) AP です。これは、壁面取り付け用に設計されており、一体型のデュアルバンド帯域アンテナを使用します。1130AG は、集中化された WLC ベースの展開での実装向けに Lightweight (LWAPP) バージョンで入手できます。スタンドアロンバージョンは、後から Lightweight 動作用にアップグレードできます。LWAPP AP の製品番号は AIR-LAP1131AG-x-K9 です。x は地域コードになります。
- AP 1240AG : 小売や倉庫業務など、厳しい RF 環境での展開向けに設計されたデュアルバンド 802.11 a/b/g AP。1241AG は、両方の帯域にアンテナのための外部接続を備えています。これは、スタンドアロン カテゴリの中で最も多機能な AP です。Lightweight (LWAPP) バージョンでも入手可能です。柔軟性をより向上させるために、スタンドアロンバージョンを後から Lightweight 動作モードにアップグレードすることもできます。その他の目立った機能としては、LWAPP 操作モード用にインストール済みの証明書やハイブリッド REAP のサポート機能などがあります。LWAPP AP の製品番号は AIR-LAP1242AG-x-K9 です。x は地域コードになります。
- AP 1300 : 屋外展開用に設計された単一帯域 802.11b/g AP/ブリッジ。一体型アンテナを備えています。また、外部アンテナアプリケーションをサポートするように、RP-TNC コネクタを付けたものを注文することもできます。LWAPP AP の製品番号は AIR-LAP1310G-x-K9 です。x は地域コードになります。

新しい第 3 世代の AP である Cisco 1252 は、新たに策定された 802.11n 規格のドラフト 2 をサポートする、ビジネス クラスの AP です。802.11n では、Multiple-Input Multiple-Output (MIMO) テクノロジーを使用して、最高 600 Mbps の合計データ レートが実現されます。Cisco 1252 は、デュアルバンド a/b/g、またはシングルバンド b/g 無線設定で使用可能であり、スタンドアロン AP (スタンドアロン) として、または統合 (コントローラ) 無線展開の一部として展開できます。Cisco 1252 には、展開の柔軟性を最大限に向上させるための、各種 2.4 GHz および 5 GHz 外部アンテナで使用可能な RP-TNC コネクタが備わっています。また、Cisco 1252 は、802.11n でのスループット レートをより高めるための、ギガビット 10/100/1000 インターフェイスを内蔵しています。Cisco 1252 は、高帯域幅を必要とする厳しい RF 環境への展開を前提に設計されています。スタンドアロンバージョンの製品番号は、AIR-AP1252AG-x-K9 (デュアルバンド) および AIR-AP1252G-x-K9 (シングルバンド) です。Cisco Unified Wireless バージョンの製品番号は、AIR-LAP1252AG-x-K9 (デュアルバンド) および AIR-LAP1252G-x-K9 (シングルバンド) です。

Cisco LWAPP AP

このカテゴリの AP は、従来の Airespace 製品ラインで構成されていますが、上記のスタンドアロン AP モデルも含まれています。次のモデルは、WLC トポロジだけで使用できます。

- AP 1010 : エンタープライズ向けの基本的な LWAPP/WLC 展開用の、デュアルバンドでゼロタッチ設定の 802.11a/b/g AP。1010 には、内部デュアルセクターアンテナが付属しています。製品番号は AIR-AP1010-x-K9 です。x は地域コードになります。
- AP 1020 : 1010 と同様ですが、内部セクターアンテナに加え、2.4 および 5 GHz 外部アンテナ用の RP-TNC コネクタも含まれています。製品番号は AIR-AP1020-x-K9 で、x は地域コードを示します。
- AP 1030 : REAP AP または リモート エッジ AP とも呼ばれます。1030 は 1020 と同じ能力、機能、パフォーマンスを有していますが、これに加え、小規模な支社のように WLC を展開するには実用的ではない環境に展開できます。製品番号は AIR-AP1030-x-K9 です。x は地域コードになります。
- AP 1500 : 屋外、ポイントツーポイント、マルチポイント MESH 展開用に特別に設計されたデュアルバンド AP。802.11a 帯域はバックホールに使用され、b/g 帯域は無線クライアントアクセスに使用されます。1500 は、MESH トポロジでの最適なルーティングのために（特許出願中の） Adaptive Wireless Path Protocol (AWPP) を使用します。

表 2-2 および表 2-3 はここで説明した AP の比較の要約です。

表 2-2 AP の比較 (1)

Cisco シリーズ	802.11b/g	802.11a	802.11n	スタンドアロン	LWAPP	ブロードキャストされる SSID の数	インストール済みの証明書
1000	はい	はい	いいえ	いいえ	はい	16	はい
1100	はい	いいえ	いいえ	はい	はい	8 ¹	いいえ
1130AG	はい	はい	いいえ	はい	はい	8 ¹	はい ²
1200	はい	オプション	いいえ	はい	はい	8 ¹	はい ²
1230AG	はい	はい	いいえ	はい	はい	8 ¹	はい ²
1240AG	はい	はい	いいえ	はい	はい	8 ¹	はい ²
1252AG	はい	はい	はい	はい	はい	8 ¹	はい
1252G	はい	いいえ	はい	はい	はい	8 ¹	はい
1300	はい	いいえ	いいえ	はい	はい	8 ¹	いいえ
1500	はい	はい	いいえ	いいえ	はい	16	はい

1. 16 BSSID は、将来のリリースでサポートが予定されています。
2. 2005 年 8 月より前に出荷された装置では、シスコより提供されるユーティリティを使用して自己署名証明書をロードする必要があり、11g 無線が必要となります。

表 2-3 AP の比較 (2)

Cisco シリーズ	オフィスおよび同様の環境	厳しい屋内環境	屋外
1010	推奨 ¹	推奨しない	推奨しない
1020	推奨 ¹	推奨 ¹	推奨しない
1100	推奨	推奨しない	推奨しない
1130AG	理想	推奨しない	推奨しない
1200	推奨 ²	推奨	推奨 ²
1230AG	推奨	推奨	推奨 ²
1240AG	推奨 ²	理想	推奨 ²
1300	推奨しない	推奨しない	理想 ³
1500	推奨しない	推奨しない	理想 ¹

1. またはリモート オフィスの場合は 1030LWAPP 展開のみ。
2. 耐候性 NEMA 定格の筐体で展開する場合は屋外で使用可能。特に、吊り天井の上での展開に適しています。
3. スタンドアロン展開のみ。

詳しくは、次のリンクを参照してください。

http://www.cisco.com/en/US/partner/products/ps6108/prod_brochure0900aecd8035a015.html

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 アーキテクチャにおける重要な「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 アーキテクチャ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。動作および設定の詳細は、次の URL を参照してください。

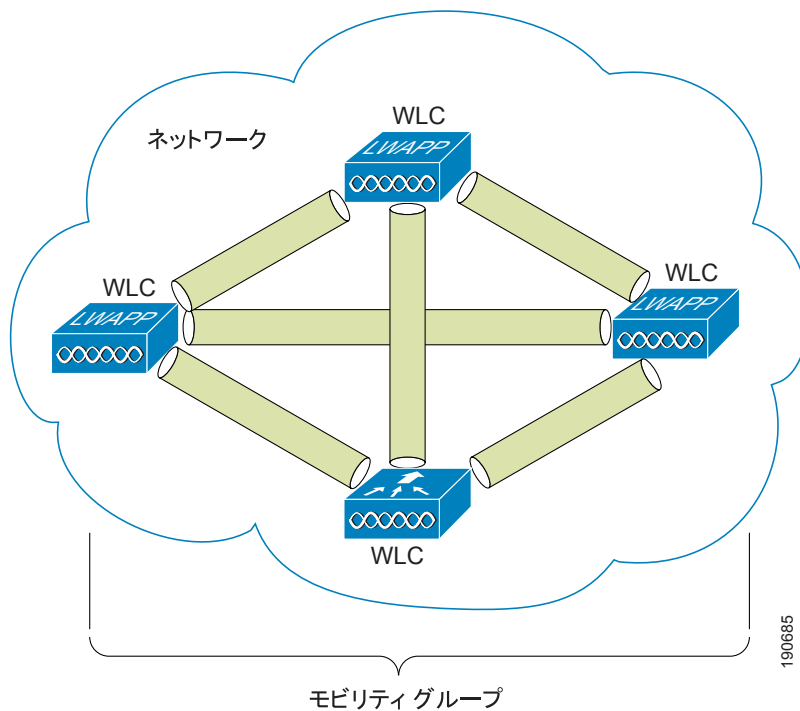
- Deploying Cisco 440X Series Wireless LAN Controller
<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
<http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfg40.html>

モビリティグループ

モビリティグループとは、必須のエンドクライアント、AP、およびRF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が、以下の点に留意してください。

- モビリティ グループごとに、最大 24 の WLAN コントローラおよび 3600 の AP がサポートされています。企業で、複数の WLAN コントローラおよび AP が使用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 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。たとえば、4402、4404、WiSM、WLCM、3750G 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。ソフトウェアが違っているとモビリティ グループを構成できないわけではありませんが、統合無線展開全体で機能の同一性を保証するには、共通のソフトウェア バージョンの使用を強くお勧めします。
- 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」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) の間で無線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、WLAN の 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、無線カバレッジ領域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、キャンパスや支社、キャンパス内の複数のビル間など、それぞれ異なるコントローラ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 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、無線ゲスト 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 にマップできる (外部) WLC の数は、24 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ありません。「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 Guest Access Service」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プされます。しかし、ここで、最大 100 台までの AP をサポートする 4404-100 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、2,500 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。WLC の AP グループ機能により、コントローラ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プします。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。これについては、このデザインガイドの後半で詳しく説明します。

図 2-7 APグループとサイト固有のVLAN

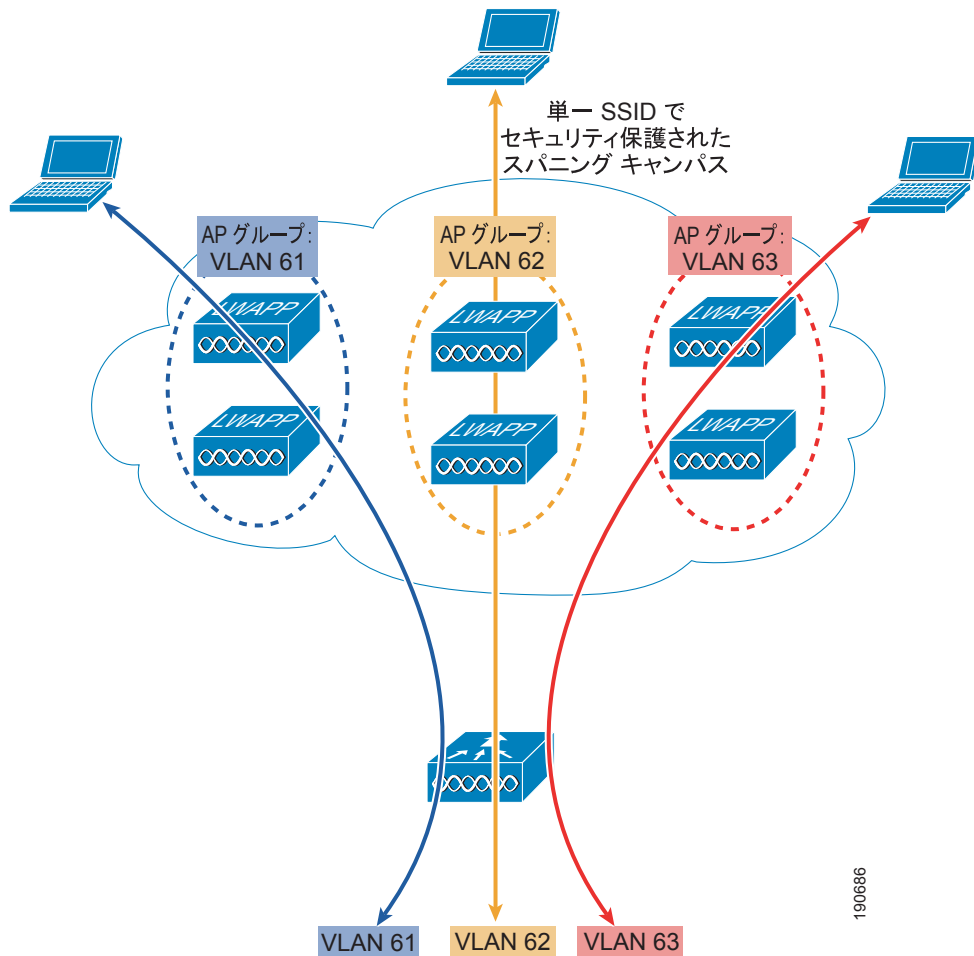


図 2-7 では、3つの動的インターフェイスが設定され、それぞれがサイト固有の VLAN (61、62、および 63) にマッピングされています。サイト固有の VLAN およびアソシエートされた AP は、それぞれ AP グループ機能を使用して同一の WLAN SSID にマッピングされます。VLAN 61 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 61 IP サブネットで IP アドレスを取得します。同様に、VLAN 62 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 62 サブネットで 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、無線 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 Radio Resource Management (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、このドキュメントの後半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。

- LWAPP 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。異なる 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、ダンピ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。更新間隔の合い間に、RF グループ リーダーは RF グループの各メンバにキープ 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

企業の 802.11 ネットワークのローミングは、802.11 クライアントがその AP アソシエーションを ESS 内のある AP から同じ ESS 内の別の AP に変更することを表します。ネットワークの機能および設定によっては、クライアント、WLC、およびネットワークのアップストリーム ホップでイベントがいくつか発生する可能性があります。基本的には、ローミングは単に AP アソシエーションの変更にはすぎません。

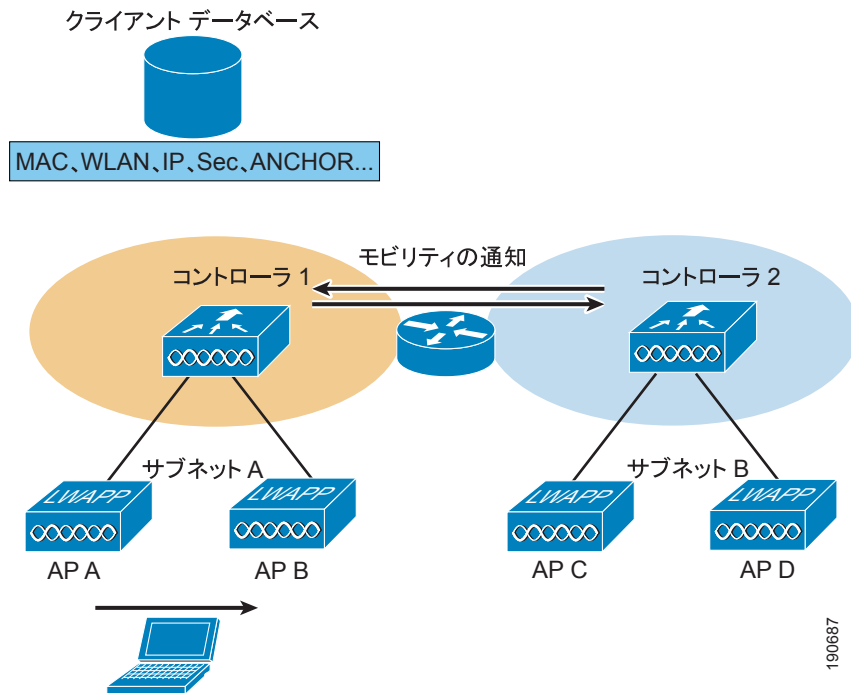
無線クライアントが AP の認証を受けて AP にアソシエートするときには、対応する WLC (AP の接続先) により、クライアント データベースにそのクライアントのためのエントリが作成されます。このエントリには、クライアントの MAC および IP アドレス、セキュリティ コンテキストおよびアソシエーション、QoS コンテキスト、WLAN、およびアソシエートされた AP が含まれます。WLC はこの情報を使用して、フレームを転送し、無線クライアント間で送受信されるトラフィックを管理します。

無線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、WLC はクライアント データベースの新しい AP に関する情報をアップデートするだけです。必要に応じて、新しいセキュリティ コンテキストおよびアソシエーションも確立されます。

レイヤ 2 のローミングは、同じクライアント サブネットで、クライアントがある AP を離れて別の AP に再アソシエートするときに発生します。ほとんどの場合、ローミング先の AP は元の AP と同じ WLC に接続されています。

上の説明は、1 つの WLC データベースがクライアントに関するすべての情報を保持している最も単純なローミング シナリオを例にしたものです。WLC よりアップストリームにあるネットワーク要素は、図 2-8 に示すように、ある AP から別の AP にクライアントが移動しても影響を受けません。

図 2-8 レイヤ 2 でのローミング



WLAN を同一のサブネットに接続している WLC が複数存在しているときに、クライアントが異なる WLC に接続されている AP の間をローミングする場合は、WLC の間でモビリティ通知が交換されます。このモビリティ通知により、WLC の間でクライアントのコンテキスト情報が渡されます。

クライアントサブネット間での WLC から WLC へのローミング

異なる WLC に接続されている AP 間でクライアントがローミングするときに、これらの WLC でクライアントサブネットや VLAN が同一ではないと、レイヤ 3 ローミングが実行されます。ローミング先 (外部 (foreign)) のモビリティデータベースとホーム (アンカー) WLC のモビリティデータベースの間で、モビリティ通知が交換されます。

レイヤ 3 ローミングは、無線クライアントが 1 つの VLAN またはサブネットから別の VLAN またはサブネットに移動する、より複雑なローミング方法です。WLAN システムにより、クライアントサブネットを透過的に変更するための措置が講じられない限り、レイヤ 3 ローミングイベントは、アップストリームサービスを使用するクライアント通信に悪影響を与えます。既存のクライアントセッションは、ハングするか、最終的にタイムアウトして切断されます。Cisco Unified Wireless ソリューションでは、モビリティトンネルを使用し、アップストリームネットワークに対して透過的にレイヤ 3 ローミングが実行されます。モビリティトンネルには、次の 2 種類があります。

- アシンメトリックモビリティトンネル (WLC リリース 4.0 以前のデフォルト)
- シンメトリックモビリティトンネル (WLC リリース 4.1 以降の新規オプション)



(注)

WLC リリース 4.1 では、デフォルトでアシンメトリックトンネリングが使用されます。シンメトリックトンネルを使用する場合は、管理者が明示的に設定する必要があります。

レイヤ 3 ローミング: アシンメトリックモビリティトンネル

レイヤ 3 ローミングシナリオでは、無線クライアントに戻るトラフィックは、アンカー WLC を通過します。アンカー WLC は、Ethernet-over-IP (EoIP) トンネルを確立して、クライアントトラフィックを外部 WLC へ転送します。その後、クライアントトラフィックは、外部 WLC からクライアントへ配信されます。クライアントからのトラフィックはすべて、外部 WLC での WLAN のマップ先である、対応する VLAN インターフェイスに転送されます。クライアントの元の IP アドレスとデフォルトゲートウェイ IP (MAC) アドレスは変更されません。ローカルサブネット宛のトラフィックを除き、すべてのトラフィックはデフォルトルータに転送されます。ここで、外部 WLC により、クライアントのデフォルトゲートウェイ MAC アドレスが、外部コントローラで動的インターフェイスまたは VLAN とアソシエートされているデフォルトゲートウェイの MAC アドレスに置き換えられます。

図 2-9 は、アシンメトリックモビリティトンネルを使用したクライアントレイヤ 3 ローミングを示しています。

図 2-9 レイヤ 3 でのローミング

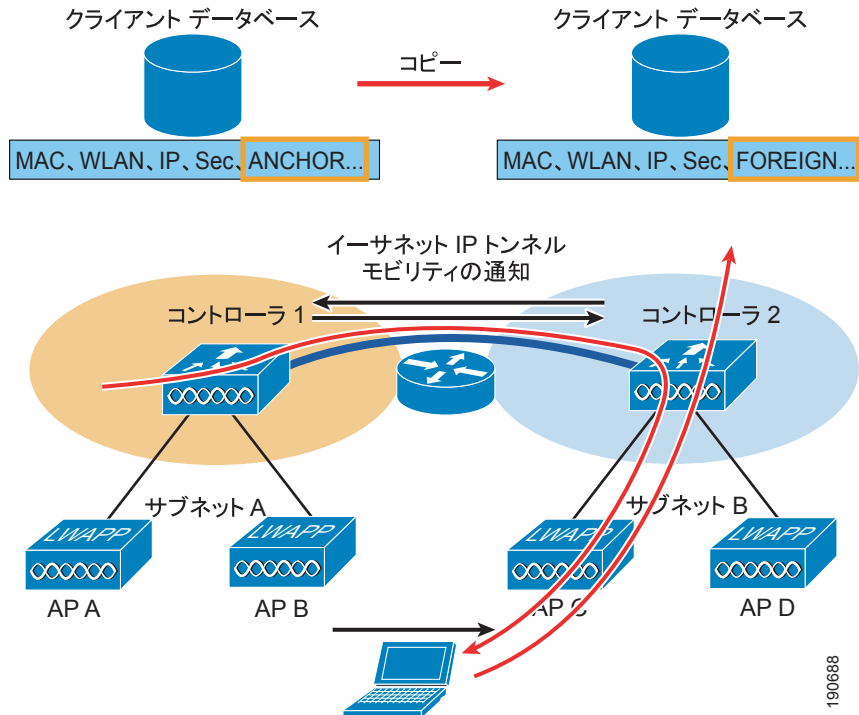


図 2-9 では、レイヤ 3 境界を越えたクライアントのローミング時に以下が実行されます。

1. クライアントは、WLC 1 上の AP B への接続を開始します。
2. これにより、WLC 1 のクライアント データベースに ANCHOR エントリが作成されます。
3. クライアントが AP B から移動し、AP C とのアソシエーションを開始すると、WLC 2 は、クライアント MAC アドレスに関する情報を持つ WLC を求めて、モビリティ グループのピアにモビリティ通知を送信します。
4. WLC 1 は通知、ハンドシェイク、および ACK に応答します。
5. ローミング クライアントのクライアント データベース エントリが WLC 2 にコピーされ、FOREIGN としてマークされます。PMK データ (RADIUS サーバからのマスター キー データ) も WLC 2 にコピーされます。これにより、RADIUS サーバから完全な再認証を受ける必要がなくなるため、WPA2/802.11i クライアントのローミング時間が短縮されます。
6. クライアントと AP 間で簡単なキー交換が実行され、クライアントは WLC 2 のデータベースに追加されます。このデータベースは、クライアント エントリが FOREIGN とマークされている点を除けば、アンカー コントローラのエントリとほとんど同じです。
7. WLAN クライアントに送信されるデータは、アンカー WLC から外部 (foreign) WLC へ EoIP でトンネルされます。
8. WLAN クライアントにより送信されるデータは、外部コントローラのローカル インターフェイス VLAN から送出されます。

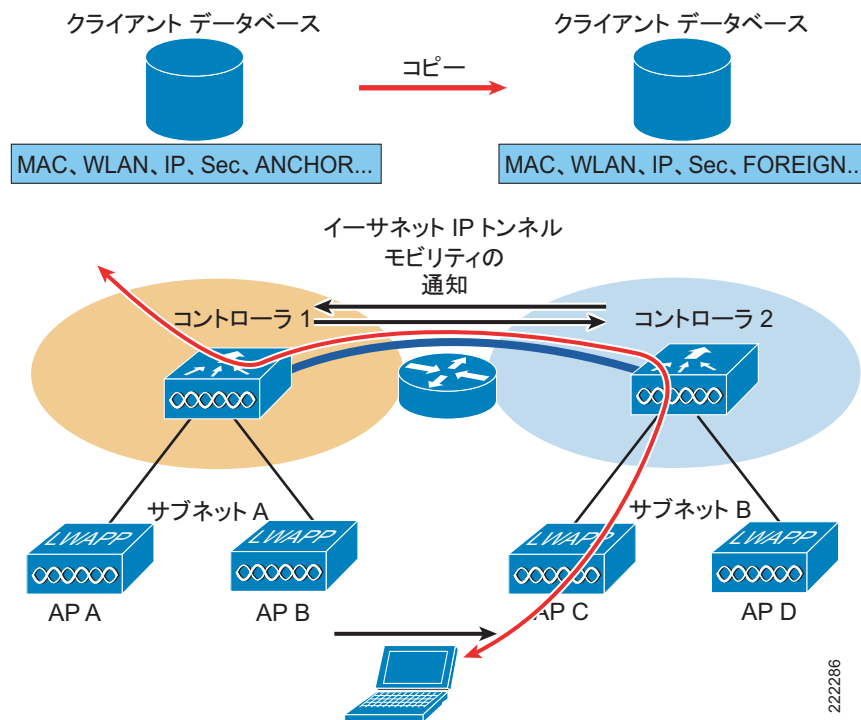
前述の「アシンメトリック」レイヤ 3 ローミング手順では、レイヤ 3 境界を越えた透過的なローミングの問題は解決されますが、アシンメトリック フローは、アップストリーム ネットワークで別の問題が発生する原因になります。特に、無線クライアント トラフィックが、ファイアウォール、NAC、IPS/IDS アプライアンスなどの近接するアプライアンスやモジュールを通じて双方向にフローすると予想される場合には、問題が発生することがあります。また、たとえば、次ホップの

ルーテッドインターフェイスで uRPF チェックが有効になっている場合、クライアントが別のサブネットにローミングした後でトラフィックがドロップされます。これが、Cisco Unified Wireless ソリューションにシンメトリック モビリティ トンネル機能が導入された理由です。

レイヤ 3 ローミング：シンメトリック モビリティ トンネル

WLC リリース 4.1 以降、[図 2-10](#) に示すとおり、外部 AP/WLC とアンカー WLC の間の動的な双方向トンネリングをサポートするように WLC を設定できるようになりました。

図 2-10 レイヤ 3 ローミング：シンメトリック モビリティ トンネル



WLC のレイヤ 3 モビリティ ハンドオフ手順はそのままであり、変更されていません。ただし、WLC リリース 4.1 では、クライアントがレイヤ 3 ローミングを実行するときに、ソリューションの自動アンカー トンネリング メカニズムに関連する既存の機能を使用して、動的なシンメトリック トンネルが作成されます。

デフォルトでは、シンメトリック トンネリングは有効になっていません。コントローラの Web 設定インターフェイス、WCS テンプレート、またはコントローラの CLI を使用して、明示的に設定する必要があります。シンメトリック モビリティ トンネル動作は、特定のモビリティ グループのメンバであるコントローラ全てに対し有効にしてください。そうしないと、予期しない動作が発生する可能性があります。

[図 2-11](#) と [図 2-12](#) は、双方向モビリティ トンネルの Wireshark プロトコル トレースを示しています。

図 2-11 双方向モビリティトンネル (1)

```

Ethernet II, Src: Airespac_40:8a:a3 (00:0b:85:40:8a:a3), Dst: Airespac_40:7e:e0 (00:0b:85:40:7e:e0)
Internet Protocol, Src: 10.15.9.13 (10.15.9.13), Dst: 10.15.9.11 (10.15.9.11)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 100
  Identification: 0xef32 (61234)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 127
  Protocol: Ether in IP (0x61)
  Header checksum: 0x25d1 [correct]
  Source: 10.15.9.13 (10.15.9.13)
  Destination: 10.15.9.11 (10.15.9.11)
EtherIP, Version 0
Ethernet II, Src: Aironet_ac:5f:f7 (00:40:96:ac:5f:f7), Dst: HewlettP_0e:de:51 (00:15:60:0e:de:51)
802.1Q Virtual LAN
Internet Protocol, Src: 10.20.32.100 (10.20.32.100), Dst: 209.131.36.158 (209.131.36.158)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 60
  Identification: 0x6b67 (27495)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (0x01)
  Header checksum: 0xae0 [correct]
  Source: 10.20.32.100 (10.20.32.100)
  Destination: 209.131.36.158 (209.131.36.158)
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xd9d2 [correct]
  Identifier: 0x0200
  Sequence number: 0x7189
  Data (32 bytes)

```

222284

図 2-12 双方向モビリティトンネル (2)

```

Frame 8 (114 bytes on wire (114 bytes captured)
Ethernet II, Src: Airespac_40:7e:e3 (00:0b:85:40:7e:e3), Dst: Airespac_40:8a:a0 (00:0b:85:40:8a:a0)
Internet Protocol, Src: 10.15.9.11 (10.15.9.11), Dst: 10.15.9.13 (10.15.9.13)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 100
  Identification: 0xabde (43998)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 127
  Protocol: Ether in IP (0x61)
  Header checksum: 0x6925 [correct]
  Source: 10.15.9.11 (10.15.9.11)
  Destination: 10.15.9.13 (10.15.9.13)
EtherIP, version 0
Ethernet II, Src: HewlettP_0e:de:51 (00:15:60:0e:de:51), Dst: Aironet_ac:5f:f7 (00:40:96:ac:5f:f7)
802.1Q Virtual LAN
Internet Protocol, Src: 209.131.36.158 (209.131.36.158), Dst: 10.20.32.100 (10.20.32.100)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 60
  Identification: 0x850a (34058)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 45
  Protocol: ICMP (0x01)
  Header checksum: 0xe81d [correct]
  Source: 209.131.36.158 (209.131.36.158)
  Destination: 10.20.32.100 (10.20.32.100)
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xe1d2 [correct]
  Identifier: 0x0200
  Sequence number: 0x7189
  Data (32 bytes)

```

222285

前述のプロトコルトレースでは、シンメトリック モビリティ トンネル (EtherIP) は、10.15.9.11 (アンカー) と 10.15.9.13 (外部) の 2 つの WLC 間に確立されています。図 2-11 では、コントローラ 10.15.9.13 上の AP にローミングしたクライアント 10.20.32.100 が、インターネット サイト 208.131.36.158 (yahoo.com) に ICMP ping 要求を送信しています。外部コントローラがクライアントのパケットをアンカー コントローラへトンネルしている点に注意してください。コントローラがアシンメトリック モビリティ トンネリング用に設定されていた場合、このパケットは、外部コントローラにより、WLAN にアソシエートされている VLAN インターフェイスにローカルで転送されるため、トレースには表示されません。図 2-12 では、ping 応答は、アンカー コントローラにより受信され、同じモビリティ トンネルを経由して、外部コントローラに転送されています。これは、シンメトリック トンネルと同じです。

レイヤ 3 ローミングに関する重要な情報

レイヤ 3 ローミングは非常に便利な機能ですが、4.1 ソフトウェア リリースで展開する場合は、次の点に注意する必要があります。

- 現時点では、マルチキャストのグループ メンバーシップはクライアント ローミング中に転送されません。つまり、クライアントがマルチキャスト ストリームを受信し、マルチキャスト ストリームが壊れる外部 WLC に移動した場合は、再確立する必要があります。
- Unified Wireless ソリューションでは、モビリティアンカーと EoIP トンネルの概念に基づいたレイヤ 3 ローミングが使用されています。「アンカー WLC」は、クライアントが初めて WLAN にアソシエートしたときに使用された WLC です。その後、クライアントには、アンカー コントローラで WLAN に割り当てられたインターフェイスまたはサブネットに対応するアドレスが DHCP 経由で割り当てられます。現在、Unified Wireless ソリューションでは、ある WLAN に対して定義されたサブネット以外の静的 IP アドレスを持つクライアントが、その WLAN に接続することは許可されていません。静的クライアントアクセスが必要な展開シナリオで使用可能なソリューションとしては、モバイル IP の使用を検討してください。モバイル IP、およびモバイル IP の Cisco Unified Wireless アーキテクチャの互換性の詳細は、第 12 章「Cisco Unified Wireless とモバイル IP」を参照してください。

WLC でのブロードキャストおよびマルチキャスト

ここでは、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 2-13 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、無線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 2-13 802.11 ブロードキャスト / マルチキャスト

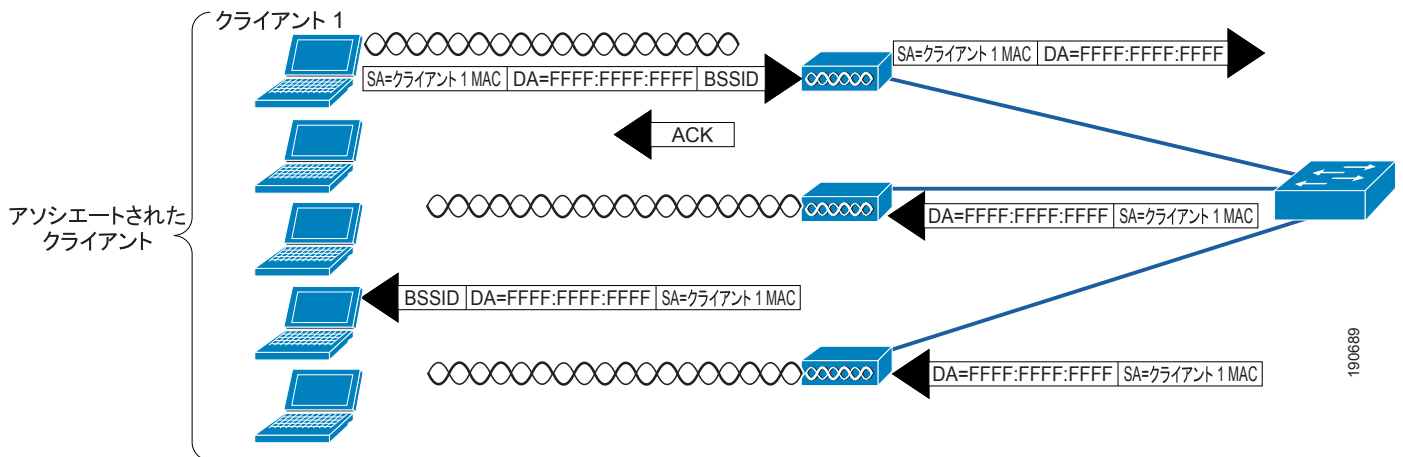


図 2-13 に示されているように、AP と同じ有線 VLAN 上に別の AP がある場合、それらの AP は、有線ブロードキャスト パケットを無線インターフェイスに転送します。

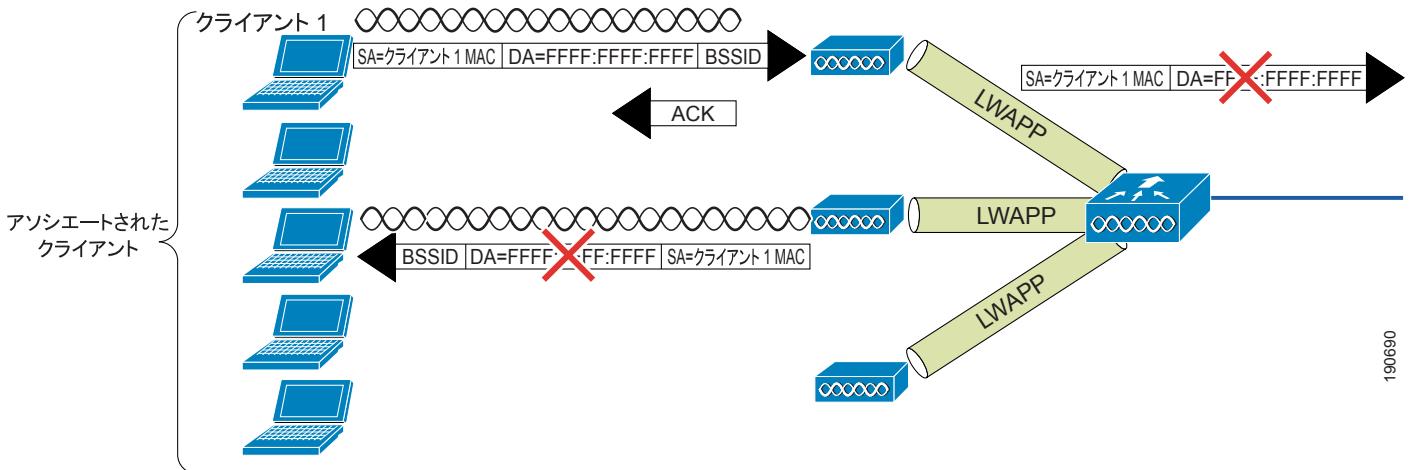
WLC の LWAPP スプリット MAC 方式では、図 2-17 に示すように、別の方法でブロードキャスト トラフィックを処理します。この場合、クライアントからブロードキャスト パケットが送信されると、AP またはコントローラは、そのパケットを WLAN に転送せず、ブロードキャスト メッセージと考えられるすべてのメッセージのサブセットのみを、WLC で指定された WLAN の有線インターフェイスに転送します。



(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。

図 2-14 WLC ブロードキャストのデフォルトの動作



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。そして、それらのトラフィックを特別に処理することによって、アソシエートされているすべての無線デバイスで、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 からその他の無線クライアント 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 (DHCP から) 取得して IP アドレスを MAC アドレスに解決 (ARP) する以外の理由では、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、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、有線または無線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。

前述の手順では、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 DoS 攻撃 (サービス拒絶攻撃) を軽減できるようになります。

- WLC は、DHCP サーバの実際の IP アドレスではなく、仮想 IP アドレスを使用して、DHCP 応答メッセージをリレーできるようになります。前述の動作は WLC の CLI により設定されるもので、デフォルトで有効になっています。この仮想アドレスは、モビリティグループを構成するすべての WLC により共有されます。DHCP プロキシの利点は、L3 クライアントローミング中、または AP グループ境界を越えたクライアントローミングで活かされます。このような場合、WLC はクライアントの DHCP 更新要求を受け取り、そのときに、クライアントがモビリティグループ内でローミングしていることを確認して、クライアントが外部 WLC の新しいサブネットにローミングしたとしても既存の IP アドレスやサブネットの割り当てを更新（維持）できるようにします。ローミング (P. 2-18) を参照してください。



(注)

アシンメトリック モビリティ トンネル方式が設定されている場合（デフォルト）、前述の仮想 IP/Proxy DHCP の動作は必須です。詳細は、前述の「ローミング」の項を参照してください。シンメトリック トンネル方式が使用されている場合には、WLC ベースの DHCP プロキシは必要ありません。これはクライアントトラフィックと DHCP 要求が常にアンカーコントローラにトンネルして戻されるからです。

ARP

WLAN クライアントは、他の IP クライアントに IP パケットを送信する前に、フレームの転送先となるターゲットクライアントの MAC アドレスを知っておく必要があります。このために、クライアントは通信先となる IP ホストの MAC アドレスを要求する ARP クエリをブロードキャストします (図 2-15 を参照)。

図 2-15 ARP フレーム

```

Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 192.168.11.11 (00:40:96:aa:22:32)
  Sender IP address: 192.168.11.11 (192.168.11.11)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.11.3 (192.168.11.3)
  
```

無線クライアントの ARP 要求を認識した WLC は、もう 1 つの無線クライアントのための ARP プロキシとして直接応答するか、または別の WLC に解決してもらうために有線インターフェイスに要求を転送します。この WLC が ARP ブロードキャストを WLAN に転送することはありません。

WLC のデフォルトの動作では、WLC のローカル ARP キャッシュに基づいて直接 ARP クエリーに応答します。この動作をオーバーライドするには、WLC CLI コマンド : **network arpunicast enable** を使用します。この場合、WLC はターゲットのために応答するのではなく、ターゲットホストに直接 ARP 要求をユニキャストします。このターゲットは、要求元ホストに対して ARP 応答をユニキャストします。このコマンドの目的は、WLAN ネットワークから移動した可能性のある WLAN クライアントへ IP クライアントが過剰に再試行するのを防ぐことにあります。

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 (デフォルト) は、無線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。Unified Wireless 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 WLC ではありません。したがって、次の手順の追加を検討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ります。あることを覚えておいてください。

設計上の考慮事項

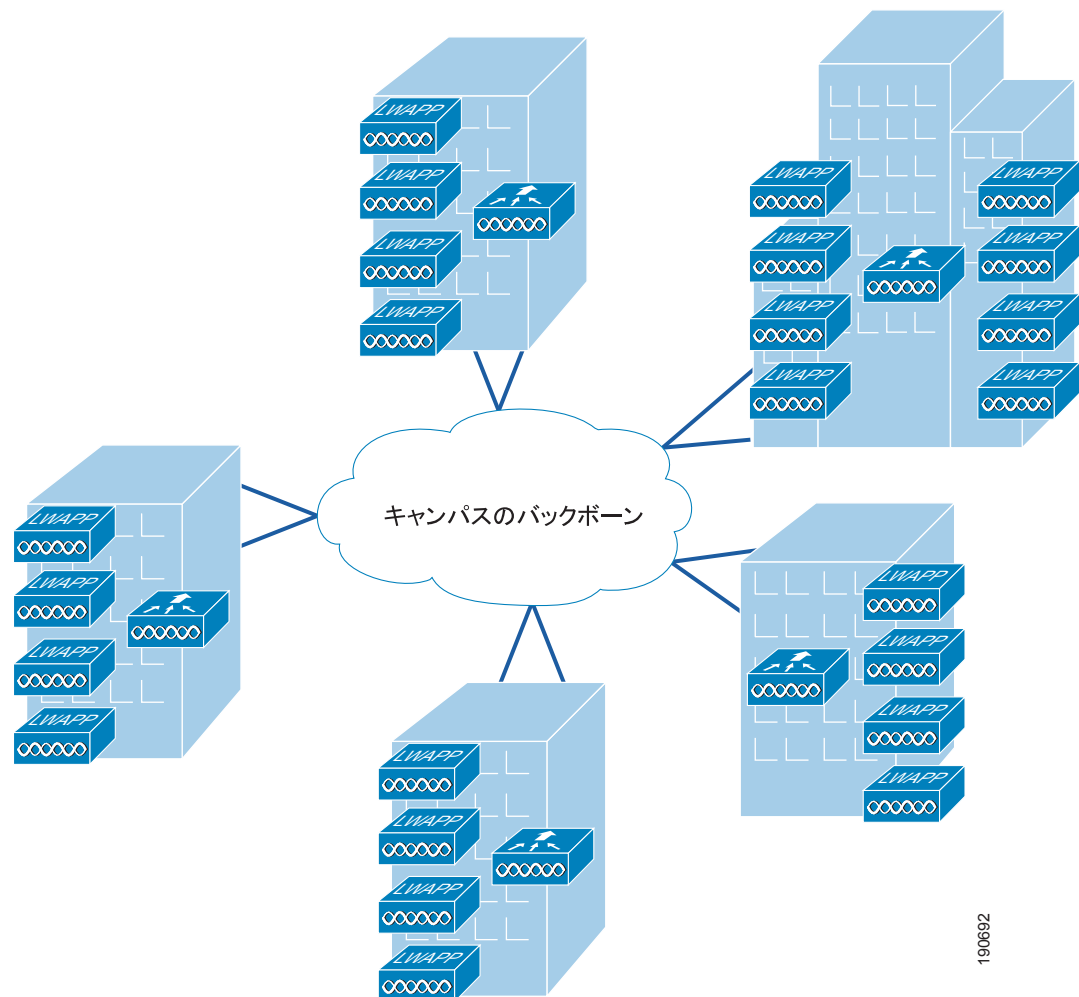
Cisco Unified Wireless 展開の設計における主な考慮事項は、AP 接続と WLC の場所および接続です。この項では、これらのトピックについて簡単にまとめ、必要に応じて標準的な推奨事項について説明します。

WLC の場所

Cisco Unified Wireless LAN ソリューションの柔軟性から、WLC の設置場所に関して、次のような選択肢が考えられます。

- 分散された WLC 展開：分散モデルでは、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は、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 LWAPP トンネルは通常ビルディング内にとどまります。図 2-16 は分散された WLC 展開を示しています。
- WLAN カバレッジがビルディング間で重複しない限り、分散された 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。

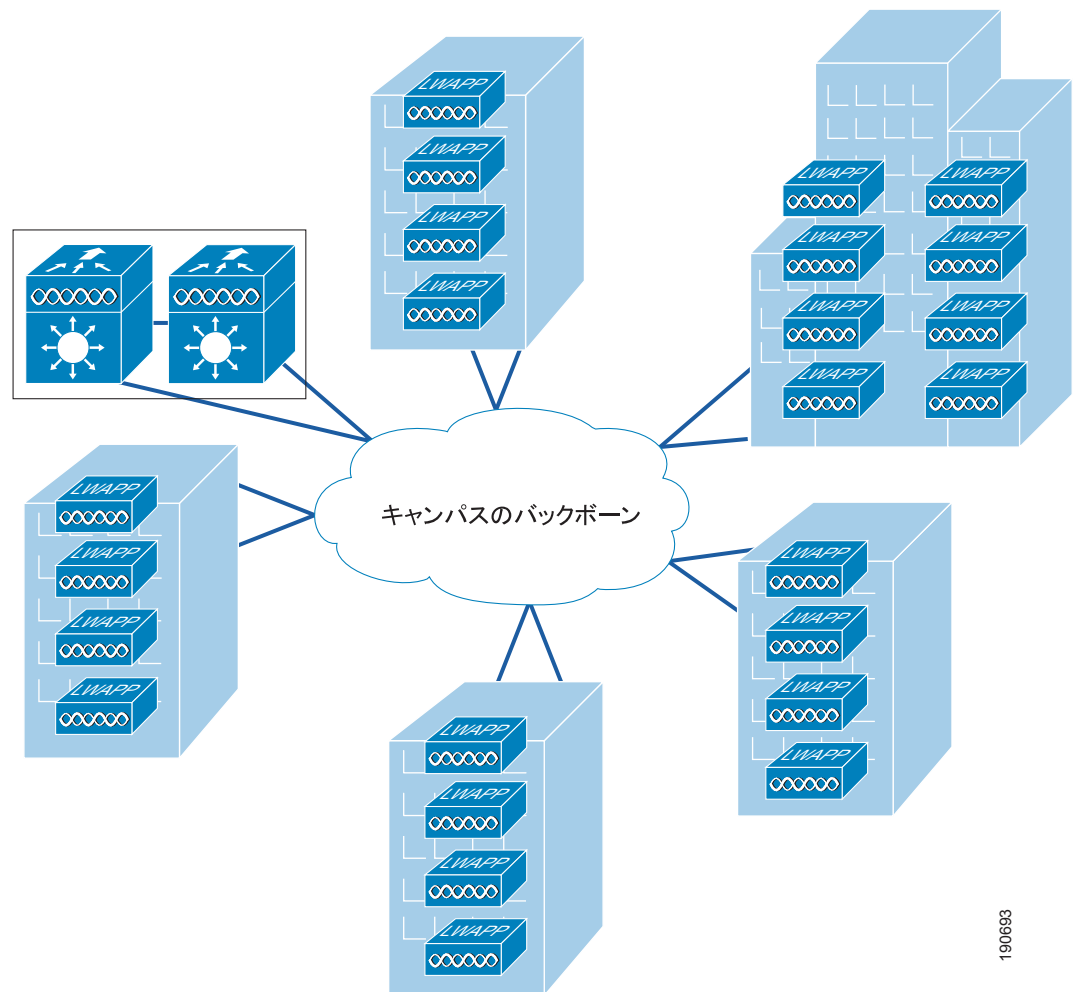
図 2-16 分散された WLC



190692

- 集中化された WLC 展開：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 LWAPP トンネルが必要です。集中化された WLC 展開の例を図 2-17 に示します。ただし、下の例では、集中化された WLC (Catalyst 6500 にある WiSM のペア) は、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。集中化された WLC クラスタは専用スイッチブロック経由でキャンパスの中心に接続されます。キャンパスの中心は、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 2-17 集中化された WLC



WLC の集中化

このデザインガイドでは、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。リリース 4.1 以前は、そのほかにも、分散展開を非現実的なものにする機能的な問題（トンネル QoS およびアシンメトリック トンネリング）がありましたが、それらも解決されています。

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。

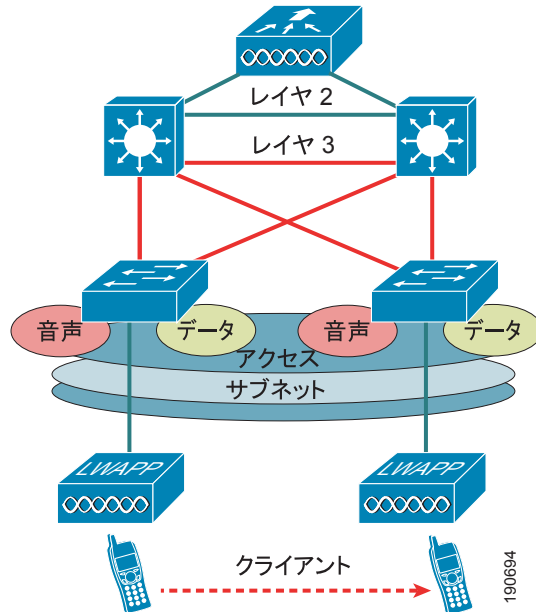
WLC を他のインフラストラクチャコンポーネントと統合する場合にも同様の原理が当てはまります。集中化された WLC により、統合ポイントおよび統合デバイスの数を最小限に抑えられます。たとえば、NAC アプライアンスのようなインラインセキュリティデバイスの実装を決定したとき、集中化された WLC の場合は統合ポイントが 1 か所ですが、分散ソリューションの場合は統合ポイントが n か所になります。 n は、WLC の展開箇所の数を示します。

要約すると、集中化された WLC 展開の使用が推奨されるということです。集中化された 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 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ー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 が果たす役割は大変大きいからです。

分散された WLC ネットワークの接続

前述のとおり、分散された WLC は通常、キャンパス ネットワーク内のディストリビューション レイヤ ルータに接続されます。このような場合は、図 2-18 に示すように、レイヤ 2 リンクを経由して WLC をディストリビューション レイヤに接続することはお勧めしません。

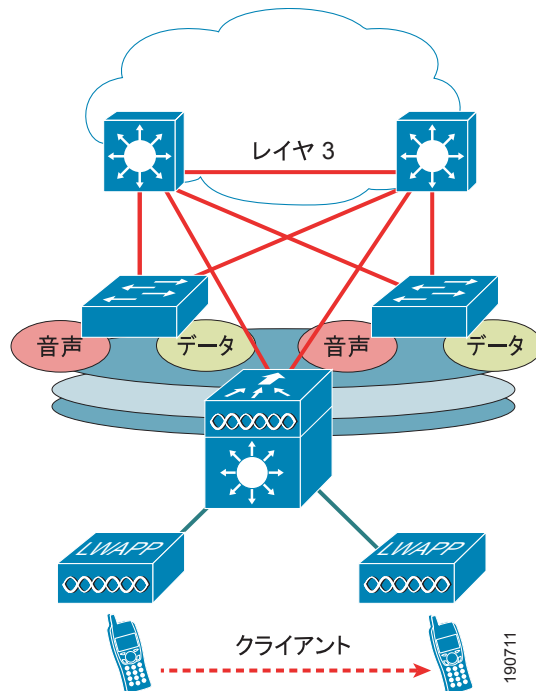
図 2-18 レイヤ 2 に接続された WLC



この推奨は、以下を含む多数の理由によるものです。

- 一般的なベスト プラクティスであるキャンパス設計では、レイヤ 3 アクセスを使用し、高速なコンバージェンスと簡単な操作を提供するために接続を分散することをお勧めします。レイヤ 2 に接続された WLC を入れると、このモデルは壊れます。
- レイヤ 2 WLC 接続では、HSRP など、ディストリビューション レイヤでのアクセス レイヤ機能およびアクセス レイヤのセキュリティ機能の導入が必要になります。ただし、ディストリビューション レイヤが適切なすべてのアクセス スイッチをサポートしていない場合や、アクセス機能をサポートするためにソフトウェアのバージョンを変更する必要がある場合は、問題になる可能性があります。
- 図 2-19 に示すように、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 2-19 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

Unified Wireless 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 LWAPP 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、分散された WLC 展開と集中化された 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 LWAPP 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。

- LWAPP コントロール トラフィックのボリューム: LWAPP 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。通常、ソフトウェアのアップグレード中や WLC のリポート中は多くなります。しかし、トラフィックの調査では、LWAPP 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 0.35Kb/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、集中化された WLC 展開と分散された 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: レイヤ 3 LWAPP 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 バイト以下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、集中化された WLC 展開と分散された 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: 集中化された WLC にトンネルされた WLAN トラフィックはすべて、WLC の場所からネットワークでの終点にルーティングされます。トンネルの距離と WLC の場所によっては、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 トポロジや分散された 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、集中化された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目的地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、集中化された WLC 展開と分散された 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と一致しています。さらに、Catalyst Integrated Security Features (CISF) を LWAPP 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お勧めします（H-REAP AP 接続については、第2章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」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、LWAPP 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 展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、次のようにさまざまな WLC ディスカバリ メカニズム（前述）により、LWAPP AP の初期展開は非常に簡単になります。

- 制御された環境での WLC を使用して前もって行われる LWAPP 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、DNS、または OTP）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 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 の分散

WLC ディスカバリ プロセスについては、この章ですでに説明しました。典型的な初期展開では、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ツールは、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、マスター WLC はプライマリ、セカンダリ、およびターシャリ WLC で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 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。

ファームウェアの変更

Cisco Unified Wireless Network を運用するときには、WLAN ネットワーク全体の中断を最小限に抑えながら WLC ファームウェアをアップグレードする方法を考えることも重要です。そうしないと、ある WLC にアソシエートされているすべての AP が新しいソフトウェアをダウンロードしている間に、その WLC を単にアップグレードしたりリブートしたりしただけで、一部のロケーションの WLAN カバレッジが失われる可能性があります。

規定どおりの方法で AP をセカンダリ WLC に移行し、プライマリ WLC をアップグレードしてから、アップグレードした WLC に AP を戻すことをお勧めします。

この手順は、高可用性を実現できるように展開が設計された 1+1 シナリオでは、多少異なります。

- AP をプライマリ WLC からセカンダリへ移動
- プライマリ WLC をアップグレード
- すべての AP をプライマリ WLC に戻す
- セカンダリ WLC をアップグレード
- セカンダリ AP をセカンダリ WLC に戻す

N+1 シナリオの場合

- WLC のアップグレードの間、各 WLC がその AP を +1 WLC に移動する
- アップグレード後、AP をプライマリ WLC に戻す
- WLC がすべてアップグレードされたら、+1 WLC をアップグレードする



(注)

プライマリ AP を制御された方法でプライマリ WLC に戻せるように、AP フェールバックは無効にしておく必要があります。

