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 を導入する場合の、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
- ローミング
- WLC でのブロードキャストおよびマルチキャスト
- 設計上の考慮事項
- 運用およびメンテナンス


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導入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

Internet Engineering Task Force（IETF）標準規格の Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、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、AP と WLAN コントローラ（WLC）の間の WLAN クライアント トラフィックのカプセル化と転送に加えて、AP と WLAN の設定および管理を行います。

CAPWAP は Lightweight Access Point Protocol（LWAPP）に基づいていますが、Datagram Transport Layer Security（DTLS）によるセキュリティ強化が追加されています。CAPWAP では User Datagram Protocol（UDP）を使用しており、インターネット プロトコル バージョン 4（IPv4）とインターネット プロトコル バージョン 6（IPv6）のどちらでも動作します。表 2-1 に、各 CAPWAP バージョンのプロトコルとポートの実装を示します。

*表 2-1　CAPWAP のプロトコルおよびポート*

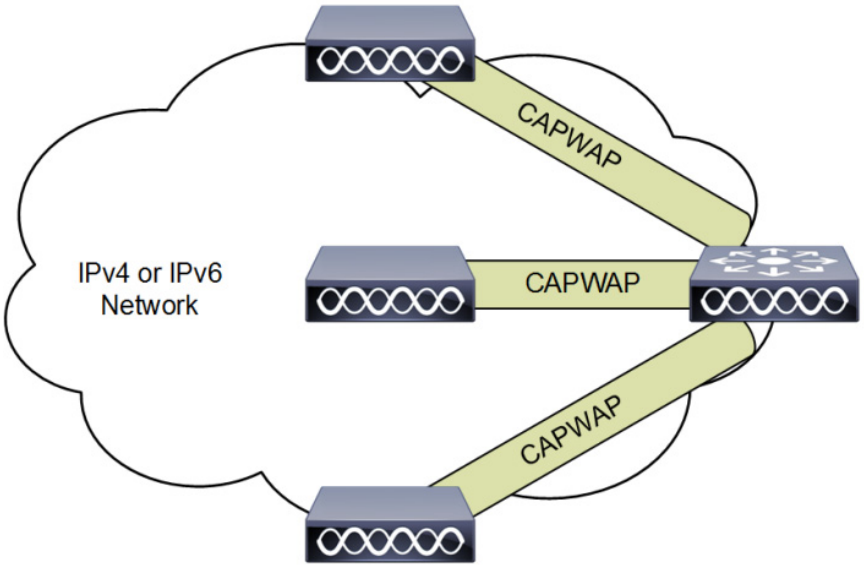
| インターネット プロトコル | IP プロトコル | 宛先ポート | 説明 |
|---|---|---|---|
| バージョン 4 | 17（UDP） | 5,246 | CAPWAPv4 制御チャネル |
| | 17（UDP） | 5,247 | CAPWAPv4 データ チャネル |
| バージョン 6 | 136（UDP Lite） | 5,246 | CAPWAPv6 制御チャネル |
| | 136（UDP Lite） | 5,247 | CAPWAPv6 データ チャネル |

IPv6 では、AP と WLC のパフォーマンスに影響を与える User Datagram Protocol（UDP）の完全なペイロード チェックサムが必須です。IPv6 導入に対するパフォーマンスを最大化するために、AP および WLC では、ペイロード全体ではなくヘッダーのみのチェックサムを実行する UDP Lite を実装しています。

（注）　リリース 5.2 以降では、LWAPP は非推奨になっており、CAPWAP によって置換されています。5.2 以降で動作している WLC に接続する古い LWAPP AP は CAPWAP をサポートするように自動的にアップグレードされます。

図 2-1 は、CAPWAP AP が CAPWAP プロトコル経由で WLC に接続する基本的な中央集中型 WLAN 展開の概略図を示しています。リリース 8.0 以降では、CAPWAP は IPv4 と IPv6 のいずれのトランスポート モードでも動作可能です。デフォルトでは、IPv4 が推奨されますが設定可能です（この項で後述）。

*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、本書では中央集中型 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。

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

- IP アドレッシング：WLC を正常に検出し、通信できるようにするには、AP に静的または動的な IPv4 または IPv6 アドレスを割り当てる必要があります。レイヤ 2 モードは CAPWAP ではサポートされません。
- ファイアウォール ルールおよび ACL：AP と WLC の間に配置されているデバイスに定義されているすべてのファイアウォール ルールおよび ACL は、CAPWAP プロトコルを許可するように設定されている必要があります（表 2-1 を参照）。
- IPv6 導入：IPv6 をサポートしていない古いファームウェアで動作している AP をサポートするために、少なくとも 1 台の WLC は IPv4 と IPv6 の両方用に設定されている必要があります。

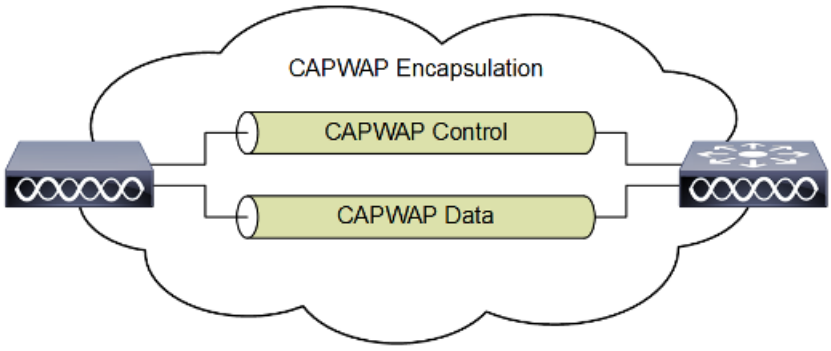
CAPWAP の主要機能は、以下のとおりです。

- スプリット MAC アーキテクチャ
- 暗号化
- レイヤ 3 トンネル
- WLC ディスカバリおよび選択

# スプリット MAC アーキテクチャ

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 の概念を示しています。

*図 2-2　スプリット MAC アーキテクチャ*




Access Point MAC Functions:

- 802.11: Beacons, Probe Responses.
- 802.11 Control: Packet Acknowledgements and Transmission.
- 802.11e: Frame Queuing and Packet Prioritization.
- 802.11i: MAC Layer Data Encryption and Decryption.

Controller MAC Functions:

- 802.11 MAC: Management: Association Requests and Actions.
- 802.11e: Resource Reservation.
- 802.11i: Authentication and Key Management.

図 2-3 に示す最も単純な汎用 802.11 AP は、基本サービス セット識別子（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、前述のシングル AP の概念が拡張され、図 2-4 に示すように、複数台の AP で Extended Service Set（ESS）を提供できます。この場合、複数台の AP で同じ ESS Identifier（ESSID、通常 SSID と呼ばれます）を使用することで、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ます。

図 2-5 の 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、次の 2 つの機能コンポーネントに割り振ります。

- CAPWAP AP
- WLC

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、導入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 の導入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 2-3　シングル AP*

*図 2-4　ESS に組み込まれた AP*

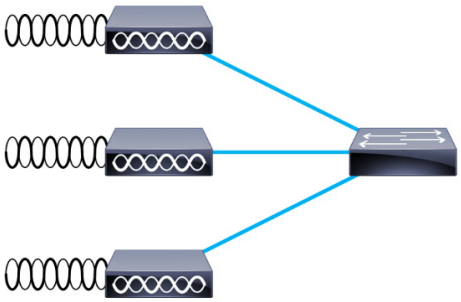
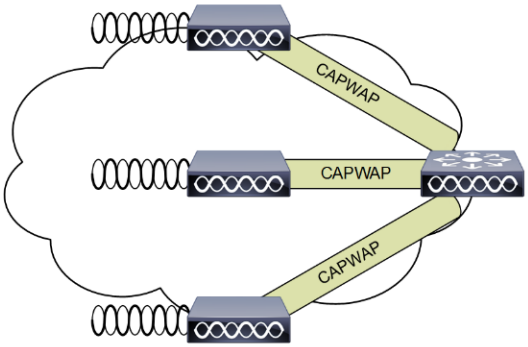


*図 2-5　CAPWAP スプリット MAC ESS*




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 フレームの伝送。
- 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伝送。
- 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。

その他の機能も WLC によって処理されます。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ング
- 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、FlexConnect AP（本書の後半で説明）は除く

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。
- ワイヤレス 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、WLC で対応するインターフェイス（VLAN）またはインターフェイス グループ（VLAN プール）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 の構成時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、WLC でローカルに定義したポリシーか、認証が正常に終了した時点でアップストリーム AAA サーバから転送される RADIUS が返却する属性に基づいて、WLAN クライアントを特定の VLAN に動的にマッピングすることもできます。

一般的な 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 名
- Operational State
- 無線ポリシー
- 認証およびセキュリティ方式
- QoS/アプリケーションの可視性と制御
- ポリシーのマッピング

# 暗号化

リリース 6.0 以降では、DTLS を使用して AP と WLC の間で交換される CAPWAP コントロール パケットおよびデータ パケットの暗号化のサポートを提供しています。DTLS は TLS に基づいた IETF プロトコルです。すべての Cisco アクセス ポイントおよびコントローラには、AP および WLC が相互認証と暗号キーの生成にデフォルトで使用する、製造元でインストールされる証明書（MIC）が付属しています。Cisco では、独自の認証局（CA）から証明書を発行することを希望する企業向けに追加のセキュリティを提供するローカルで有効な証明書（LSC）もサポートしています。

（注）　DTLS ではデフォルトで、**config ap dtls-cipher-suite** コマンドを使用してグローバルに定義されている RSA 128 ビット AES/SHA-1 暗号スイートを使用します。代替暗号方式としては、SHA-1 または SHA-256 を使用する 256 ビット AES があります。

CAPWAP 制御チャネルを保護するために DTLS は、デフォルトではイネーブルになっていますが、データ チャネルではデフォルトでディセーブルになっています。制御チャネルを保護するために、DTLS ライセンスは必要ありません。AP と WLC の間で交換されるすべての CAPWAP 管理トラフィックおよびコントロール トラフィックは、コントロール プレーン プライバシーを提供するためと中間者（MIM）攻撃を防止するためにデフォルトで暗号化および保護されます。

CAPWAP データ暗号化はオプションであり、AP ごとに有効化されます。データ暗号化を使用するには、AP で有効化する前に、WLC に DTLS ライセンスをインストールしておく必要があります。有効化されている場合、すべての WLAN クライアント トラフィックは AP で暗号化されてから WLC に転送されます。この逆も同様です。DTLS データ暗号化は OfficeExtend AP に対しては自動的に有効化されますが、他のすべての AP に対してはデフォルトで無効化されます。ほとんどの AP はデータ暗号化を必要としない保護されたネットワークに導入されます。反対に、OfficeExtend AP と WLC の間のトラフィックは保護されていないパブリック ネットワーク越しに転送されるため、これらの AP ではデータ暗号化が重要です。

（注）　現地の規制において DTLS 暗号化が許可されていることをご確認ください。たとえば、DTLS データ暗号化は現在ロシアでは禁止されています。

WLC での DTLS データ暗号化可用性は次のとおりです。

- Cisco 5508：DTLS データ サポートありでもなしでも注文できます。cisco.com では、DTLS サポートがあるファームウェア イメージと DTLS サポートがないファームウェア イメージが個別に提供されています。
- Cisco 2500、3504、5520、8540、WiSM2、vWLC：DTLS データ サポートを有効化するには、ライセンスを別途購入する必要があります。
- Cisco 3504、Flex 7500 および 8510：DTLS データ サポートが組み込まれています。DTLS データ サポートを有効化するためにライセンスを別途購入またはインストールする必要はありません。

DTLS データ暗号化が使用できる AP は次のとおりです。

- Cisco 1522、1530、1540、1550、1552、1560、1600、1700、1810、1815、1850、2600、2700、2800、3500、3600、3700、および 3800 シリーズ：DTLS データ暗号化はハードウェアで行われます。

(注)　DTLS データ暗号化を有効にすると、AP と WLC の両方のパフォーマンスに影響します。したがって DTLS データ暗号化は、保護されていないネットワーク越しに導入されている AP だけで有効化する必要があります。

# レイヤ 3 トンネル

レイヤ 2 とレイヤ 3 のいずれのモードでも動作する LWAPP とは異なり、CAPWAP はレイヤ 3 でのみ動作し、AP と WLC の両方で IP アドレスの提示を必要とします。CAPWAP では、IPv4 導入には UDP、IPv6 導入には UDP または UDP Lite（デフォルト）を使用することで、中間ネットワーク越しの AP と WLC 間の通信を円滑にしています。CAPWAP でトンネル パケットのフラグメンテーションおよびリアセンブルを実施できます。これにより、WLAN クライアント トラフィックでは 1500 バイトの MTU 全体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リアセンブル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 を導入するうえ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。

以下の図は、IPv4 ネットワーク越しの CAPWAP 操作を示すための CAPWAP パケット キャプチャです。復号化のサンプルは、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。

図 2-6 は、CAPWAP コントロール パケットの復号化を示しています。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 UDP 宛先ポート 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 により使用されるコンフィギュレーション コマンドを表します。CAPWAP コントロール パケットのペイロードは、AP が WLC に接続している場合、デフォルトで DTLS を使用して AES 暗号化されます。

*図 2-6　CAPWAP コントロール パケット*

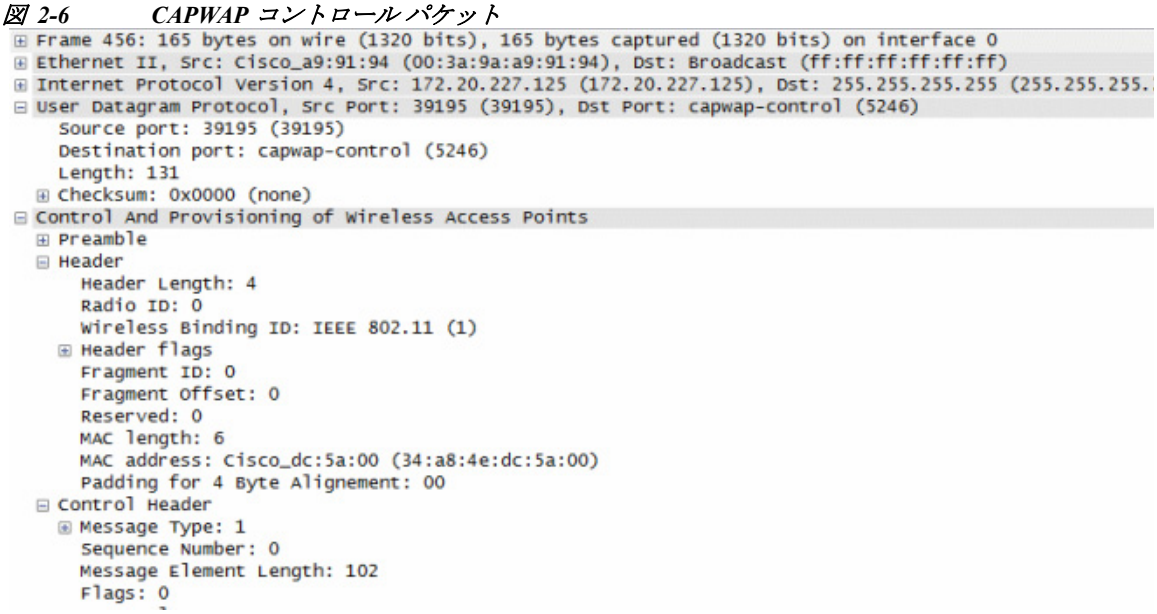



図 2-7 は、802.11 プローブ要求を含む CAPWAP パケットの復号化の一部を示しています。すべての CAPWAP でカプセル化される 802.11 フレームと同様、このパケットも UDP 宛先ポート 5246 を使用して CAPWAP AP から WLC に送られるパケットです。この例では、RF 情報を WLC に提供するために、CAPWAP パケットには、受信信号強度表示（RSSI）の値と信号対雑音比（SNR）の値も含まれています。この例では、DTLS データ暗号化は有効になっていません。

*図 2-7　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 2-8 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 2-7 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。この図は、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 2-8 は、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。

**（注）** Wireshark 復号化では、フレーム制御復号化バイトがスワップされています。これは、一部の 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。この例では、DTLS データ暗号化は有効になっていません。

*図 2-8　CAPWAP 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
```

# CAPWAP モード

リリース 8.0 以降、Cisco Unified Wireless Network（CUWN）では、IPv4 と IPv6 のいずれのアドレッシングを使用しているアクセス ポイントおよびコントローラもサポートしています。ネットワーク管理者は AP と WLC の導入に純然たる IPv4 または IPv6 のネットワークを使用することもできれば、デュアルスタック ネットワークを使用して IPv4 から IPv6 への遷移を円滑にすることもできます。8.0 リリースの一環として CAPWAP プロトコルおよびディスカバリ メカニズムが拡張され、IPv6 がサポートされるようになりました。CAPWAP は、特定のネットワーク環境向けに IPv4（CAPWAPv4）モードまたは IPv6（CAPWAPv6）モードで動作可能になりました。

ネットワーク管理者は、両方の IP プロトコル バージョンをサポートするために、AP が WLC を接続するときの優先 CAPWAP モード（CAPWAPv4 または CAPWAPv6）を設定できます。優先モードは次の 2 つのレベルで設定できます。

- グローバル設定（図 2-9）
- AP グループ固有（図 2-10）

*図 2-9　CAPWAP 優先モード(グローバル設定)*

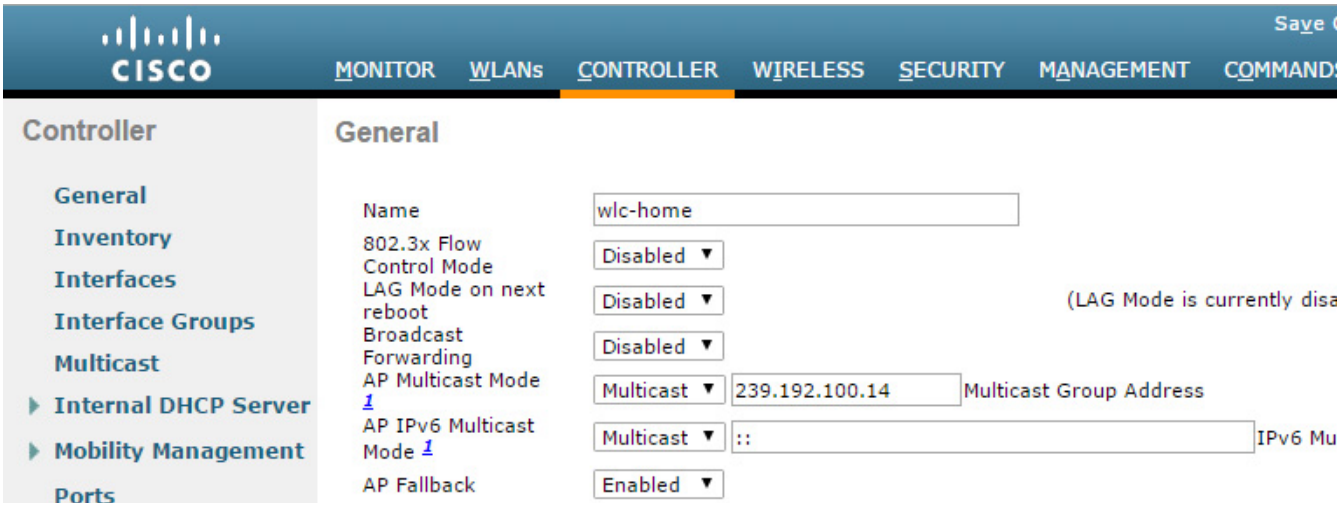
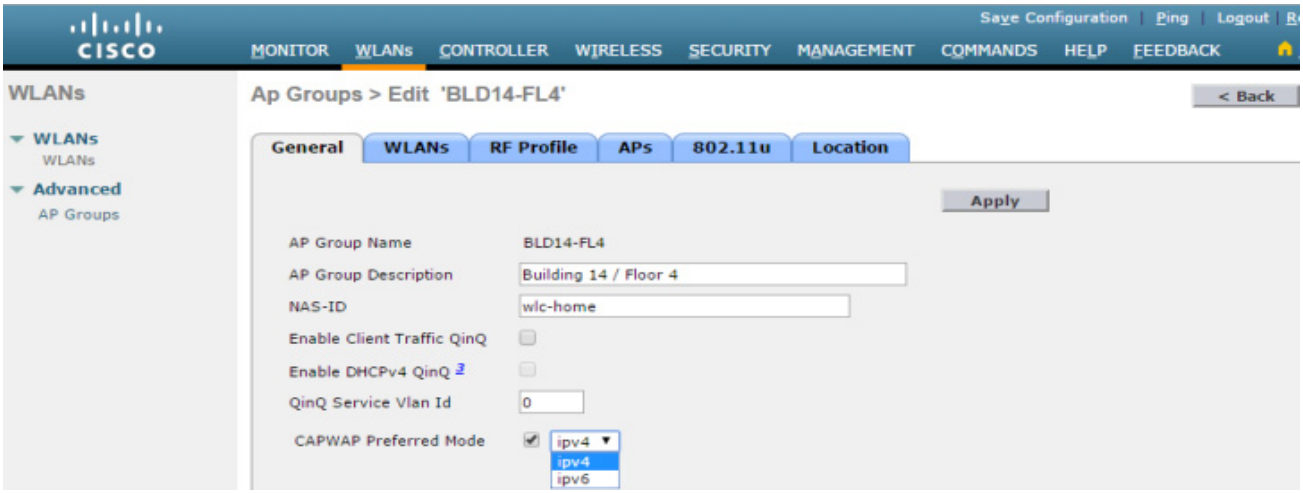



*図 2-10　CAPWAP 優先モード(AP グループ固有)*




CAPWAP モードでは、AP による選択は、AP と WLC の両方に実装されている IP アドレス バージョン、AP に定義されているプライマリ、セカンダリ、ターシャリの WLC アドレス、AP にプッシュされた優先モードなど、さまざまな要因に基づいて行われます。

使用可能な CAPWAP 動作モードの設定の概要を次に示します。

- デフォルト:グローバル優先モードは、IPv4 に設定され、デフォルト AP グループ優先モードは未設定に設定されます。AP にプライマリ、セカンダリ、またはターシャリ WLC IPv6 アドレスが準備されていない場合を除き、AP ではデフォルトでは IPv4 を優先することになります。
- AP グループ固有:優先モード(IPv4 または IPv6)は、AP グループの優先モードが設定されており、AP がそのグループに属している場合のみ、AP に適用されます。優先モードが定義されていない場合はグローバル優先モードが継承されます。
- グローバル:この優先モードは、デフォルト AP グループおよび優先モードが設定されていないその他のすべての AP グループに適用されます。デフォルト AP グループの優先モードは手動で定義できないことに注意してください。

- 接続失敗：優先モードが設定されている AP がコントローラに接続しようとして失敗すると、他のモードにフォールバックして同じコントローラへの接続を試行します。両方のモードが失敗すると、AP は次のディスカバリ応答に移動します。
- 静的設定：静的 IP 設定はグローバルまたは AP グループ固有の優先モードよりも優先されます。たとえば、グローバル優先モードが IPv4 に設定されており、AP にプライマリ コントローラの静的 IPv6 アドレスが定義されている場合、AP では CAPWAPv6 モードを使用して WLC を接続します。

AP グループ固有の優先モードを使用すると、さまざまな AP グループで利用する CAPWAP トランスポート モードに管理者が具体的に影響を与えることができるため柔軟性が向上します。これにより、異なるビルディングまたはサイトをまたがって導入されている AP が異なる CAPWAP モードを使用して動作できます。たとえば、すでに IPv6 に移行したキャンパスにある AP では CAPWAPv6 を使用して WLC を接続できる一方で、IPv6 にまだ移行していないリモート サイトにある AP では CAPWAPv4 を使用して WLC を接続できます。デュアルスタック設定の個々の WLC では、CAPWAPv4 モードと CAPWAPv6 モードのいずれのモードで動作している CAPWAP AP でもサポートできます。

（注）　IPv6 に対応していない古いイメージを実行している AP は、WLC に IPv4 アドレスが割り当てられている場合に限り、IPv6 対応 WLC を接続できます。IPv4 対応 WLC を接続しようとしている IPv6 対応 AP でも同様です（AP に IPv4 アドレスが割り当てられていることが前提）。IPv6 導入では、検出可能な WLC を 1 台以上、IPv4 をサポートするように設定することをお勧めします。

8.0 で追加された IPv6 強化の詳細については、『Cisco Wireless LAN Controller IPv6 Deployment Guide』を参照してください。

# WLC ディスカバリおよび選択

CAPWAP 環境では、Lightweight AP は CAPWAP ディスカバリ メカニズムによって WLC を検知し、コントローラに CAPWAP 接続要求を送信します。AP が WLC を接続すると、WLC によって AP の構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。CAPWAP AP を Cisco Unified Wireless Network のアクティブ パートにするには、その前に AP が WLC を検出して接続する必要があります。

各 Cisco AP では、次のディスカバリのプロセスがサポートされています。

**ステップ 1**　ブロードキャスト ディスカバリ：AP は、IPv4 ブロードキャスト アドレス（255.255.255.255）に CAPWAP ディスカバリ メッセージを送信します。同じ VLAN に接続されているすべての WLC がディスカバリ メッセージを受信することになり、ユニキャスト IPv4 ディスカバリ応答で応じることになります。

**ステップ 2**　マルチキャスト ディスカバリ：AP は、すべてのコントローラ マルチキャスト グループ アドレス（FF01::18C）に CAPWAP ディスカバリ メッセージを送信します。同じ VLAN に接続されているすべての WLC がディスカバリ メッセージを受信することになり、IPv6 ディスカバリ応答で応じることになります。

**ステップ 3**　ローカルに保存されているコントローラの IPv4 または IPv6 アドレス ディスカバリ：AP が事前に WLC に関連付けられていた場合は、プライマリ、セカンダリ、およびターシャリ コントローラの IPv4 または IPv6 アドレスが AP の不揮発性メモリ（NVRAM）に保存されています。今後の導入用に AP にコントローラの IPv4 または IPv6 アドレスを保存するこのプロセスは、「*アクセス ポイントのプライミング*」と呼ばれます。

**ステップ 4**　DHCP ディスカバリ：DHCPv4 サーバや DHCPv6 サーバは、ベンダー固有のオプションを使用して AP に WLC の IP アドレスをアドバタイズするように設定されます。

- オプション 43 を使用した DHCPv4 ディスカバリ：DHCPv4 サーバはオプション 43 を使用して、1 個以上の WLC 管理 IPv4 アドレスを AP に提供します。オプション 43 値は DHCPv4 の OFFER パケットおよび確認応答パケットで AP に提供されます。
- オプション 52 を使用した DHCPv6 ディスカバリ：DHCPv6 サーバはオプション 52 を使用して、1 個以上の WLC 管理 IPv6 アドレスを AP に提供します。オプション 52 値は DHCPv6 のアドバタイズ パケットおよびリプライ パケットで AP に提供されます。

**ステップ 5**　DNS ディスカバリ：AP は cisco-capwap-controller.*localdomain*（localdomain は DHCP が割り当てる AP ドメイン名）を解決しようとして DNSv4 サーバや DNSv6 サーバに DNS クエリを送信します。

- DNSv4 ディスカバリ：WLC で管理しており、AP に提供される IPv4 アドレスごとに、cisco-capwap-controller ホスト名用のネーム サーバ上にアドレス レコードが定義されます。ネーム サーバでは、定義された各 A レコードに対する IPv4 アドレスのリストをクエリに対して返信します。
- DNSv6 ディスカバリ：WLC で管理しており、AP に提供される IPv6 アドレスごとに、cisco-capwap-controller ホスト名用のネーム サーバ上にアドレス レコードが定義されます。ネーム サーバでは、定義された各 AAAA レコードに対する IPv6 アドレスのリストをクエリに対して返信します。

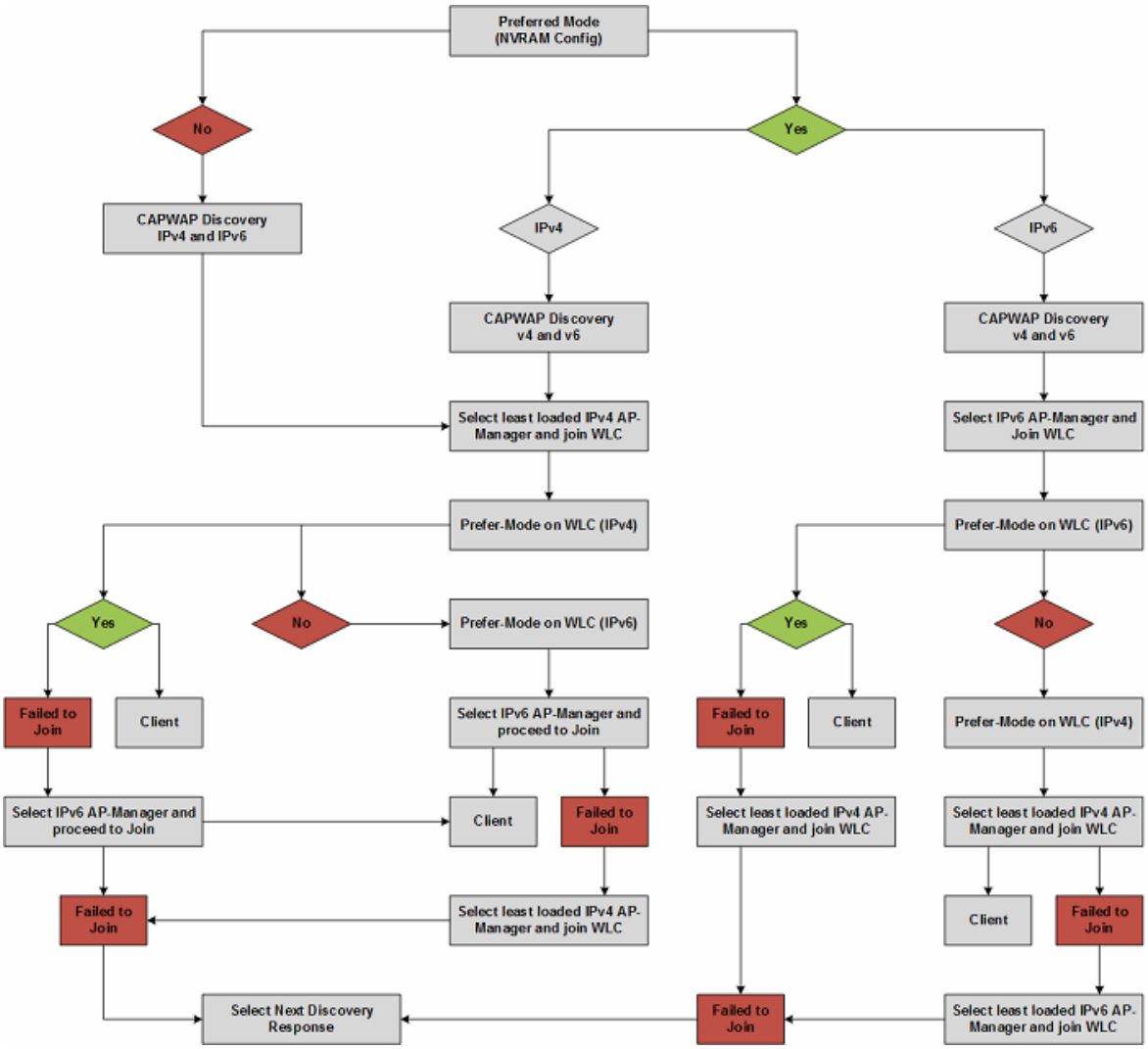
AP に提供するために DNSv4 または DNSv6 ネーム サーバに最大 3 個のアドレス レコードを定義できます。各レコードは、プライマリ、セカンダリ、およびターシャリの WLC の IPv4 または IPv6 アドレスに対応します。

**ステップ 6**　ステップ 1 ～ 5 の後、CAPWAP ディスカバリ応答が受信されない場合、AP はディスカバリのプロセスをリセットしてから、再開します。

---

WLC の選択を終えた AP では、この AP にプッシュされた CAPWAP 優先モードに応じて、CAPWAPv4 と CAPWAPv6 のいずれによって接続するのかを選択します。

*図 2-11　　AP CAPWAP ディスカバリの図*

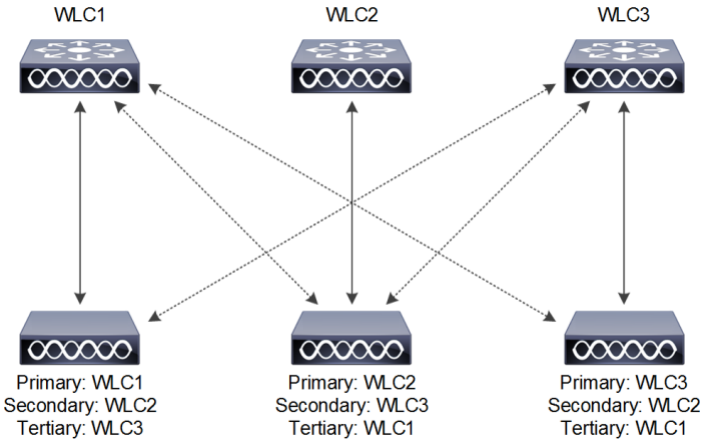


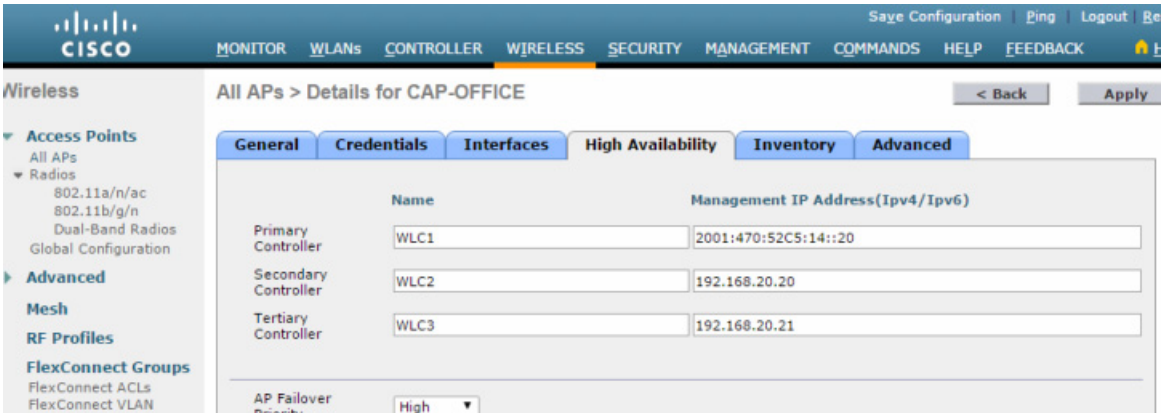

# AP プライミング

大部分の導入では、DHCP または DNS ディスカバリを使用して 1 個以上のシード WLC アドレスが提供されます。後続の WLC ディスカバリ応答によって、WLC モビリティ グループ メンバーの完全なリストが AP に提供されます。通常、AP には、優先 WLC を表す、1 ～ 3 個の WLC 管理 IP アドレスのリスト（プライマリ、セカンダリ、およびターシャリ）が設定されています。

優先 WLC が使用できなくなるか、オーバーサブスクライブされている場合、AP は CAPWAP ディスカバリ応答で確認された WLC のリストから別の WLC、つまり、最も負荷の少ない WLC を選択します。

*図 2-12　　AP プライミングの例*




(注)　AP のプライミングを行う場合、プライマリ コントローラ、セカンダリ コントローラ、およびターシャリ コントローラの管理アドレスは、IPv4 と IPv6 のどちらも使用できます。定義されているアドレスに AP によって到達可能であれば問題ありません。ただし、単一のエントリに IPv4 アドレスと IPv6 アドレスの両方は定義できません。各エントリは、IPv4 または IPv6 のアドレス 1 個のみを含むことができます。

# コア コンポーネント

Cisco Unified Wireless Network（CUWN）は、企業およびサービス プロバイダーに高性能でスケーラブルな 802.11ac ワイヤレス サービスを提供するように設計されています。Cisco ワイヤレス ソリューションは、中央集中型または分散型の導入における大規模無線 LAN の導入および管理をシンプルにするとともに同クラス最高のセキュリティ、ユーザ エクスペリエンス、およびサービスを提供します。

Cisco Unified Wireless Network は次の要素によって構成されます。

- Cisco Wireless LAN Controller（WLC）
- Cisco Aironet アクセス ポイント（AP）

- Cisco Prime Infrastructure（PI）
- Cisco Mobility Services Engine（MSE）

この項では、選択可能な WLC、AP、および PI の製品オプションについて説明します。詳細については、『Cisco Mobility Services Engine』を参照してください。

（注）　便宜上の理由からと一貫性を維持するために、このマニュアルでは、すべての Cisco Wireless LAN Controller を WLC、Aironet アクセス ポイントを AP、Cisco Prime Infrastructure を PI と表記します。

# Cisco ワイヤレス LAN コントローラ

Cisco Wireless LAN Controller は、802.11a/n/ac プロトコルおよび 802.11b/g/n プロトコルをサポートする、エンタープライズクラスの高性能ワイヤレス スイッチング プラットフォームです。無線リソース管理（RRM）機能が搭載されているオペレーティング システムの制御下でコントローラを稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する CUWN ソリューションが実現されます。コントローラは、高性能なネットワークおよびセキュリティ ハードウェアを中心に設計されており、他に例のないセキュリティを備えた信頼性の高い 802.11 エンタープライズ ネットワークを実現します。

ここでは、8.1 リリースでサポートされている Cisco WLC の各種モデルおよびその機能について説明します。

*表 2-2　シスコのワイヤレス コントローラの概要*

| | **Cisco 2504 ワイヤレス コントローラ** | **Cisco 5508 ワイヤレス コントローラ** | **Cisco 5520 ワイヤレス コントローラ** | **Cisco Flex 7510 ワイヤレス コントローラ** | **Cisco 8510 ワイヤレス コントローラ** | **Cisco 8540 ワイヤレス コントローラ** | **ワイヤレス サービス モジュール 2** | **仮想ワイヤレス コントローラ** |
|---|---|---|---|---|---|---|---|---|
| フォーム ファクタ | 1U アプライアンス | 1U アプライアンス | 1U アプライアンス | 1U アプライアンス | 1U アプライアンス | 2U アプライアンス | - | ソフトウェア |
| プラットフォーム統合 | 該当なし | 該当なし | 該当なし | 該当なし | 該当なし | 該当なし | - | 該当なし |
| 拡張性 | 75 X アクセス ポイント<br>1,000 X クライアント<br>1 Gbps スループット | 500 X アクセス ポイント<br>7,000 X クライアント<br>8 Gbps スループット | 1500 X アクセス ポイント<br>20,000 X クライアント<br>20 Gbps スループット | 6000 X アクセス ポイント<br>64,000 X クライアント<br>2000 X FlexConnect グループ | 6000 X アクセス ポイント<br>64,000 X クライアント<br>10 Gbps スループット | 6000 X アクセス ポイント<br>64,000 X クライアント<br>40 Gbps スループット | - | 200（小）/3000（大）アクセス ポイント<br>6,000（小）クライアント/ 32,000（大）X クライアント<br>200（小）/3000（大）X FlexConne ct グループ |

*表 2-2　シスコのワイヤレス コントローラの概要（続き）*

| | Cisco 2504 ワイヤレス コントローラ | Cisco 5508 ワイヤレス コントローラ | Cisco 5520 ワイヤレス コントローラ | Cisco Flex 7510 ワイヤレス コントローラ | Cisco 8510 ワイヤレス コントローラ | Cisco 8540 ワイヤレス コントローラ | ワイヤレス サービス モジュール 2 | 仮想ワイヤレス コントローラ |
|---|---|---|---|---|---|---|---|---|
| 基本 AP ライセンス | 0.5、15、25、50 台の AP | 0、12、25、50、100、250 台の AP の増分（CISL ベース） | 0、50 台の AP | 0、300、500、1000、2000、3000、6000 台の AP | 0、300、500、1000、2000、3000、6000 台の AP | 0 および 1000 AP | - | 5 台の AP |
| AP 追加ライセンス | 1.5、25 台の AP の増分（CISL ベース） | 5、25、50、100、250 台の AP の増分（CISL ベース） | 1 台の AP の増分（使用権） | 100、200、500、1000 台の AP の増分（使用権） | 100、200、500、1000 台の AP の増分（使用権） | 1 AP の増分（使用権） | - | 1,5 および 25 AP の増分（使用権） |
| High Availability（高可用性） | N+1 | N+1 SSO | N+1 SSO | N+1 SSO | N+1 SSO | N+1 SSO | - | N+1 |
| アップリンク インターフェイス | 4 X 1G イーサネット ポート（RJ45） | 8 X 1G イーサネット ポート（SFP） | 2 X 1G/10G イーサネット ポート（SFP/SFP+） | 1 X 10G イーサネット ポート（SFP+） | 1 X 10G イーサネット ポート（SFP+） | 4 X 1 G/10 G イーサネット ポート（SFP/SFP+） | - | 1 X 仮想 |
| 電源 | 外部 AC 電源 | AC（冗長 PSU オプション） | AC（冗長 PSU オプション） | AC/DC（デュアル冗長） | AC/DC（デュアル冗長） | AC/DC（デュアル冗長） | AC/DC (Catalyst シャーシ) | ホストに依存 |
| 位置付け | ブランチ、小規模オフィス | 企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス | 企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス | 多数の分散したコントローラなしのブランチ オフィスに対応するセントラル サイトのコントローラ | 企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ | 企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ | エンタープライズ キャンパス | SP-Wi-Fi、コントローラなしのブランチ、小規模オフィス |

# Cisco 2504 ワイヤレス コントローラ

Cisco 2504 ワイヤレス コントローラは、中小企業およびブランチ オフィスにおいて、ワイヤレス機能をシステム全体で実現します。802.11n と 802.11ac の性能に合わせて設計された Cisco 2504 ワイヤレス コントローラは、Cisco Aironet アクセス ポイント間のリアルタイム通信を実現してワイヤレス ネットワークの導入と運用をシンプルにするエントリレベルのコントローラです。

| | | |
|---|---|---|
| Cisco 2504 ワイヤレス コントローラ | **導入タイプ** | ブランチ、小規模オフィス |
| | **動作モード** | すべてのモード |
| | **最大スケール** | 75 AP<br>1,000 クライアント |
| | **AP 数の範囲** | 5 ～ 75 |
| | **ライセンスの権限付与** | CISL ベース |
| | **Connectivity** | 4 X 1G イーサネット ポート（RJ-45） |
| | **電源** | 外部 AC 電源 |
| | **最大スループット** | 1 Gbps |
| | **FlexConnect の最大グループ数** | 30 |
| | **FlexConnect グループあたり最大 AP 数** | 20 |
| | **最大不正 AP 数** | 2,000 |
| | **最大不正クライアント数** | 2,500 台 |
| | **最大 RFID タグ数** | 500 |
| | **RF グループあたり最大 AP 数** | 500 |
| | **最大 AP グループ数** | 75 |
| | **最大インターフェイス グループ数** | 64 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 16 |
| | **最大 WLAN 数** | 16 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 700 |

Cisco 2504 ワイヤレス コントローラの詳細については、『Cisco 2500 Series Wireless Controllers』を参照してください。

# Cisco 3504 ワイヤレス コントローラ

Cisco 3504 ワイヤレス コントローラは、コンパクト性、優れた拡張性、豊富なサービス、回復力、柔軟性を備えた業界初のマルチギガビット イーサネット プラットフォームで、中小企業および展開において次世代のワイヤレス ネットワークを可能にします。802.11ac Wave2 の性能に合わせて最適化された Cisco 3504 ワイヤレス コントローラは、中小企業およびブランチ オフィスに一元化された制御、管理、トラブルシューティングを提供します。

| | | |
|---|---|---|
| Cisco 3504 ワイヤレス コントローラ | **導入タイプ** | 小～中規模のエンタープライズ キャンパスおよびフル サービス ブランチ |
| | **動作モード** | すべてのモード |
| | **最大スケール** | 150 台の AP<br>3,000 のクライアント |
| | **AP 数の範囲** | 1 - 150 |
| | **ライセンスの権限付与** | 使用権（EULA）、Cisco SMART Licensing |
| | **Connectivity** | 1 X MGig（1、2.5、5 Gbps）、4 X 1 G イーサネット ポート（RJ-45） |
| | **電源** | 外部 AC 電源 |
| | **最大スループット** | 4 Gbps |
| | **最大 FlexConnect グループ数** | 100 |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 600 |
| | **最大不正クライアント数** | 1,500 |
| | **最大 RFID タグ数** | 1,500 |
| | **RF グループあたり最大 AP 数** | 500 |
| | **最大 AP グループ数** | 150 |
| | **最大インターフェイス グループ数** | 512 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 4094 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 14,00 |

Cisco 2504 ワイヤレス コントローラの詳細については、Cisco 3500 Series Wireless Controllers（Cisco 3500 シリーズ ワイヤレス コントローラ）を参照してください。

# Cisco 5508 ワイヤレス コントローラ

Cisco 5508 ワイヤレス コントローラは、ミッションクリティカルなワイヤレス用に信頼性の高いパフォーマンス、強化された柔軟性、およびゼロ サービスロスを提供します。音声やビデオなどのインタラクティブなマルチメディア アプリケーションがワイヤレス ネットワーク越しにそつなく動作可能になっており、クライアントはサービスの中断なしにタイミングよくローミング可能です。柔軟性の高いライセンスによってアクセス ポイントのサポートや高性能ソフトウェア機能を簡単に追加できます。

| | | |
|---|---|---|
| Cisco 5508 ワイヤレス コントローラ | **導入タイプ** | 企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス |
| | **動作モード** | すべての AP モード |
| | **最大スケール** | 500 AP<br>7,000 クライアント |
| | **AP 数の範囲** | 12 ～ 500 |
| | **ライセンスの権限付与** | CISL ベース |
| | **Connectivity** | 8 X 1G イーサネット ポート（SFP） |
| | **電源** | AC（冗長 PSU オプション） |
| | **最大スループット** | 8 Gbps |
| | **FlexConnect の最大グループ数** | 100 |
| | **FlexConnect グループあたり最大 AP 数** | 25 |
| | **最大不正 AP 数** | 2,000 |
| | **最大不正クライアント数** | 2,500 台 |
| | **最大 RFID タグ数** | 5000 |
| | **RF グループあたり最大 AP 数** | 1000 |
| | **最大 AP グループ数** | 500 |
| | **最大インターフェイス グループ数** | 64 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 512 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 14,000 |

Cisco 5508 ワイヤレス コントローラの詳細については、『Cisco 5500 Series Wireless Controllers』を参照してください。

# Cisco 5520 ワイヤレス コントローラ

Cisco 5520 シリーズ ワイヤレス LAN コントローラは、高度なスケーラビリティ、豊富なサービス、回復力、および柔軟性を備えたプラットフォームで、中規模から大規模なエンタープライズおよびキャンパスでの導入に最適です。シスコ ユニファイド アクセス ソリューションの一部である 5520 は次世代ワイヤレス ネットワークの 802.11ac Wave 2 用に最適化されています。

| | | |
|---|---|---|
| Cisco 5520 ワイヤレス コントローラ | **導入タイプ** | 企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス |
| | **動作モード** | すべての AP モード |
| | **最大スケール** | 1,500 AP<br>20,000 クライアント |
| | **AP 数の範囲** | 1 ～ 1,500 |
| | **ライセンスの権限付与** | 使用権（EULA） |
| | **Connectivity** | 2 X 10G イーサネット ポート（SFP+） |
| | **電源** | AC（冗長 PSU オプション） |
| | **最大スループット** | 20 Gbps |
| | **FlexConnect の最大グループ数** | 1、500 |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 24000 |
| | **最大不正クライアント数** | 32,000 |
| | **最大 RFID タグ数** | 25,000 |
| | **RF グループあたり最大 AP 数** | 3000 |
| | **最大 AP グループ数** | 1,500 |
| | **最大インターフェイス グループ数** | 512 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 4,095 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 40,000 |

Cisco 5520 ワイヤレス コントローラの詳細については、『Cisco 5500 Series Wireless Controller』を参照してください。

# Cisco Flex 7500 ワイヤレス コントローラ

Cisco Flex 7500 ワイヤレス コントローラには、ブランチ ネットワーク内に FlexConnect ソリューションを導入する際のスケーリング要件を満たすように設計されたモデルがあります。FlexConnect は、アクセス ポイントが中央のコントローラによって制御および管理されながら、データはブランチ サイト内でローカルにスイッチングできるようにすることで、ワイヤレス ブランチ ネットワークをサポートするように設計されています。Cisco Flex 7500 シリーズ クラウド コントローラは、規模が大きいときにコスト効率の良い FlexConnect ソリューションを実現することを目指しています。

| | | |
|---|---|---|
| Cisco 5520 ワイヤレス コントローラ | **導入タイプ** | 多数の分散したコントローラなしのブランチ オフィスに対応するセントラル サイトのコントローラ |
| | **動作モード** | FlexConnect、フレックス + ブリッジ |
| | **最大スケール** | 6,000 台の AP<br>64,000 クライアント |
| | **AP 数の範囲** | 300 ～ 6,000 |
| | **ライセンスの権限付与** | 使用権（EULA） |
| | **Connectivity** | 2 X 10G イーサネット ポート（SFP+）/1 つがアクティブ |
| | **電源** | AC/DC（デュアル冗長） |
| | **最大スループット** | — |
| | **FlexConnect の最大グループ数** | 2,000 |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 32,000 |
| | **最大不正クライアント数** | 24000 |
| | **最大 RFID タグ数** | 50,000 |
| | **RF グループあたり最大 AP 数** | 6000 |
| | **最大 AP グループ数** | 6000 |
| | **最大インターフェイス グループ数** | 512 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 4,095 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 64,000 |

詳細については、『Cisco Flex 7500 Series Wireless Controllers』を参照してください。

# Cisco 8510 ワイヤレス コントローラ

Cisco 8510 ワイヤレス コントローラは、非常にスケーラブルで柔軟性の高いプラットフォームであり、企業やサービス プロバイダーへの導入においてミッション クリティカルなワイヤレス ネットワーキングを実現します。

| | | |
|---|---|---|
| Cisco 8510 ワイヤレス コントローラ | **導入タイプ** | 企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ |
| | **動作モード** | すべての AP モード |
| | **最大スケール** | 6,000 台の AP<br>64,000 クライアント |
| | **AP 数の範囲** | 300 ～ 6,000 |
| | **ライセンスの権限付与** | 使用権（EULA） |
| | **Connectivity** | 2 X 10G イーサネット ポート（SFP+）/1 つがアクティブ |
| | **電源** | AC/DC（デュアル冗長） |
| | **最大スループット** | 10 Gbps |
| | **FlexConnect の最大グループ数** | 2,000 |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 32,000 |
| | **最大不正クライアント数** | 24000 |
| | **最大 RFID タグ数** | 50,000 |
| | **RF グループあたり最大 AP 数** | 6000 |
| | **最大 AP グループ数** | 6000 |
| | **最大インターフェイス グループ数** | 512 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 4,095 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 64,000 |

Cisco 8510 ワイヤレス コントローラの詳細については、『Cisco 8500 Series Wireless Controllers』を参照してください。

# Cisco 8540 ワイヤレス コントローラ

802.11ac Wave2 の性能に合わせて最適化された Cisco 8540 ワイヤレス コントローラは、高度なスケーラビリティ、豊富なサービス、回復力、および柔軟性を備えたプラットフォームで、中規模から大規模なエンタープライズおよびキャンパスでの導入において次世代のワイヤレス ネットワークを可能にします。

| | | |
|---|---|---|
| Cisco 8540 ワイヤレス コントローラ | **導入タイプ** | 企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ |
| | **動作モード** | すべての AP モード |
| | **最大スケール** | 6,000 台の AP<br>64,000 クライアント |
| | **AP 数の範囲** | 1 ～ 6,000 |
| | **ライセンスの権限付与** | 使用権（EULA） |
| | **Connectivity** | 4 X 10G イーサネット ポート（SFP+） |
| | **電源** | AC/DC（ホットスワップ可能デュアル冗長 PSU） |
| | **最大スループット** | 40 Gbps |
| | **FlexConnect の最大グループ数** | 2,000 |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 32,000 |
| | **最大不正クライアント数** | 24000 |
| | **最大 RFID タグ数** | 50,000 |
| | **RF グループあたり最大 AP 数** | 6000 |
| | **最大 AP グループ数** | 6000 |
| | **最大インターフェイス グループ数** | 512 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 4,095 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 64,000 |

Cisco 8540 ワイヤレス コントローラの詳細については、『Cisco 8500 Series Wireless Controllers』を参照してください。

# Cisco ワイヤレス サービス モジュール 2

Catalyst 6500 シリーズ スイッチ用の Cisco Wireless Services Module 2（WiSM2）は統合ソリューションが適している中規模から大規模の単一サイト WLAN 環境におけるミッションクリティカルなワイヤレス ネットワーキングに最適です。WiSM2 はハードウェアのコストの削減に役立ち、またワイヤレス ネットワークの運用と所有にかかる総コストを減らすことができる柔軟な設定オプションが用意されています。

| | | |
|---|---|---|
| Cisco Wireless Services Module 2（WiSM2） | **導入タイプ** | 企業の構内 |
| | **動作モード** | すべての AP モード |
| | **最大スケール** | 1,000 AP<br>15,000 クライアント |
| | **AP 数の範囲** | 100 ～ 1,000 |
| | **ライセンスの権限付与** | CISL ベース |
| | **Connectivity** | Catalyst バックプレーン内部 |
| | **電源** | AC/DC（Catalyst シャーシの冗長 PSU オプション） |
| | **最大スループット** | 10 Gbps |
| | **FlexConnect の最大グループ数** | 100 |
| | **FlexConnect グループあたり最大 AP 数** | 25 |
| | **最大不正 AP 数** | 4,000 |
| | **最大不正クライアント数** | 5,000 |
| | **最大 RFID タグ数** | 10,000 |
| | **RF グループあたり最大 AP 数** | 2,000 |
| | **最大 AP グループ数** | 500 |
| | **最大インターフェイス グループ数** | 64 |
| | **最大インターフェイス/インターフェイス グループ** | 64 |
| | **最大 VLAN 数** | 512 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 30,000 |

詳細については、『Cisco Wireless Services Module 2』を参照してください。

# 仮想ワイヤレス LAN コントローラ

IT 管理者は、最大 3000 台のアクセス ポイントおよび 32000 のクライアントの設定、管理、トラブルシューティングを実行できます。Cisco Virtual Wireless Controller は、セキュアなゲスト アクセス、Payment Card Industry（PCI）基準に準拠した不正検出、ブランチ（ローカルでスイッチングが行われる）オフィスでの Wi-Fi による音声およびビデオに対応しています。

| | | |
|---|---|---|
| Cisco Virtual Wireless Controller（vWLC） | **導入タイプ** | SP-Wi-Fi、コントローラなしのブランチ、小規模オフィス |
| | **動作モード** | FlexConnect、フレックス + ブリッジ |
| | **最大スケール** | 200 AP（小）/3,000 AP（大）<br>6,000 クライアント（小）/<br>32,000 クライアント（大） |
| | **AP 数の範囲** | 5 ～ 200 |
| | **ライセンスの権限付与** | 使用権（EULA） |
| | **Connectivity** | 1（仮想） |
| | **電源** | ホスト依存 |
| | **最大スループット** | N/A |
| | **最大 FlexConnect グループ数** | 200（小）/3,000（大） |
| | **FlexConnect グループあたり最大 AP 数** | 100 |
| | **最大不正 AP 数** | 800 |
| | **最大不正クライアント数** | 1,500 |
| | **最大 RFID タグ数** | 3,000 |
| | **RF グループあたり最大 AP 数** | 1,000 |
| | **最大 AP グループ数** | 200 |
| | **最大インターフェイス グループ数** | — |
| | **最大インターフェイス/インターフェイス グループ** | — |
| | **最大 VLAN 数** | 4,094 |
| | **最大 WLAN 数** | 512 |
| | **高速セキュア ローミング クライアント/PMK キャッシュ** | 6,000 |

詳細については、『Cisco Virtual Wireless Controller』を参照してください。

（注）　Cisco Virtual Wireless Controller は、VMWare の ESXi（5.x 以降）、Microsoft Hyper-V、Linux KVM を含む業界標準の仮想化インフラストラクチャでサポートされます。vWLC は、第 2 世代サービス統合型ルータ向用の Cisco Unified Computing System Express（UCS Express）でもサポートされます。8.5 リリースでは、Amazon AWS のサポートが追加されました。

# Cisco Aironet アクセス ポイント

Cisco Aironet シリーズ ワイヤレス アクセス ポイントはブランチ オフィス、キャンパス、または大規模なエンタープライズの分散型または中央集中型のネットワークに導入できます。これらのワイヤレス アクセス ポイントは次のような多様な機能を提供し、ワイヤレス ネットワークのエンドユーザ エクスペリエンスを向上させます。

- Cisco CleanAir テクノロジー：RF 干渉を回避できるセルフヒーリング（自己修復）および自己最適化ネットワークを実現します。
- Cisco ClientLink 2.0 および 3.0：クライアントの信頼性とカバレッジを向上します。
- Cisco BandSelect：混合クライアント環境における 5 GHz クライアント接続を強化します。
- Cisco VideoStream：マルチキャストを使い、マルチメディア アプリケーションの機能を向上します。

（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 導入のガイドラインについては、本書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』を参照してください。

## 屋内 802.11n アクセス ポイント

ここでは、8.1 リリースでサポートされている Cisco 屋内 802.11n AP の各種モデルおよびその機能について説明します。

| | Cisco Aironet 600 シリーズ | Cisco Aironet 700W シリーズ | Cisco Aironet 1600 シリーズ | Cisco Aironet 2600 シリーズ | Cisco Aironet 3600 シリーズ |
|---|---|---|---|---|---|
| Wi-Fi 標準 | 802.11a/b/g/n | 802.11a/b/g/n | 802.11a/b/g/n | 802.11a/b/g/n | 802.11a/b/g/n/ac |
| 無線数 | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） | トリプル（2.4 GHz および 5 GHz） |
| 最大データ レート | 300 Mbps | 300 Mbps | 300 Mbps | 450 Mbps | 450 Mbps（802.11n）<br>1.3 Gbps（802.11ac モジュール） |
| MIMO 無線の設計 | 2 X 3 | 2 X 2 | 3 X 3 | 3 X 4 | 802.11n：4 X 4<br>802.11ac：3 X 3 |
| 空間ストリーム | 2 つの空間ストリーム | 2 つの空間ストリーム | 2 つの空間ストリーム | 3 つの空間ストリーム | 3 つの空間ストリーム |
| アンテナ | 内部 | 内部 | 1600i 内蔵<br>1600e 外付け | 2600i：内蔵<br>2600e：外付け | 3600i：内蔵<br>3600e：外付け<br>3600p：外付け |
| CleanAir 2.0 | — | — | CleanAir Express | Yes | Yes |
| ClientLink 2.0 | — | — | Yes | Yes | Yes |

| | Cisco Aironet 600 シリーズ | Cisco Aironet 700W シリーズ | Cisco Aironet 1600 シリーズ | Cisco Aironet 2600 シリーズ | Cisco Aironet 3600 シリーズ |
|---|---|---|---|---|---|
| シスコの革新技術 | — | BandSelect<br>VideoStream | BandSelect<br>VideoStream | BandSelect<br>VideoStream | BandSelect<br>VideoStream |
| モジュール方式 | USB* | — | — | — | 802.11ac Wave 1 モジュール<br>USC スモール セル モジュール<br>ワイヤレス セキュリティ モジュール（WSM） |
| 電源 | AC | DC、802.3afPoE、802.3at PoE+ | DC、802.3afPoE | DC、802.3afPoE | DC、802.3afPoE、802.3at PoE+、Enhanced PoE、Universal PoE |
| インターフェイス | 5 X 1G イーサネット ポート（RJ-45）<br>1 X 1G イーサネット WAN ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45）<br>4 X 1G イーサネット ユーザ ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45） |

### Cisco Aironet 600 シリーズ OfficeExtend

Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントは、家庭環境における安全性の高いエンタープライズ ワイヤレス カバレッジを実現します。これらのデュアル バンド 802.11n アクセス ポイントによって社内ネットワークが在宅テレワーカーおよびモバイル契約業者まで拡張されます。このアクセス ポイントは、自宅のブロードバンド インターネット アクセスに接続し、社内ネットワークへのセキュアなトンネルを確立します。これにより、リモートの従業員は、データ、音声、ビデオ、およびクラウド サービスにアクセスできるため、会社のオフィスにいるのと同じようなモビリティ エクスペリエンスを実現します。デュアル バンドで 2.4 GHz と 5 GHz の無線周波数を同時にサポートすることは、2.4 GHz 帯域を使用する一般的な家庭用デバイスによる輻輳の影響を社内のデバイスが受けないことを請け合うために役立ちます。Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントは、家庭内のトラフィックのセグメント化を行って個人の家庭内のデバイス用に企業データ アクセスの保護をサポートすることと、接続性を維持することによってテレワーカー向けに特に設計されています。

| | | |
|---|---|---|
| Cisco Aironet 600 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n |
| | **動作モード** | OfficeExtend |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 300 Mbps |
| | **MIMO の設計** | 2 X 3 |
| | **空間ストリーム** | 2 |
| | **最大クライアント数** | 15 |
| | **最大 ClientLink 数** | — |
| | **ClientLink 2.0** | — |
| | **CleanAir** | — |
| | **VideoStream** | — |
| | **BandSelect** | — |
| | **不良 AP 検出** | — |
| | **適応型 wIPS** | — |
| | **電源** | AC |
| | **アンテナ** | 内部 |

Cisco Aironet 600 シリーズの詳細については、『Cisco Aironet 600 Series OfficeExtend Access Point』を参照してください。

### Cisco Aironet 700W シリーズ

Cisco Aironet 700W シリーズは、ますます複雑化していく今日のワイヤレス アクセス需要に対応できるようにネットワークを刷新したいと考える接客業および教育業界のお客様向けのコンパクトで壁面プレートに取り付け可能なアクセス ポイントです。

Cisco Aironet 700W シリーズは、既存の 802.11a/g ネットワークの 6 倍以上のスループットを実現する 802.11n デュアルラジオ 2 X 2 多入力、多出力（MIMO）テクノロジーを採用することにより、802.11n 品質の高いパフォーマンスを低コストで実現します。

700W シリーズ アクセス ポイントは Cisco Unified Wireless Network の構成要素として、既存のネットワークとシームレスに統合できるため、総所有コストを抑え、投資を保護することができます。

| | | |
|---|---|---|
| Cisco Aironet 700W シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n |
| | **動作モード** | 中央集中型、FlexConnect |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 300 Mbps |
| | **MIMO の設計** | 2 X 2 |
| | **空間ストリーム** | 2 |
| | **最大クライアント数** | 100 ワイヤレス/4 有線 |
| | **最大 ClientLink 数** | — |
| | **ClientLink 2.0** | — |
| | **CleanAir** | — |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3af PoE+ |
| | **アンテナ** | 内部 |

詳細については、『Cisco Aironet 700W Series』を参照してください。

### Cisco Aironet 1600 シリーズ

新しい Cisco Aironet 1600 シリーズ アクセス ポイントは、エンタープライズクラスのパフォーマンスを発揮するエントリ レベルの 802.11n ベースのアクセス ポイントで、中小企業におけるネットワークのワイヤレス接続のニーズに対応できます。

Aironet 1600 シリーズは適切な価格でお客様に優れた性能を提供するだけでなく、スペクトル インテリジェンスによってカバレッジを向上する CleanAir Express、混合クライアント ベースを持つエントリ レベル ネットワーク用の ClientLink 2.0 などの高度な機能を提供します。これらの機能に加え、Aironet 1600 シリーズには 2 つの空間ストリームを備えた 802.11n ベースの 3 X 3 MIMO テクノロジーが搭載されているため、中小企業に最適です。

Aironet 1600 シリーズは、既存の 802.11a/g ネットワークの 6 倍以上のスループットを提供します。Cisco Aironet 1600 シリーズ アクセス ポイントは、Cisco Aironet ワイヤレス ポートフォリオの一員として、既存のネットワークとシームレスに統合できるため、総所有コストを抑え、投資を保護することができます。802.11n に移行するためのエントリ レベル パスを持つ Aironet 1600 シリーズは、拡張するアプリケーションおよび帯域幅に合わせた将来の拡張のためにネットワークにキャパシティを追加できます。

急速に進化するモビリティのニーズを考慮して設計された Cisco Aironet 1600 シリーズ アクセス ポイントは、適切な料金で高度な機能を提供することにより、個人所有デバイスの持ち込み（BYOD）の動向に対応します。

| | | |
|---|---|---|
| Cisco Aironet 1600 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 300 Mbps |
| | **MIMO の設計** | 3 X 3 |
| | **空間ストリーム** | 2 |
| | **最大クライアント数** | 128 |
| | **最大 ClientLink 数** | 32 |
| | **ClientLink 2.0** | Yes |
| | **CleanAir** | Yes：CleanAir Express |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE |
| | **アンテナ** | 1600i：内蔵<br>1600e：外付け |

詳細については、『Cisco Aironet 1600 Series』を参照してください。

## Cisco Aironet 2600 シリーズ

Cisco Aironet 2600 シリーズ アクセス ポイントは、性能、機能性、および信頼性に優れた、クラス最先端の機能を魅力的な価格で提供します。802.11n ベースの Aironet 2600 シリーズには 3 X 4 MIMO が装備されており、3 つの空間ストリーム、Cisco CleanAir、ClientLink 2.0、および VideoStream テクノロジーを搭載し、干渉のない、高速なワイヤレス アプリケーション エクスペリエンスを実現します。Cisco Aironet 3600 シリーズに次ぐパフォーマンスと機能を備えた Aironet 2600 シリーズは、企業のワイヤレス テクノロジーに新しい基準を設定します。

急速に進化するモビリティのニーズを考慮して設計された Aironet 2600 シリーズ アクセス ポイントには、他のアクセス ポイントと比べて強化された BYOD 対応機能が適切な料金で組み込まれています。新しい Cisco Aironet 2600 シリーズは、他社製品と比較して、アクセス ポイントからより離れた範囲に信頼性の高い高速接続を維持することができます。その結果、450 Mbps データ レートをより広いエリアに提供します。コンシューマ デバイス用に最適化されている Aironet 2600 シリーズでは、競合ソリューションと比べてクライアント接続は高速で、モバイル デバイスのバッテリ電力は節約されます。

| | | |
|---|---|---|
| Cisco Aironet 2600 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 450 Mbps |
| | **MIMO の設計** | 3 X 4 |
| | **空間ストリーム** | 3 |
| | **最大クライアント数** | 200 |
| | **最大 ClientLink 数** | 128 |
| | **ClientLink 2.0** | Yes |
| | **CleanAir** | Yes |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3af PoE+ |
| | **アンテナ** | 2600i：内蔵<br>2600e：外付け |

詳細については、『Cisco Aironet 2600 Series』を参照してください。

## Cisco Aironet 3600 シリーズ

タブレット、スマートフォン、および高性能ラップトップの使用時に、他社製品と比較して最大 3 倍のカバレッジを提供します。業界初の 4 X 4 MIMO および 3 つの空間ストリームに対応したアクセス ポイントであり、ミッション クリティカルな用途に耐える高い信頼性を発揮します。モバイル デバイスやモバイル アプリケーションが急激に多様化し、それに伴うワイヤレス ネットワークのニーズも増加しており、昨今のソリューションはその対応に追われています。Cisco Aironet 3600 シリーズは、他社製品と比較して、アクセス ポイントからより離れた範囲に信頼性の高い高速接続を維持することができます。その結果、速度 450 Mbps の接続を最大 3 倍の広さのエリアに提供し、より多くのモバイル デバイスに最適なパフォーマンスを提供できます。Cisco Aironet 3600 シリーズは画期的なモジュラ型のプラットフォームであり、1.3 Gbps レートで稼動する着信 802.11ac クライアントをサポートする追加のモジュール拡張や、包括的なセキュリティおよび周波数帯の監視と制御を提供して、優れた投資保護を実現します。

Cisco Aironet 3600 シリーズは、パフォーマンスとクライアント カバレッジ範囲を増強する Cisco ClientLink 2.0 と、ネットワークのセルフヒーリング（自己修復）および自己最適化を可能にする Cisco CleanAir スペクトル インテリジェンスを搭載します。

| | | |
|---|---|---|
| Cisco Aironet 3600 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n<br>802.11ac（モジュール搭載） |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | トリプル（2.4 GHz、5 GHz、およびモジュール） |
| | **最大データ レート** | 802.11n：450 Mbps<br>802.11ac：1.3 Gbps |
| | **MIMO の設計** | 802.11n：4 X 4<br>802.11ac：3 X 3 |
| | **空間ストリーム** | 3 |
| | **最大クライアント数** | 802.11n：200<br>802.11ac：50 |
| | **最大 ClientLink 数** | 802.11n：128<br>802.11ac：7（ECBF） |
| | **ClientLink 2.0** | Yes（802.11ac クライアントに対する ECBF） |
| | **CleanAir** | Yes |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3at（PoE+）、Enhanced PoE、Universal PoE（UPOE） |
| | **アンテナ** | 3600i：内蔵<br>3600e：外付け<br>3600p：外付け |

詳細については、『Cisco Aironet 3600 Series』を参照してください。

# 屋内 802.11ac アクセス ポイント

ここでは、8.1 リリースでサポートされている Cisco 屋内 802.11ac AP の各種モデルおよびその機能について説明します。

| | Cisco Aironet 1700 シリーズ | Cisco Aironet 1850 シリーズ | Cisco Aironet 2700 シリーズ | Cisco Aironet 3700 シリーズ |
|---|---|---|---|---|
| Wi-Fi 標準 | 802.11a/b/g/n/ac（Wave 1） | 802.11a/b/g/n/ac（Wave 2） | 802.11a/b/g/n/ac（Wave 1） | 802.11a/b/g/n/ac（Wave 1） |
| 無線数 | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） | デュアル（2.4 GHz および 5 GHz） |
| 最大データ レート | 867 Mbps | 1.7 Gbps | 1.3 Gbps | 1.3 Gbps |
| MIMO 無線の設計 | 3 X 3 | 4 X 4 | 3 X 4 | 4 X 4 |
| 空間ストリーム | 2 つの空間ストリーム | 4 つの空間ストリーム（SU MIMO）<br>3 つの空間ストリーム（MU MIMO） | 3 つの空間ストリーム | 3 つの空間ストリーム |
| アンテナ | 1700i：内蔵 | 1850i 内蔵<br>1850e：外付け | 2700i 内蔵<br>2700e 外付け | 3700i：内蔵<br>3700e：外付け<br>3700p：外付け |
| CleanAir 2.0 | CleanAir Express | CleanAir Express | Yes | Yes |
| ClientLink 3.0 | 送信ビーム フォーミング | 送信ビーム フォーミング | Yes | Yes |
| シスコの革新技術 | BandSelect VideoStream | BandSelect VideoStream | BandSelect<br>High Density Experience VideoStream | BandSelect<br>StadiumVision<br>High Density Experience VideoStream |
| モジュール方式 | — | USB 2.0* | — | 802.11ac Wave 2 モジュール<br>USC スモール セル モジュール<br>ハイパーロケーション モジュール<br>ワイヤレス セキュリティ モジュール（WSM） |
| 電源 | DC、802.3afPoE、+、Enhanced PoE | DC、802.3afPoE、+、Enhanced PoE | DC、802.3afPoE、+、Enhanced PoE | DC、802.3afPoE、802.3at PoE+、Enhanced PoE、Universal PoE |

| | Cisco Aironet 1700 シリーズ | Cisco Aironet 1850 シリーズ | Cisco Aironet 2700 シリーズ | Cisco Aironet 3700 シリーズ |
|---|---|---|---|---|
| インターフェイス | 1 X 1G イーサネット アップリンク ポート（RJ-45）<br>1 X 1G イーサネット AUX ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45）自動 LAG あり<br>1 X 1G イーサネット AUX ポート（RJ-45）自動 LAG あり | 1 X 1G イーサネット アップリンク ポート（RJ-45）<br>1 X 1G イーサネット AUX ポート（RJ-45） | 1 X 1G イーサネット アップリンク ポート（RJ-45） |

## Cisco Aironet 1700 シリーズ

小規模または中規模のエンタープライズ ネットワークを運用している場合、Cisco Aironet 1700 シリーズ アクセス ポイントを導入することで、お手頃な価格で最新の 802.11ac Wi-Fi テクノロジーを入手できます。1700 シリーズは、802.11n よりも優れたパフォーマンスや重要な RF 管理機能を提供することで、ワイヤレス ネットワークの高まる要件に対応し、ワイヤレス エクスペリエンスを向上させます。

1700 シリーズは、802.11ac Wave 1 の標準機能をサポートしています。これには、最大 867 Mbps の理論的な接続レートが含まれます。

| | | |
|---|---|---|
| Cisco Aironet 1700 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n/ac（Wave 1） |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 867 Mbps |
| | **MIMO の設計** | 3 X 3 |
| | **空間ストリーム** | 2 |
| | **最大クライアント数** | 200 |
| | **最大 ClientLink 数** | — |
| | **ClientLink 2.0** | Yes：送信ビームフォーミング（TxBF） |
| | **CleanAir** | Yes：CleanAir Express |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3at PoE+、Enhanced PoE |
| | **アンテナ** | 1700i：内蔵<br>1700e：外付け |

詳細については、『Cisco Aironet 1700 Series』を参照してください。

## Cisco Aironet 1850 シリーズ

小規模および中規模のネットワークに最適な Cisco Aironet 1850 シリーズは、エンタープライズ クラスの 4 X 4 MIMO（IEEE の新しい 802.11ac Wave 2 仕様をサポートする 4 空間ストリームのアクセス ポイント）を通じて、企業やサービス プロバイダーに業界トップクラスのパフォーマンスを提供します。Aironet 1850 シリーズは、スマートフォン、タブレット、高性能ラップトップなど、802.11ac Wave 1 または Wave 2 サポートを統合した新しい世代の Wi-Fi クライアントにも対応しています。

| | | |
|---|---|---|
| Cisco Aironet 1850 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n/ac（Wave 2） |
| | **動作モード** | 中央集中型、FlexConnect（将来） |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 1.7 Gbps |
| | **MIMO の設計** | 4 X 4 |
| | **空間ストリーム** | 4（SU-MIMO）<br>3（MU-MIMO） |
| | **最大クライアント数** | 200 |
| | **最大 ClientLink 数** | — |
| | **ClientLink 3.0** | Yes：送信ビームフォーミング（TxBF） |
| | **CleanAir 2.0** | Yes |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3af PoE+、Enhanced PoE |
| | **アンテナ** | 1850i：内蔵<br>1850e：外付け |

詳細については、『Cisco Aironet 1850 Series』を参照してください。

## Cisco Aironet 2700 シリーズ

Cisco Aironet 2700 シリーズ Wi-Fi アクセス ポイント（AP）は、高密度の屋内環境にキャパシティを追加し、カバレッジ ギャップを埋めるために最適な料金で業界トップクラスの 802.11ac のパフォーマンスを提供します。Aironet 2700 シリーズでは、高速な 802.11ac Wi-Fi 無線を搭載するようになった新世代のスマートフォン、タブレット、および高性能ラップトップに、802.11ac の速度と機能を拡張します。

Aironet 2700 シリーズでは、最初の実装である 802.11ac Wave 1 をサポートしており、最大 1.3 Gbps の理論的な接続レートを提供します。今日のハイエンド 802.11n AP の概ね 3 倍となるレートが実現します。この高速化は、1 台だけではなく複数台の Wi-Fi デバイスを使用することが一般的な最近のモバイル ワーカーによる性能と帯域幅に対する期待を越えるために役立ちます。このため、ユーザは相対的に大きなトラフィック負荷を無線 LAN に加えており、これはデフォルトの企業アクセス ネットワークであるイーサネットを超えています。

| | | |
|---|---|---|
| Cisco Aironet 2700 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n/ac（Wave 1） |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | デュアル（2.4 GHz および 5 GHz） |
| | **最大データ レート** | 1.3 Mbps |
| | **MIMO の設計** | 3 X 4 |
| | **空間ストリーム** | 3 |
| | **最大クライアント数** | 200 |
| | **最大 ClientLink 数** | 128 |
| | **ClientLink 3.0** | Yes |
| | **CleanAir 2.0** | Yes |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3at PoE+、Enhanced PoE |
| | **アンテナ** | 2700i：内蔵<br>2700e：外付け |

詳細については、『Cisco Aironet 2700 Series Access Point』を参照してください。

## Cisco Aironet 3700 シリーズ

Cisco Aironet 3700 シリーズは、IEEE 802.11ac Wave 1 仕様に対応している、業界唯一の 4 X 4 MIMO、3 空間ストリームのエンタープライズ クラス アクセス ポイントです。企業とサービス プロバイダーのいずれのお客様にも業界トップクラスのパフォーマンスと高密度エクスペリエンス（HD エクスペリエンス）を提供します。Aironet 3700 シリーズを使用することで、スマートフォン、タブレット、高性能ラップトップなど、統合された 802.11ac サポートを含む新世代の Wi-Fi クライアントにもサポート対象を拡大できます。

最初の実装である 802.11ac Wave 1 では、現在のハイエンド 802.11n アクセス ポイントの約 3 倍に相当する最大 1.3 Gbps の速度を提供します。この製品により、エンタープライズ ネットワークおよびサービス プロバイダー ネットワークで、ワイヤレス ユーザの期待やニーズを超えるレベルのパフォーマンスと帯域幅を同様に提供できる必要な基盤を確立できます。

ワイヤレス アクセスは、その便利さにより、企業ユーザのネットワーク接続手段として急速に普及しつつあります。それに伴い、ワイヤレスに対する期待も拡大し、高密度エクスペリエンスを実現する同クラス最高の RF アーキテクチャを備えた革新的な専用チップセットを利用することで、ユーザに社内環境での自由な移動を許可しながら、日常の業務効率を低下させることなく、高い性能を提供できることが求められています。

| | | |
|---|---|---|
| Cisco Aironet 3700 シリーズ | **Wi-Fi 標準** | 802.11a/b/g/n/ac（Wave 1） |
| | **動作モード** | 中央集中型、FlexConnect、屋内メッシュ、OfficeExtend |
| | **無線数** | トリプル（2.4 GHz、5 GHz、およびモジュール） |
| | **最大データ レート** | 1.3 Mbps |
| | **MIMO の設計** | 4 X 4 |
| | **空間ストリーム** | 3 |
| | **最大クライアント数** | 200 |
| | **最大 ClientLink 数** | 128 |
| | **ClientLink 3.0** | Yes |
| | **CleanAir 2.0** | Yes |
| | **VideoStream** | Yes |
| | **BandSelect** | Yes |
| | **不良 AP 検出** | Yes |
| | **適応型 wIPS** | Yes |
| | **電源** | DC、802.3af PoE、802.3at PoE+、Enhanced PoE、Universal PoE（UPOE） |
| | **アンテナ** | 3700i：内蔵<br>3700e：外付け<br>3700p：外付け |

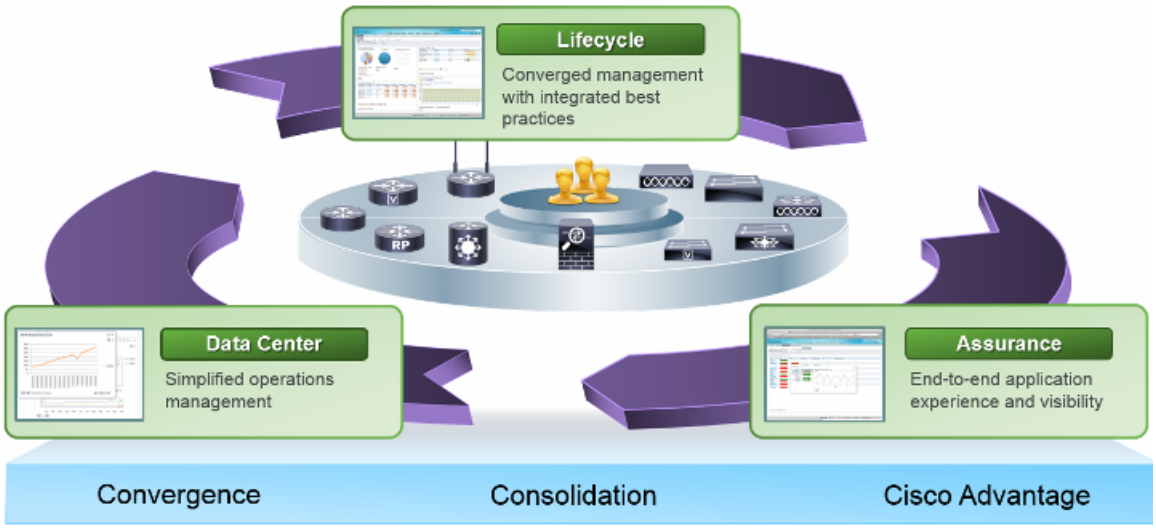
詳細については、『Cisco Aironet 3700 Series』を参照してください。

# Cisco Prime Infrastructure

変化とは経験したことのない事件です。モバイル デバイスの急増、音声とビデオの広範なコラボレーション、クラウドとデータセンターの仮想化により、ネットワークはかつてない変化を迎えようとしています。新たな機会の到来に伴って、新たな多くの課題が到来します。高いサービス レベル、確実なアプリケーション配信、簡易化されたエンドユーザ エクスペリエンスを提供しながら、ビジネスの継続性を維持し、運用コストを管理することが必要とされています。

IT プロフェッショナルたちはこれらの課題に対処するために、単一のグラフィカル インターフェイスからネットワークを管理できる包括的なソリューションを必要としています。それが Cisco Prime Infrastructure ソリューションです。ブランチ オフィスにいるワイヤレス ユーザに、WAN をまたがり、アクセス レイヤを通じ、データセンターにまで拡張された、ネットワーク全体のライフサイクル管理とサービス アシュアランスを提供します。これを One Management（一元管理）と呼びます（図 2-13）。

*図 2-13　Cisco Prime Infrastructure :One Management*




Cisco Prime Infrastructure はネットワークをデバイス、ユーザ、アプリケーションにエンドツーエンドで接続し、すべてを兼ね備えたネットワーク管理です。装備する機能によって次の内容を実現できます。

- 一括管理：Day-0 および Day-1 プロビジョニングと、それ以降の保証のために単一の統合プラットフォームを提供します。これによりデバイスとサービスの導入が加速化され、エンドユーザ エクスペリエンスに影響を及ぼす問題をすばやく解決できるようになります。ネットワーク管理に要する時間を短縮できるため、ビジネスを拡大させるためにこれを利用する時間を最大化できます。
- シスコの付加価値機能を簡単に導入：シスコの差別化機能やサービスをより迅速かつ効率的に設計し、実装することができます。Intelligent WAN（IWAN）、コンバージド アクセスを実現した分散ワイヤレス、Application Visibility and Control（AVC）、ゾーンベース ファイアウォール、Cisco TrustSec 2.0 Identity-Based Networking Services などのテクノロジーをサポートしているため、シスコ デバイスに組み込まれたインテリジェンス機能を可能な限り迅速に活用できます。
- アプリケーションの可視性：パフォーマンス データを埋め込んだ Cisco 機器および業界標準の技術を設定し、ソースとして使用されてネットワーク全体のアプリケーション対応の可視性を提供します。これらのテクノロジーには、NetFlow、Network-Based Application Recognition 2（NBAR2）、Cisco Medianet テクノロジー、Simple Network Management Protocol（SNMP）などがあります。Cisco Prime Infrastructure では、アプリケーションの可視性とライフサイクル管理という斬新な組み合わせによって、基盤となるインフラストラクチャの実行状況のコンテキストからアプリケーションおよびサービスの実行状況に関する情報を提供することにより、問題の検出と解決を容易にします。
- モバイル コラボレーションの管理：ワイヤレス アクセスに関する誰が、いつ、どこで、何を、どのようにに答えます。これには、802.11ac サポート、相関する有線/無線クライアントの可視化、ユニファイド アクセス インフラストラクチャの可視化、空間マップ、Cisco Identity Services Engine（ISE）統合によるコンバージド型のセキュリティ/ポリシーの監視とトラブルシューティング、Cisco モビリティ サービス エンジン（MSE）および Cisco CleanAir 統合を使用したロケーション ベースの干渉源/不正/Wi-Fi クライアントの追跡、ライフサイクル管理、RF 予測ツールなどが含まれます。

- ネットワークをまたがる管理とコンピューティング：強力なライフサイクル管理およびサービス アシュアランスを提供して、ブランチ オフィス、キャンパス、およびデータセンターのネットワークで実行されている多数のデバイスおよびサービスの維持管理に役立ちます。ディスカバリ、インベントリ、構成、モニタリング、トラブルシューティング、レポート作成、管理などの重要な機能を提供します。単一のビューと単一の管理ポイントによってネットワークとコンピュータの両方にまたがる One Management（一元管理）のメリットを実現します。
- 分散ネットワークの可視性の一元化：大規模またはグローバルな組織は、通常、ドメイン、地域、または国ごとにネットワーク管理を分散しています。Cisco Prime Infrastructure オペレーション センターを使用すると、最大 10 個の Cisco Prime Infrastructure インスタンスを可視化できるため、中央での可視性と制御を維持しながら、ネットワーク管理インフラストラクチャを拡張できます。

## ライセンス オプション

Cisco Prime Infrastructure は、インストール可能な単一のソフトウェア パッケージであり、ライセンス オプションによって機能とカバレッジを必要に応じて拡大、拡張できます。

- ライフサイクル：ルータ、スイッチ、アクセス ポイントなどのシスコ デバイスの全ライフサイクル フェーズ（設計、導入、運用、レポート）を通して、ネットワーク インフラストラクチャの管理に関連する日常の運用上の作業をシンプルにします。
- アシュアランス：豊富なパフォーマンス データのソースとして装置機器を使用しながらアプリケーション パフォーマンスの可視性を提供して、アプリケーション配信の一貫性と最適なエンドユーザ エクスペリエンスの保証に役立ちます。
- Cisco UCS サーバの管理：Cisco UCS B シリーズおよび C シリーズのサーバに対するライフサイクル管理および Assurance Management を提供します。
- オペレーション センター：中央の一元管理コンソールから最大 10 個の Cisco Prime Infrastructure インスタンスを可視化できます。Cisco Prime Infrastructure でサポートするインスタンスごとに 1 ライセンスが必要です。
- 高可用性使用権（RTU）：高可用性ペアを構成する 1 個のプライマリ インスタンスと 1 個のセカンダリ インスタンスを持つ高可用性構成が可能です。
- コレクタ：Cisco Prime Infrastructure 管理ノードでの NetFlow 処理の制限を上げます。このライセンスは、アシュアランス ライセンスと併せてご利用ください。
- 使用準備済みゲートウェイ RTU：使用準備済み機能で使用する別のゲートウェイを導入する権限が付与されます。この機能では、新しいデバイスがゲートウェイに接続して設定およびソフトウェア イメージを受信できます。

（注）　Cisco Prime Infrastructure 2.2 は新しいお客様に提供され、先行バージョンを実行している既存のお客様にはアップグレード オプションが提供されます。アップグレード オプションは、Cisco Network Control System（NCS）、Cisco Wireless Control System（WCS）、および Cisco Prime LAN Management Solution（LMS）をご利用のお客様にも提供されます。詳細については、http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/datasheet-listing.html を参照してください。

# スケーリング

Cisco Prime Infrastructure 2.2 は、仮想アプライアンスまたは物理アプライアンスとして購入可能です。仮想アプライアンスは業界標準の VMware ハイパーバイザ上にインストールでき、さまざまな規模のネットワークをサポートするために複数のバージョンが提供されています。物理アプライアンスは大規模ネットワーク導入でも使用できます。この場合は、専用の CPU およびメモリ リソースが必要です。

- 物理アプライアンス（第 2 世代）：Cisco UCS C220 M4 ラック サーバがベースです。
- 仮想アプライアンス：ESXi バージョン 5.0、5.1、または 5.5。

表 2-3 に、Cisco Prime Infrastructure 2.2 の仮想アプライアンスと物理アプライアンスの両方に対する拡張マトリックスを示します。

*表 2-3　Cisco Prime Infrastructure 2.2 の拡張マトリックス*

| パラメータ | | Express 仮想アプライアンス | Express Plus 仮想アプライアンス | Standard 仮想アプライアンス | Pro 仮想アプライアンス | 物理アプライアンス（Gen 1） | 物理アプライアンス（Gen 2） |
|---|---|---|---|---|---|---|---|
| デバイス | 最大 Unified AP 数 | 300 | 2,500 台 | 5,000 | 20,000 | 5,000 | 20,000 |
| | 最大 Autonomous AP 数 | 300 | 500 | 3,000 | 3,000 | 3,000 | 3,000 |
| | 最大 WLAN コントローラ数 | 5 | 25 | 500 | 1,000 | 500 | 1,000 |
| | 最大有線 | 300 | 1,000 | 6,000 | 13,000 | 6,000 | 13,000 |
| | 最大 NAM 数 | 5 | | | | | |
| | 最大デバイス数 | 1,000 | 4,000 | 15,000 | 20,000 | 15,000 | 20,000 |
| クライアント | 最大有線クライアント数 | 6,000 | 50,000 | 50,000 | 5=20,000 | 15,000 | 20,000 |
| | 最大無線クライアント数 | 4,000 | 30,000 | 75,000 | 200,000 | 75,000 | 200,000 |
| | 一時的ワイヤレス クライアント数（5 分間隔ごとのクライアント数） | 1,000 | 5,000 | 25,000 | 40,000 | 25,000 | 40,000 |
| モニタリング | 維持イベント数/秒 | 100 | 100 | 300 | 1,000 | 300 | 1,000 |
| | Netflow（フロー数/秒） | 3,000 | 3,000 | 16,000 | 80,000 | 16,000 | 80,000 |
| | Max Interfaces | 12,000 | 50,000 | 250,000 | 350,000 | 250,000 | 350,000 |
| | 最大有効 NAM データ ポーリング数 | 5 | 5 | 20 | 40 | 20 | 40 |

*表 2-3　Cisco Prime Infrastructure 2.2 の拡張マトリックス（続き）*

| パラメータ | | Express 仮想アプライアンス | Express Plus 仮想アプライアンス | Standard 仮想アプライアンス | Pro 仮想アプライアンス | 物理アプライアンス（Gen 1） | 物理アプライアンス（Gen 2） |
|---|---|---|---|---|---|---|---|
| システム | 最大サイト数/キャンパス | 200 | 500 | 2,500 | 2,500 | 2,500 | 2,500 |
| | 最大グループ数 | 50 | 100 | 150 | 150 | 150 | 150 |
| | 最大仮想ドメイン数 | 100 | 500 | 1,200 | 1,200 | 1,200 | 1,200 |
| | 最大 GUI クライアント数 | 5 | 10 | 25 | 50 | 25 | 50 |
| | 最大 API クライアント数 | 2 | 2 | 5 | 5 | 5 | 5 |

# ハイ アベイラビリティ

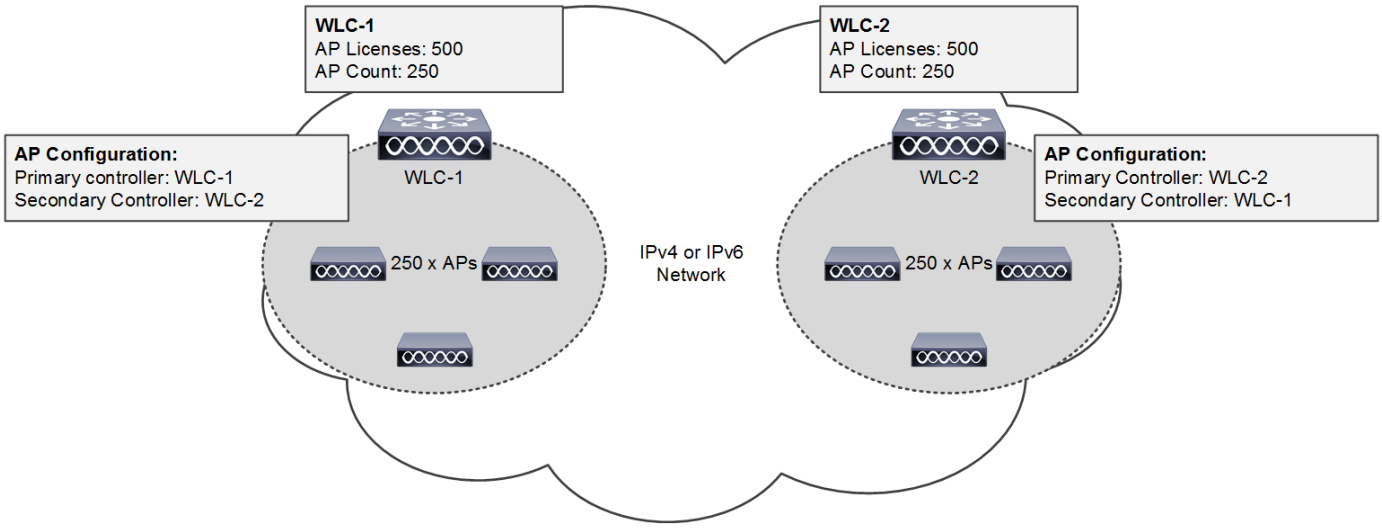
この項では、Cisco Unified Wireless Network で利用可能な高可用性（HA）導入オプションの概要を説明します。

## AP およびクライアントのフェールオーバー

### ワイヤレス コントローラの N+1 冗長性

WLC の冗長性は長い実績があり、よく知られています。冗長性は、バックアップとなり負荷を分担する複数のコントローラをネットワークに導入することによって実現されます。各 AP には IP アドレスおよび、優先されるプライマリと、セカンダリおよびターシャリの WLC の名前が設定されています。AP のプライマリ WLC が到達不能になった場合、AP は設定されているセカンダリ WLC にフェールオーバーします（その先も同様）。この冗長性モデルを N+1 と呼び、1 台（以上）のプライマリ WLC が到達不能になったときに AP および負荷をサポートする追加の WLC が利用可能であることを意味します（図 2-14 を参照）。

*図 2-14　　ワイヤレス コントローラの N+1 冗長性*




N+1 冗長性モデルを利用するには、バックアップ WLC ごとに追加の永続 AP ライセンスを購入する必要があります。バックアップ WLC は冗長性専用にしても、通常動作時に AP のサポートに使用してもかまいません。各 WLC は個別に管理され、設定を共有しません。障害発生時のシームレスな運用を確保するには、必要な WLAN、AP グループ、および RF グループを各バックアップ WLC に定義する必要があります。

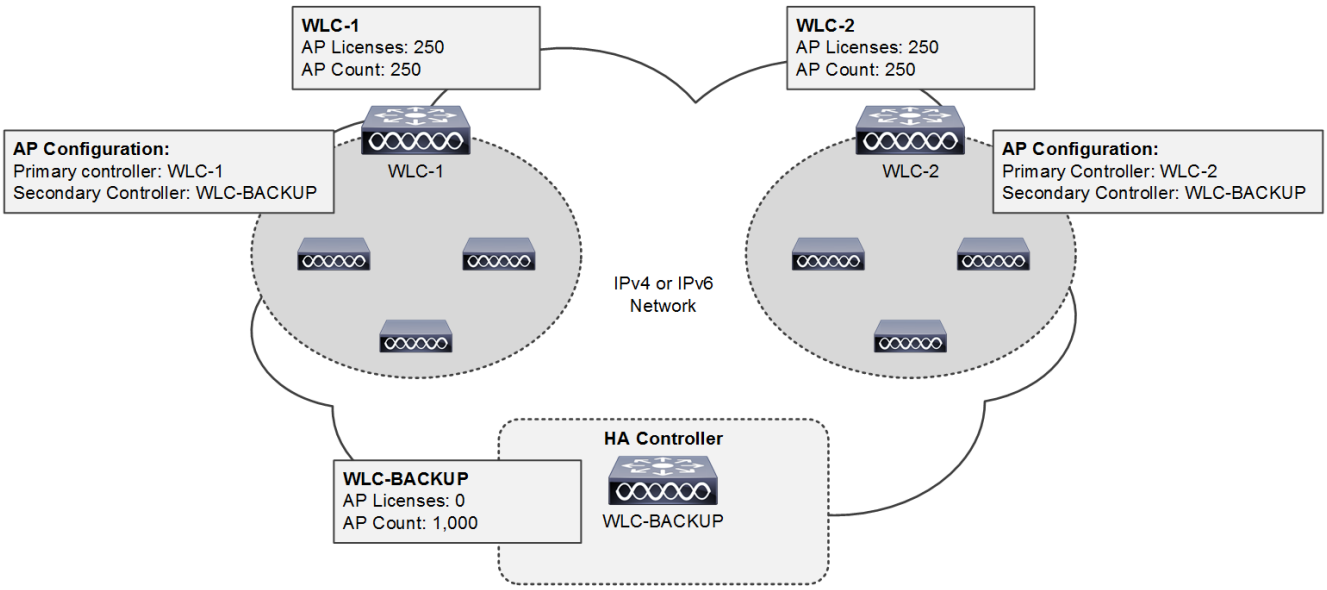
図 2-14 の例は、通常動作時にそれぞれ 250 台の AP をサポートしている 2 台の WLC を使用したシンプルな N+1 導入を示します。冗長性を実現するために各 WLC には 500 個の永続 AP ライセンスがインストールされており、WLC の 1 台が到達不能になったときにすべての AP が確実にサポートされるようになっています。WLC-1 に接続されている AP は WLC-2 をセカンダリ WLC として使用するように設定されている一方で、WLC-2 に接続されている AP は WLC-1 をセカンダリ WLC として使用するように設定されています。

(注)　大規模導入では、優先 WLC が使用できなくなるかオーバーサブスクライブされている場合、AP は CAPWAP ディスカバリ応答で確認された、モビリティ グループ内の WLC のリストから別の WLC、つまり、最も負荷の少ない WLC を選択します。

## ワイヤレス コントローラの N+1 HA 冗長性

N+1 HA 機能は N+1 冗長性モデルを基礎として構築されており、複数のプライマリ WLC のバックアップとして単一の WLC を導入できるようになっています。前述したように、N+1 導入では、通常動作時に使用されないバックアップ WLC 用に追加の AP ライセンスを購入する必要があります。N+1 HA 導入では、複数のプライマリ WLC のバックアップ WLC として、HA-SKU WLC が追加の永続 AP ライセンスを必要とすることなく導入されています(図 2-15 を参照)。

*図 2-15　　ワイヤレス コントローラの N+1 HA 冗長性*




N+1 HA アーキテクチャでは、中央集中型と FlexConnect の両方の AP 導入に冗長性を提供できます。WLC 冗長性は同じキャンパスまたはサイト内で実現することも、地理的に離れたデータセンター間で実現することもできます。HA WLC は個別に管理され、プライマリ WLC と設定を共有しません。各 WLC は別々に設定および管理する必要があります。フェールオーバー時のシームレスな運用を確保するには、必要な WLAN、AP グループ、および RF グループを各 HA WLC に定義する必要があります。

プライマリ WLC が到達不能になるか故障すると、影響を受けた AP は HA WLC にフェールオーバーします。HA WLC には AP を最大 90 日間サポートするライセンスのみが付与されています。AP が HA WLC を接続し次第、90 日間のタイマーが開始されます。90 日間の有効期日を過ぎても AP が HA WLC に存在する場合は、警告メッセージが表示されます。HA WLC は、90 日間に限り、警告メッセージなしでセカンダリ WLC として使用できます。

図 2-15 の例は、500 台の AP を導入するためのシンプルな N+1 HA 導入を示します。両方のプライマリ WLC に 250 個の永続 AP ライセンスがインストールされています。この HA WLC モデルは当初 500 台の AP をサポートし、今後の拡張の余地をもたらすために選択されています。WLC-1 および WLC-2 に接続された AP は、セカンダリ WLC として WLC-BACKUP を使用するように設定されています。

（注）　HA-SKU は、2500 シリーズ、5500 シリーズ、7500 シリーズ、8500 シリーズのワイヤレス コントローラと WiSM2 で使用できます。N+1 HA 展開は、さまざまなモデルの WLC で構成できます（たとえば、5508 WLC をプライマリとして、5520 WLC HA-SKU をバックアップとして稼働するなど）。

（注）　vWLC の N+1 HA は、リリース 8.4 以降でサポートされます。

# HA ステートフル スイッチオーバー ワイヤレス コントローラ冗長性

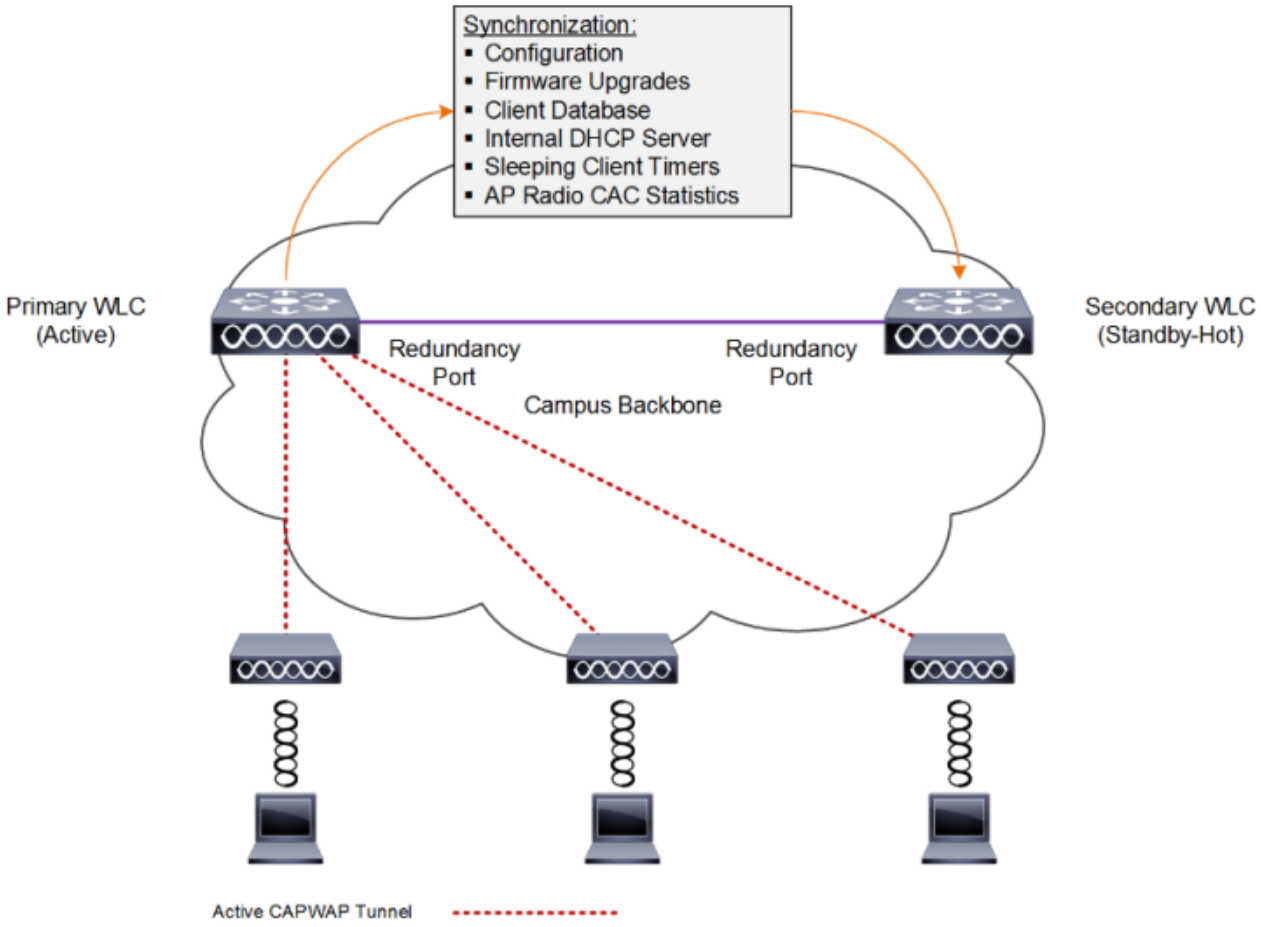
これまでの項で説明した N+1 と N+1 HA の冗長性アーキテクチャはいずれも、プライマリ WLC が到達不能になったときの AP フェールオーバーを実現しています。いずれのアーキテクチャも、プライマリ WLC に到達不能であることを AP が検出してセカンダリまたはターシャリの WLC にフェールオーバーする間、ワイヤレス サービスに影響が出ます。サービスに影響を与えない HA を実現するには、WLC 間で AP とクライアントの両方をシームレスに移行できるようにする必要があります。この WLC には、AP ステートフル スイッチオーバー（AP SSO）とクライアント ステートフル スイッチオーバー（クライアント SSO）の両方が実装されており、WLC フェールオーバー時のクライアント サービスのダウンタイムがゼロになり、SSID の非停止が実現されます。

HA ステートフル スイッチオーバー（SSO）は CUWN での推奨される HA 導入アーキテクチャです。この設計は、2 台の WLC が 1:1 プライマリ/セカンダリ ペアとして導入されている N+1 HA アーキテクチャを基盤としています。現在の構成および AP とクライアントの状態情報がプライマリとセカンダリのピア間で自動的に同期されます。大部分の導入では、プライマリ WLC には永続 AP ライセンスがインストールされている一方で、セカンダリ WLC は HA-SKU です（図 2-16 を参照）。

通常動作中、プライマリ WLC はアクティブ ロールを担当する一方で、セカンダリ WLC はスタンバイホット ロールを担当します。スイッチオーバーの発生後は、セカンダリ WLC がアクティブ ロールを担当し、プライマリ WLC がスタンバイホット ロールを担当します。それ以降のスイッチオーバーの後、ロールはプライマリおよびセカンダリ WLC 間で交換されます。これらの WLC は、冗長性管理インターフェイス（RMI）を通じて UDP キープアライブ パケットを交換することで、ピアと管理ゲートウェイの到達可能性をチェックします。

HA-SSO が有効化されるとすべての構成がアクティブ WLC で実行され、これがスタンバイホット WLC に自動的に同期されます。スタンバイホット WLC 上の CLI や Web UI では構成を実施できません。ファームウェア イメージもスタンバイホット WLC に配布されます。

*図 2-16　　ワイヤレス コントローラの HA-SSO 冗長性*




**（注）** 詳細については、『High Availability (SSO) deployment guide』（http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html）を参照してください。

HA-SSO アーキテクチャは、AP SSO とクライアント SSO の両方で構成されており、これらが組み合わさって、クライアントへのワイヤレス サービスに影響を与えることなく、1 秒未満の障害検出とフェールオーバーが実現されます。AP SSO が最初に追加されたのはリリース 7.3 であり、クライアント SSO が追加されたのはリリース 7.5 でした。

- AP SSO：AP でアクティブ WLC と CAPWAP トンネルを設定して、AP データベースのミラーコピーをスタンバイホット WLC と共有できます。AP はフェールオーバーの際に CAPWAP ディスカバリ状態になりません。任意の時点で、AP とアクティブ状態の WLC の間で維持される CAPWAP トンネルは 1 つだけです。AP SSO では、WLC またはネットワークのフェールオーバーなどによる、障害状態によって引き起こされるワイヤレス ネットワークの大規模なダウンタイムを削減することを全体的な目標としています。

- クライアント SSO：サービスに影響を与えずにシームレスなフェールオーバーを実現するには、クライアントおよび AP の両方をアクティブ WLC からスタンバイホット WLC へシームレスに移行できるようにする必要があります。SSO クライアントを使用すると、アクティブ WLC にクライアントが関連付けられたとき、またはクライアントのパラメータが変更されたときに、クライアント情報がスタンバイホット WLC に同期されます。完全に認証されたすべてのクライアントはスタンバイホット WLC に同期されるため、スイッチオーバー時のクライアント再関連付けが回避されて、クライアントに加え AP のフェールオーバーがシームレスになります。その結果、クライアント サービスのダウンタイムがゼロになり、SSID の停止が回避されます。

AP SSO とクライアント SSO は、3504、5500 シリーズ、7500 シリーズ、および 8500 シリーズの WLC と Wireless Services Module 2 でサポートされます。アプライアンス ベースの各 WLC では専用の冗長ポートがサポートされ、WiSM2 では冗長 VLAN が実装されています。冗長ポートはキープアライブ メッセージを交換するためと、設定および状態情報を同期するために使用されます。冗長ポートは直接接続されているか、中間レイヤ 2 ネットワークを通じて間接的に接続されています。表 2-4 に、WLC のモデルごとに HA SSO サポートの概要について説明します。

*表 2-4　コントローラ プラットフォームごとの HA-SSO のサポート*

| プラットフォーム | 冗長ポート | AP SSO | クライアント SSO |
|---|---|---|---|
| Cisco 2504 ワイヤレス コントローラ | × | × | No |
| Cisco 3504 ワイヤレス コントローラ | 対応 | 対応（8.5 以上） | 対応（8.5 以上） |
| Cisco 5508 ワイヤレス コントローラ | Yes | Yes（7.3 以上） | Yes（7.5 以上） |
| Cisco 5520 ワイヤレス コントローラ | Yes | Yes（8.1 以上） | Yes（8.1 以上） |
| Cisco Flex 7500 ワイヤレス コントローラ | Yes | Yes（7.3 以上） | Yes（7.5 以上） |
| Cisco 8510 ワイヤレス コントローラ | Yes | Yes（7.3 以上） | Yes（7.5 以上） |
| Cisco 8540 ワイヤレス コントローラ | Yes | Yes（8.1 以上） | Yes（8.1 以上） |
| Cisco ワイヤレス サービス モジュール 2 | Yes：VLAN | Yes | 対応 |
| 仮想ワイヤレス コントローラ（vWLC） | × | × | No |

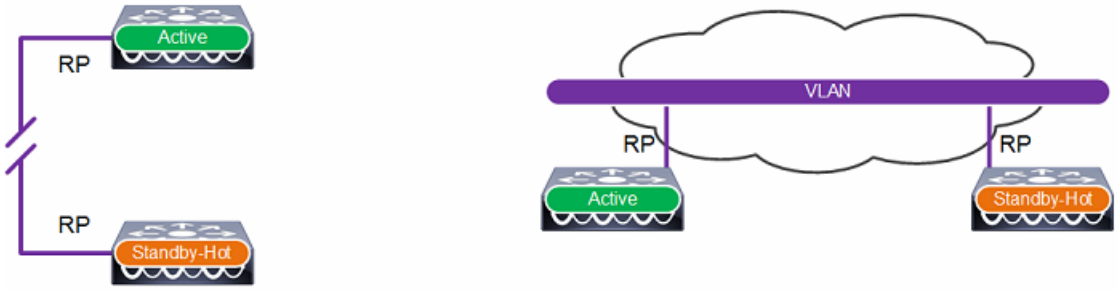
（注）　AP SSO およびクライアント SSO の実装はプライマリおよびセカンダリ WLC で動作しているソフトウェア リリースによって決まり、単独では設定できません。たとえば、HA が有効化されており、両方の WLC で 8.1 をサポートしている場合は、AP SSO とクライアント SSO の両方が実装されます。

## 冗長ポートおよび VLAN 設定

冗長ポートおよび VLAN は HA-SSO 導入では必須であり、設定および状態を同期するためと、キープアライブ パケットを交換するために使用されます。冗長ポート/VLAN はロール ネゴシエーションにも使用されます。3504、5500 シリーズ、7500 シリーズ、および 8500 シリーズ コントローラなどのアプライアンス ベースの WLC は専用のイーサネット冗長ポートを実装し、WiSM2 は冗長 VLAN を実装しています。

リリース 7.5 以降では、アプライアンス ベースの WLC の冗長ポートは、専用のイーサネット ケーブルを介して相互接続することも、専用のルーティング不能 VLAN を使用し、中間スイッチを介してレイヤ 2 で接続することもできます。光ファイバによるメディア コンバータ越しの直接接続もサポートされています。図 2-17 に、サポートされている冗長ポート接続オプションを示します。

*図 2-17　冗長ポートの相互接続*




WiSM-2 ベースの導入では、単一シャーシと複数シャーシの両方の導入で HA-SSO がサポートされています。複数シャーシ導入は、VSS を使用するか、リダンダンシー VLAN を拡張することでサポートされます。リダンダンシー VLAN はルーティング不可能な専用 VLAN である必要があります。図 2-18 に、シャーシ展開オプションを示します。

*図 2-18　WiSM2 リダンダンシー VLAN*

### 考慮事項

中間 L2 ネットワーク越しに冗長ポートまたは VLAN を接続するときは、次の考慮事項を満たす必要があります。

- ピア間のラウンド トリップ時間（RTT）遅延は 400 ミリ秒以下である必要があります（デフォルトでは 80 ミリ秒）。RTT は 100（デフォルト）～ 400 ミリ秒の範囲で設定可能なキープアライブ タイマーの 80 % です。RTT を大きくするときは、キープアライブ タイマーの設定を大きくする必要があります。
- ピア間に最低 60 Mbps の帯域幅が必要です。
- ピア間に最低 1,500 バイトの MTU パスが必要です。

## トポロジ

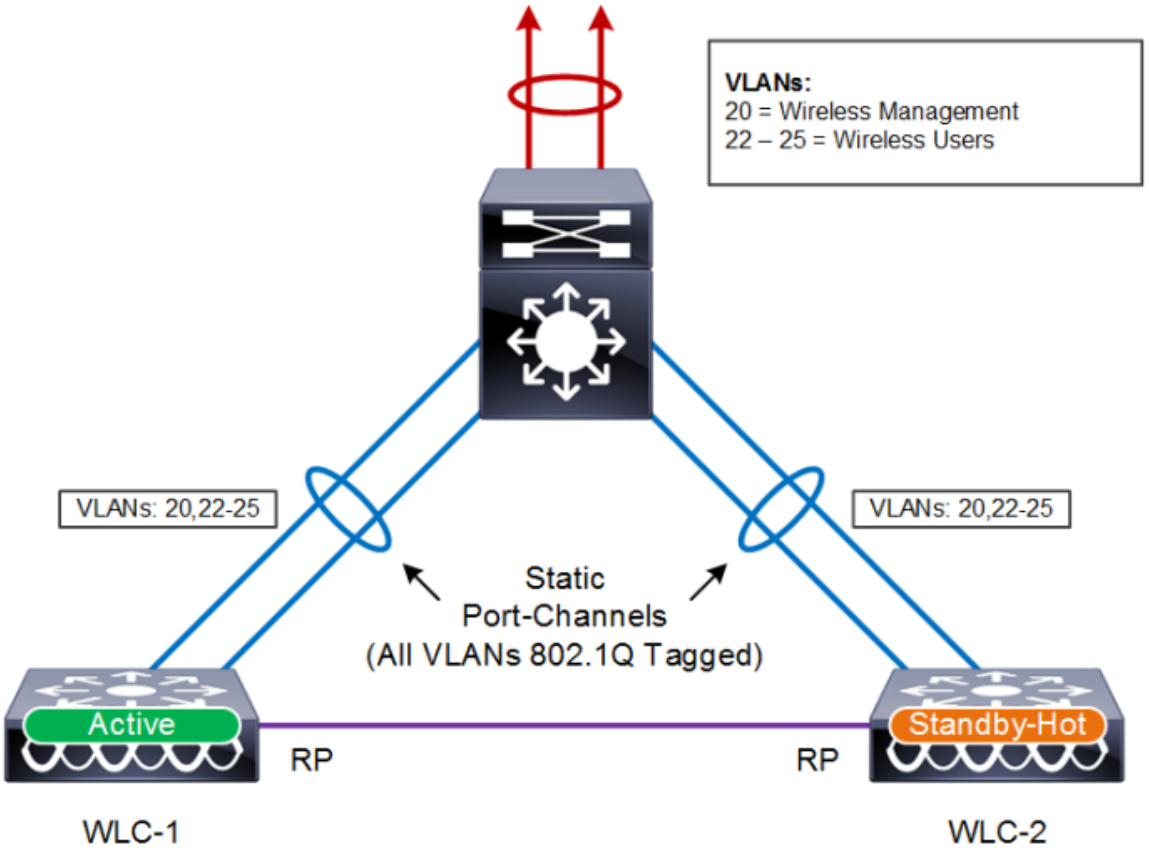
次の項では、Cisco Unified Wireless Network（CUWN）内に HA-SSO を導入するときの一般的なトポロジの概要を説明します。シンプルにするために、冗長ポートを直接接続したアプライアンス ベースの WLC を各例で示してあります。各トポロジは WiSM2 導入にも適用されます。

以下の各設計では、Catalyst ディストリビューション スイッチがワイヤレス サービス ブロックとコア レイヤの境界になっています。この境界は、LAN の 2 つの主要機能を実現しています。レイヤ 2 側では、ディストリビューション レイヤがスパニング ツリー プロトコル（STP）用の境界になって、レイヤ 2 障害の伝播を制限しています。レイヤ 3 側では、ディストリビューション レイヤは、ネットワークに入るときに IP ルーティング情報を要約する理論上の点になっています。この要約によって IP ルート テーブルが削減されてトラブルシューティングが容易になり、プロトコル オーバーヘッドが削減されて障害からのリカバリが迅速になります。

### スタンドアロン ディストリビューション スイッチ

図 2-19 のトポロジは、ワイヤレス サービス ブロック内のスタンドアロン Catalyst スイッチに接続されている WLC の HA-SSO ペアを示します。冗長性は、復元力のあるスタックを形成するように複数のライン カードまたはスイッチを導入することによって実現されます。この設計では、シャーシまたはスタック全体の障害によって HA-SSO WLC がそれ以外のネットワークから孤立するため、ネットワークおよびハードウェアの障害に対する保護は最低限になっています。

*図 2-19　スタンドアロン ディストリビューション スイッチを使用する HA-SSO*




(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。これと等価な WiSM2 設計は、2 台の WiSM2 モジュールを設置した単一の Catalyst 6500 シリーズ シャーシで構成されます。

### マルチレイヤ ディストリビューション スイッチ

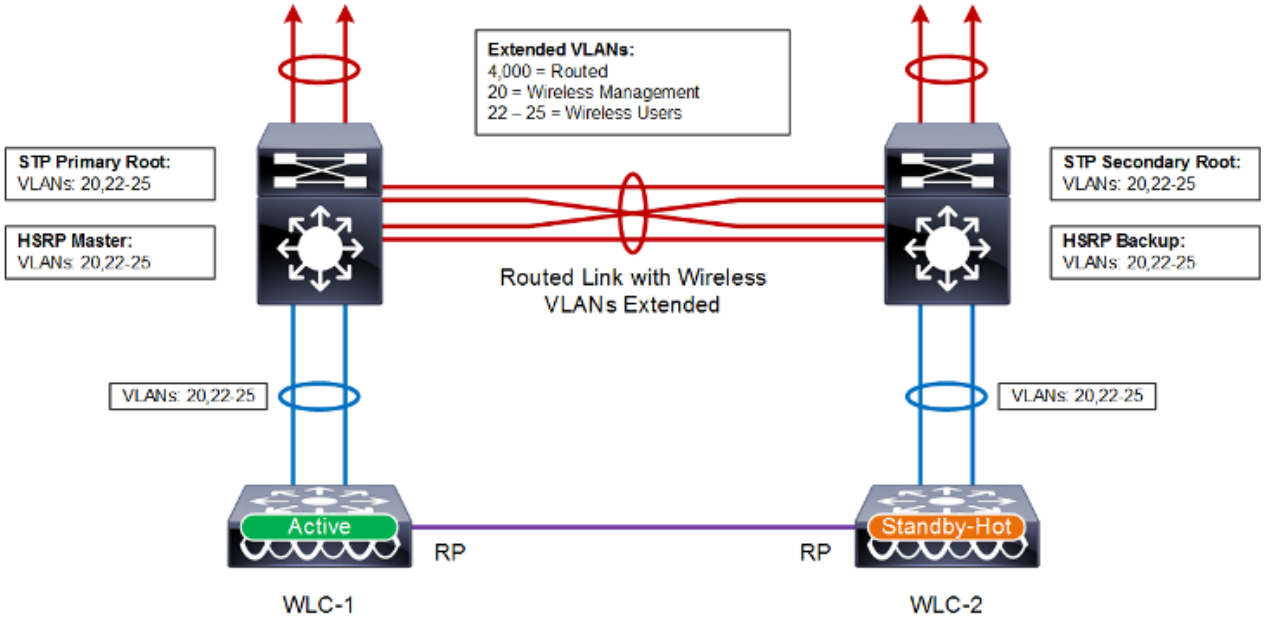
図 2-20 のトポロジは、マルチレイヤ設計を実装しているワイヤレス サービス ブロック内の Catalyst スイッチのペアに接続されている WLC の HA-SSO ペアを示します。このサンプル トポロジの Catalyst スイッチはレイヤ 3 接続であり、Catalyst スイッチ間でワイヤレス管理とワイヤレス ユーザ VLAN の拡張が必要であるため、複雑な設計になります。これは、スパニング ツリー プロトコルとファーストホップ ルーティング プロトコルを必要とするループを持つマルチレイヤ アーキテクチャに行き着きます。

- このアーキテクチャでは、Catalyst スイッチ間にルーテッド ポートもルーテッド ポートチャネルも実装できません。代わりに、リンクローカル VLAN とスイッチ仮想インターフェイス（SVI）の組み合わせを使用する必要があります。これにより、マルチレイヤ設計を維持しながら、Catalyst スイッチ間にワイヤレス VLAN を拡張できます。
- ループを避けるために、ワイヤレス VLAN ごとにスパニング ツリー プロトコル（STP）を有効化する必要があります。プライマリ WLC に接続している Catalyst スイッチを各 VLAN の STP ルート ブリッジとして設定する必要があります。

- 各ワイヤレス VLAN で、HSRP などのファーストホップ ルータの冗長性を有効化および設定する必要があります。プライマリ WLC に接続しているディストリビューション スイッチを各 VLAN の HSRP マスターとして設定する必要があります。

通常動作中は、アクティブ WLC に接続している Catalyst スイッチが各ワイヤレス管理 VLAN およびワイヤレス ユーザ VLAN のファーストホップ ルータです。これにより、STP ルートと HSRP マスターの両方を兼ねることで、Catalysts スイッチのペアをつなぐリンクを通過するトラフィックが最低限になります。プライマリ Catalyst スイッチが故障すると、HA-SSO によってスタンバイホット WLC へのフェールオーバーが行われます。プライマリ Catalyst スイッチがコアネットワークへの接続を失った場合、プライマリ WLC では、2 台の Catalyst スイッチ間で確立されたポートチャネルを通じてスタンバイホット WLC と引き続き通信できるため HA-SSO フェールオーバーは行われません。

*図 2-20　マルチレイヤ ディストリビューション スイッチを使用した HA-SSO*

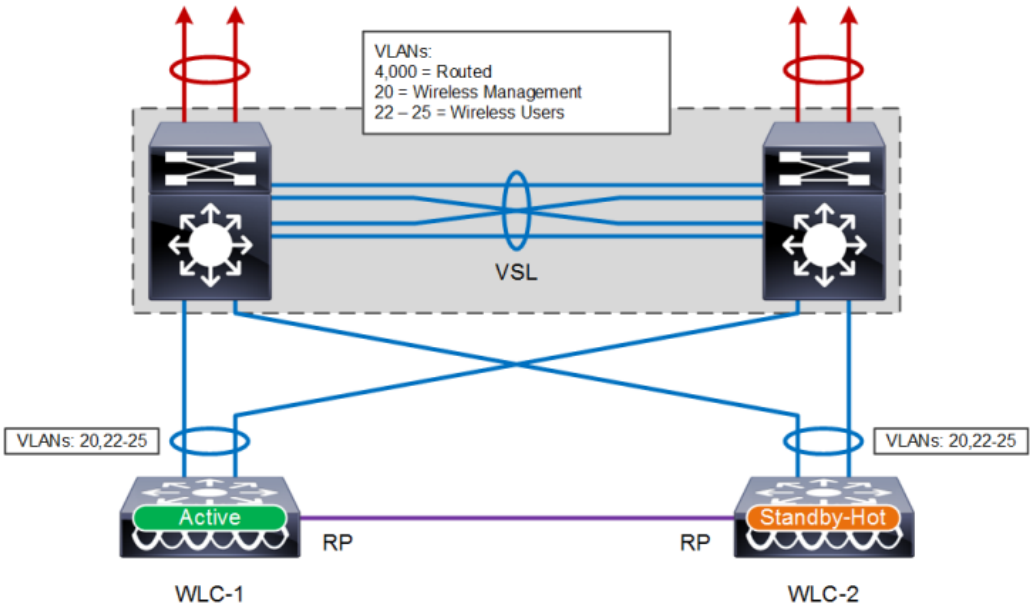



(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。同等な WiSM2 設計は、それぞれ 1 台の WiSM2 モジュールを設置したマルチレイヤ運用のために設定された 2 台の Catalyst 6500 シリーズ シャーシで構成されます。

### VSS ディストリビューション スイッチ

図 2-21 のトポロジは、ワイヤレス サービス ブロック内のディストリビューション スイッチの VSS ペアに接続されている WLC の HA-SSO ペアを示しており、推奨される設計です。この設計では、通常運用時に VSS ペアの Catalyst スイッチをつなぐ仮想スイッチ リンクを通過するトラフィックが最低限になります。これは、アクティブとスタンバイホットのどちらの WLC も、どちらのスイッチとポートを介して接続されているためです。この設計では、VSS ペアでスイッチ障害が発生したときに、アクティブ WLC からスタンバイホット WLC へのスイッチオーバーも回避されます。ただし、VSS ペアでスイッチ障害が発生した場合、アクティブ WLC に接続されているポートの数が半減するおそれがあります。

*図 2-21　VSS を使用した HA-SSO*




(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。同等な WiSM2 設計は、それぞれ 1 台の WiSM2 モジュールを設置した、VSS 構成に含まれる 2 台の Catalyst 6500 シリーズ シャーシで構成されます。

## 考慮事項

HA-SSO を実装するときは、次の考慮事項を検討する必要があります。

- Catalyst スイッチは、次の URL で公開されている Cisco Validated Design（CVD）で説明されている Cisco 推奨のベスト プラクティスに従って設定および導入されている必要があります: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html。
- HA-SSO フェールオーバー時間は、ルーティング プロトコル、スパニング ツリー プロトコル、およびファーストホップ ルータの冗長性プロトコルによって添加されたコンバージェンス時間によって決まります。
- ワイヤレス管理、ワイヤレス ユーザ VLAN は、Catalyst スイッチと WLC の間で 802.1Q タギングされている必要があります。
- リンク アグリゲーション（LAG）を使用して Catalyst スイッチに HA-SSO WLC を接続することをお勧めします。WLC ポートは、復元力のあるスタックに含まれているシャーシまたはスイッチに搭載された異なるライン カード上のポート間で分散されている必要があります。VSS が導入されている場合、WLC ポートは両方の Catalyst スイッチ間で分散できます。
- WLC に接続しているネイバー Catalyst スイッチまたは VSS のポートチャネルのチャネル モードはモード オン（静的）に設定されている必要があります。WLC ソフトウェア リリース 8.1 では LACP プロトコルも PaGP プロトコルもサポートしていません。
- HA-SSO WLC をマルチレイヤ ディストリビューション スイッチに接続するときは、次の事項が適用されます。
- ワイヤレス管理 VLAN およびユーザ VLAN は、Catalyst ディストリビューション スイッチ間で 802.1Q タギングされます。この結果、ループを持つマルチレイヤ設計になります。

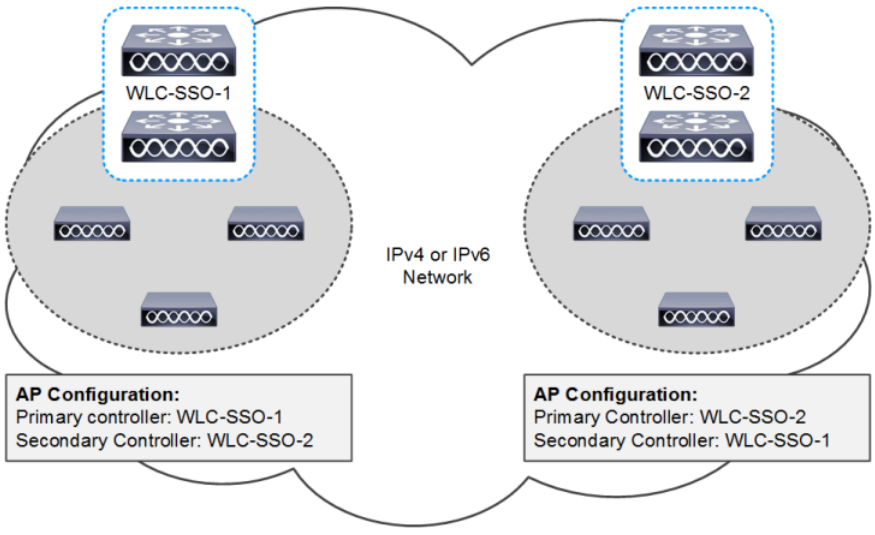
- ループを防止するために、ワイヤレス管理 VLAN およびワイヤレス ユーザ VLAN で Rapid Spanning Tree Protocol を有効化することをお勧めします。通常動作時にプライマリ WLC に接続している Catalyst スイッチは、各ワイヤレス VLAN の STP ルート ブリッジとして設定する必要があります。
- ワイヤレス管理 VLAN およびユーザ VLAN で HSRP などのファーストホップ ルーティング プロトコルを有効化する必要があります。通常動作時に プライマリ WLC に接続している Catalyst スイッチは、各 ワイヤレス VLAN の HSRP マスターとして設定する必要があります。
- アプライアンス ベースの WLC 冗長ポートは直接接続することも、レイヤ 2 で間接的に接続することもできます。間接的に接続するときは、各 Catalyst スイッチ間にルーティング不可能な専用 VLAN 2 つを拡張することをお勧めします。
- 冗長ポートが中間 L2 ネットワークを越えて拡張されている場合は、直前の項で説明した遅延、帯域幅、および MTU の要件を満たす必要があります。

## HA-SSO と N+1 冗長性

大規模 Cisco Unified Wireless Network（CUWN）導入では、HA-SSO と N+1 冗長性の両方を組み合わせて、SSO-HA WLC が到達不能になった場合の AP フェールオーバーを実現できます（図 2-22）。これは、ビルディング、フロアなど明確な構造内でさまざまな HA-SSO ペアをサービス AP に割り当てる大規模 CUWN 導入で推奨される設計です。

この構成は、AP にプライマリ、セカンダリ、およびターシャリ WLC が設定されている N+1 HA 導入と完全に同様に機能します。AP のプライマリ WLC は割り当てられた HA-SSO WLC ペアとして設定されている一方で、セカンダリ（および任意でターシャリの）WLC は別の HA-SSO WLC ペアまたはスタンドアロン WLC として設定できます。AP は、プライマリ HA-SSO ペアのアクティブとスタンバイホットの両方の WLC が到達不能になったときに限り、セカンダリ WLC にフェールオーバーすることになります。セカンダリまたはターシャリ WLC へのフェールオーバーはステートレスです。

*図 2-22　HA-SSO と N+1 冗長性*



# 高速再起動

高速再起動の強化では、次の機能に変更を加える際のネットワークとサービスのダウンタイムを最大 73 % 削減することを目標としています。

- LAG コンフィギュレーションの変更
- モビリティ モードの変更
- Web 認証証明書の変更
- Clear Configuration

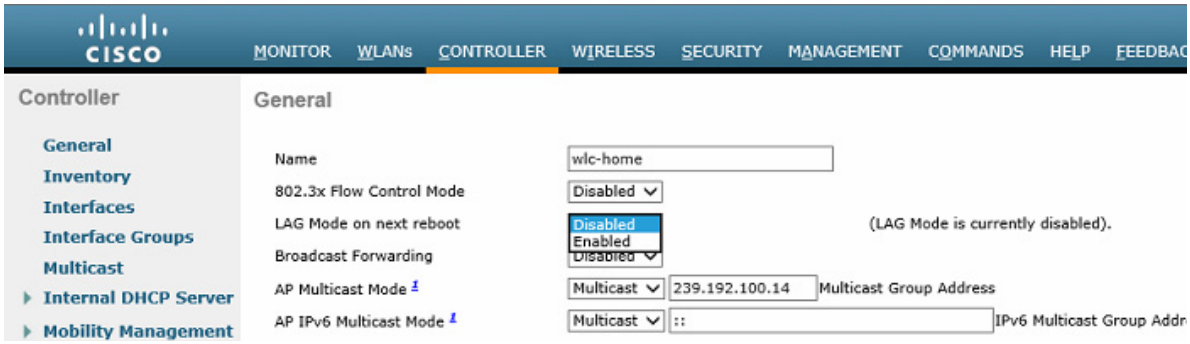
高速再起動がない場合、上記の変更を行うにはシステムの完全な再起動が必要です。高速再起動機能は、Cisco WLC 3504、WLC 5520、7510、8510、8540、およびリリース 8.1 以降の vWLC でサポートされます。高速再起動機能を呼び出すには、CLI で Restart コマンドを実行するか、Web UI で [Save and Restart] をクリックします。

# リンク アグリゲーション(LAG)

リンク集約(LAG)は、802.3ad ポート集約標準の部分的な実装です。有効にした場合、WLC とネイバー スイッチの間に追加の帯域幅および耐障害性があれば、WLC のすべてのイーサネット ポートが LAG によって単一の 802.3ad ポートチャネルにバンドルされます。いずれかの WLC ポートまたは接続で障害が発生すると、トラフィックは、このバンドルに含まれる残存する他のいずれかのイーサネット ポートに自動的に移行されます。少なくとも 1 つのイーサネット ポートが機能している限り、ワイヤレス システムは稼働し続け、AP は存続し、クライアントはデータを送受信できます。

LAG は、WLC でグローバルに有効にされ(図 2-23)、Cisco WLC 2504、WLC 3504、5508、5520、および 8540 でサポートされます。LAG を有効にすると、すべてのイーサネット ポートがバンドルの対象になります。LAG を有効にするには、WLC のシステム全体をすぐに再起動するか、高速再起動を行う必要があります。

*図 2-23　LAG モード*



## 考慮事項

LAG を実装するときは、次の考慮事項を検討する必要があります。

- Cisco WLC は、LAG のインターフェイスで CDP アドバタイズメントを送信しません。
- LAG に含まれるすべての WLC イーサネット ポートは、同じ速度で動作する必要があります。ギガビット ポートと 10 ギガビット ポートを混在させることはできません。
- WLC に接続しているネイバー Catalyst スイッチまたは VSS のポートチャネルのチャネル モードはモード オン（静的）に設定されている必要があります。WLC ソフトウェア リリース 8.1 では LACP プロトコルも PaGP プロトコルもサポートしていません。
- WLC イーサネット ポートを別々の LAG グループに分けることはできません。
- すべてのイーサネット ポートが単一の論理ポートにバンドルされるため、サポートされる AP マネージャ インターフェイスは 1 つだけです。
- LAG を有効にした場合、動的 AP マネージャ インターフェイス、およびタグの付いていないインターフェイスはすべて削除されます。同時に、WLAN がすべて無効になり、管理インターフェイスにマッピングされます。管理インターフェイス、スタティック AP マネージャ インターフェイス、および VLAN タグ付き動的インターフェイスは、LAG ポートに割り当てられます。
- LAG が有効化されているときは、WLC がパケットを受信したポートと同じポートからパケットが送信されます。AP からの CAPWAP パケットがコントローラの物理ポート 1 に入ると、WLC によって CAPWAP ラッパーが除去され、パケットが処理され、物理ポート 1 からネットワークに転送されます。

# モビリティ グループ、AP グループ、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

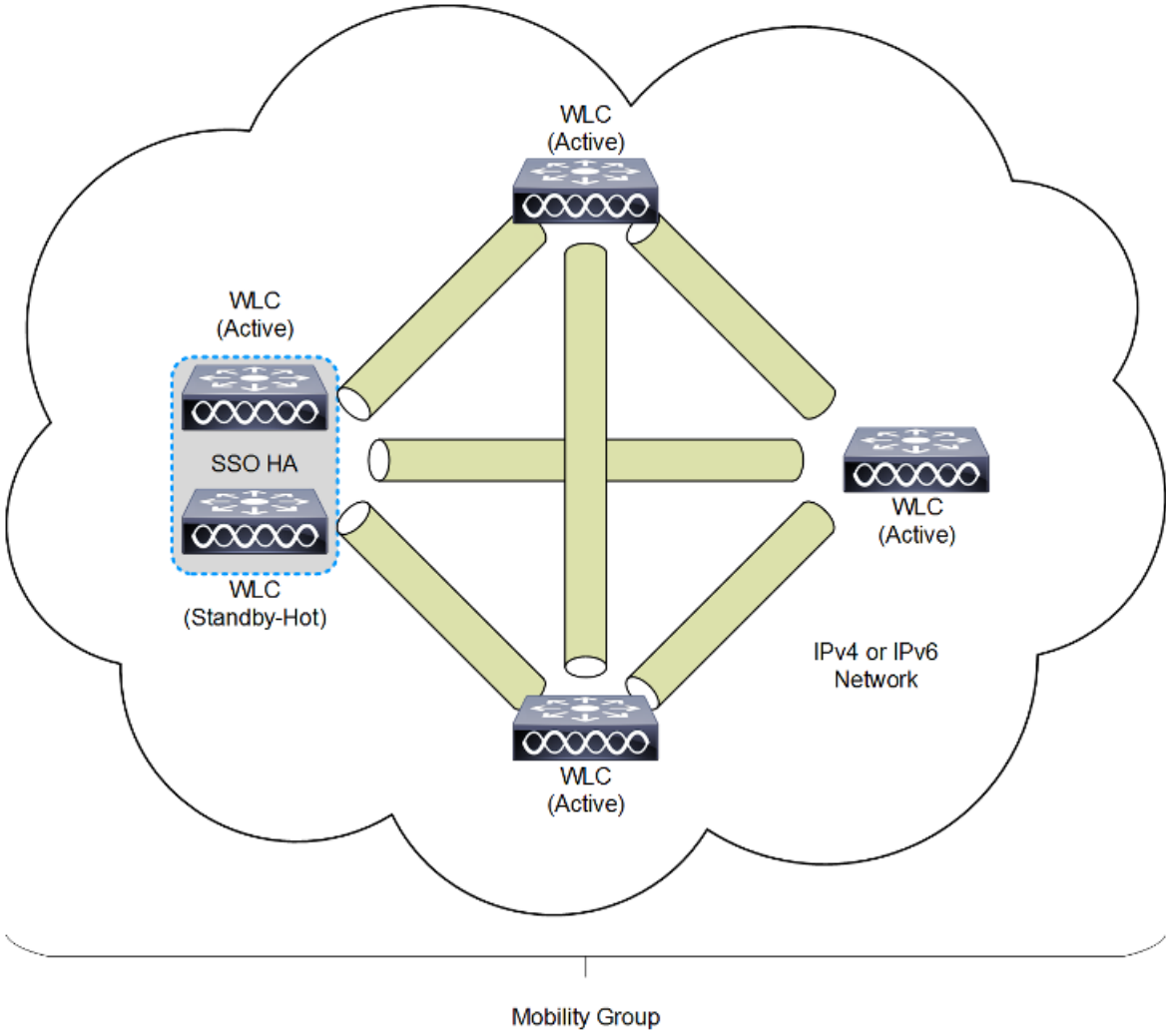
この項では、Cisco Unified Wireless Network におけるこれらのグループの目的と用途について説明します。

## モビリティ グループ

モビリティ グループは、同じモビリティ グループ名で識別されるコントローラのセットで、ワイヤレス クライアントのローミングをシームレスに行う範囲を定義します。モビリティ グループを作成すると、ネットワーク内で複数の WLC を有効にして、コントローラ間またはサブネット間のローミングが発生した際に、クライアント、AP、RF に関する不可欠な情報を動的に共有してデータ トラフィックを転送できるようになります。同じモビリティ グループ内の WLC は、相互のアクセス ポイントを不正なデバイスとして認識しないように、クライアント デバイスのコンテキストと状態およびアクセス ポイントのリストを共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。

モビリティ グループは、図 2-24 に示すように、メンバー WLC 間にメッシュ状の認証トンネルを形成し、WLC がグループ内の他の WLC に直接問い合わせることができるようにします。

*図 2-24　　WLC モビリティ グループ*




リリース 8.0 以上では、インターネット プロトコル バージョン 4（IPv4）またはインターネット プロトコル バージョン 6（IPv6）を使用して WLC ピア間でモビリティ トンネルを設定できます。IPv4 トンネルまたは IPv6 トンネルの実装は各ピア用に定義されているモビリティ構成に基づきます。表 2-5 に、各モビリティ トンネル バージョンで実装されているプロトコルとポートの一覧を示します。

*表 2-5　　モビリティ トンネルのプロトコルおよびポート*

| インターネット プロトコル | IP プロトコル | 宛先ポート | 説明 |
|---|---|---|---|
| バージョン 4 | 17（UDP） | 16,666 | IPv4 モビリティ トンネル制御チャネル |
| | 97（EITHERIP） | - | IPv4 モビリティ トンネル データ チャネル |
| バージョン 6 | 17（UDP） | 16,666 | IPv6 モビリティ トンネル制御チャネル |
| | 17（UDP） | 16,667 | IPv6 モビリティ トンネル データ チャネル |

## モビリティ グループの考慮事項

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考慮事項があります。

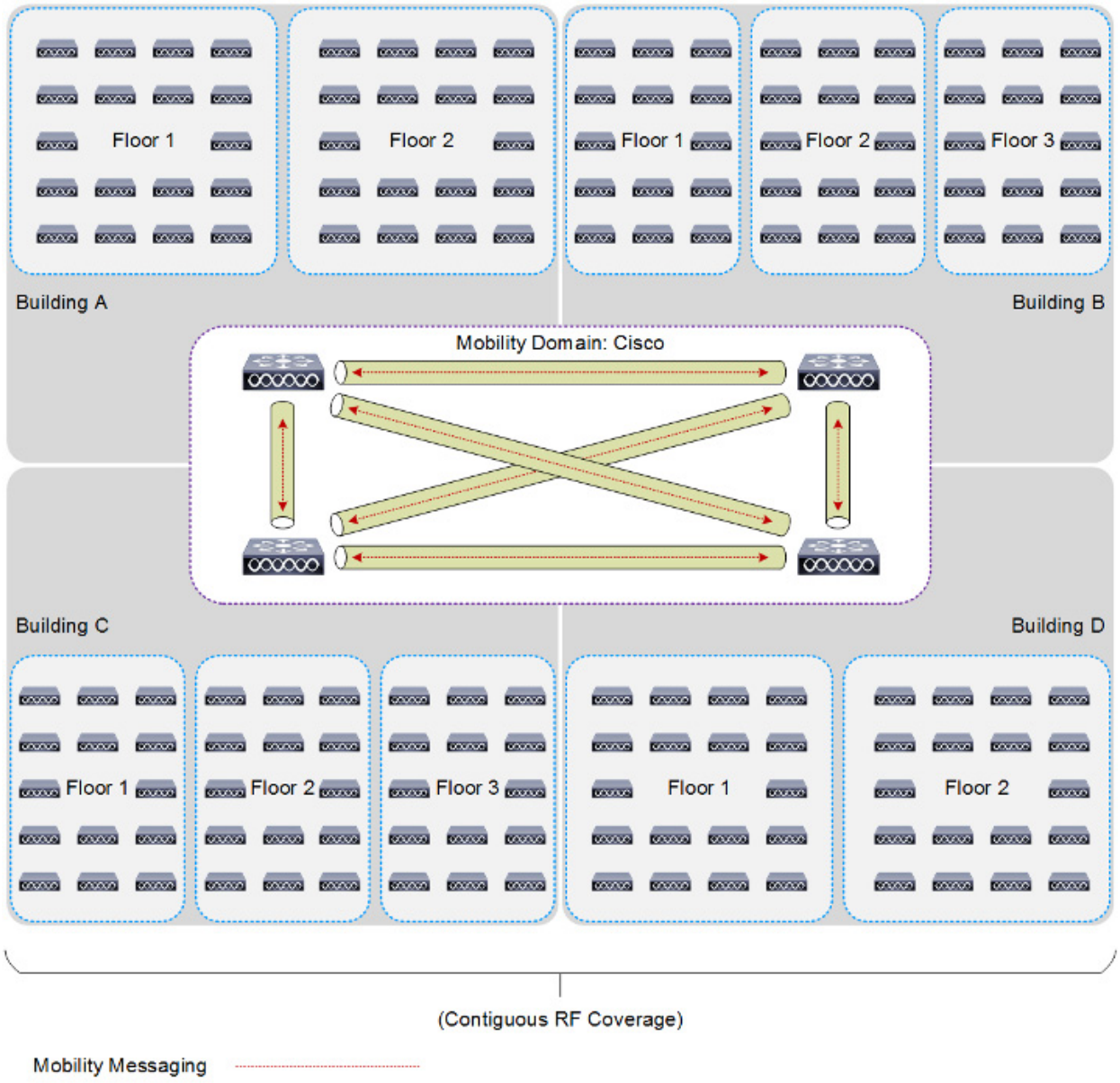
- 最大 24 台の WLC（任意のモデル）を単一のモビリティ グループに割り当てることができます。単一のモビリティ グループで、最大 144,000 台の AP がサポートされます（24 台の WLC X 6,000 台の AP = 144,000 台の AP）。エンタープライズ導入では、さらに多くの WLC および AP が構成されていることがありますが、これらは別のモビリティ グループのメンバーとして設定する必要があります。
- WLC は同一のモデルやタイプでなくても、モビリティ グループのメンバーにできます。ただし、各メンバーで同じバージョンのソフトウェアを実行している必要があります。
- メンバー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、Cisco Unified Wireless Network 導入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。
- スイッチオーバー（SSO）ありで WLC を導入する場合、各 WLC SSO ペアは単一のモビリティ ピアと見なされます。
- 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 で同一のモビリティ ドメイン名を使用する必要があり、相互の [Static Mobility Members] リストでピアとして定義する必要があります。この規則の例外となるのは、ゲスト アンカーを導入する場合であり、この場合は、ゲスト アンカー用に別のモビリティ グループを導入することをお勧めします。
- モビリティ グループ メンバー（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 とセキュリティの設定が一貫性を持っている必要があります。
- Cisco のベスト プラクティスでは、モビリティ グループのすべてのメンバーでマルチキャスト モビリティ機能を有効にすることをお勧めしています。この機能を利用するには、モビリティ グループの各メンバーに共通のローカル グループ マルチキャスト IPv4 アドレスを定義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 によって設定されたカバレッジが重複する導入の場合にだけ効果的です。それぞれ異なる WLC に関連付けられている 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（連続）していない場合には、モビリティ グループにメリットはありません。たとえば、キャンパスとブランチの間や複数のブランチ間のローミングです。

*図 2-25　　モビリティ グループの例*



## 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 サービスおよび BYOD サービスの導入時に使用します。

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、わずか 71 個です。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 メンバー 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 メンバー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 グループのメンバーにしかなれません。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 グループのメンバーであると同時に、別のモビリティ グループのメンバーである外部 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 アンカー構成については、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 グループ数

AP グループは、WLAN、RF、Hotspot 2.0、およびロケーション設定が共通している、ビルディング、フロア、リモート ブランチ オフィスなどの明確な区域内の AP の論理的なグループです。AP グループを利用してさまざまな AP グループに管理者が具体的な設定を割り当てできるため、Cisco Unified Wireless Network 導入で有用です。たとえば、AP グループを使用すると、キャンパス内のさまざまなビルディングにアドバタイズされる WLAN、WLAN クライアントに割り当てられるインターフェイスまたはインターフェイス グループ、高密度設計をサポートする特定のカバレッジ エリアの無線用の RRM と 802.11 の無線パラメータを制御できます。

サポートされている AP グループ固有の設定には次が含まれます。

- CAPWAP 優先モード：AP で IPv4 と IPv6 のいずれの CAPWAP モードを優先するのかを判別するために使用されます。
- NAS-ID：RADIUS 認証およびアカウンティングのために WLC によって使用されます。
- WLAN：WLAN 割り当て、インターフェイスとインターフェイス グループのマッピング、および NAC 状態。
- RF プロファイル割り当て：802.11、RRM、高密度、およびクライアント ロード バランシングの設定。
- Hotspot 2.0：802.11u の場所の構成および言語。
- ロケーション：HyperLocation 構成。

デフォルトでは、各 AP は「default-group」というデフォルト AP グループに自動的に割り当てられ、WLAN ID（1 ～ 16）がこのデフォルト グループにマッピングされます。16 を超える ID を含む WLAN には、カスタム AP グループを定義する必要があります。カスタマイズした AP グループが WLC に定義されている場合は、AP を手動でこの AP グループに割り当てる必要があります。

(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、http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch5_QoS.html を参照してください。

*表 2-6　シスコ ワイヤレス コントローラ AP グループの拡張(プラットフォーム別)*

| コントローラ プラットフォーム | 最大 AP グループ数 | AP グループあたり最大 AP 数 |
|---|---|---|
| Cisco 2504 ワイヤレス コントローラ | 75 | 75 |
| Cisco 3504 ワイヤレス コントローラ | 150 | 150 |
| Cisco 5508 ワイヤレス コントローラ | 500 | 500 |
| Cisco 5520 ワイヤレス コントローラ | 1,500 | 1,500 |
| Cisco Flex 7500 ワイヤレス コントローラ | 6,000 | 6,000 |
| Cisco 8510 ワイヤレス コントローラ | 6,000 | 6,000 |
| Cisco 8540 ワイヤレス コントローラ | 6,000 | 6,000 |
| Cisco ワイヤレス サービス モジュール 2 | 1,000 | 1,000 |
| Cisco 仮想ワイヤレス コントローラ | 3,000 | 3,000 |

## AP グループの考慮事項

AP 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考慮事項があります。

- AP は、AP グループに属していない場合には、「default-group」というデフォルト AP グループに割り当てられ、そのデフォルト グループに適用されているすべての設定を継承します。
- Cisco のベスト プラクティスとして、プライマリ、セカンダリ、およびターシャリ WLC 上のカスタマイズした AP グループ設定を一貫させることをお勧めします。定義されていない AP グループ名を持つ WLC を AP が接続する場合、AP では割り当てられた AP グループ(NVRAM)を維持しますが、default-group に適用されているすべての設定を継承することになります。その結果、AP の設定を誤り、ユーザ エクスペリエンスを低下させることがあります。
- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。WLAN インターフェイスが変更されると、AP グループ テーブル内の WLAN に対するインターフェイス マッピングにも反映されて新しい WLAN インターフェイスに変わります。
- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。WLAN インターフェイスが変更されても、AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。
- コントローラ上の設定をクリアすると、すべての AP グループ(「default-group」という AP グループを除く)が非表示となります。

- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。16 を超える ID を含む WLAN には、カスタム AP グループを定義する必要があります。
- OfficeExtend 600 シリーズ アクセス ポイントでは、最大で 2 つの WLAN と 1 つのリモート LAN がサポートされます。3 つ以上の WLAN と 1 つのリモート LAN を WLC で設定した場合は、カスタマイズした AP グループに Office Extend 600 シリーズ アクセス ポイントを割り当てる必要があります。WLAN 2 つとリモート LAN 1 つをサポートしている場合は、引き続きデフォルトの AP グループに該当します。さらに、WLAN およびリモート LAN の ID は 8 未満である必要があります。
- OfficeExtend アクセス ポイントはすべて同じ AP グループ内にあり、この AP グループに含まれる WLAN は 15 個以下にする必要があります。アクセス ポイント グループ内の OfficeExtend アクセス ポイントを持つコントローラは、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセス ポイントに最大 15 個の WLAN しか公開しません。
- すべての FlexConnect AP（同じブランチ/サイト内）を同じ AP グループおよび同じ FlexConnect グループに設定することをお勧めします。これにより、単一サイトのすべての AP で正しい WLAN-VLAN マッピングを継承するようになります。

## AP グループの用途

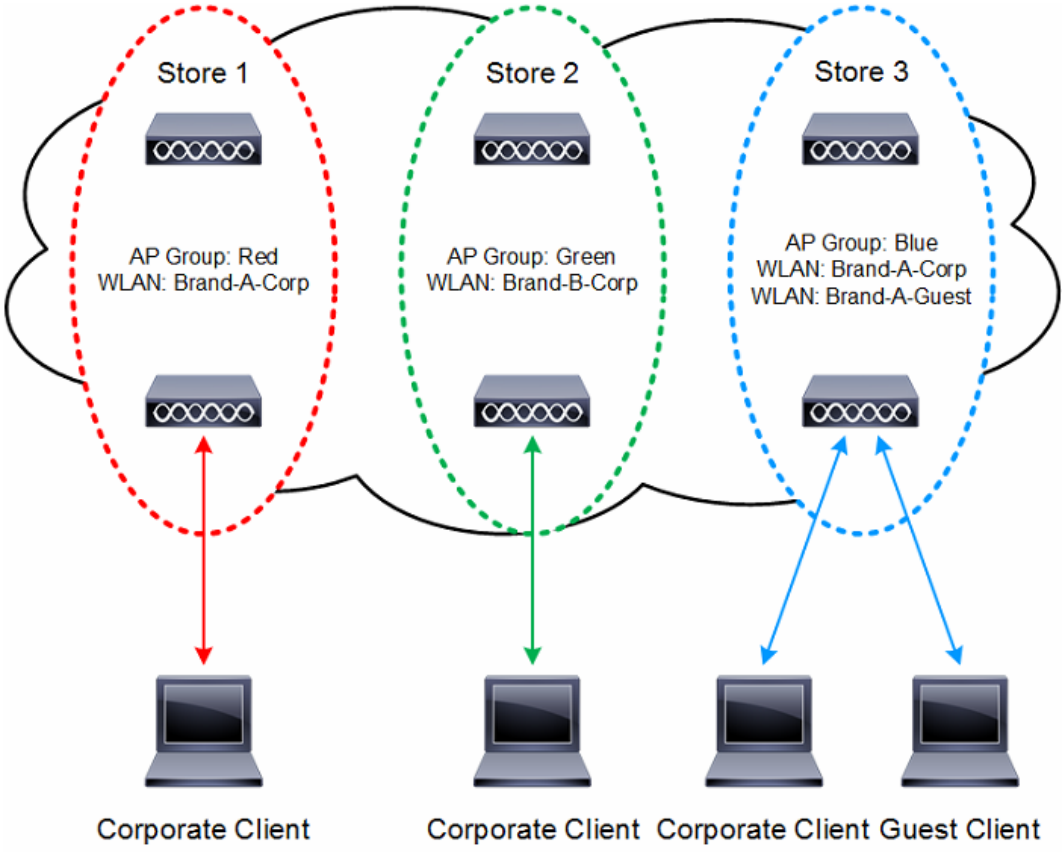
AP グループを使用すると、Cisco Unified Wireless Network に関する業務上の複数の課題を解決できます。ここでは、AP グループによってこれらの問題を解決できる一般的ないくつかの用途を解説します。

- 特定の地理的ロケーション内で AP によってアドバタイズされる WLAN を制御します。たとえば、キャンパス導入では、別々の AP グループを利用してゲスト WLAN を共用部分のみにアドバタイズすることも、キャンパス全体にすることもできます。小売店での導入では、AP グループを利用してさまざまなブランド ショップ（合併および買収）用に一意の SSID をアドバタイズしたり、ゲスト Wi-Fi サービスを一部の小売店に提供したりできます。

図 2-26 に示すように、リモート FlexConnect AP をサポートしている WLC には、異なるブランドのリモートの小売店をサポートするためとクライアント サポートのために 3 個の個別 AP グループが設定されています。ショップ 1 および 3 は同じブランドであり、企業の SSID は共通していますが、ショップ 3 では常連客向けにゲスト Wi-Fi を提供している一方でショップ 1 では提供していないため、ショップ 3 用に別の AP グループが必要です。

ショップ 2 は異なる企業 SSID を実装している異なるブランドです。ショップ 2 にあるクライアント デバイスはまだ標準の企業 SSID に移行されていないため、このショップをサポートするために個別の AP グループが必要です。

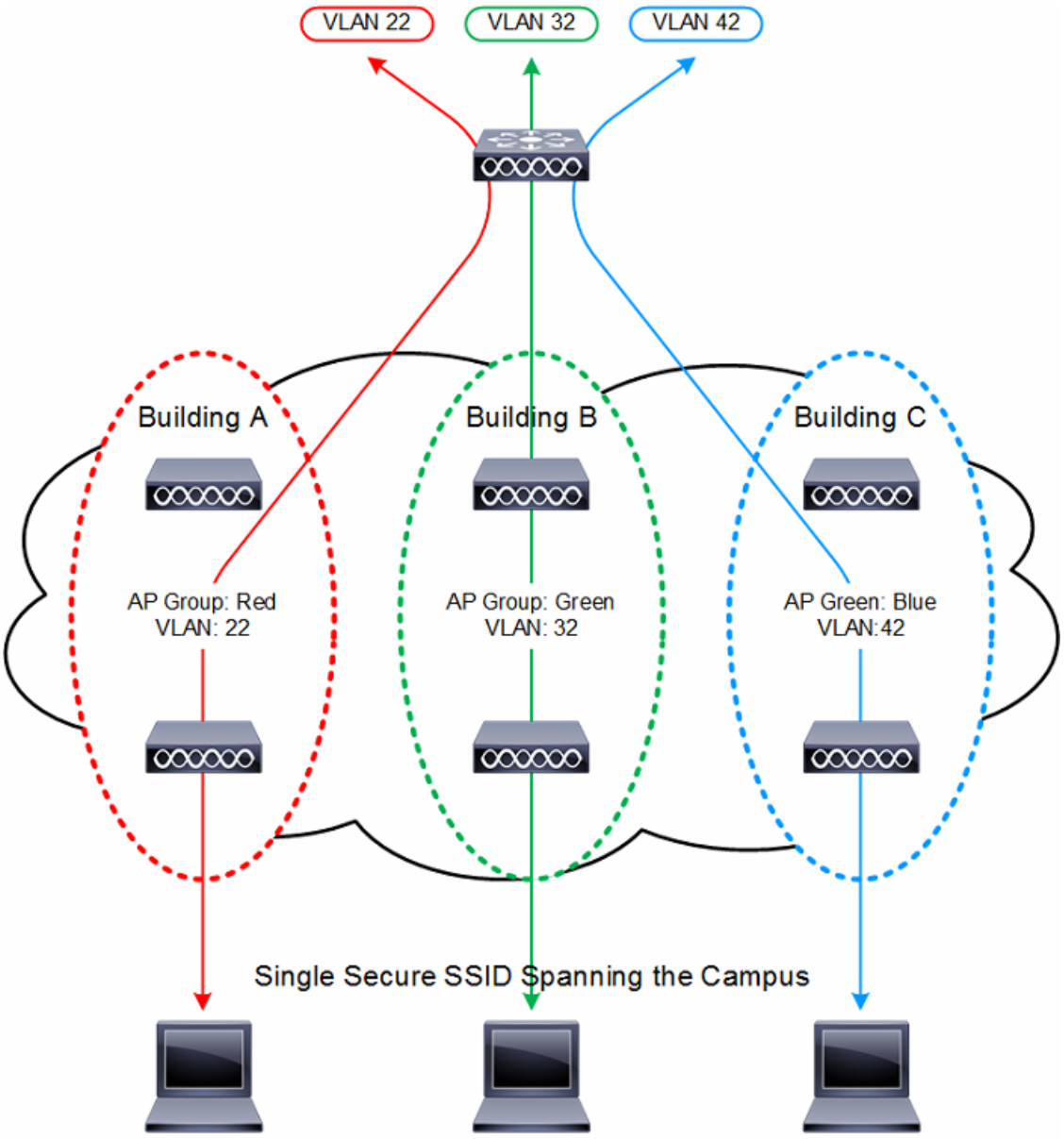
*図 2-26　WLAN 割り当て用の AP グループ*




- WLC 内の別のインターフェイスまたはインターフェイス グループに WLAN クライアントをマッピングすることによって、ブロードキャスト ドメインのサイズを縮小します。たとえば、キャンパス導入では、AP グループを利用して別々のビルディングまたはフロアにある WLAN クライアントを単一の WLC 上で別々のインターフェイスまたはインターフェイス グループにマッピングできます。

図 2-27 では、3 つの動的インターフェイスが WLC に設定され、それぞれにサイト固有の VLAN（VLAN 22、32、42）があります。サイト固有の VLAN および関連付けられた AP は、それぞれ AP グループを使用して同一の WLAN SSID にマッピングされます。VLAN 22 に対応する AP グループ内の AP 上の WLAN に関連付けられている企業ユーザは、VLAN 22 サブネットで IP アドレスを取得します。同様に、VLAN 32 に対応する AP グループ内の AP 上の WLAN に関連付けられている企業ユーザは、VLAN 32 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、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。

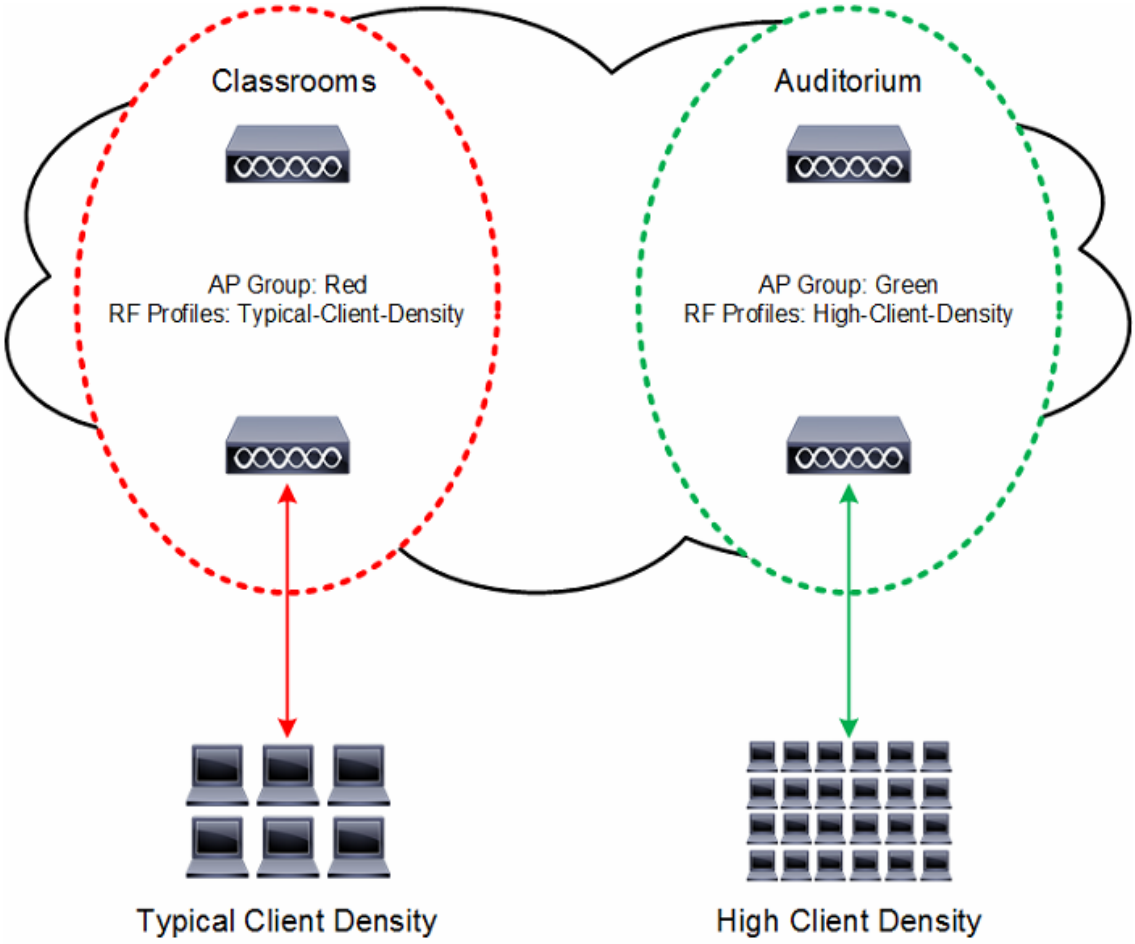
*図 2-27　インターフェイス/インターフェイス グループ割り当て用の AP グループ*




- 地理的ロケーション内で RF 環境を最適化して、さまざまなクライアント密度をサポートします。カバレッジ エリアにある AP を、異なるクライアント ニーズまたは密度をサポートするように最適化された異なる RF プロファイルに割り当てることができます。

図 2-28 に示すように、異なる AP およびクライアントの密度をサポートするように 2 つの AP グループが WLC に設定されています。1 つ目の AP グループは一般的な密度で導入されている AP およびクライアント用に設定されている一方で、2 つ目の AP グループは高密度で分布する AP とクライアントをサポートするように設定されています。

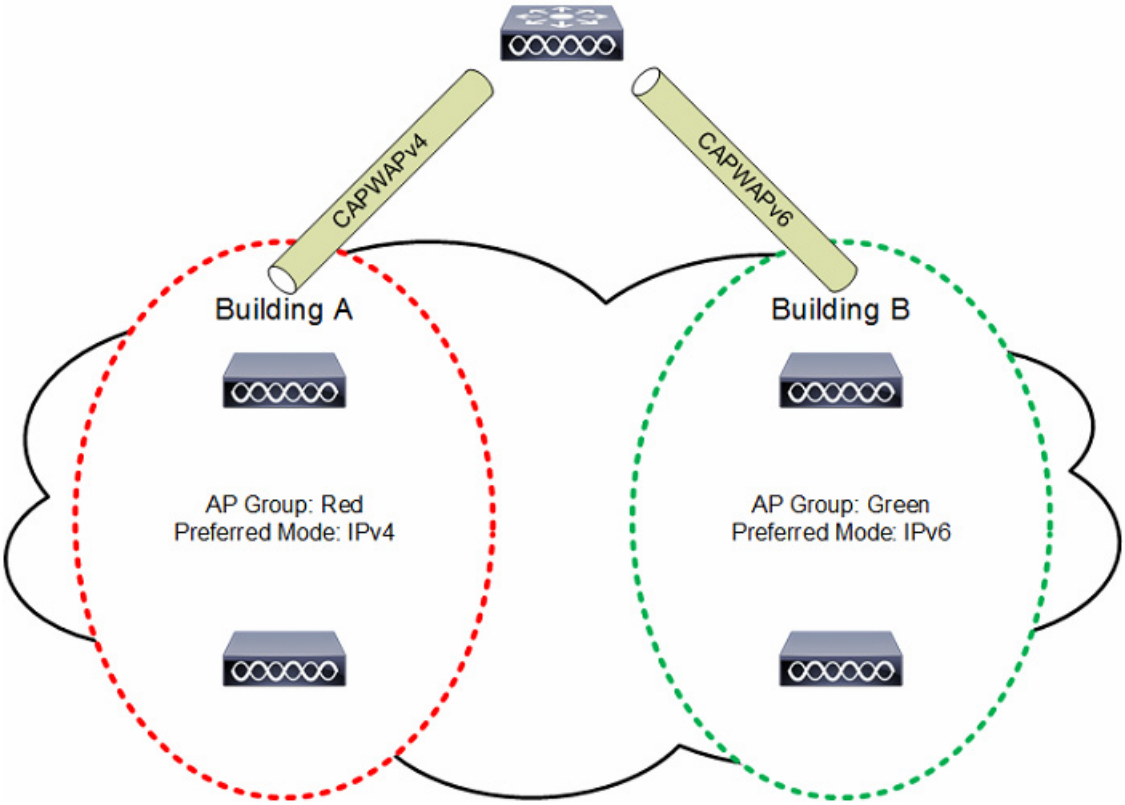
*図 2-28　RF 最適化およびクライアント密度用の AP グループ*




- インターネット プロトコル バージョン 4（IPv4）からインターネット プロトコル バージョン 6（IPv6）に AP を移行します。AP グループを利用すると、個々のビルディングまたはサイトの遷移に応じて AP CAPWAP 優先モードを IPv4 から IPv6 に切り替えることができます。

図 2-29 では、IPv4 から IPv6 への移行を支援する 2 つの AP グループが WLC に設定されています。各 AP グループには、WLC を接続するときに AP で使用する IP プロトコルを決定する、固有の CAPWAP 優先モードが設定されています。

*図 2-29　　IPv6 移行用の AP グループ*




# RF グループ

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。コントローラ ソフトウェアは、1 つの RF グループで最大 20 台の WLC と 6,000 台の AP をサポートするように拡張できます。

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 グループのメンバーになります。
- RF グループのメンバーによって、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）します。
  - 802.11 の同一チャネル干渉および競合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ーは、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 メンバーにキープアライブ 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 WLC 数は 20 です。

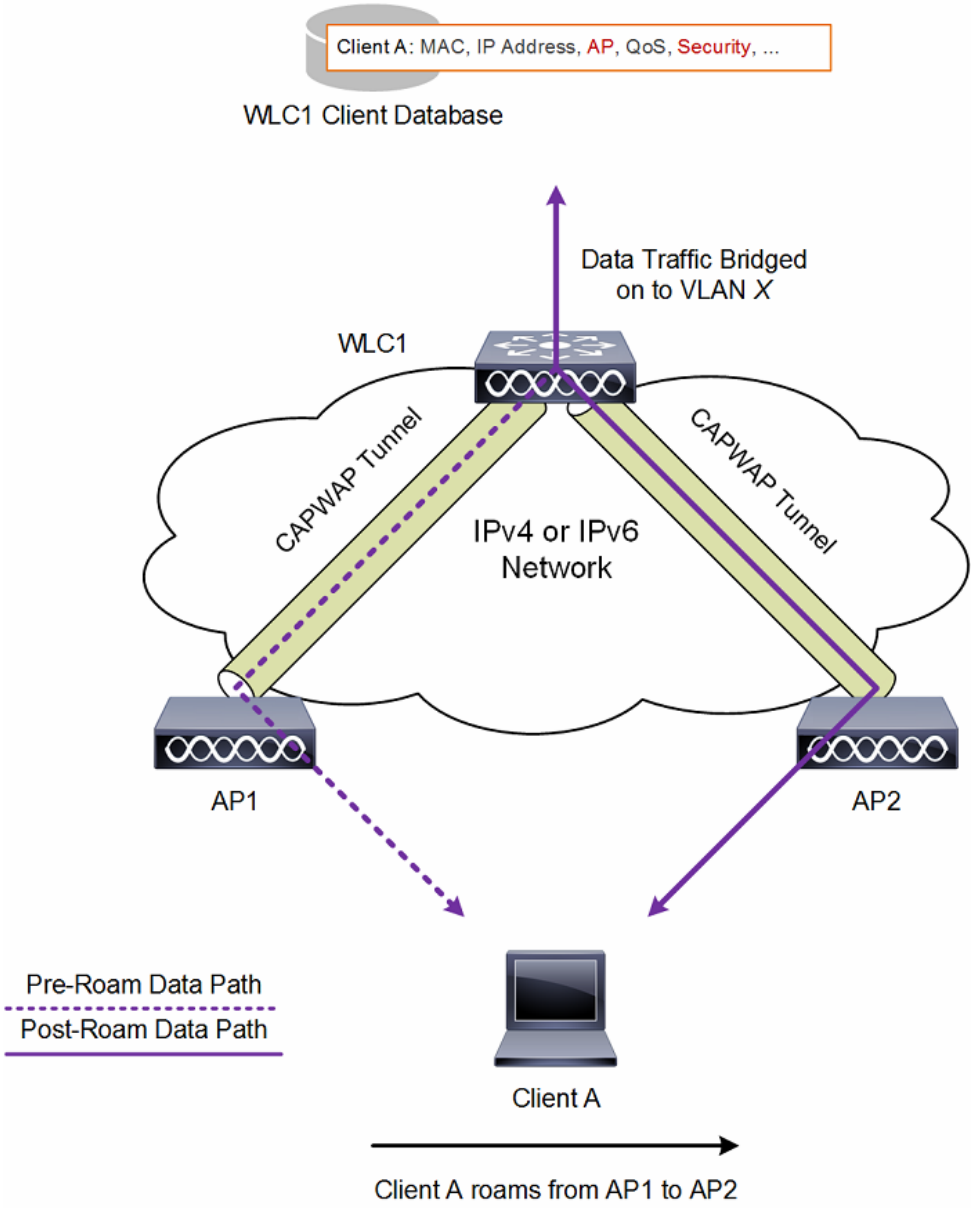
（注）　RF グループとモビリティ グループは、どちらも WLC のクラスタを定義するという点では同じですが、用途に関しては異なります。RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティと WLC の冗長性を実現します。

# 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、安全に、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 WLAN クライアントの機能です。この項では、WLC が Cisco Unified Wireless Network に含まれている場合のモビリティの動作について説明します。

ある WLAN クライアントが AP に関連付けして認証すると、WLC 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、Quality of Service（QoS）コンテキスト、WLAN、SSID、および関連付けられた 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、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 2-30 は、同じコントローラに参加している 2 つの AP の一方からもう一方にローミングするワイヤレス クライアントを示しています。

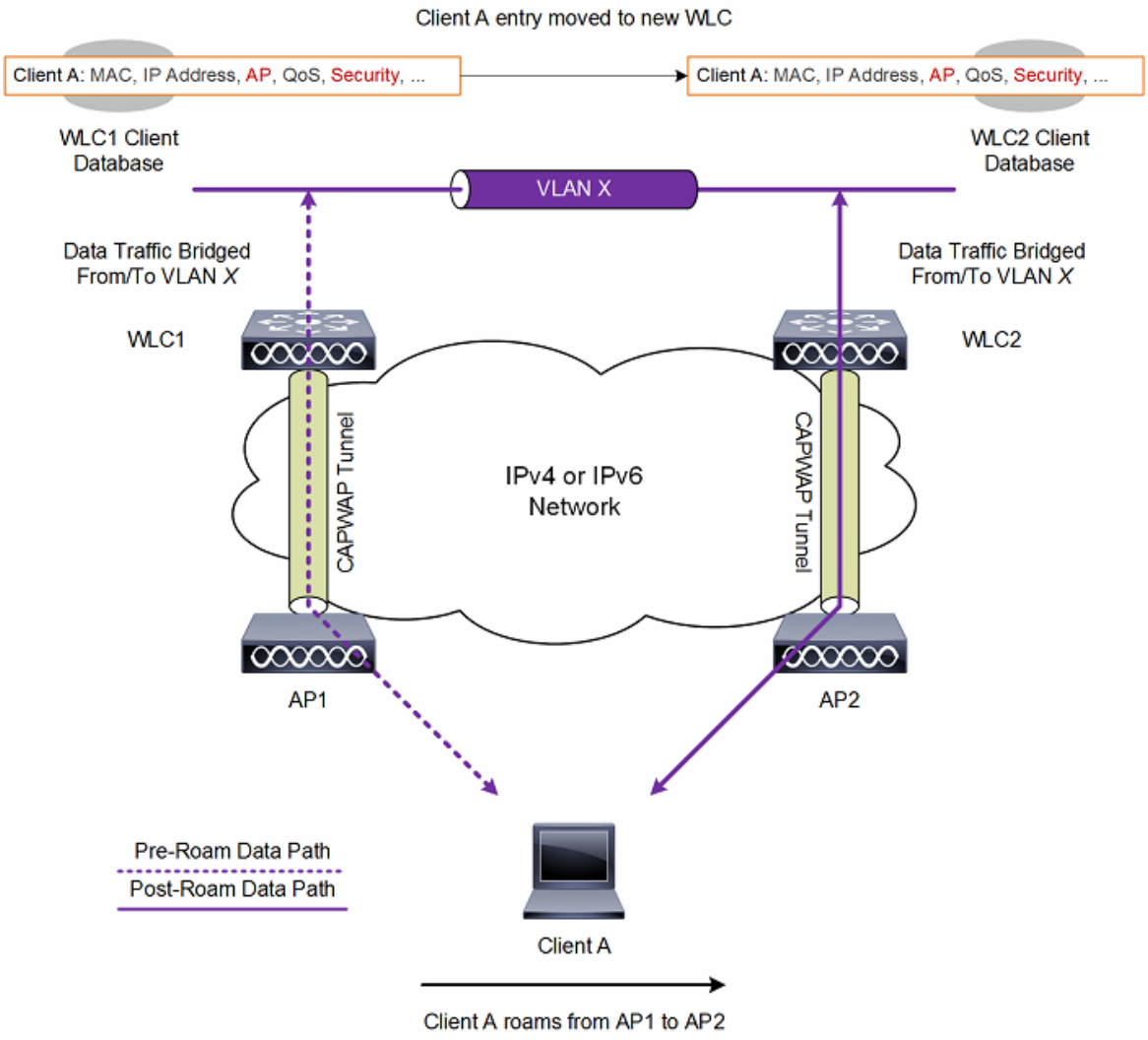
*図 2-30　　コントローラ内ローミング*




WLAN 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 は新規に関連付けられた 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 WLC に接続された AP から別の WLC 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 VLAN 上でこれらの WLC が動作しているかどうかによっても異なります。図 2-31 は、WLC インターフェイスまたはインターフェイス グループが同じ VLAN をサポートしてい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。

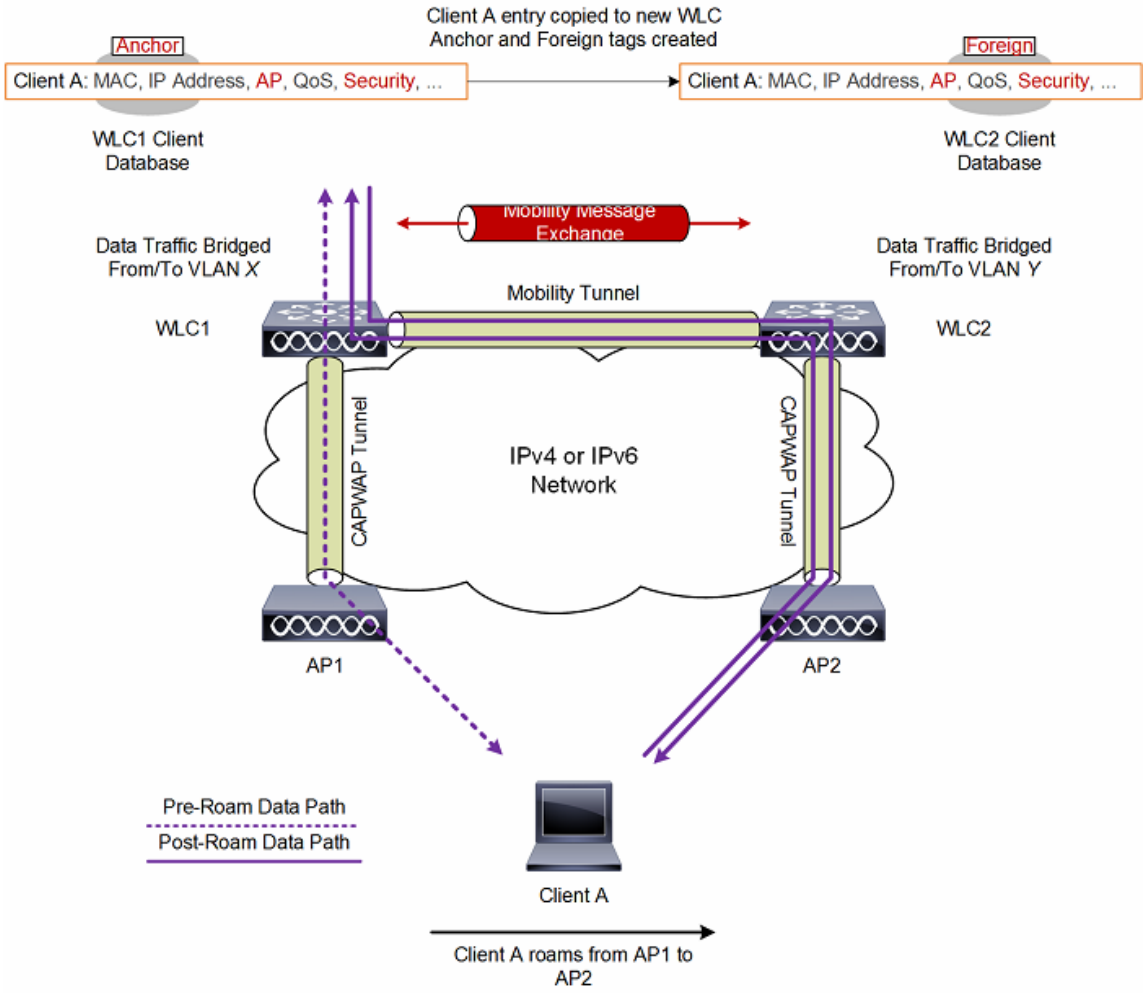
*図 2-31　　コントローラ間ローミング*




クライアントが新たなコントローラに接続された AP へ関連付けする場合、新たな WLC はモビリティ メッセージを元の WLC 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 WLC 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 用に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。

図 2-32 は、WLC インターフェイスが異なる VLAN 上にある場合に起こるサブネット間ローミングを示しています。

*図 2-32　　サブネット間ローミング*




サブネット間ローミングは、WLC 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 WLC 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 WLC 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 VLAN メンバーシップおよび元の 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 WLC 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。そうしない場合、ハンドオフ後クライアントに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。

# IPv6 クライアント モビリティ

WLC をまたがる IPv6 クライアントのローミングに対応するためには、Neighbor Solicitation（NS）、Neighbor Advertisement（NA）、Router Advertisement（RA）、Router Solicitation（RS）などの ICMPv6 メッセージに対処して、IPv6 クライアントが確実に同じレイヤ 3 ネットワーク上にとどまるようにする必要があります。IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。必要な唯一の設定は、WLC が、同じモビリティ グループに属している必要があることです。

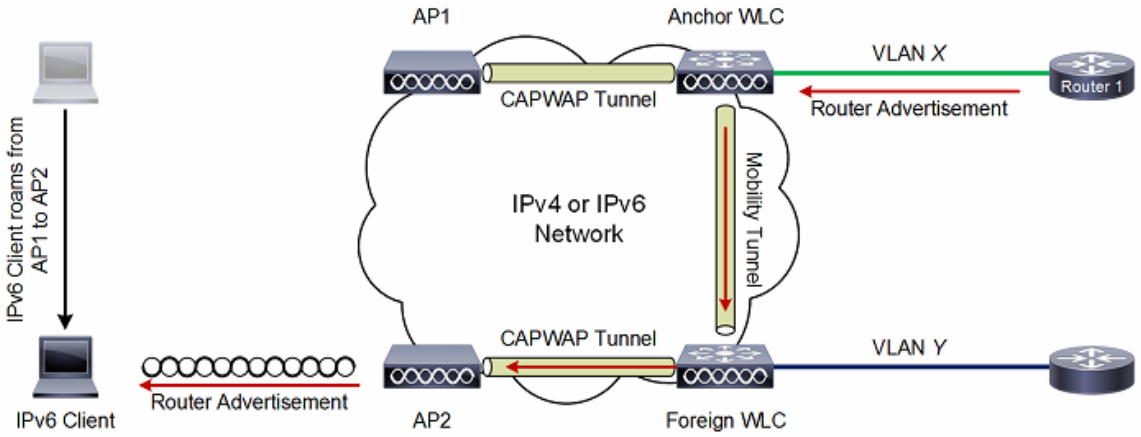
WLC をまたがる IPv6 クライアント モビリティのプロセスは次のとおりです。

- クライアントで元々接続していた VLAN に両方の WLC がアクセスできる場合、ローミングは、クライアント レコードが新しい WLC にコピーされる単なるレイヤ 2 ローミング イベントであり、トンネリングによってアンカー WLC に戻されるトラフィックはありません。
- クライアントが接続されていた元の VLAN に 2 台目の WLC がアクセスできない場合は、レイヤ 3 ローミング イベントが発生することになります。クライアントからのすべてのトラフィックはアンカー コントローラへのモビリティ トンネルを使用してトンネリングされる必要があります。リリース 7.x と 8.x による混合 WLC 導入では、モビリティ トンネルは EtherIP を使用する IPv4 ベースになります。純然たる 8.0 導入では、モビリティ トンネルは IPv4 ベースと IPv6 ベースのどちらも可能で、EtherIP（IPv4）または CAPWAP（IPv6）を使用することになります。
  - クライアントで元の IPv6 アドレスを保持することを確実化するために、元の VLAN からの RA がアンカー WLC によって外部 WLC に送信され、ここで AP からの L2 ユニキャストを使用してクライアントに配送されます。
  - ローミングされたクライアントが DHCPv6 を介してアドレスを更新するか、SLAAC を介して新しいアドレスを生成する場合、RS、NA、および NS のパケットは引き続き元の VLAN にトンネリングされるため、クライアントでは割り当てられた VLAN に適用できる IPv6 アドレスを受信します。

---

図 2-33 は、WLC インターフェイスが異なる VLAN 上にある場合に起こる、IPv6 クライアントのサブネット間ローミングを示しています。このプロセスは、ローミングされたクライアントのトラフィックがアンカー WLC にトンネリングされる、図 2-32 に示すサブネット間ローミングと同一です。ICMPv6 の RS、NA、および NS パケットすべてがアンカー WLC にトンネリングされるため、IPv6 クライアントは元の VLAN および IPv6 アドレスを維持でき、シームレスなローミング エクスペリエンスが実現されます。

*図 2-33　　IPv6 サブネット間ローミング*




(注)　リリース 8.5 以降では、IPv6 インターフェイスで SNMP over IPSec（Simple Network Management Protocol over Internet Protocol Security）がサポートされます（セキュア ローミング）。

Cisco Unified Wireless Network（CUWN）でサポートされている各種の高速ローミング方式について説明する前に、クライアントが PSK または 802.1X キー管理を使用して WPA2 WLAN に接続するときの認証方法と検証方法を理解することが重要です。この情報は、各方式用に高速セキュア ローミングを実装する方法を理解するうえで、追加のコンテキストを提供するため重要です。

WPA/WPA2-PSK 方式と WPA/WPA2-EAP 方式では、WLAN クライアントの認証と検証の方法は異なりますが、キー管理プロセスのルールは両方式で同一です。WPA2 WLAN のキー管理が PSK と 802.1X のいずれでも、使用した特定の認証方式によってクライアントがいったん検証されると、Master Session Key（MSK）を元のキー マテリアルとして使用して、フォーウェイ ハンドシェイクと呼ばれるプロセスが WLC/AP とクライアントの間のキー ネゴシエーションを開始します。

プロセスの概要を次に示します。

- MSK は、802.1X キー管理による WPA/WPA2 では EAP 認証フェーズで取得され、PSK による WPA/WPA2 では事前共有キーから取得されます。
- クライアントおよび WLC/AP では、この MSK からペアワイズ マスター キー（PMK）を取得します。
- この 2 種類のマスター キーを取得し終えると、クライアントおよび WLC/AP は、マスター キーをシードとするフォーウェイ ハンドシェイクを開始して実際の暗号化キーをネゴシエートします。
  - Pairwise Transient Key（PTK）：PTK は PMK から取得され、クライアントとのユニキャスト フレームを暗号化するために使用されます。
  - Group Transient Key（GTK）：Group Transient Key（GTK）は GMK から取得され、この特定の SSID または AP でのマルチキャストまたはブロードキャストを暗号化するために使用されます。

高速セキュア ローミングは、CUWN に含まれる AP 間でのクライアント ローミングの所要時間を短縮することを目的としています。高速ローミングは、ローミング時の後続の EAP 認証やフォーウェイ ハンドシェイクを回避できる、キー管理と配布の巧みなテクニックを実装することによって実現されます。これらのフェーズを回避することでクライアントが新しい AP に再関連付けするための所要時間が短縮され、Voice over IP（VoIP）などの時間的精度が要求されるアプリケーションに関する知覚可能な遅延を限定的にします。

次の項では、8.0 リリースで使用可能な、サポートされている各高速セキュア ローミング方式の概要を説明します。

（注）　この項で説明する各高速セキュア ローミング方式の詳細（パケットのキャプチャおよびデバッグを含む）については、次の URL にある Cisco トラブルシューティング テックノート『802.11 WLAN Roaming and Fast-Secure roaming』を参照してください：
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html。

## Cisco Centralized Key Management

Cisco Centralized Key Management（CCKM）は、シスコが企業 WLAN 用に開発した最初の高速セキュア ローミング方式であり、WLAN で 802.1X セキュリティまたは EAP セキュリティが有効化されている場合のローミングの遅延を軽減するソリューションです。これはシスコの独自プロトコルであるため、Cisco Compatible Extension（CCX）互換のシスコおよびサードパーティ製のクライアントのみでサポートされています。

CCKM は、WEP、TKIP、AES など WLAN で使用可能な多様な暗号化方式のいずれでも実装できます。複数の EAP 方式もサポートしています（クライアント デバイスでサポートされている CCX バージョンに依存）。

CCKM を使用する場合、WLAN への最初のアソシエーションは WPA および WPA2 と類似しており、MSK（ここでは、ネットワーク セッション キーとも呼ぶ）は RADIUS サーバとの成功した認証から相互に取得されます。このマスター キーは認証成功後にサーバから WLC に送信されて、このクライアント セッションの存続中に後続のキーを生成するためのベースとしてキャッシュされます。WLC およびクライアントは、ユニキャスト（PTK）および、マルチキャストとブロードキャスト（GTK）の暗号化キーを取得するために、フォーウェイ ハンドシェイクを実施しながら（WPA および WPA2 と同様）、CCKM に基づいて高速セキュア ローミングに使用されるシード情報を取得します。

CCKM クライアントが新しい AP にローミングする場合、クライアントでは単一の再アソシエーション要求フレームを CAPWAP AP に送信し（単一の MIC および順次増分される乱数を含む）、新しい PTK を取得するために十分な情報（新しい BSSID MAC アドレスを含む）を提供します。この再アソシエーション要求では、WLC および新しい AP は新しい PTK を取得するために十分な情報も持っているため、単に単一の再アソシエーション応答で応答し、EAP 認証とフォーウェイ ハンドシェイクの両方が回避されます。

概要：

- CCX 互換のシスコおよびサードパーティ製のクライアントのみでサポートされます。
- さまざまな暗号化方式および EAP 方式をサポートしています（CCX のバージョンに依存）。
- 高速ローミングは、802.1X 認証と EAP 認証およびフォーウェイ ハンドシェイクを回避することによって実行されます。

- 中央集中型導入と FlexConnect 導入（ローカルまたは中央でスイッチング）の両方でサポートされています。
  - 中央集中型：同じモビリティ グループ内の AP および WLC をまたがって機能します。
  - FlexConnect：同じ FlexConnect グループ内の AP をまたがって機能します。
- FlexConnect WLAN は、中央またはローカルのスイッチングを使用するローカル認証または中央集中型認証用に設定できます。
- FlexConnect AP は接続モードとスタンドアロン モードでサポートされていますが、スタンドアロン モードでの MSK の共有方法に関する制限事項があります。

## ペアワイズ マスター キー キャッシング

ペアワイズ マスター キー（PMK）キャッシング、別名 Sticky Key Caching（SKC）は、802.11i のセキュリティの改定の一環として IEEE 802.11 標準によって推奨された、第 1 の高速セキュア ローミング方式です。PMK キャッシングでは、クライアントによる AP との関連付けが可能であり、802.1X 認証または EAP 認証と、フォーウェイ ハンドシェイクに成功すると、PMK がキャッシュに保存されます。ローミングによって AP を去ったクライアントが戻ってきた場合、クライアントでは 802.1X 認証または EAP 認証を回避できます。

PMK キャッシングは 802.1X または PSK キー管理を使用して WPA2 WLAN でサポートされており、WLAN インフラストラクチャとクライアント サポートの両方を必要とします。

- 任意の AP への最初のアソシエーションは WLAN への通常の初回認証と似ており、802.1X または PSK の認証と、フォーウェイ ハンドシェイクが成功してからでないと、クライアントはデータ フレームを送信できません。
- ワイヤレス クライアントが、新しい AP（それまでに関連付けしたことのない AP）にローミングした場合、クライアントは 802.1X または PSK の認証とフォーウェイ ハンドシェイク全体を再度実行する必要があります。

このワイヤレス クライアントがローミングによって AP（それまでに関連付けしたことのある AP）に戻る場合、このクライアントは複数の PMKID をリストしている再アソシエーション要求フレームを送信します。このフレームは、クライアントがそれまでに認証されたことのあるすべての AP からキャッシュした PMK をこの AP に伝達します。クライアントはこのクライアント用の PMK もキャッシュしている AP にローミングして戻ってきているため、新しい PMK を取得するための再認証を必要としません。クライアントでは、新しい一時的な暗号化キーを取得するために、WPA2 フォーウェイ ハンドシェイクを行うのみです。ローミングによる復帰はクライアントに設定可能な限定された時間間隔内（Windows でのデフォルト 720 分）に発生する必要があります。

CUWN 中央集中型導入では、各 CAPWAP AP 用のキャッシュ済み PMK は WLC によって管理および維持されます。各 AP のクライアントごとに別々の PMK が生成されるため、拡張性は限られています。したがって、PMK キャッシングは大規模エンタープライズ導入には推奨されず、広く採用されてはいません。

概要：

- シスコのマニュアルでは、Sticky Key Caching（SKC）と呼ばれています。
- 802.1X または PSK キー管理を使用した WPA2 WLAN でのみサポートされています。

- 効率的でないキー管理により拡張性が大幅に制限されるため、大規模エンタープライズ導入に適していません。WLC でキャッシュできる PMK エントリは、クライアントあたり最大 8 台の AP に限られます。クライアントが 8 台を超える AP 間をローミングすると、新しく作成されたエントリを保存するために古いキャッシュ エントリが削除されます。
- 高速ローミングはローミング時の 802.1X または PSK の認証を回避することによって実施されます。高速ローミングは次の場合に限り実現されます。
  - クライアントはそれまでに関連付けされたことのある AP にローミングします。
  - AP および WLC にはこのクライアント用の PMK キャッシュ エントリがあります。つまり、このキャッシュ エントリは一連のローミングによって削除されていません。
- モビリティ ドメインの WLC をまたがっては機能しません。WLC ではモビリティ ピアと PMK を交換しません。
- FlexConnect 導入ではサポートされていません。

## Proactive Key Caching

事前認証とも呼ばれる Proactive Key Caching（PKC）は、802.11i のセキュリティの改定の一環として IEEE 802.11 標準によって推奨された、第 2 の高速セキュア ローミング方式です。PKC は Autonomous AP を使用した導入を目的としていましたが、CUWN で効率良く機能するように改変されました（詳細は後述）。

PKC は、実装の目的を反映して、ローミングに先だって、WPA2 802.1X クライアントによるネイバー AP との 802.1X 認証や EAP 認証が可能です。WPA2 クライアントでは現在の AP に接続されている間に 802.1X 認証を実行できます。事前認証は、現在の AP によって実施され、EAPOL パケットがネイバー AP に中継されて、ここで RADIUS サーバへのクエリが行われ、PMK がキャッシュされます。ネイバー AP の選択方法を判別する検出メカニズムがなかったことが、事前認証の大きな課題になっています。その結果、最初のクライアント関連付けは、システムに存在する AP と同じ数の RADIUS 認証と PMK に至ることがありました。

CUWN では、クライアントの PMK を中央でキャッシュおよび管理することにより、インテリジェントで効率的な実装を実現します。この仕組みが機能するためには、AP が共通の管理統制下にあって、PMK をキャッシュして WLAN システム内のすべての AP に配布する中央集中型デバイスが配置されている必要があります。CUWN では、WLC が制御下のすべての CAPWAP AP 用にこの作業を実行し、モビリティ メッセージングを使用してモビリティ グループ内の他の WLC 間で PMK を交換します。キャッシュされたクライアントの PMK はクライアント セッションの存続中使用されます。

この高速セキュア ローミング方式では、クライアントおよび WLC によってキャッシュされた元の PMK を再利用するため、ローミング時に 802.1X 認証および EAP 認証が回避されます。クライアントでは、新しい暗号化キーを取得するために実行する必要があるのは WPA2 フォーウェイ ハンドシェイクのみです。

- ワイヤレス クライアントが特定の AP に接続するたびに、クライアント MAC アドレス、AP MAC アドレス（WLAN の BSSID）、およびこの AP によって取得された PMK に基づいて PMKID がハッシュされます。PKC ではすべての AP および特定のクライアント用に同じ元の PMK をキャッシュするため、クライアントが別の AP にローミングする場合、新しい PMKID をハッシュするうえで変更される値は新しい AP MAC アドレスのみです。

- クライアントが新しい AP へのローミングを開始して再アソシエーション要求フレームを送信するとき、キャッシュされた PMK を高速セキュア ローミングに使用したことを AP に伝達する必要がある場合、クライアントは WPA2 RSN 情報要素に PMKID を追加します。クライアントは、ローミング先の BSSID（AP）の MAC アドレスをすでにわかっているため、この再アソシエーション要求で使用されている新しい PMKID をハッシュするだけになります。クライアントからこの要求を受信すると、AP は、すでに保持している値（キャッシュした PMK、クライアント MAC アドレス、およびそれ自体の AP MAC アドレス）を使用して PMKID のハッシュも行い、PMKID が一致したことを確認する正常再アソシエーション応答によって応答します。新しい暗号化キーを取得するための WPA2 フォーウェイ ハンドシェイクを開始するシードとして、キャッシュした PMK を使用できるため、EAP 認証フェーズが回避されます。

概要：

- シスコのマニュアルでは Proactive Key Caching（PKC）と呼ばれていますが、802.11i の改定の一環として定義されている内容と同じ実装ではありません。
- WPA2 WLAN では、802.1X キー管理を使用してデフォルトで有効化されています。
- 高速ローミングはローミング時の 802.1X 認証および EAP 認証を回避することによって実施されます。
- 中央集中型導入用にサポートされています。
- 拡張に対応しているため、大規模エンタープライズ導入に適しています。
- 単一モビリティ ドメイン内の WLC をまたがって機能します。
- FlexConnect 導入ではサポートされていません。

## Opportunistic Key Caching

WLAN ベンダー各社は Opportunistic Key Caching（OKC）という語と Proactive Key Caching（PKC）という語を互換的に使用していますが、両者は同一ではありません。この 2 方式の主な違いは、OKC は IEEE 802.11 で規定されていないため、標準ではない点です。OKC は、PMK の管理と AP 間での配布の方法についても PKC とは動作が異なります。

前述したように、PKC（事前認証）には、クライアントを事前認証しているネイバー AP を判別するメカニズムがなかったという大きな制限事項がありました。単一の WPA2 クライアント接続が、システム内の AP 数と同数の RADIUS 認証および PMK に至ることがありました。

ベンダー各社は、規定されているモビリティ ゾーン内のすべての AP にクライアントの最初の PMK を配布することにより、こういった効率の悪さを OKC によって解消しようとしました。クライアントは接続時に 802.1X 認証または EAP 認証と、フォーウェイ ハンドシェイクを実行し、クライアントの接続先のゾーンにあるすべての AP に取得した PMK を配布します。その結果、クライアントは各ネイバー AP で RADIUS 認証を実行する必要なくネイバー AP で事前認証されます。高速ローミングは、モビリティ ゾーン内の別の AP にクライアントがローミングするときに、802.1X および EAP の交換を回避することで実施されます。

OKC の主な欠点は、モビリティ ゾーン内の AP に PMK を配布する方法にあります。Datagram Transport Layer Security（DTLS）などのメカニズムを使用して AP の管理および制御プロトコルを保護していない場合、PMK の配布は保護されていません。

CUWN では、FlexConnect 導入用に 802.1X キー管理を使用して WPA2 WLAN 上で OKC がデフォルトでサポートされています。FlexConnect 導入では、FlexConnect グループに PMK を配布する AP がモビリティ ゾーンによって定義されます。クライアントが正常に認証されると、FlexConnect グループ内のすべての AP に WLC によって PMK が配布されます。シスコの CAPWAP 実装は DTLS を使用して保護されているため、PMK キーの配布が保護されています。

PMK の配布は WLC によって管理されているため、すべての FlexConnect AP が接続モードである必要があります。サイトにある FlexConnect AP がスタンドアロン モードに遷移した場合、高速セキュア ローミングは既存のクライアントに対してのみ提供可能です。

概要:

- Opportunistic Key Caching（OKC）という語は Proactive Key Caching（PKC）という語と互換的に使用されていますが、両者は同一ではありません。
- IEEE 802.11 標準として規定されていません。
- FlexConnect 導入用に 802.1X キー管理を使用して WPA2 WLAN でデフォルトで有効化されています。
- 高速ローミングはローミング時の 802.1X 認証および EAP 認証を回避することによって実施されます。
- FlexConnect のみでサポートされています（ローカルまたは中央でスイッチング）。
- PMK を最初に生成する時点で、FlexConnect AP が接続モードである必要があります。
- 同じ WLC に関連付けられている同じ FlexConnect グループ内の AP をまたがって機能します。

## 802.11r を使用した高速セキュア ローミング

802.11r（802.11 標準による正式名称は Fast BSS Transition、別名 FT）は、AP 間の高速遷移を実行するためのソリューションとして IEEE によって正式に承認された、最初の高速セキュア ローミング方式です。802.11r の改定は 2008 年に正式に承認されており、WLAN 上でキーを処理およびキャッシングするためのキー階層を明確に定義しています。

このテクニックの説明は他の方式と比べて複雑になっています。これは、新しい概念と、別々のデバイスにキャッシュされる PMK の複数階層（各デバイスが別々のロールを持つ）が導入されており、高速セキュア ローミングのためのオプションが増えているためです。そこで、この方式と、選択可能なオプションごとの実装方法について概要を説明します。

- ハンドシェイク メッセージング（PMKID、ANonce、SNonce 交換など）は再アソシエーション フレームではなく、802.11 の認証フレームまたはアクション フレームで行われます。PMKID キャッシング方式とは異なり、アソシエーション（または再アソシエーション）メッセージ交換の後で実行される個別のフォーウェイ ハンドシェイク フェーズは回避されます。新しい AP とのキー ハンドシェイクは、この新しい AP にクライアントが完全にローミングまたは再関連付けする前に開始されます。
- 高速ローミング ハンドシェイクの方式は、Over-the-Air と Over-the-DS（分散システム）の 2 方式が提供されています。
- 802.11r ではキー階層の層が増えています。
- このプロトコルでは、クライアントがローミングするときのキー管理用のフォーウェイ ハンドシェイクを回避しているため（このハンドシェイクを必要としないで新しい暗号化キーの PTK および GTK を生成）、802.1X または EAP を認証に使用する場合に限らず、PSK を使用する WPA2 セットアップにも適用できます。これにより、これらのセットアップでのローミングがさらに高速化されます。EAP およびフォーウェイ ハンドシェイクの交換は発生しません。

802.11r では、最初の AP への接続が確立されるときにワイヤレス クライアントが WLAN インフラストラクチャに対する最初の認証を 1 回だけ実行し、同じ FT モビリティ ドメインにある AP 間でのローミング時には高速セキュア ローミングを実行します。同じ SSID（別名 Extended Service Set（ESS））を使用する AP は同じ FT キーを処理します。AP で FT モビリティ ドメイン キーを処理する方法は、PKC および OKC と同じです。CUWN では、WLC が制御下のすべての CAPWAP AP 用にこの作業を実行し、モビリティ メッセージングを使用してモビリティ グループ内の他の WLC ピア間で FT キーを交換します。

次にキー階層の概要を示します。

- MSK は引き続き、最初の 802.1X および EAP の認証フェーズからクライアント サプリカントおよび RADIUS サーバ上で取得されます（認証成功時に RADIUS サーバから WLC に転送）。この MSK は、FT キー階層のシードとして使用されます。EAP 認証方式ではなく WPA2-PSK を使用する場合は、PSK が MSK です。
- ペアワイズ マスター キー R0（PMK-R0）は、FT キー階層の第 1 レベルのキーである MSK から取得されます。この PMK-R0 のキーを保持しているのは WLC およびクライアントです。
- ペアワイズ マスター キー R1（PMK-R1）という第 2 レベルのキーは PMK-R0 から取得されます。このキーを保持しているのは、クライアントと、PMK-R0 を保持している WLC によって管理されている AP です。
- FT キー階層の最後のレベルである第 3 レベルのキーは PTK です。これは、802.11 ユニキャスト データ フレームを暗号化するために使用される最後のキーです（WPA/TKIP または WPA2/AES を使用する他の方式と同様）。この PTK は FT で PMK-R1 から取得され、キーを保持しているのはクライアントと、この WLC によって管理されている AP です。

802.11r は、デフォルトで、中央集中型導入と FlexConnect 導入（中央またはローカルでスイッチング）の両方でサポートされています。FlexConnect を採用するためには中央集中型の WLAN 認証にする必要があります。802.11r はローカル認証を使用している FlexConnect AP やスタンドアロン モードで動作している FlexConnect AP ではサポートされません。所定の 802.11r ローミング ドメインに含まれている FlexConnect AP は、同じ FlexConnect グループに属している必要があります。

概要：

1. PSK または 802.1X キー管理を使用している WPA2 WLAN でのみサポートされています。
2. 高速ローミングはローミング時に 802.1X 認証および EAP 認証とフォーウェイ ハンドシェイクを回避することによって実施されます。
3. 中央集中型導入と FlexConnect（中央とローカルでスイッチング）導入の両方でサポートされています。
   a. 中央集中型：同じモビリティ グループ内の WLC をまたがって機能します。
   b. FlexConnect：同じ FlexConnect グループ内の AP をまたがって機能します。
4. FlexConnect を使用するには、WLAN が中央集中型認証用に設定されている必要があります。ローカル認証はサポートされません。高速セキュア ローミングはスタンドアロン モードで動作している FlexConnect AP ではサポートされていません。

（注）　IEEE 802.11r およびその他の 802.11 修正の詳細については、802.11r Fast Transition ローミングを参照してください。

## 考慮事項

高速セキュア ローミング方式を WLAN で選択する場合に検討する必要のある複数の考慮事項を次に示します。

- 高速セキュア ローミング方式は、セキュリティが有効化されている WPA2 WLAN 上の AP 間をクライアントが移動するときのローミング プロセスを高速化するために開発された方式であるという点を理解することが重要です。WLAN セキュリティを設定していない場合は、802.1X 認証、EAP 認証、フォーウェイ ハンドシェイクのいずれもなく、これらを回避することでローミングを高速化できません。
- 802.11r は、WPA2-PSK をサポートしている唯一の高速セキュア ローミング方式です。802.11r は、フォーウェイ ハンドシェイクを回避して WPA2-PSK ローミング イベントを高速化します。
- WLAN がローカル認証用に設定されている場合は、いずれの高速セキュア ローミング方式も FlexConnect 導入で機能しません。ローカル認証が有効化されている場合、クライアントはローミング時に完全な認証を実行することになります。
- すべての高速セキュア ローミング方式に長所と短所がありますが、最終的には、実装しようとしている特定の方式がワイヤレス クライアント ステーションでサポートされていることを確認する必要があります。特定の WLAN/SSID に接続するワイヤレス クライアントによってサポートされている最良の方式を選択する必要があります。たとえば、導入によっては、シスコ ワイヤレス IP フォン（CCKM を使用する WPA2/AES はサポートし、802.11r はサポートしない）用に CCKM を使用する WLAN を作成してから、802.11r をサポートしているワイヤレス クライアント用に 802.11r/FT を介して WPA2/AES を使用する（またはサポートされていれば OKC/PKC を使用する）別の WLAN を作成できます。
- 使用可能ないずれの高速セキュア ローミング方式もサポートしない 802.1X クライアントの場合は、AP 間のローミング時に常に遅延が発生します。この 802.1X クライアントは、ローミング イベントの際に、802.1X または EAP の認証とフォーウェイ ハンドシェイク全体を実行する必要があります。この結果、アプリケーションおよびサービスに中断が発生するおそれがあります。
- 別の WLC によって管理される AP 間では、WLC が同じモビリティ グループに属している限り、すべての高速セキュア ローミング方式（PMKID/SKC を除く）がサポートされます（コントローラ間ローミング）。

# Adaptive 11r

802.11r 対応 WLAN は、ワイヤレス クライアント デバイスのローミングを高速化します。ローミング エクスペリエンスを向上させるためには、Apple iOS デバイスを 11r 対応 WLAN に接続できるようにすることをお勧めします。ただし、WLAN で 11r を有効にすると、FT AKM のビーコンおよびプローブ応答を認識しないレガシー デバイスを WLAN に接続できなくなります。何らかの方法で、クライアント デバイスの機能を識別して 11r 対応デバイスを FT 対応デバイスとして WLAN に接続可能にし、同時に、レガシー デバイスを 11i/WPA2 デバイスとして接続できるようにする必要があります。Cisco WLC ソフトウェア リリース 8.3 は、802.11i 対応 WLAN 上の 802.11r を Apple デバイスに対して選択的に有効化することができます . 対応する Apple デバイスはこの機能を識別し、WLAN で FT アソシエーションを行います。シスコ ワイヤレス インフラストラクチャでは、非 FT WLAN で FT アソシエーションをネゴシエートできるデバイスから、WLAN 上で FT アソシエーションを行うことが、可能になります。

さらに、AireOS コード 8.3 が動作している WLC では、SSID 上で 802.11k および 11v 機能がデフォルトで有効になります。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要な時にスキャニングして時間を無駄にすることがなくなるので、クライアントのローミング状況の改善に役立ちます。Apple デバイスはデュアルバンドをサポートするため、802.11k ネイバー リストは、[1] に適応してデュアルバンドで更新されます。

シスコのインフラストラクチャ側では、シスコの AP がビーコンとプローブで Adaptive 802.11r のサポートをアドバタイズし、Over-the-DS FT 機能が設定されます。

クライアント側では、iOS 10 以降を実行する Apple デバイスが IE 上で Adaptive 11r 機能サポートを検索します。capability bit が設定されている場合は、機能ビットが AKM（dot1x または PSK）を検索し、それに応じて FT dot1x または FT PSK を使用します。Apple デバイスは、FT をサポートする IE をアソシエーション要求で送信します。それにはベンダー固有の OUI も含まれます。

Cisco WLAN は、アソシエーション要求を処理し、アソシエーション応答で 802.11r サポートに応答して FT アソシエーションを許可します。フォーウェイ ハンドシェイクには FT アソシエーションが含まれています。

この機能は、ローカル モードおよび FlexConnect モードの AP、すべての 802.11n および 802.11ac Wave 1 AP、Wave2 AP 用の AireOS コード リリース 8.3[2] 以降および 8.3.11.0 でサポートされます。

# 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 2-34 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。AP と同じ有線 VLAN 上に別の AP がある場合、それらも、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。

1. 最適な WiFi 接続ソリューションをサポートしている Apple デバイスは次のとおりです。

iPhone 6s 以降

iPhone 6s Plus 以降

iPad Air 2 以降

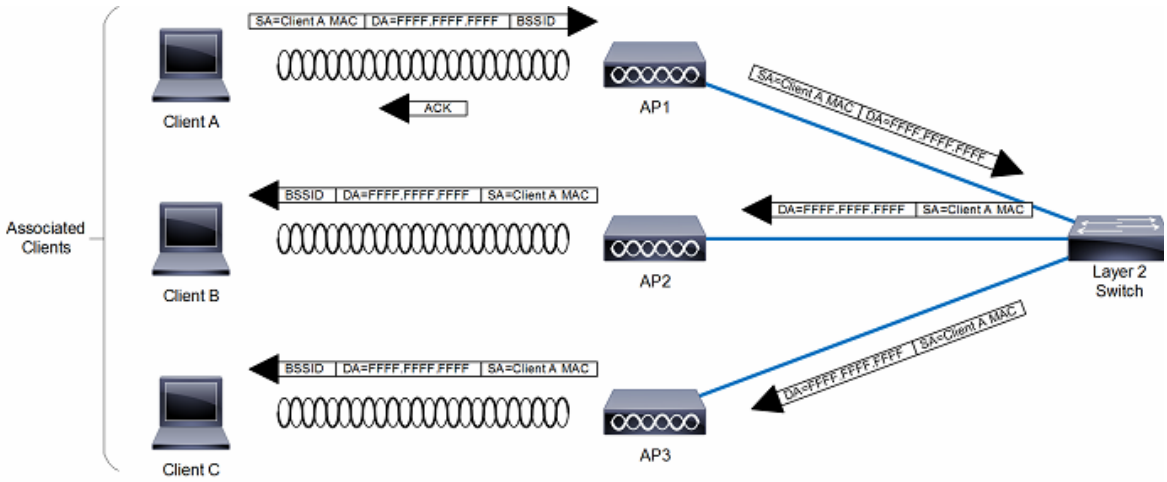
iPad mini 4 以降

iPad Pro 以降

iPhone SE

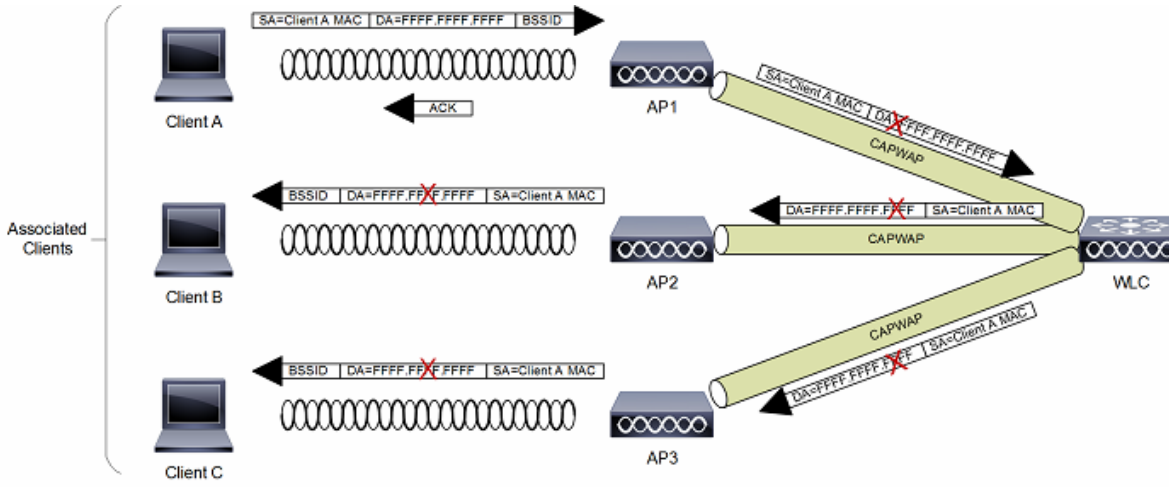
2. AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、ハイパーロケーション モジュール、3602P、AP3700 シリーズ アクセス ポイント + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、AP1040/1140/1260 シリーズ アクセス ポイント。

*図 2-34　802.11 ブロードキャスト/マルチキャストの動作*




WLC の CAPWAP スプリット MAC 方式では、図 2-35 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 2-35　WLC 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データ 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、関連付け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の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、関連付けされている 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 に関連付けされます。DHCP リレー要求は、指定された動的インターフェイスの送信元 IP アドレスを使用して、この動的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、有線およびワイヤレス 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。

この方式により、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妨害（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。ベスト プラクティスとして、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お勧めします。
- クライアント デバイス上の IP アドレスを確認します。デバイスには、それぞれの VLAN の IP アドレスが必要です。
- AP にコントローラが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/ac の速度で設定された WLAN に関連付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「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明示的に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 リンク層とネットワーク層のマルチキャスト 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、リンク層のマルチキャスト 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 導入の設計における主な考慮事項は、WLC のロケーションと AP および WLC の接続です。この項では、中央集中型（ローカル モード）AP 導入に関するトピックについて簡単にまとめ、標準的な推奨事項について適宜説明します。FlexConnect AP 展開における推奨事項と設計上の考慮事項については、この項では扱いません。代わりに第 7 章「FlexConnect」で説明します。

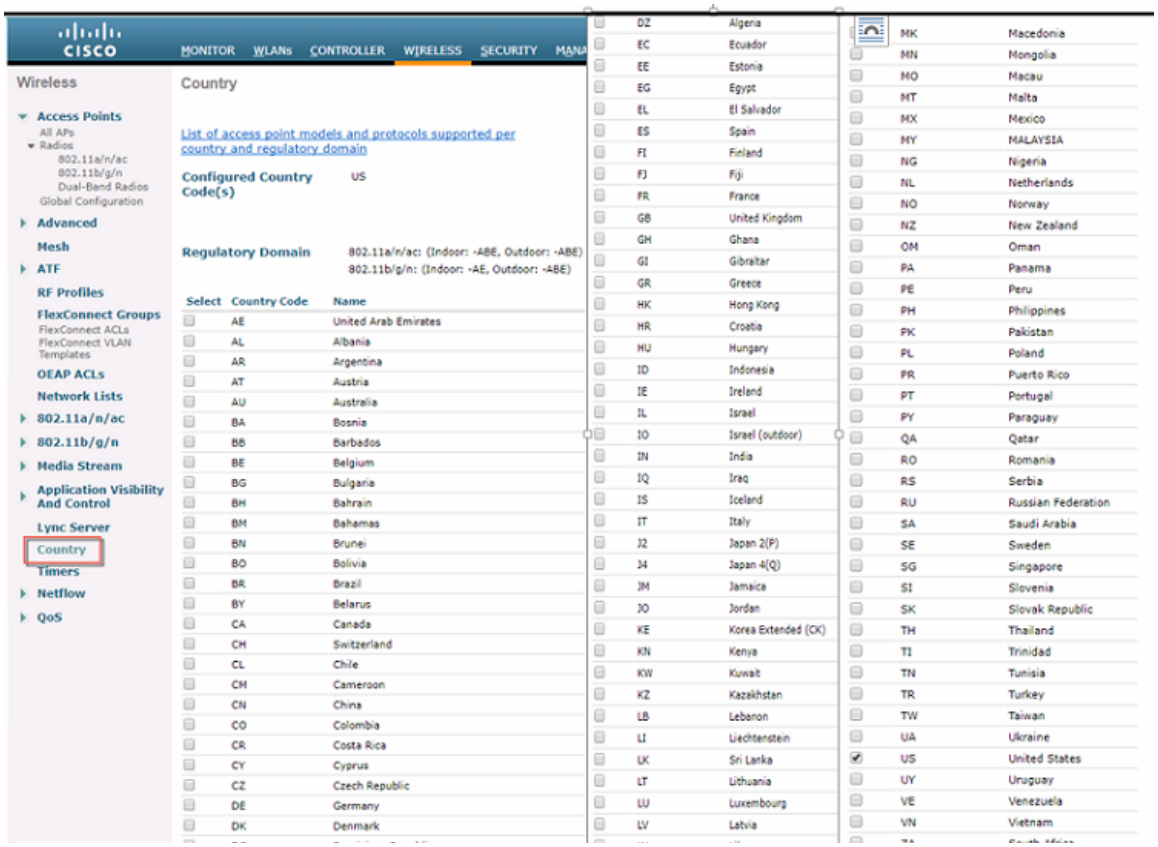
# WLC のロケーション

Cisco Unified Wireless Network では、導入の規模と種類に応じて、WLC を中央に配置することも、キャンパス内に分散させることもできます。さまざまな展開タイプと考慮事項については、以下の項で説明します。

## 分散型の WLC 導入

8.2 より前のリリースでは、WLC で 20 カ国しかサポートされませんでした。リリース 8.2 以降の WLC では、さまざまな地域固有の AP による分散コントローラ構成と同時国サポートが 110 カ国を対象にサポートされます。

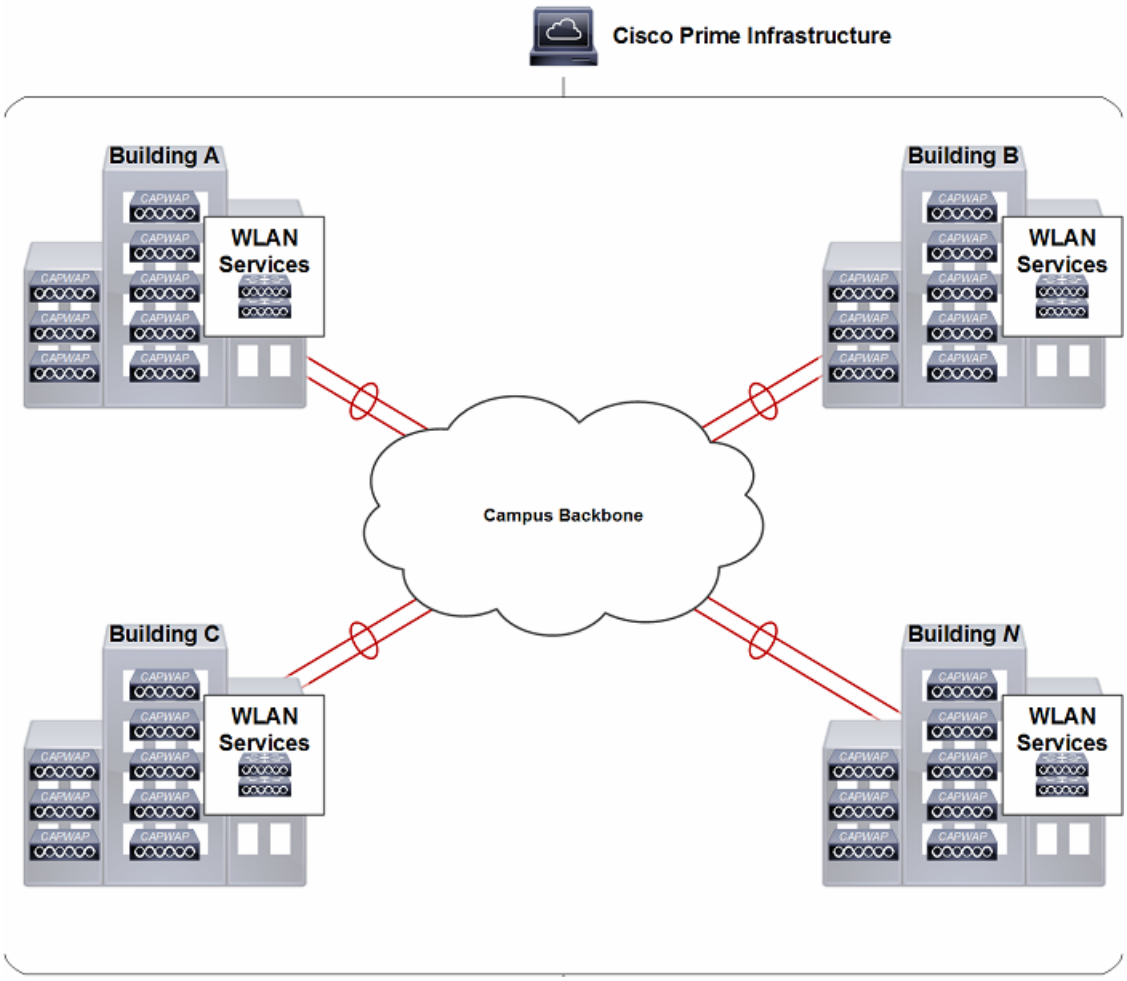
http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html#wp9005314




## 分散型の WLC 展開

図 2-36 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、各ビルディング内のディストリビューション レイヤ スイッチが使用されます。このシナリオでは、AP と WLC の間の CAPWAP トンネルは各ビルディング内にとどまります。

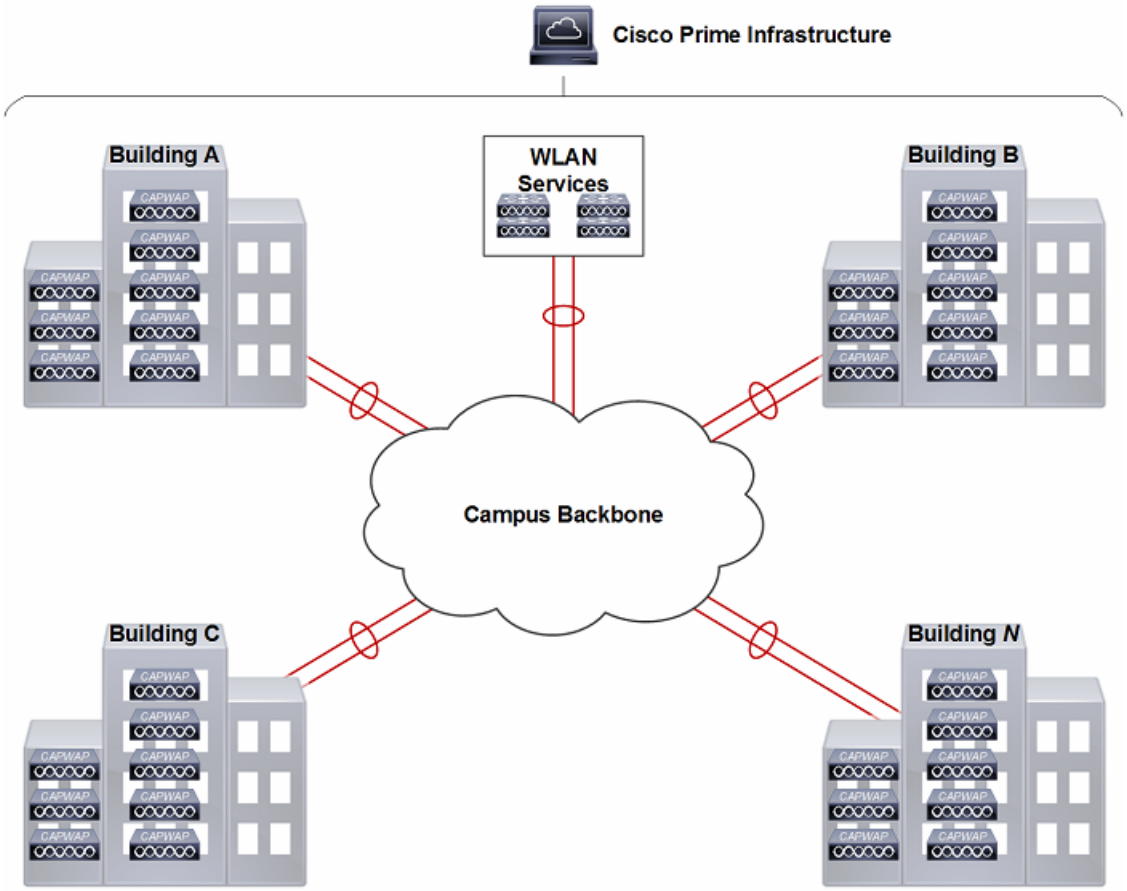
*図 2-36　分散型の FWLC 導入*




## 中央集中型の WLC 導入

図 2-37 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 はキャンパス ネットワークの集中化された場所に配置されます。この導入モデルでは、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 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 のプールは専用スイッチ 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。データセンター内と WLC プールでは、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 2-37　　キャンパス内の中央集中型 WLC*




## リファレンス アーキテクチャ

WLC の配置に関するシスコの推奨事項は、Cisco Unified Wireless Network 導入の規模と拡張によって異なります。次の項では、それぞれシスコの階層型設計の方針に基づく小規模、中規模、大規模、およびきわめて大規模なキャンパス ネットワークの推奨される WLC 配置と冗長構成によるリファレンス アーキテクチャについて説明します。ローカルモード AP を使用するリモート ブランチ オフィス導入のリファレンス アーキテクチャも、この項の終わりに示してあります。

(注)　Cisco Validated Design およびベスト プラクティスの詳細については、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html を参照してください

### 小規模キャンパス

図 2-38 は、コラスプト コアとして動作するディストリビューション レイヤを実装する小規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。ディストリビューション レイヤは、WLC、WAN、およびインターネット エッジへの接続を提供します。WLC は LAN の規模に応じてディストリビューション レイヤに直接接続することも、専用スイッチ ブロックを介して接続することもできます(図を参照)。この例の小規模キャンパスは、複数台のアクセス レイヤ スイッチを配置した単一のビルディングです。

*図 2-38　　小規模キャンパスのリファレンス設計*

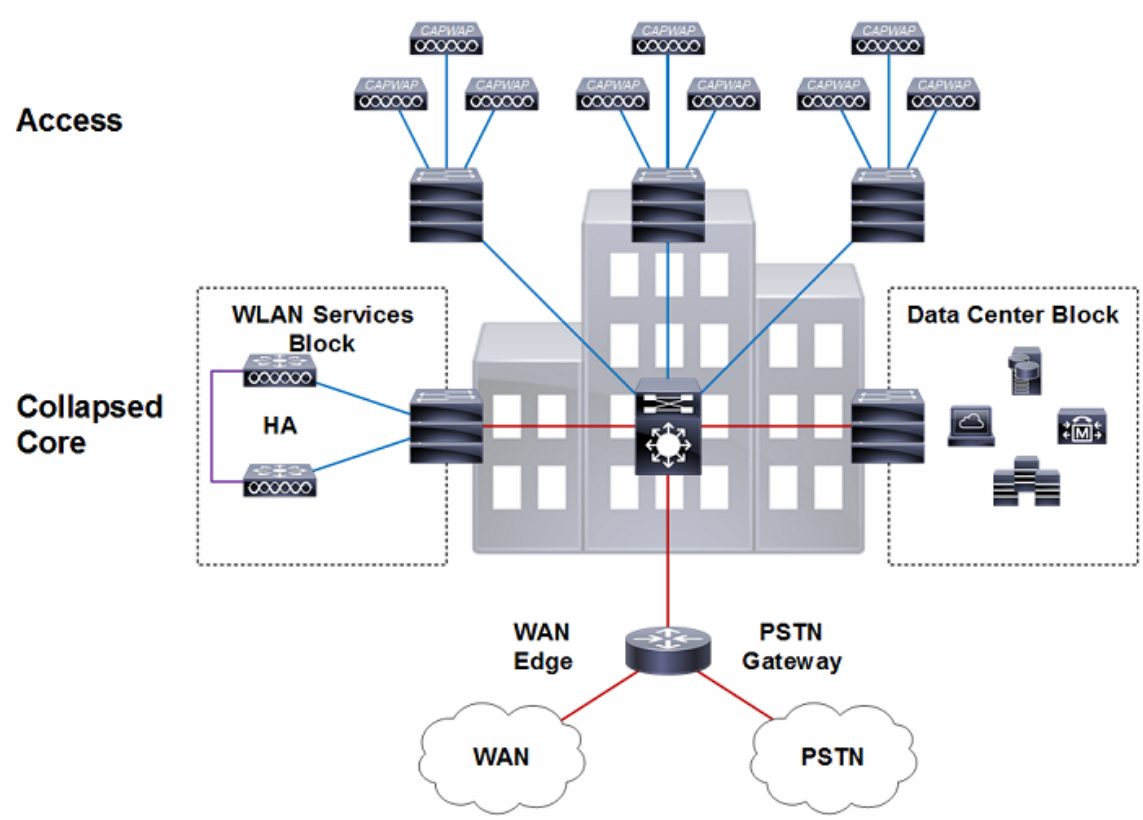
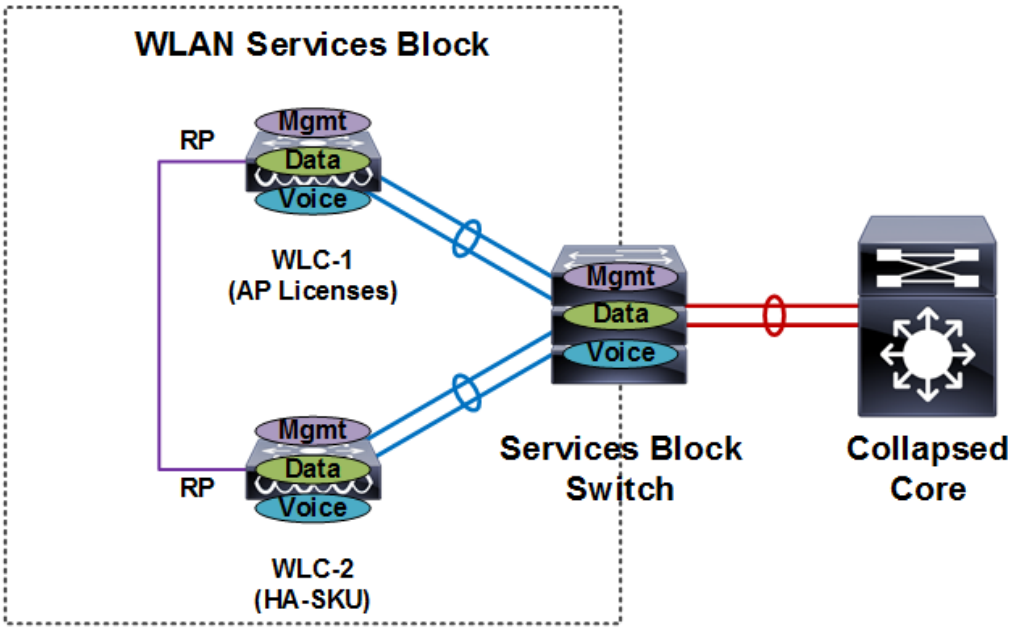



図 2-39 は、小規模キャンパス ネットワーク導入用のワイヤレス サービス ブロックの詳細を示します。この例では、ディストリビューション レイヤに接続する専用サービス スイッチ ブロック（Catalyst シャーシ、つまり復元力のあるスタック）に WLC のペアが接続されています。このサービス スイッチ ブロックはサービス専用にすることも、データセンターとサービス ブロックの両方に接続することもできます。このスイッチ ブロックはルート集約用に EIGRP または OSPF を実装しているレイヤ 3 リンクを使用してディストリビューション レイヤに接続されています。この例の WLC は中央集中型であると見なされます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してサービス スイッチ ブロックに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とサービス スイッチ ブロックの間でいずれも 802.1Q タギングされています。このサービス スイッチ ブロックは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

*図 2-39　小規模キャンパスとワイヤレス サービス ブロックの詳細*




小規模キャンパス導入では Cisco 5508 または Cisco 5520 WLC のペアを HA-SSO 用に設定することをお勧めします。選択する WLC モデルは、サイトで必要とされる具体的なスループットによって決まることになります。両方の WLC が同じ物理データセンターにあるため、両方の WLC 用の冗長ポートは直接接続されています。AP は HA-SSO ペアをプライマリ WLC として使用するように設定されています。アクティブとスタンバイホットの WLC 間ですべての構成が自動的に同期されます。

## 中規模キャンパス

図 2-40 は、専用のディストリビューション レイヤを実装する中規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。大規模なネットワーク用に専用ディストリビューション レイヤを導入するメリットは詳しく文書化され、理解されています。このアーキテクチャの WLC は、専用スイッチ ブロックを介してコア レイヤに直接接続しています。この例の中規模キャンパスは、それぞれ複数のアクセス レイヤ スイッチが配置されている複数のフロアのある単一のビルディングです。

*図 2-40　　キャンパス WLC 導入の詳細*

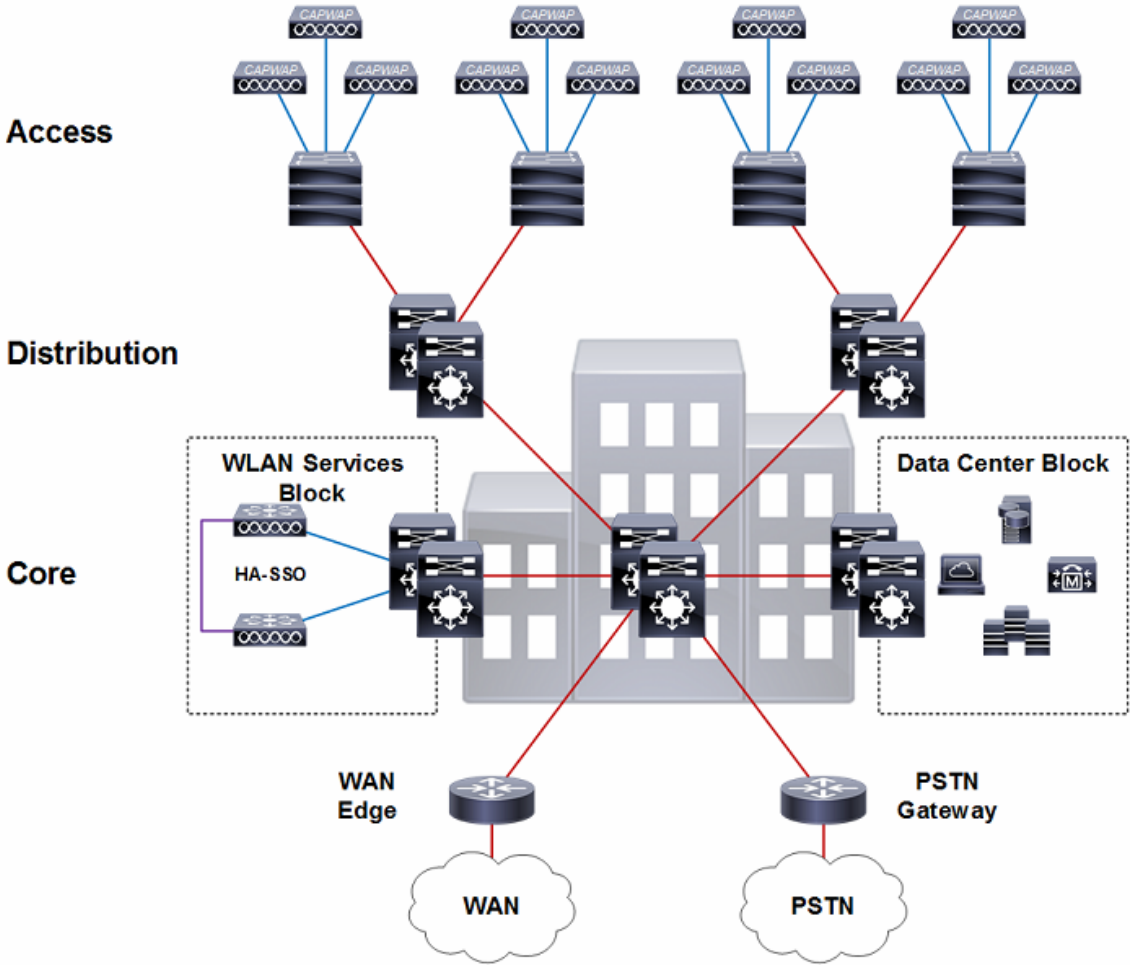
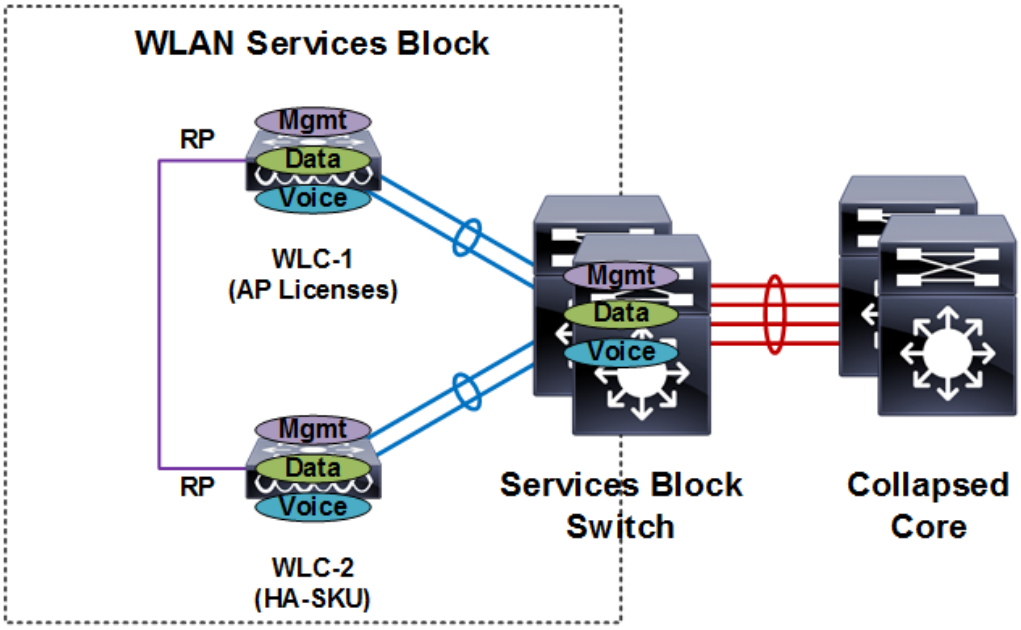



図 2-41 は、中規模キャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、コア レイヤに接続する専用サービス スイッチ ブロックに WLC のペアが接続されています。このサービス スイッチ ブロックはマルチレイヤまたは VSS 用に設定されている Catalyst スイッチのペアです。このサービス スイッチ ブロックはルート集約用に EIGRP または OSPF を実装しているレイヤ 3 リンクを使用してコア レイヤに接続されています。この例の WLC は中央集中型であると見なされます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してサービス スイッチ ブロックに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とサービス スイッチ ブロックの間でいずれも 802.1Q タギングされています。このサービス スイッチ ブロックは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

*図 2-41　　中規模キャンパスとワイヤレス サービス ブロックの詳細*



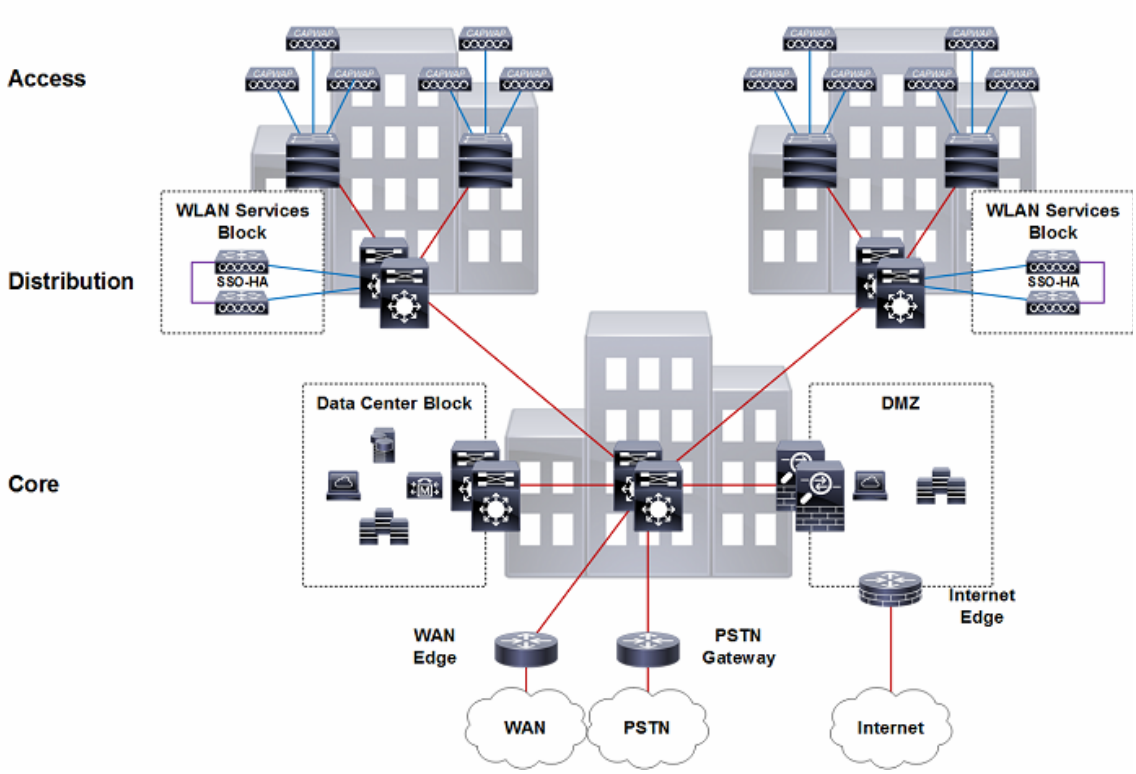

中規模キャンパス展開では、HA-SSO 用に設定された Cisco 3504、Cisco 5508、または Cisco 5520 WLCのペアを使用することを推奨します。選択する WLC モデルは、サイトで必要とされる具体的なスループットによって決まることになります。両方の WLC が同じ物理データセンターにあるため、両方の WLC 用の冗長ポートは直接接続されています。AP は HA-SSO ペアをプライマリ WLC として使用するように設定されています。アクティブとスタンバイホットの WLC 間ですべての構成が自動的に同期されます。

## 大規模キャンパス

図 2-42 は、キャンパス コアに接続される複数のビルディングで構成される大規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。このアーキテクチャの WLC はビルディング間で分散されており、WLC の各ペアが所定のビルディングにある AP を管理します。このアーキテクチャの WLC は各ビルディング内でディストリビューション レイヤに直接接続されています。

WLC の複数のペアがキャンパス全体に分散されているため、各 WLC は同じモビリティ グループのメンバーとして割り当てられて、ローミングするクライアントにキャンパス全体でシームレスなモビリティを提供します。各ビルディングの WLC には、所定の各ビルディングのディストリビューション レイヤで終端されている異なるワイヤレス管理 VLAN およびユーザ VLAN が割り当てられています。モビリティ トンネルは、キャンパス コアを通じて外部 WLC とアンカー WLC の間でローミング ユーザのトラフィックを転送するために使用されます。

*図 2-42　大規模キャンパスのリファレンス設計*




WLC をビルディング間に分散させると、1 つの CUWN によってサポートされるワイヤレス クライアントの数が増えるため、拡張性に関する複数の長所があります。ワイヤレス ネットワークに追加されるデバイスが増えるほど、サービス ブロック スイッチによって処理および保守されるレイヤ 2 およびレイヤ 3 のテーブル エントリの数が指数関数的に増えます。この結果、サービス ブロック スイッチで CPU 負荷が高くなります。

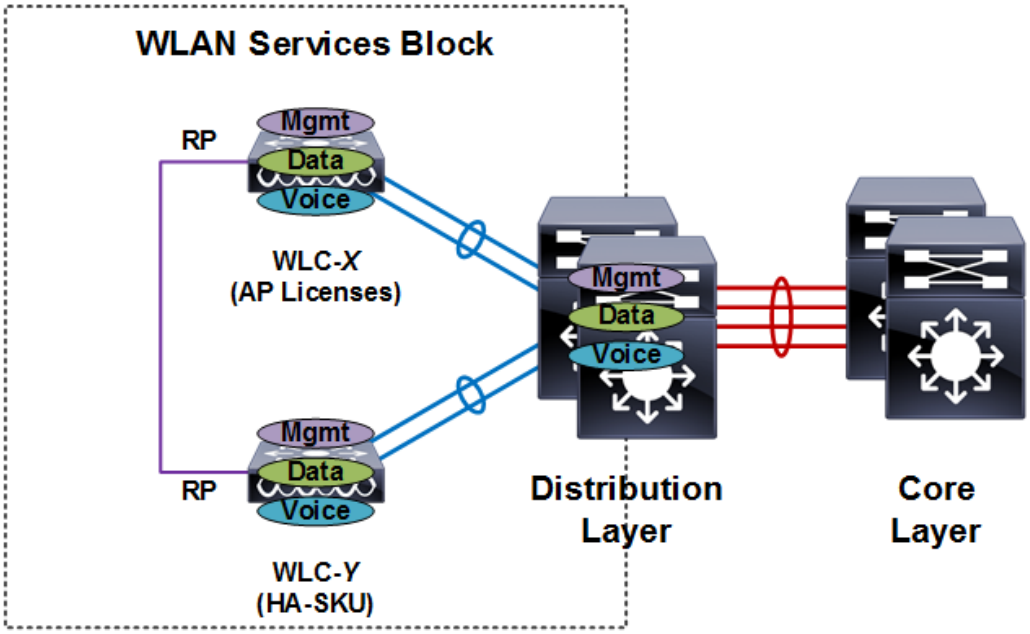
この考慮事項が重要であるのはなぜでしょう。現行世代の WLC は、最大 6,000 台の AP と 64,000 台のクライアントをサポートするように拡張できます。純然たる IPv4 環境では、この結果、サービス ブロック スイッチで処理および保守するエントリが 128,000 個に及ぶことがあります。大部分のワイヤレス クライアントはデュアルスタックもサポートしているため、処理と保守の対象となるエントリの数がさらに増えます。

ベスト プラクティスとして、25,000 台以上のワイヤレス クライアントをサポートしている大規模キャンパス導入では WLC を分散させることをお勧めします。WLC を分散させると、MAC、ARP、および ND の処理およびテーブル メンテナンスがディストリビューション レイヤ スイッチ間に展開されて、CPU の負荷が低下します。このアーキテクチャでは、ディストリビューション レイヤ障害の際に影響を受けたディストリビューション レイヤが学習し直す必要があるのはエントリのサブセットのみであるためコンバージェンスも高速です。サポートしているクライアントが 25,000 台未満のキャンパス導入の場合は、専用スイッチ ブロックを介して WLC がコアに接続されている中央集中型 WLC アーキテクチャを利用できます（「中規模キャンパス」を参照）。

図 2-43 は、大規模キャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、各ビルディング内のディストリビューション レイヤ スイッチに WLC の各ペアが接続されています。ディストリビューション レイヤ スイッチは、レイヤ 3 リンクを使用してコア レイヤに接続している、マルチレイヤまたは VSS として設定された Catalyst スイッチです。EIGRP または OSPF がルート集約に使用されます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してディストリビューション スイッチに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とディストリビューション スイッチの間でいずれも 802.1Q タギングされています。このディストリビューション スイッチは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

*図 2-43　大規模キャンパスとワイヤレス サービス ブロックの詳細*




大規模キャンパス導入では、各ディストリビューション レイヤ内の Cisco 5520 または 8540 WLC のペアを HA-SSO 用に設定することをお勧めします。ビルディングごとに選択する WLC モデルは、各ビルディングで必要な AP の数とスループットによって決まります。ディストリビューション レイヤ スイッチの物理的な場所に応じて、両方の WLC の冗長ポートを直接接続することも専用レイヤ 2 VLAN 越しに拡張することもできます。

各ビルディング内の AP はローカル HA-SSO ペアをプライマリ WLC として使用するように設定されています。異なるビルディングの HA-SSO ペアをセカンダリ WLC として設定して N+1 冗長性を使用することで追加の冗長性が実現されます。必要な WLAN、AP グループ、および RF グループはプライマリとセカンダリの両方の HA-SSO ペアに定義されています。

(注)　ディストリビューション レイヤ スイッチの構成要件は、マルチレイヤと VSS のいずれとして設定されているかに応じて異なります。実装ごとの要件の詳細については、この章のハイ アベイラビリティ (2-42 ページ)を参照してください。

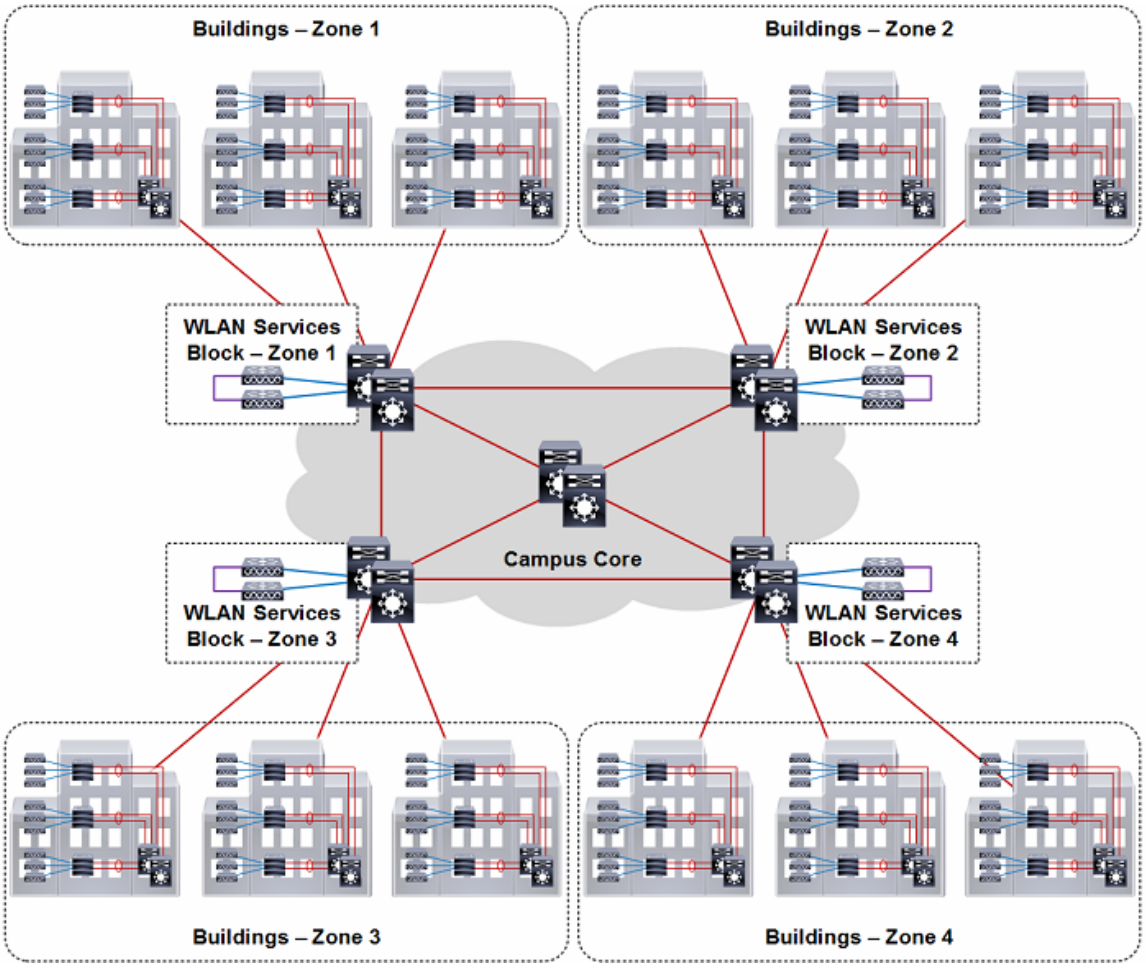
## きわめて大規模なキャンパス

図 2-44 に、分散されたコア レイヤに接続している数百棟のビルディングをサポートしているきわめて大規模なキャンパス ネットワーク用の CUWN 導入に推奨される WLC の配置を示します。分散された各コア スイッチはキャンパス コア内でディストリビューション レイヤとして機能しています。キャンパス内の大規模ビルディングは独自のディストリビューション レイヤおよびアクセス レイヤを実装する一方で、小規模ビルディングはアクセス レイヤのみを実装します。

このアーキテクチャの WLC は、コア レイヤ スイッチ間で配分されて、ここで WLC の各ペアがビルディングのグループの AP を管理します。各ワイヤレス サービス ブロックは最大 6,000 台の AP、25,000 台のクライアント、および 40 Gbps のスループットをサポートできます。各ワイヤレス サービス ブロック内の WLC には、ビルディングの各グループを処理している分散スイッチまたはコア レイヤ スイッチで終端されている異なるワイヤレス管理 VLAN およびユーザ VLAN が割り当てられています。必要なワイヤレス サービス ブロックの数は、サポートする必要のあるワイヤレス デバイスの数に基づいて決定されます。

図 2-44 のキャンパス ネットワークの例では、4 つの個別ワイヤレス サービス ブロックを実装しており、各ブロックは特定のゾーンに配置されているビルディングのグループをサポートしています。この CUWN 設計は最大 24,000 台の AP と 100,000 台のクライアントをサポートするように容易に拡大できます。

*図 2-44　　きわめて大規模なキャンパスのリファレンス設計*



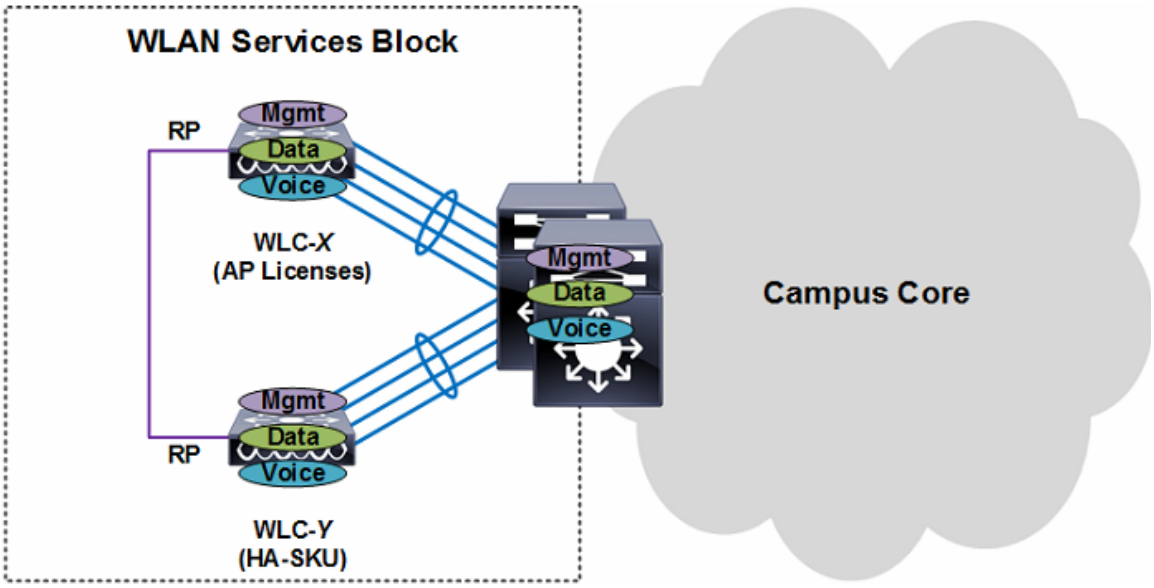
きわめて大規模なキャンパス用のモビリティ グループの設計も重要な考慮事項であり、ビルディングとゾーンの間に実現されているワイヤレス カバレッジによって異なります。理想に従って各ゾーンにビルディングが配置されており、ワイヤレス カバレッジ エリアを表しています。

- 各ゾーン内およびゾーン間に連続的なワイヤレス カバレッジが実現されている場合、定義するモビリティ グループは単一にすることができます。WLC の各ペアは同じモビリティ グループのメンバーとして設定されます。ワイヤレス クライアントは、元のネットワーク メンバーシップを維持しながらキャンパス全体でシームレスにローミングできます。
- 連続的なワイヤレス カバレッジが各ゾーン内でのみ実現されている場合は、個別のモビリティ グループを導入する必要があります。WLC の各ペアには個別のモビリティ グループを設定します。ワイヤレス クライアントはゾーン内でネットワーク メンバーシップを維持でき、別のゾーンにある AP に接続するときは新しいネットワークが割り当てられます。
- 連続的なワイヤレス カバレッジが一部のゾーン間で実現されている場合は、該当するゾーンを処理している WLC を同一のモビリティ グループに割り当てることができます。ワイヤレス クライアントは該当ゾーン内でネットワーク メンバーシップを維持でき、別のゾーンにある AP に接続するときは新しいネットワークが割り当てられます。

図 2-45 は、きわめて大規模なキャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、WLC の各ペアは、各ビルディング グループを処理するディストリビューションおよびコア レイヤ スイッチに接続されています。このディストリビューション スイッチまたはコア レイヤ スイッチは、レイヤ 3 リンクを使用して相互接続されている、マルチレイヤまたは VSS として設定されている Catalyst スイッチです。EIGRP、OSPF、または BGP がルート集約に使用されます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用して分散コア スイッチに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC と分散スイッチまたはコア スイッチの間でいずれも 802.1Q タギングされています。このディストリビューションまたはコア スイッチは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

*図 2-45　きわめて大規模なキャンパスとワイヤレス サービス ブロックの詳細*



きわめて大規模なキャンパス導入では、各ディストリビューション レイヤ内の Cisco 8540 WLC のペアを HA-SSO 用に設定することをお勧めします。ディストリビューション レイヤ スイッチの物理的な場所に応じて、両方の WLC の冗長ポートを直接接続することも専用レイヤ 2 VLAN 越しに拡張することもできます。

各ゾーン内の AP は指定された HA-SSO ペアをプライマリ WLC として使用するように設定されています。異なるゾーンの HA-SSO ペアをセカンダリ WLC として設定して N+1 冗長性を使用することで追加の冗長性が実現されます。必要な WLAN、AP グループ、および RF グループはプライマリとセカンダリの両方の HA-SSO ペアに定義されています。

(注)　ディストリビューション レイヤ スイッチの構成要件は、マルチレイヤと VSS のいずれとして設定されているかに応じて異なります。実装ごとの要件の詳細については、この章のハイ アベイラビリティ (2-42 ページ)を参照してください。

## ブランチ

Cisco Unified Wireless Network では、ワイドエリア ネットワーク (WAN) 越しに接続されているリモート ブランチ オフィスをサポートする 2 種類のアーキテクチャを提供しています。ブランチ サイトのネットワーク管理者は、ローカル モードまたは FlexConnect モードで動作する AP を実装できます。2 種類の CUWN アーキテクチャは動作が異なり、解決するビジネス ニーズも異なります。この項では、ローカル モード AP 導入に限って詳細を説明します。FlexConnect AP 導入の詳細および推奨事項については、第 7 章「FlexConnect」を参照してください。

ローカル モード AP を実装するブランチ サイトは、WLC がブランチ内に直接配置される小規模キャンパス アーキテクチャに従います。すべての CAPWAP トンネルはブランチ内にあります。ローカル モード AP を配置した複数のブランチ サイトが導入されている場合は、WAN によって接続された 1 か所以上のブランチに WLC が導入されているため、分散アーキテクチャであると見なされます。

図 2-46 は、コラスプト コアとして動作するディストリビューション レイヤを実装する小規模ブランチ ネットワークの CUWN 展開で推奨される WLC 配置を示しています。ディストリビューション レイヤは、WLC、WAN、およびインターネット エッジへの接続を提供します。WLC はブランチの規模に応じてディストリビューション レイヤに直接接続することも (図を参照)、専用スイッチ ブロックを介して接続することもできます。この例のブランチ ネットワークは、ディストリビューション レイヤ 1 つ、アクセス レイヤ スイッチ 2 台の単一のビルディングです。

*図 2-46　　小規模ブランチのリファレンス設計*

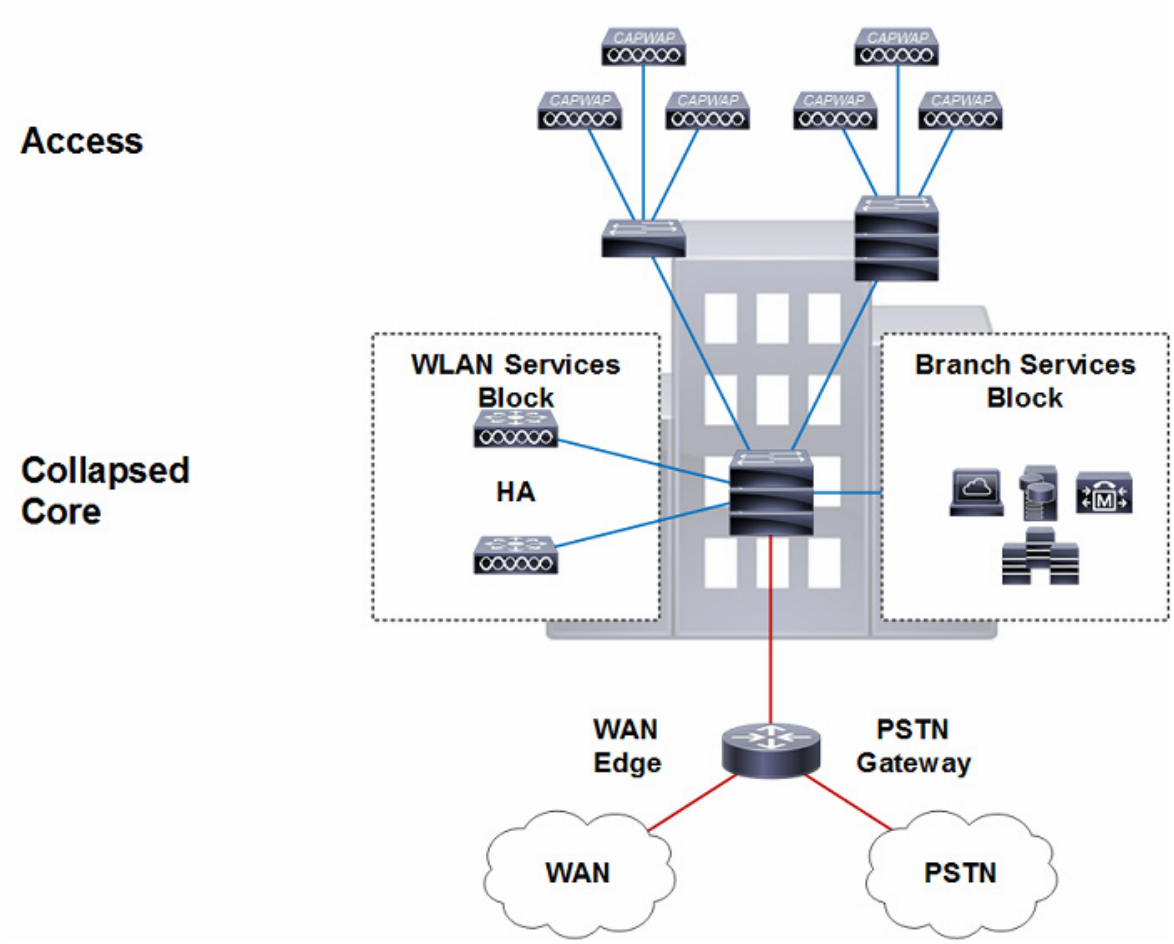
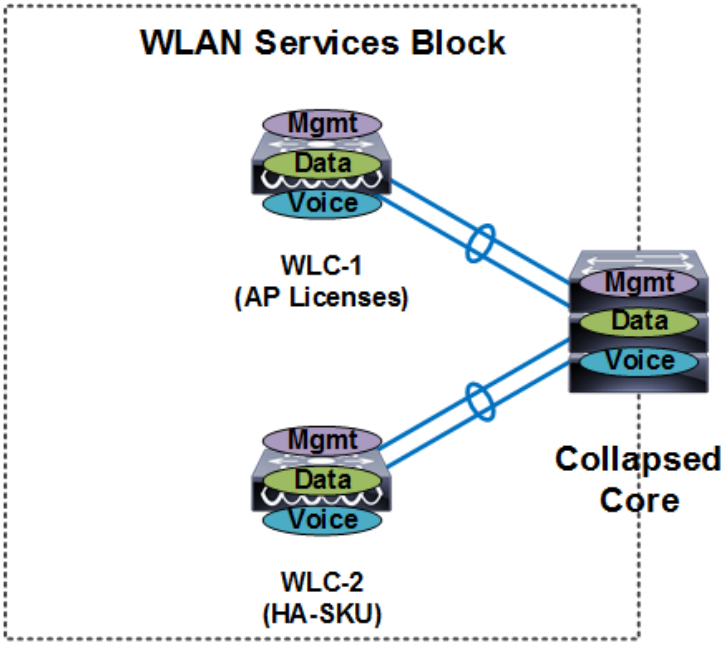



図 2-47 は、ブランチ ネットワーク導入用のワイヤレス サービス ブロックの詳細を示します。この例では、802.1Q VLAN タギング用に設定されているスタティック ポートチャネルを使用して WLC のペアがディストリビューション レイヤに直接接続されています。ワイヤレス管理、データ、および音声の VLAN は、WLC とディストリビューション レイヤの間でいずれも 802.1Q タギングされています。このディストリビューション レイヤは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

*図 2-47　　小規模ブランチとワイヤレス サービス ブロックの詳細*




ブランチ オフィスでの導入では、Cisco 2504 WLC のペアを N+1 HA 用に設定することをお勧めします。Cisco 2504 WLC は、ブランチ オフィスでの導入専用に設計されており、最大 75 台の AP をサポートするように拡張できます。両方の WLC に同じモビリティ グループが設定および割り当てられており、同じインターフェイスまたはインターフェイス グループ、WLAN、AP グループ、および RF グループをサポートするように設定されています。AP は、永続ライセンスを持つ WLC をプライマリ WLC、HA-SKU WLC をセカンダリ WLC として使用するように設定されています。

(注)　シスコでは、ワイドエリア ネットワーク越しに中央集中型 WLC を使用するローカル モード AP の導入をサポートしていません。WAN 越しにリモート AP をサポートする必要がある場合は、FlexConnect アーキテクチャを実装することをお勧めします。

# トラフィック負荷と有線ネットワークのパフォーマンス

Cisco Unified Wireless Network ソリューションを導入する場合に、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。
- ユニファイド ワイヤレス導入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 導入と中央集中型の WLC 導入の相対的なメリット。

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 の再起動中は多くなります。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 Kbps 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、中央集中型導入モデルと分散型導入モデル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。一般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、中央集中型導入モデルと分散型導入モデル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最終宛先まで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 導入の場合、クライアント トラフィックはエッジからネットワークに入り、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、中央集中型の導入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る量であり、中央集中型導入モデルと分散型導入モデル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 トラフィックのボリュームに深刻な影響が出ることはありません。

# AP 接続

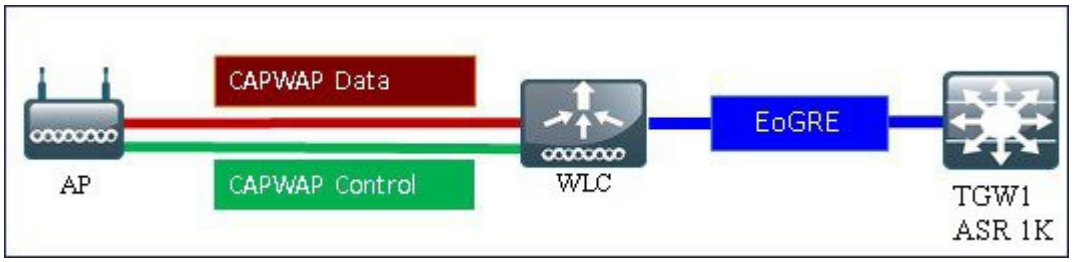
AP は、エンド ユーザ（802.11 クライアント）とは別のサブネット上になければなりません。これは、インフラストラクチャ管理インターフェイスはエンド ユーザとは別のサブネット上にあるべきであると定義している一般的なベスト プラクティスのガイドラインと一致しています。さらに、Catalyst Integrated Security Features（CISF）を CAPWAP AP スイッチ ポートで有効にして、WLAN インフラストラクチャの保護を強化することを推奨します（FlexConnect AP 接続については、第 7 章「FlexConnect」を参照）。

導入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式としては、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 内で 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。

# WLC EoGRE トンネリング

Ethernet over GRE（EoGRE）は、ホット スポットからの Wi-Fi トラフィックを集約するための新しい集約ソリューションです。このソリューションでは、顧客宅内機器（CPE）デバイスで、エンド ホストから届いたイーサネット トラフィックをブリッジし、そのトラフィックを IP GRE トンネルでイーサネット パケットにカプセル化できます。IP GRE トンネルがサービス プロバイダーのブロードバンド ネットワーク ゲートウェイで終端すると、エンド ホストのトラフィックが終了し、エンド ホストに対するサブスクライバ セッションが開始されます。




### トンネリングの一般的なメリット

- クライアントは、さまざまなテクノロジーやベンダーが混在するアクセス ネットワーク上で IP アドレスとポリシーを維持できます。
- WLC に接続する L2 スイッチでの MAC アドレスのスケーリング制限を回避できます。
- 合法的傍受（LI）。

### EoGRE トンネリングが携帯電話事業者にもたらすメリット：

- 3G および 4G トラフィックをオフロードして OpEx の削減とネットワーク効率の向上を実現することによってネットワークの輻輳を軽減します。
- 弱いセル信号がなくても 3G および 4G コアへのアクセスを提供し、サブスクライバの維持に寄与します。
- 高密度のメトロ環境においてユーザ ベースまたは帯域幅ベースの CapEx を削減します。

**EoGRE トンネリングが有線および Wi-Fi 事業者にもたらすメリット:**

- WiFi セキュリティとサブスクライバ制御を提供します。
- スケーラブルで管理しやすく安全なワイヤレス接続を提供します。
- 新しい収益分配ビジネス モデルを実現します。
- 新しいロケーションベースのサービスを提供する WiFi プラットフォームを提供します。

**EoGRE トンネリングがサブスクライバにもたらすメリット:**

- WiFi ネットワーク上のサブスクライバに高品質のエクスペリエンスを提供します。
- アクセス ネットワーク全体にわたって統一された方法で課金します。
- 3G または 4G から WiFi、WiFi から WiFi などの無線アクセス テクノロジーをまたがるモビリティを提供します。
- Wi-Fi プラットフォーム内で複数のオプションを提供し、ロケーションベースのサービスを実現します。
- リリース 8.2 以降では、EoGRE トンネリングはダイナミック インターフェイスでサポートされます。
- ダイナミックな IPv6 AP 管理インターフェイスはサポートされていません。
- リリース 8.3 では、IPv6 ダイナミック インターフェイスはトンネル インターフェイスとしてのみサポートされます。
- リリース 8.3 では、IPv6 アドレスを割り当てることができるダイナミック インターフェイスの最大数は 16 です。
- リリース 8.3 の TGW では、IPv4 と IPv6 の両方のアドレス形式がサポートされます。最大で 10 個のトンネル ゲートウェイを作成できます。
- リリース 8.4 では、WLC およびフレックス接続 AP から TGW への EoGRE IPv4 および IPv 6 トンネルがサポートされます。
- リリース 8.5 では、プライマリおよびセカンダリ TGW のフェールオーバーと冗長性のサポートが追加されました。
- リリース 8.5 では、EoGRE トンネルを管理するための SNMP MIB が追加されています。

# サポートされるコントローラと AP

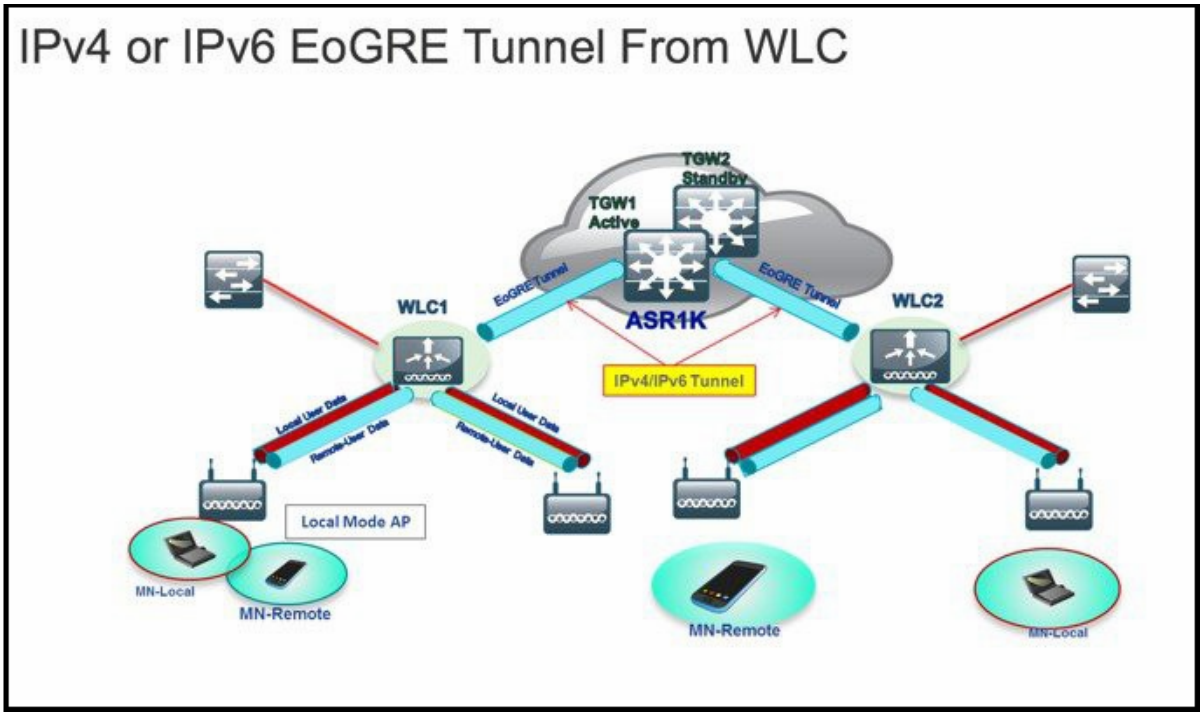
- Cisco 3504、5508、5520 シリーズ、WiSM-2、および 8500 シリーズ ワイヤレス LAN コントローラ。
- リリース 8.2 以降では、2500 シリーズおよび vWLC で EoGRE がサポートされます。
- 7500 コントローラでは、TGW への EoGRE 直接トンネルが設定されたフレックス接続 AP のみサポートされます。
- Cisco WLC 8.4 のサポート対象アクセス ポイント:3800、2800、1800、3700、2700、1700、1600、3600、2600、2700、702i、3500、702w、1540、1560、1552、1532、1572。

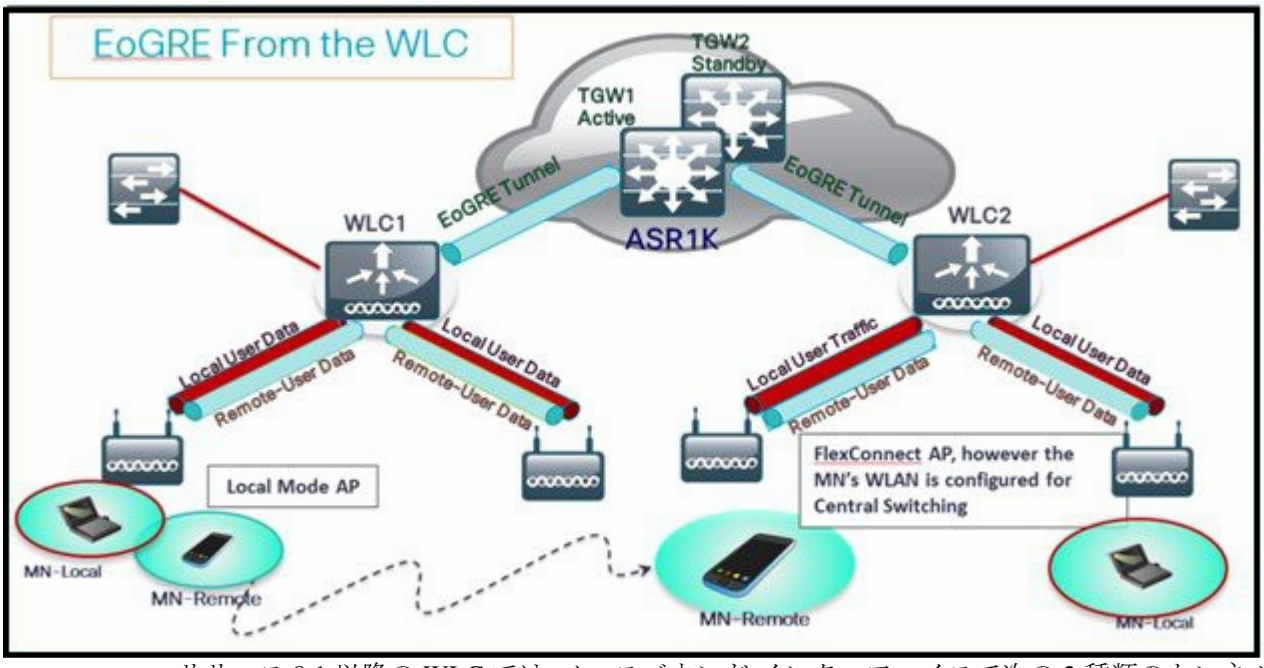
# EoGRE トンネル システムの設計オプション

## 設計 1：WLC ベースの EoGRE トンネル

- CAPWAP 制御パス（AP WLC）
- CAPWAP データ パス（AP WLC）
- EoGRE データ フロー（WLC-TGW）

この設計モデルでは、WLC から ASR 1000 などトンネル ゲートウェイへのトンネルが生成されます。リリース 8.2 以降のコントローラでは、最大で 10 個のトンネル ゲートウェイ構成、10 個の EoGRE トンネル ゲートウェイ、そしてトンネルごとに 10 個のプロファイルがサポートされます。各プロファイルは、複数のレルムを使用して設定することもできます。レルムが設定されている場合は、@ の後のユーザ名になります。レルムは @ の後の文字列です（例：user_name@realm）。冗長性を確保するために複数のトンネルを設定できます。その場合、プライマリまたはアクティブ トンネルで障害が発生すると、セカンダリまたはスタンバイ トンネルが EoGRE トンネルのオペレーションを引き継ぎます。EoGRE トンネル設定では、コントローラ内およびコントローラ間のモビリティもサポートされます。






リリース 8.1 以降の WLC では、ノースバウンド インターフェイスで次の 2 種類のトンネル設定がサポートされます。

1. PMIPv6（RFC 5213）で定義されている IP/GRE – L3
2. Ethernet over GRE – L2

(注)　このガイドでは、EoGRE トンネルについてのみ説明します。

WLAN ごとに 1 種類のトンネルのみサポートされます。EoGRE は、オープン WLAN または 802.1x ベースの WLAN でサポートされます。トンネル クライアントでは、EAP-SIM または EAP-AKA モードのみがサポートされます。その他の認証モードは、トンネル クライアントでサポートされません。

オープン SSID の WLAN を使用する場合は、すべてローカル/シンプル クライアントまたはすべてトンネル クライアントがサポートされますが、同じ WLAN 上に混在させることはできません。ただし、802.1x で認証されたシンプルまたはトンネル EoGRE クライアントは同じ WLAN 上でサポートされます。

8.3 より前のリリースでは、オープンおよび WPA2-802.1X 用に設定された WLAN のみがサポートされました。

現在は、内部 WebAuth および WPA2-PSK 用に設定された WLAN に EoGRE トンネル プロファイルを割り当てることができるようになりました、WPA2-PSK/WPA2-802.1X および内部 WebAuth が設定された WLAN もサポートされます。

クライアントは、認証に基づいてローカル モードまたはトンネル モードに分けられます。WLC では、同じ WLAN 上で**リモート トンネル**や**ローカル**などの 2 種類のユーザ トラフィックがサポートされます。

ローカル ユーザ トラフィックは、WLC によってローカルにブリッジされるトラフィックとして定義されます。

リモート トンネル ユーザ トラフィックは、リモートトンネル ユーザのトラフィックとして定義され、WLC によって TGW にトンネリングされます。

EoGRE ユーザの AAA のオーバーライドがサポートされています。トンネル ゲートウェイは AAA プロキシとして機能することもできます。

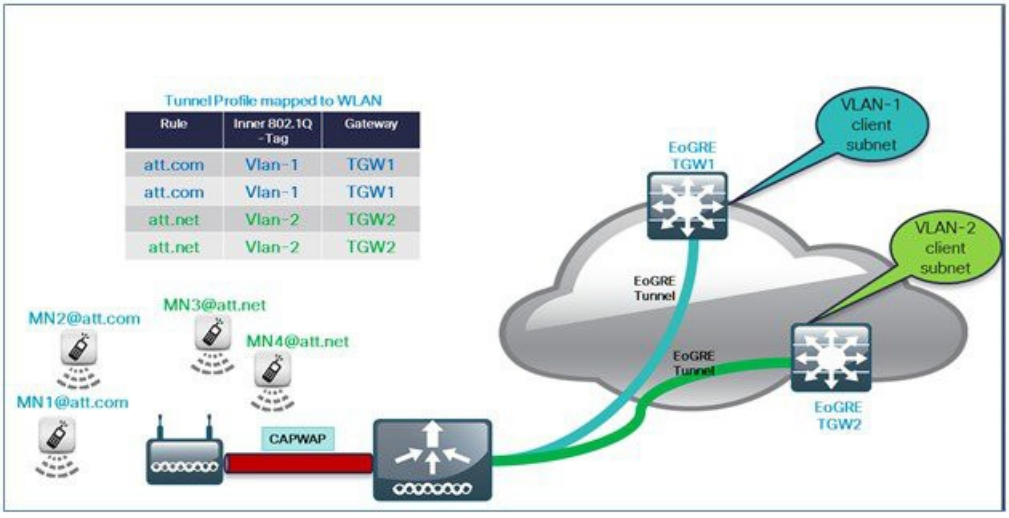
**コントローラで EoGRE EAP 認証済みクライアントの AAA オーバーライドが有効担っている場合：**

- WLC は、Access Accept を解析し、EoGRE、GTPv2、PMIPv6 などの MPC プロトコル タイプを探します。
- Protocol-Type AVP が存在する場合、WLC はそのトンネル タイプに関連するすべてのパラメータを探します。スタティック プロファイルは無視され、AAA によって提供されるパラメータがトンネルの設定に使用されます。
- AVP が存在しない場合、WLC は WLC のスタティック プロファイルを使用し、ユーザ名から抽出したレルムに基づいてトンネル タイプを判断します。
- 一部のパラメータが存在しない場合、認証は失敗します。たとえば、T-GW IP 以外のパラメータがすべて存在する場合でも、クライアント認証は失敗します。
- MPC-Protocol-Type が None の場合、MPC プロトコル タイプはシンプル IP になります。

AAA サーバから返される可能性がある属性には、User-Name、Calling-Station-Id、gw-domain-name、mn-service、cisco-mpc-protocol-interface、eogre_vlan_id などがあります。

# 一般的な展開：WLC EoGRE トポロジ

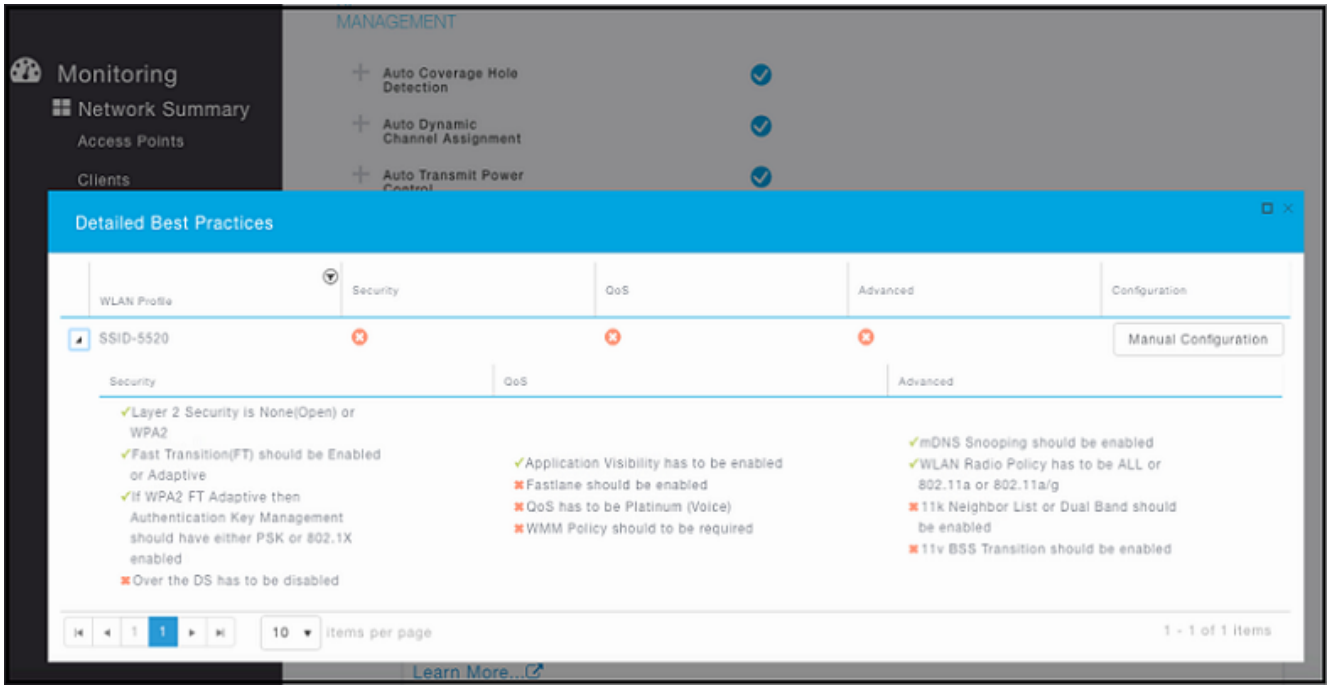
この一般的な EoGRE の展開設定では、2 人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の 2 人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続するときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN2 および TGW2 に接続する必要があります。この設定では、それぞれ 1 つのレルムを含む 2 つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。



# 設計 2：FlexConnect AP ベースの EoGRE トンネル

- CAPWAP 制御パス（フレックス AP と WLC 間）
- EoGRE データ パス（フレックス AP と TGW 間）
- トンネルが確立されると、データは FC AP から直接 TGW に流れます。

この設計では、AP からの直接トンネルにより、データ プレーンとコントロール プレーンがコントローラと AP から分離されます。ネットワークのコアへのデータ パス ルーティングが最適化されるため、中央のデータ スループットはコア ネットワークの容量によってのみ制限されます。コントローラ内またはコントローラ間のモビリティはサポートされませんが、クライアントはローカル スイッチング モードの同じ FlexConnect グループに引き続きローミングできます。

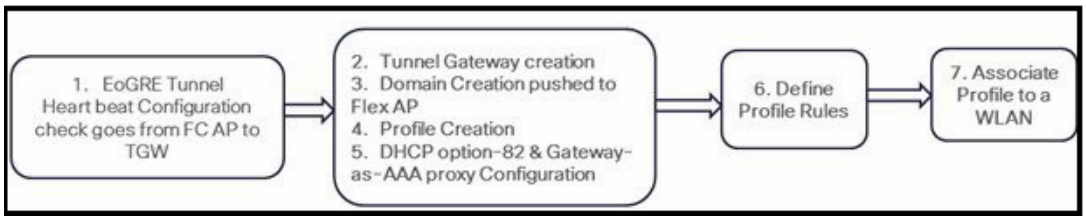



- FlexConnect AP：EoGRE は、オープン WLAN および 802.1x ベースの WLAN でサポートされます。
- 802.1x で認証された「シンプル」または「トンネル」EoGRE クライアントは同じ WLAN 上でサポートされます。
- クライアントは、認証に基づいてローカル モードまたはトンネル モードに分けられます。
- トンネル クライアントでは、EAP-SIM または EAP-AKA モードがサポートされます。
- オープン SSID WLAN では、すべてローカル クライアントまたはすべてトンネル クライアントのいずれかがサポートされます。
- EoGRE ユーザの AAA のオーバーライドがサポートされています。
- トンネル GW は AAA プロキシとして機能することもできます。
- FlexConnect AP では、TGW 障害検出と代替 TGW へのスイッチオーバーがサポートされます。

- TGW では、アクティブ/スタンバイ モードによるフォールト トレランスがサポートされます。
- コントローラ内およびコントローラ間のモビリティは、FlexConnect AP モードでサポートされます。
- スタンドアロン モードでは、モビリティは FlexConnect グループ内でのみサポートされ、トンネル GW は AAA およびアカウンティング プロキシとして設定できます。
- トンネル GW では、「設定可能」DHCP オプション 82 がサポートされます。
- リリース 8.4 以降では、FlexConnect で IPv6 アドレスがサポートされます。

# 基本的な Flex AP EoGRE 設定

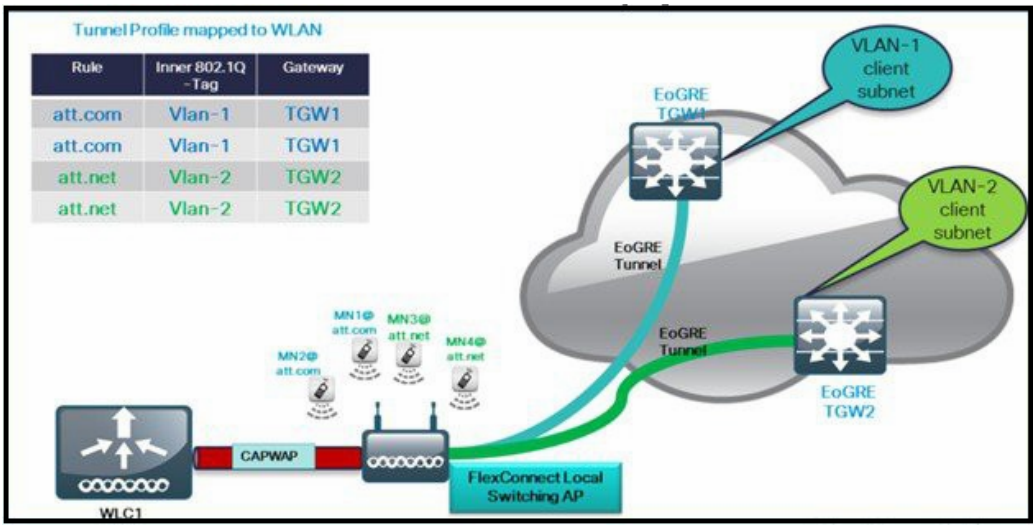
- Flex AP に EoGRE トンネルを設定する場合：
- WLAN にプロファイルを適用すると、WLC または FC AP トンネルに同じトンネル設定が適用されます。
- FC AP がローカル スイッチ モードになっている場合、FC AP ゲートウェイ トンネルが自動的に適用されます。
- ローカル モードの AP に接続しているクライアントは、WLC-TGW トンネルを介して通信します。
- FC AP に接続しているクライアントは、FC AP-TGW トンネルを介して通信します。
- クライアントの選択も、AAA またはプロファイル オーバーライドの影響を受けます。




（注）　冗長トンネル設定モードでは、EoGRE トンネル モードに設定されているすべての FC AP からキープアライブ ping が送信されます。

# 一般的な展開：FlexConnect AP - EoGRE トポロジ

この一般的な FC AP - EoGRE トンネル展開設定では、2 人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の 2 人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続するときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN-2 および TGW2 に接続する必要があります。この設定では、それぞれ 1 つのレルムを含む 2 つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。この展開シナリオでは、トンネルはローカル スイッチング モードの FlexConnect AP と TGW1 および TGW2 間に直接設定され、データ トラフィックはすべてコントローラをバイパスして流れます。




その他の設計と設定の詳細については、次のリンクにある EoGRE 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

# 運用およびメンテナンス

ここでは、Cisco Unified Wireless Network 導入の運用およびメンテナンスを簡単にするための導入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 の初期導入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導入

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 の定義が、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 の設定に加えて行われます。

# AP 分散

通常の初期 WLAN 導入では、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導入は簡単になりますが、いくつかの運用上の理由から、自動分散方式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、およびメンテナンスが簡単になり、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。

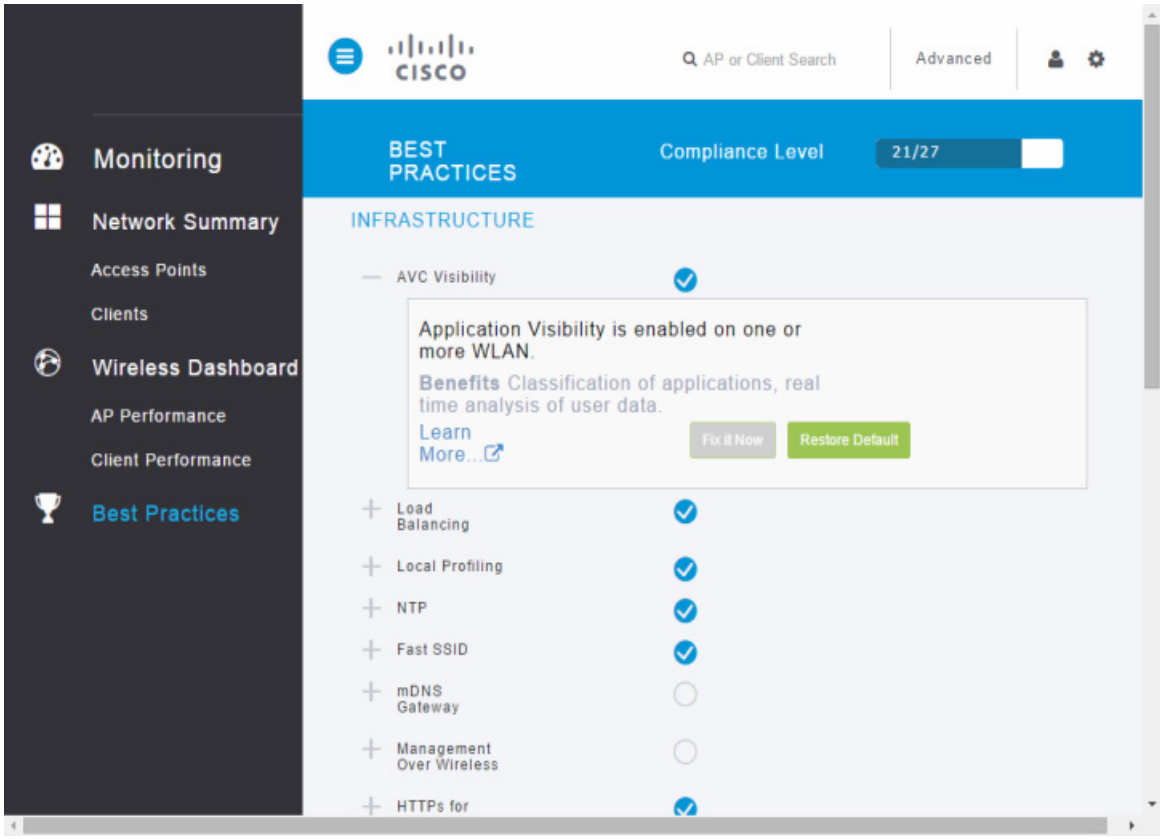
複数の WLC にわたる AP 分散を制御するために使用される要素は、次のとおりです。

- 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。

# ベスト プラクティス

CUWN ソフトウェア リリース 8.1 以降では、ネットワーク導入エンジニア向けに、WLAN コントローラ用ダッシュボードにベスト プラクティス チェックリストが提供されています（図 2-48）。このチェックリストは、シスコの推奨するベスト プラクティスに合わせて WLC 設定を微調整するために使用します。このチェックリストでは、WLC 上のローカル設定と推奨されるベスト プラクティスを比較して、異なっているすべての機能を強調表示しています。このチェックでは、ベスト プラクティスを適用するための簡単な設定パネルも提供しています。ベスト プラクティスの採用は、すべての CUWN 導入において強く推奨されます。

*図 2-48　　ベスト プラクティス ダッシュボード*




このダッシュボードでは推奨される各機能を順守していることをチェックし、それぞれの準拠に関するフィードバックを提供します。ベスト プラクティス得点は、有効化されている推奨機能の数に従って表示されます。各推奨機能はインフラストラクチャ、セキュリティ、RF 管理のいずれかに分類されており、大部分はダッシュボードからクリック 1 回で直接有効化できます。特定の機能の詳細およびメリットもダッシュボードに示されています。

*表 2-7　　リリース 8.1 のベスト プラクティス*

| インフラストラクチャ | セキュリティ | RF 管理 |
|---|---|---|
| • Application Visibility and Control（アプリケーションの可視性およびコントロール）<br>• ロード バランシング<br>• ローカル プロファイリング<br>• NTP<br>• 高速 SSID<br>• mDNS スヌーピング<br>• ワイヤレスによる管理<br>• 安全な Web アクセス<br>• Aironet IE<br>• マルチキャスト転送<br>• コントローラの高可用性 | • WLAN の 802.1X<br>• 不正ポリシー<br>• 不正しきい値<br>• SSH/Telnet アクセス<br>• Client Exclusion<br>• レガシー IDS<br>• ローカル管理パスワード ポリシー<br>• CPU ACL | • SSID 制限<br>• クライアント BandSelect<br>• 40 MHz チャネル幅<br>• 自動動的チャネル割り当て<br>• 自動送信電力制御<br>• 自動カバレッジ ホール検出<br>• CleanAir<br>• イベント駆動型無線リソース管理 |

（注）　現時点でのベスト プラクティスを網羅したリストが次の URL のダッシュボードにあります: http://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc.html

# Apple デバイスと ISE RADIUS のベスト プラクティス

リリース 8.5 では、シスコ ネットワークにおける Apple デバイスのパフォーマンス強化を目的に Apple デバイス関連のベスト プラクティスが多数追加されます。また、ISE を Radius サーバとして使用する場合に推奨される ISE のベスト プラクティスも追加されています。

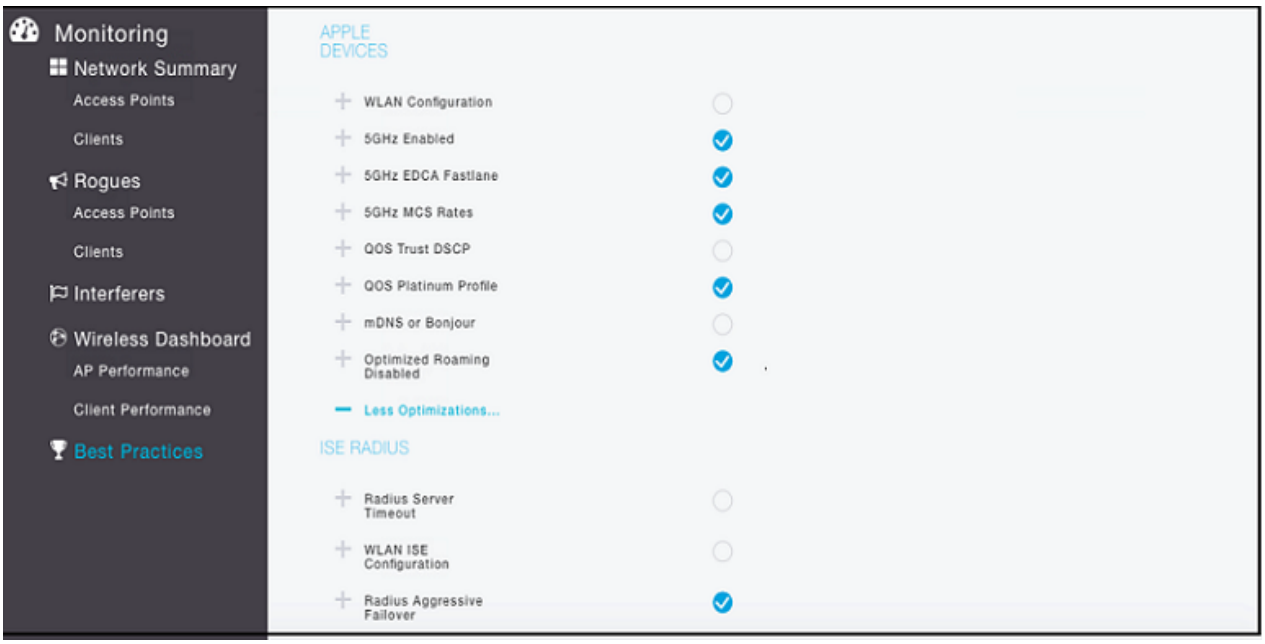
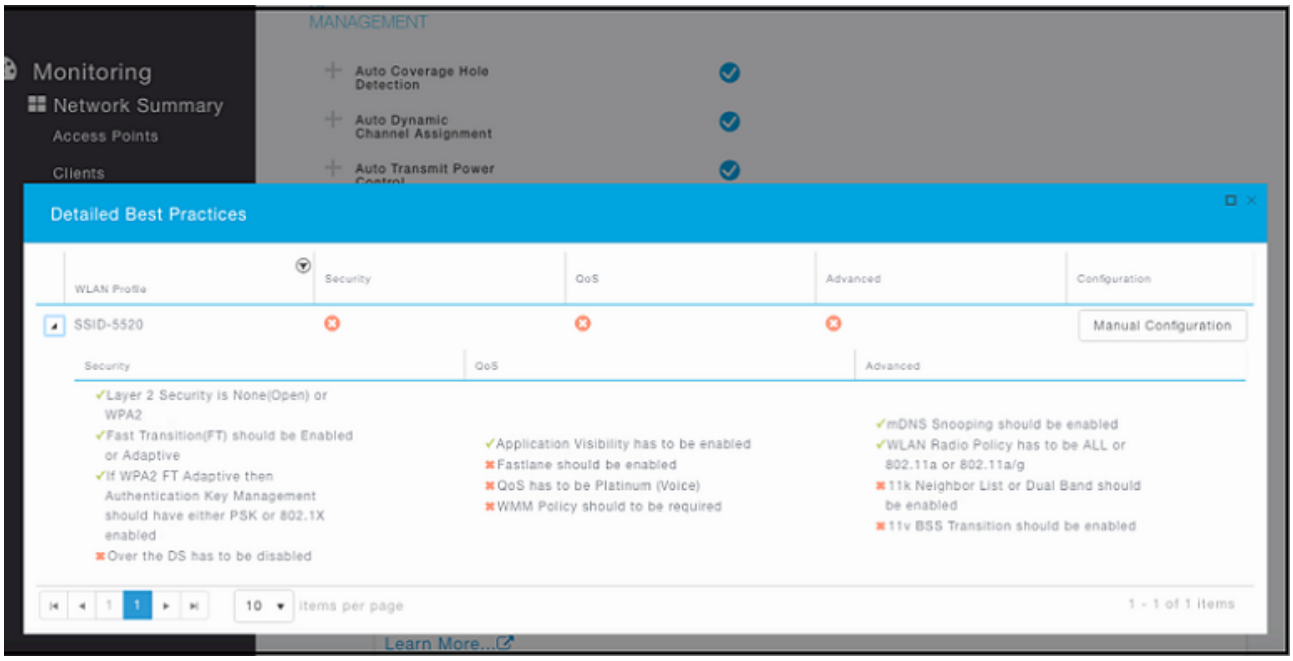
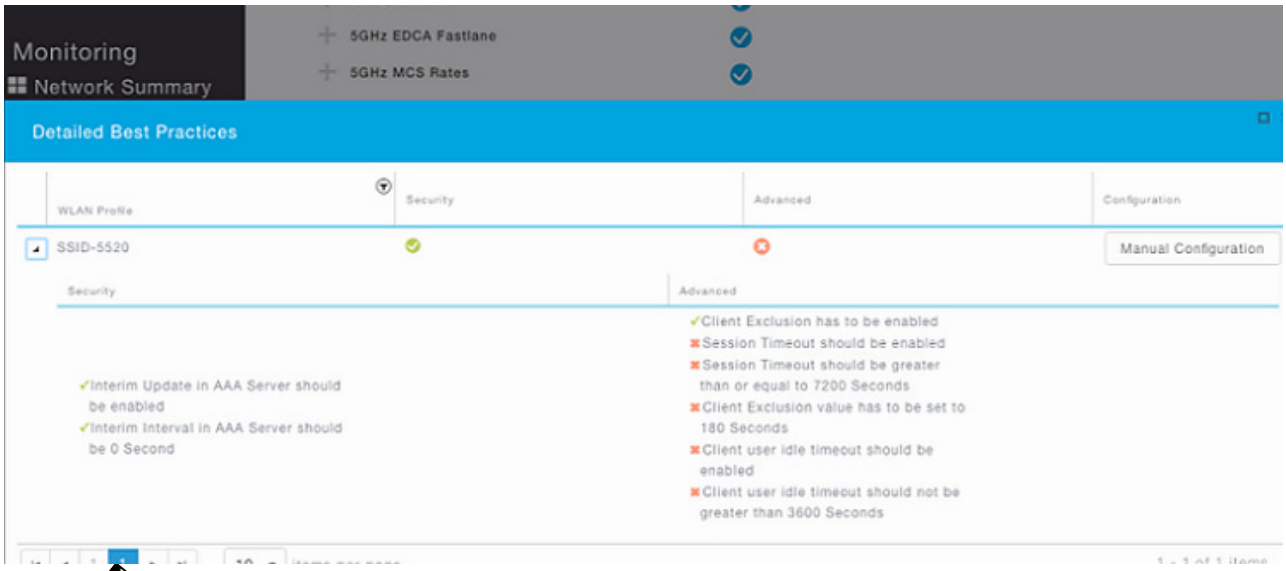



*表 2-8　リリース 8.5 のベスト プラクティス*

| Apple デバイス | ISE RADIUS |
|---|---|
| ISE RADIUS | RADIUS サーバのタイムアウト |
| 5GHz の有効化 | WLAN ISE 設定 |
| 5 GHz EDCA Fastlane | RADIUS アグレッシブ フェールオーバーの無効化 |
| 5 GHz MCS レート | |
| QoS Trust DSCP | |
| QOS Platinum プロファイル | |
| mDNS または Bonjour の有効化 | |
| 最適化されたローミングの無効化 | |

これらのセクションの WLAN 設定のベスト プラクティスを展開すると、WLAN ごとに有効化および無効化できるベスト プラクティスの詳細なリストが表示され、ベスト プラクティス機能のギャップが一目でわかります。




**（注）** ダッシュボードで提供される最新のベスト プラクティスの一覧については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc.html を参照してください。