CHAPTER 12

ワイヤレス プラグ アンド プレイ

シスコ ネットワーク プラグ アンド プレイ ソリューションは、エンタープライズ ネットワークを利用するお客様にシンプルかつセキュアで統合されたソリューションを提供し、新しいブランチまたはキャンパス デバイスのロールアウトや既存のネットワークに対する更新のプロビジョニングを簡単に行うことができるようにします。このソリューションでは、クラウド リダイレクション サービス、オンプレミス、またはその組み合わせを使用して、シスコ ルータ、スイッチ、およびワイヤレス デバイスで構成されるエンタープライズ ネットワークのプロビジョニングをほぼゼロ タッチの導入エクスペリエンスとして、統合されたアプローチを提供します。

この導入ガイドでは、ワイヤレス アクセス ポイントのためのシスコのネットワークのプラグ アンド プレイ アプリケーションについて説明します。このアプリケーションでは、リモート サイトを事前プロビジョニングできます。大規模なサイトをプロビジョニングする場合、シスコのネットワーク プラグ アンド プレイ アプリケーションを使用してサイトを事前プロビジョニングしたり、サイトにアクセス ポイントを追加できます。その場合は、アクセス ポイント情報を入力し、必要に応じてブートストラップ設定をセットアップします。ブートストラップ設定によって、プラグ アンド プレイ エージェントが、WLC info、hostname、AP group、FlexGroup、AP mode などのアクセス ポイントを設定できるようになります。

事前プロビジョニングが不要な小規模サイトを作成する場合、アクセス ポイントは、シスコのネットワーク プラグ アンド プレイ アプリケーションで事前設定せずに、そのまま展開し、正当化できます。インストーラがアクセス ポイントをインストールして電源を入れると、DHCP、DNS またはクラウド リダイレクション サービスを使用して Cisco APIC-EM コントローラを自動検出します。自動検出プロセスが完了すると、AP はローカル PnP サーバの設定に従って WLC に接続するか、クラウド リダイレクション サービスと通信し、WLC と PnP サーバのどちらをターゲットとするかを確認します。

ワイヤレス PnP のサポート:

表 12-1

プラットフォーム	モデル
Cisco Aironet ワイヤレス アクセス ポイント	802.11n Generation 2 702I、702W、1600、2600、3600 802.11ac Wave 1、17/27/3700、18/28/3800 802.11ac Wave 2

APIC EM 1.5 の要件(以下の拡張制限の表も参照):

- **サーバ**:64 ビット x86(Ubuntu 14.04 LTS)
- **vCPU**:6(2.4 GHz)以上
- **RAM**:64 GB(単一ホストの導入)/32 GB(複数ホストの導入)

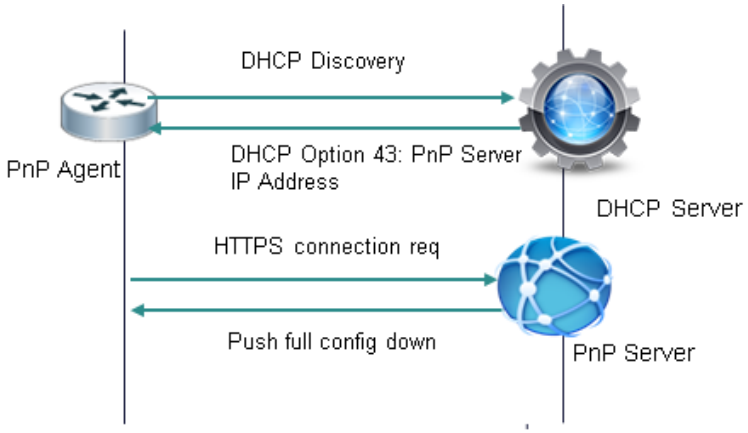
- **ネットワーク アダプタ**:1
- **ストレージ**:ハードウェア RAID 構成後に使用可能なストレージ 500 GB HDD
- **ディスク I/O**:200 MBps
- **ブラウザ**:Google Chrome または Firefox
- **ハイパーバイザ**:VMware vSphere 5.x/6.x（仮想アプライアンス）
- **アクセス ポイント**:最大 10,000

APIC EM アクセス ポイントの拡張制限:

仮想アプライアンス	コア	RAM	ハードディスク	CPU クロック速度	RAID（ハードウェア）
仮想マシン（32 GB）にインストールされた Cisco APIC-EM	12	32 GB	200 GB の内部データ ストア ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（64 GB）にインストールされた Cisco APIC-EM	8	64 GB	500 GB ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（64 GB）にインストールされた Cisco APIC-EM	12	64 GB	1 TB ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（128 GB）にインストールされた Cisco APIC-EM	20	128 GB	2 TB ディスク速度 15,000 RPM	2.9 GHz	RAID 10

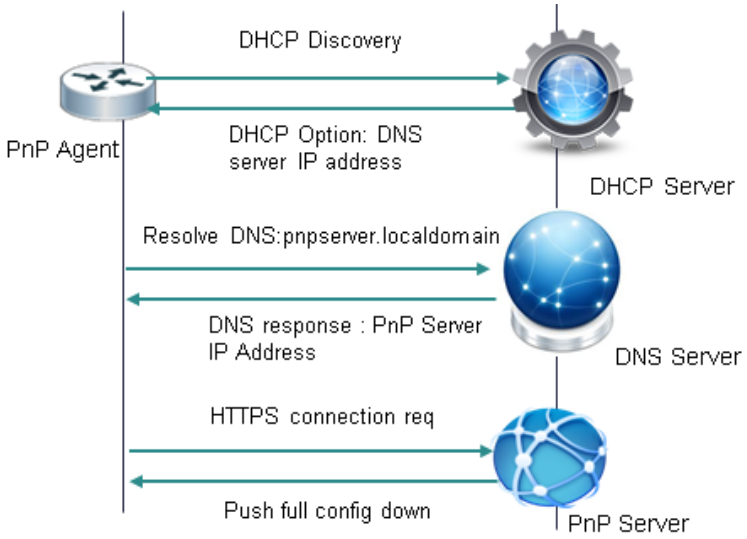
DHCP 要求/応答（Option43）:

アクセス ポイントの PnP エージェントが設定なしで起動し、DHCP を通じて IP アドレスを割り当てます。デバイスが DHCP 検出メッセージを送信します。DHCP サーバは、DHCP オプション 43 の一部として PnP サーバの IP アドレスを提供できます。DHCP 応答の一部として、PnP エージェントが APIC PnP サーバの IP アドレスである DHCP オプション 43 を受信すると、AP の PnP エージェントが PnP サーバに対する HTTPS 要求を開始します。セキュリティ クレデンシャルが検証されると、完全な設定が AP にプッシュされます。

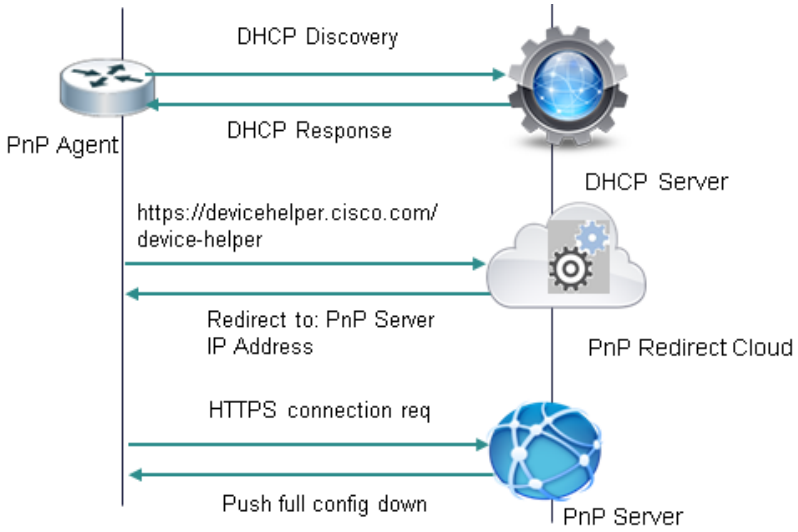


DNS レスポンス：

AP の PnP エージェントが設定なしで起動します。PnP エージェントが DHCP を通じて IP アドレスの割り当てを試みます。AP が DHCP 検出メッセージを送信します。DNS サーバの IP アドレスが DHCP 応答の一部として入力された場合は、AP の PnP エージェントが「pnpserver.localdomain」という名前に対して DNS クエリを送信します。DNS サーバは、これを APIC EM PnP サーバの IP アドレスに解決できます。AP の PnP エージェントが PnP サーバに対する HTTPS 要求を開始します。セキュリティ クレデンシャルが検証されると、完全な設定が AP にプッシュされます。



上記の例はどちらも、DHCP 応答または DNS 解決が管理されている、エンタープライズ マネージド ネットワークとサービス プロバイダー マネージド ネットワークの両方に適しています。AP が管理対象外のネットワークに接続する場合、あるいは DHCP サービスまたは DNS サービスが信頼できない場合には、PnP サーバの詳細にデバイスの所有者を関連付ける、別個のエンティティが必要になります。パブリック インターネットの Cisco PnP リダイレクト クラウド インスタンスにはこの機能があります。

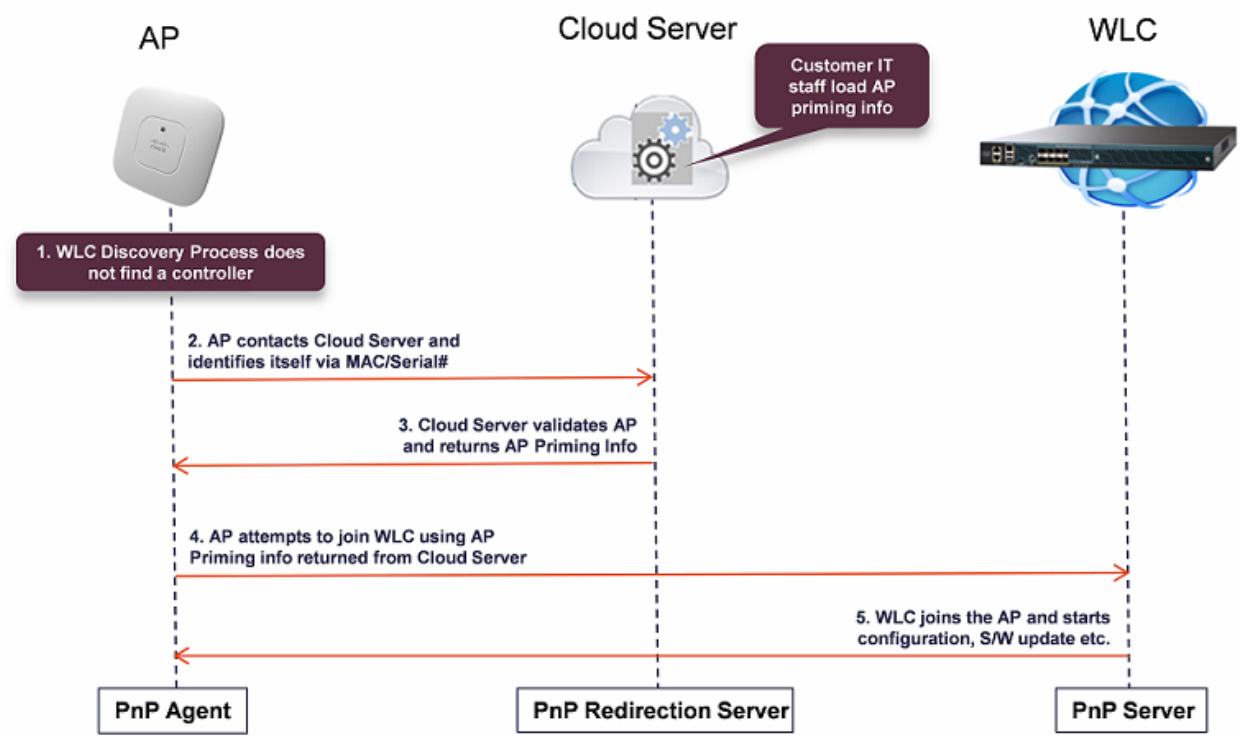


Cisco クラウド PnP リダイレクト サービス:

アクセス ポイント上の PnP エージェントは、最初に DHCP 検出を実行します。DHCP オプション 43 がなく、DNS サーバが pnpserver.localdomain を解決できない場合、AP は devicehelper.cisco.com に対する DNS ルックアップを実行します。このドメイン名は PnP リダイレクト クラウド サーバ（または PnPRC）に解決され、AP クレデンシャルが検証されます。クレデンシャルが検証されたら、顧客から提供されていた PnP サーバの IP アドレスに関連付ける必要があります。PnP サーバの IP アドレスは顧客ごとに異なり、一般的にエンタープライズまたはサービス プロバイダーでオンプレミスでホストされます。PnPRC は HTTPS GET 要求を PnP サーバの IP アドレスにリダイレクトします。このリダイレクト メカニズムは、AP が自動的にインターネット接続されるその他の使用例にも適用されます。

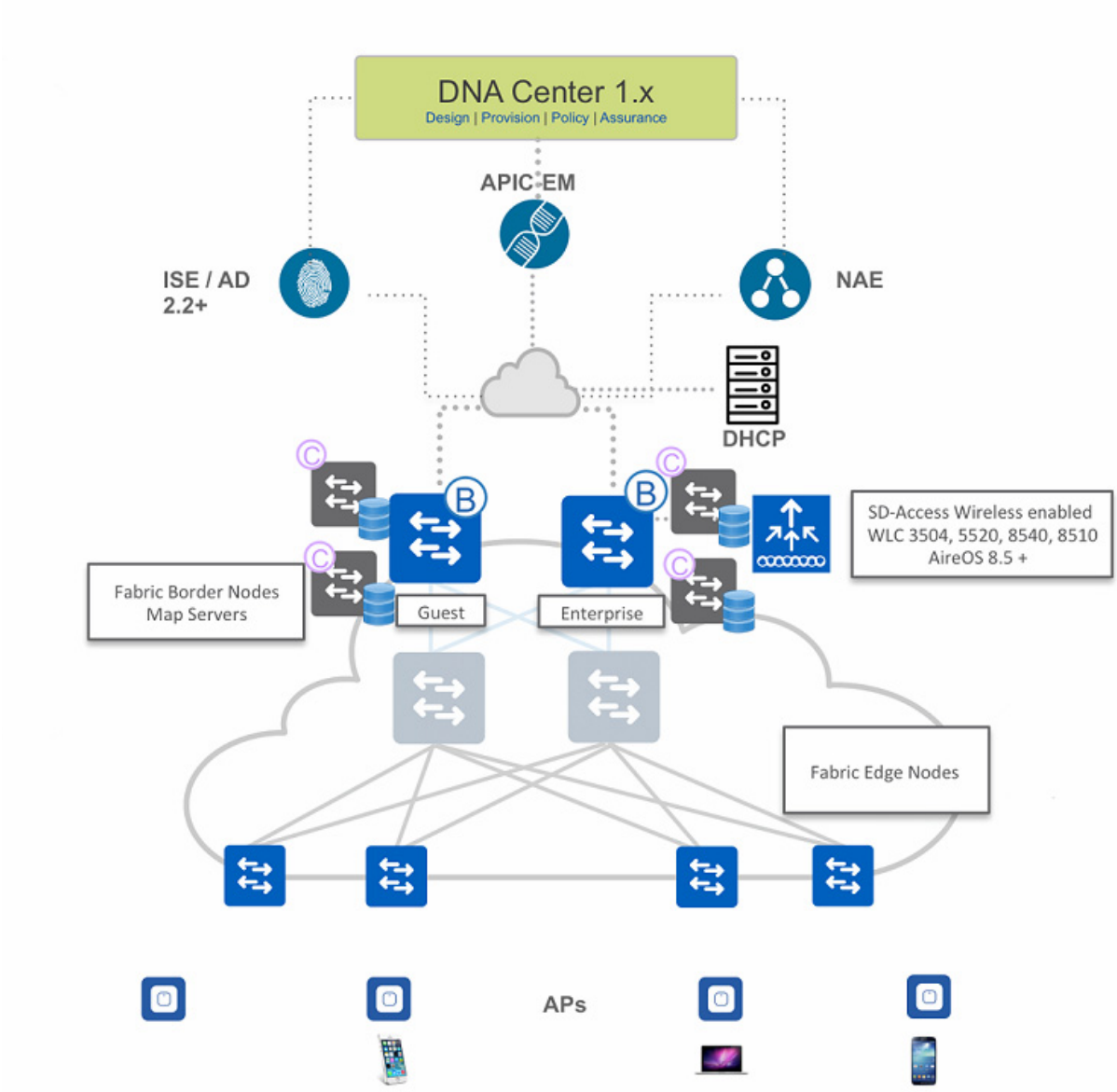
アクセス ポイント（AP）に対しては、ワイヤレス LAN コントローラ（WLC）が論理的に PnP サーバとして機能します。接続する正しい WLC を検出するために AP が使用するプロセスは、上記のプロセスに非常に似ています。WLC を検出できなかった場合、AP は PnPRC と通信して WLC の IP アドレス（論理的に PnP サーバの IP）を取得します。次に AP はこの IP アドレスを使用して、関連付けられている WLC に接続します。AP が認証されると、WLC は接続プロセスを完了し、AP のプロビジョニング プロセスを開始します。

このフローの概要を次に示します。



SD-Access ワイヤレス アーキテクチャの概要

ここでは、SD-Access ワイヤレス アーキテクチャに含まれる各種のコンポーネントのロールと用語について説明します。



- **コントロール プレーン ノード**:エンドポイント ID とデバイスの関係を管理するマップ システム
- **ボーダー ノード**:外部 L3 ネットワークを SDA ファブリックに接続するファブリック デバイス(コアなど)
- **エッジ ノード**:有線エンドポイントを SDA ファブリックに接続するファブリック デバイス(アクセス、ディストリビューションなど)
- **ファブリック ワイヤレス コントローラ**:ファブリックを有効にしたワイヤレス コントローラ(WLC)
- **ファブリック モード AP**:ファブリックを有効にしたアクセス ポイント。

- **DNA コントローラ**:エンタープライズ SDN コントローラは情報を共有する複数のサービス アプリケーションを使用して GUI 管理を抽象化します
- **グループ リポジトリ**:外部 ID サービス(ISE など)を活用して、ユーザまたはデバイスをグループに動的にマッピングし、ポリシーを定義する
- **分析エンジン**:外部データ コレクタ(NAE)を活用して、ユーザまたはデバイスのアプリケーション フローを分析し、ファブリック ステータスをモニタする

SD-Access ワイヤレス プラットフォームのサポート

SD-Access ワイヤレス アーキテクチャは AireOS リリース 8.5 以降を搭載した次のワイヤレス LAN コントローラでサポートされています。

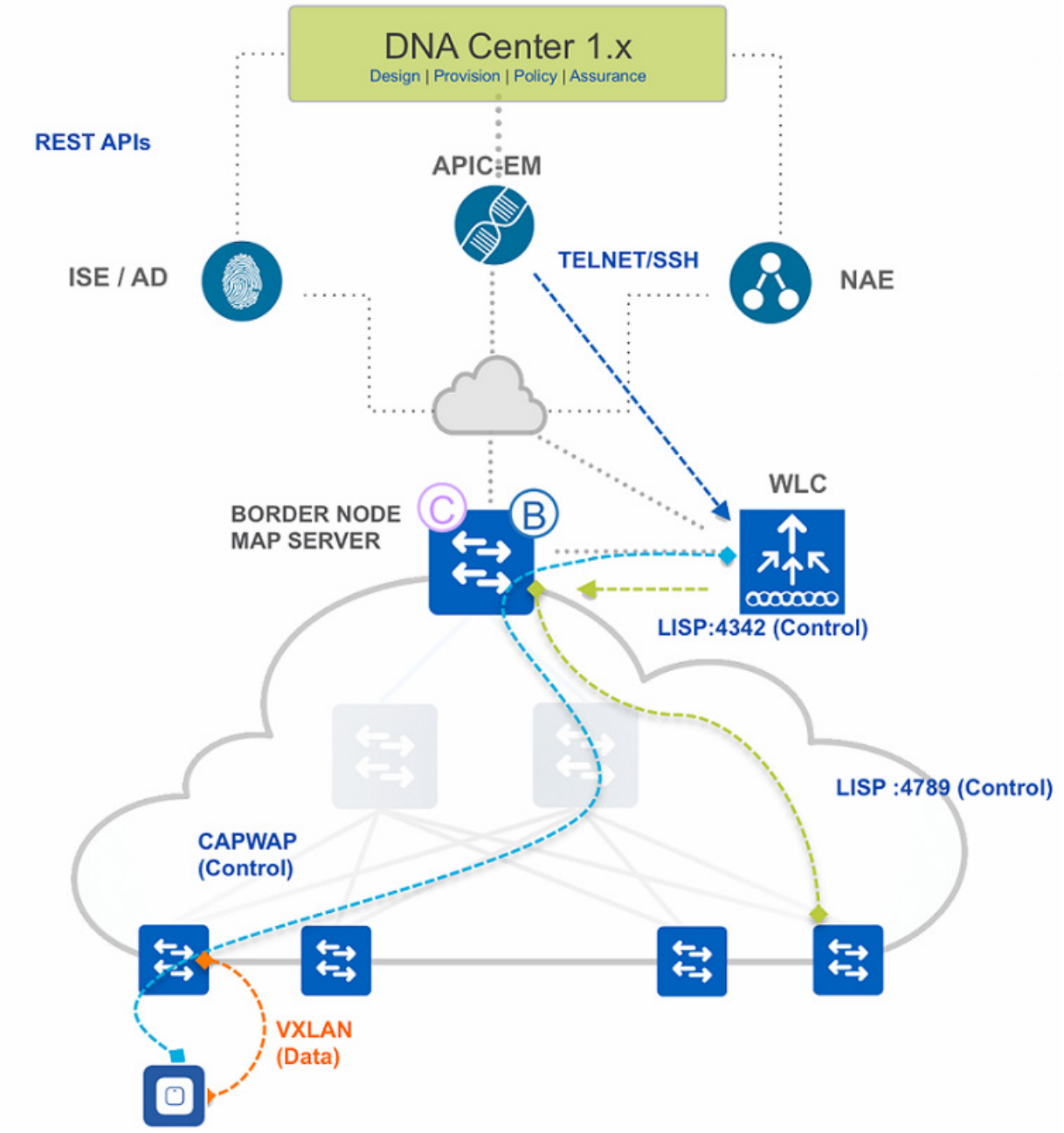
- AIR-CT3504
- AIR-CT5520
- AIR-CT8510
- AIR-CT8540

このアーキテクチャは、ローカル モードで Wave2 11ac アクセス ポイント用に最適化されています。

- AP1810
- AP1815
- AP1830
- AP1850
- AP2800
- AP3800

Wave 1 11ac アクセス ポイントでは、SD-Access ワイヤレスの限定された機能がサポートされています。

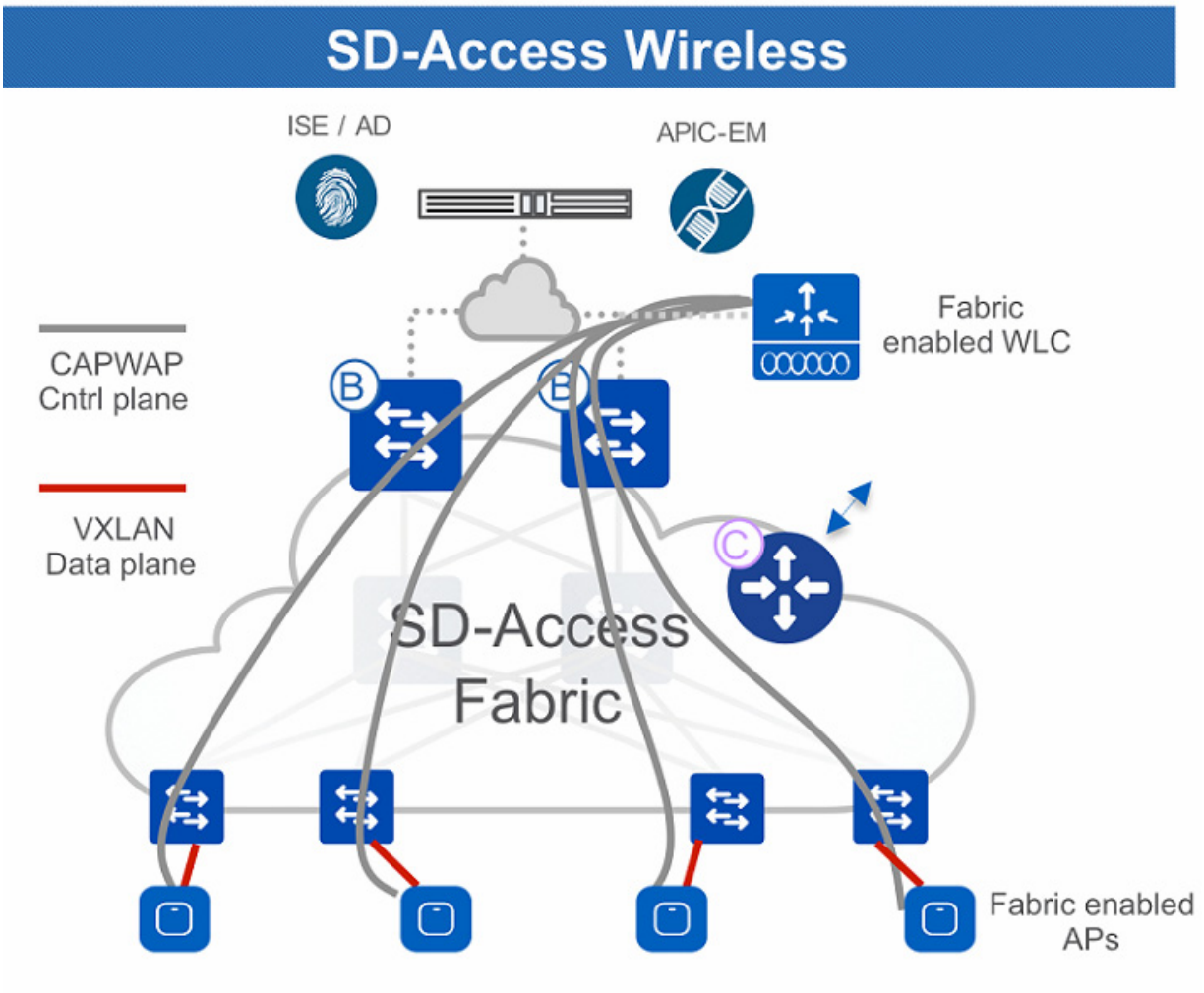
SD-Access ワイヤレス インターフェイス



- WLC <-> AP: コントロール プレーン WLC と AP の通信は、既存のモードと同様に CAPWAP を通じて行われます。
- AP <-> スイッチ:データ トラフィックが VXLAN トンネルのカプセル化によって AP からエッジ スイッチに切り替えられます。
- WLC <-> マップ サーバ:ワイヤレス LAN コントローラが、コントローラのポート 4342 で動作する LISP エージェントを使用して Mapserver と通信します。

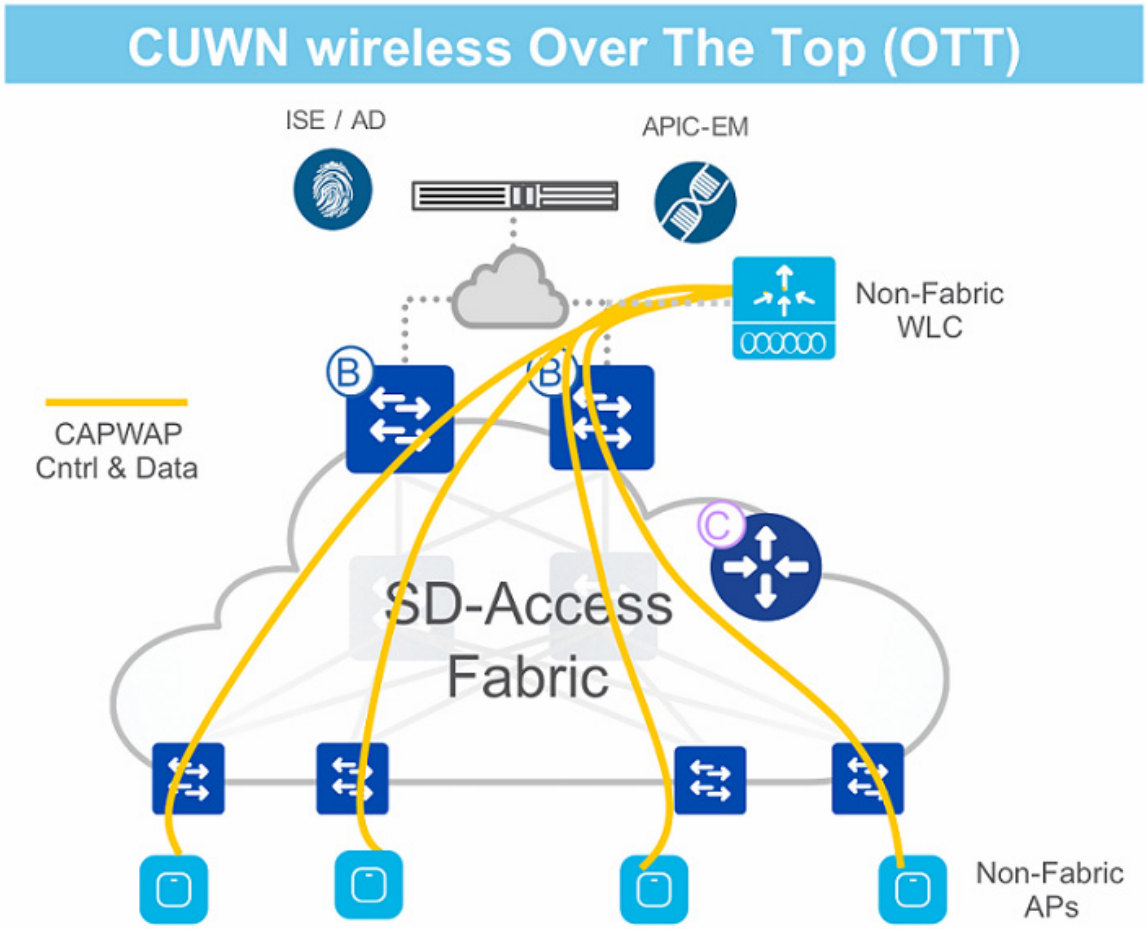
- WLC <-> APIC-EM：APIC-EM が SSH/Telnet を通じて CLI インターフェイスを使用して、WLC を設定します。
- スイッチ <-> Mapserver：ファブリック対応のスイッチが LISP ポート 4789 のマップ サーバと通信します。

サポートされている WLAN モード



- SD-Access ワイヤレスでは、トンネリングで WLC に戻る CAPWAP コントロール プレーンと、スイッチで分散処理される VXLAN データ プレーンを使用します

- WLC/AP がファブリックに統合され、アクセス ポイントがオーバーレイで接続します。



- WLC で終端するコントロール プレーンとデータ プレーン用の CAPWAP を使用した、従来型の CUWN アーキテクチャ。
- SDA ファブリックは AP と WLC 間の有線インフラストラクチャ内の伝送路にすぎません
- これが、完全な SDA 移行に向けた手順です。

SD-Access ワイヤレス機能のサポート

次の表に、SD-Access ワイヤレス アーキテクチャでサポートされている主要な機能の一部を示します。

表 12-2

オープン/固定 WEP	サポート
WPA-PSK	サポート
802.1x（WPA/WPA2）	サポート
MAC Filtering	サポート
ローカル EAP	サポート

表 12-2

AAA オーバーライド	サポート
内部/外部 WebAuth	サポート
事前認証 ACL	サポート
クライアントの IPv4 ACL	サポート
AVC	サポートあり*
ローカル プロファイリング	サポート
RADIUS プロファイル	サポート
QoS プロファイル	サポート
ユーザごとの BW 契約	サポート
wIPS	サポート
CMX 統合	サポート
NetFlow エクスポート	サポート
HA SSO	サポート

*Wave2 AP のみ