SD-Access ワイヤレス

SD-Access ワイヤレスの概要

エンタープライズファブリックは、エンドツーエンドのエンタープライズ全体のセグメンテーション、フレキシブルなサブネットアドレッシング、およびコントローラベースのネットワーキングにエンタープライズ全体にわたって統一されたポリシーとモビリティを提供します。これにより、エンタープライズネットワークは、サイト内およびサイト間のフレキシブルなレイヤ 2 拡張機能とともに、現在の VLAN 中心のアーキテクチャからユーザ グループベースのエンタープライズ アーキテクチャへと移行します。

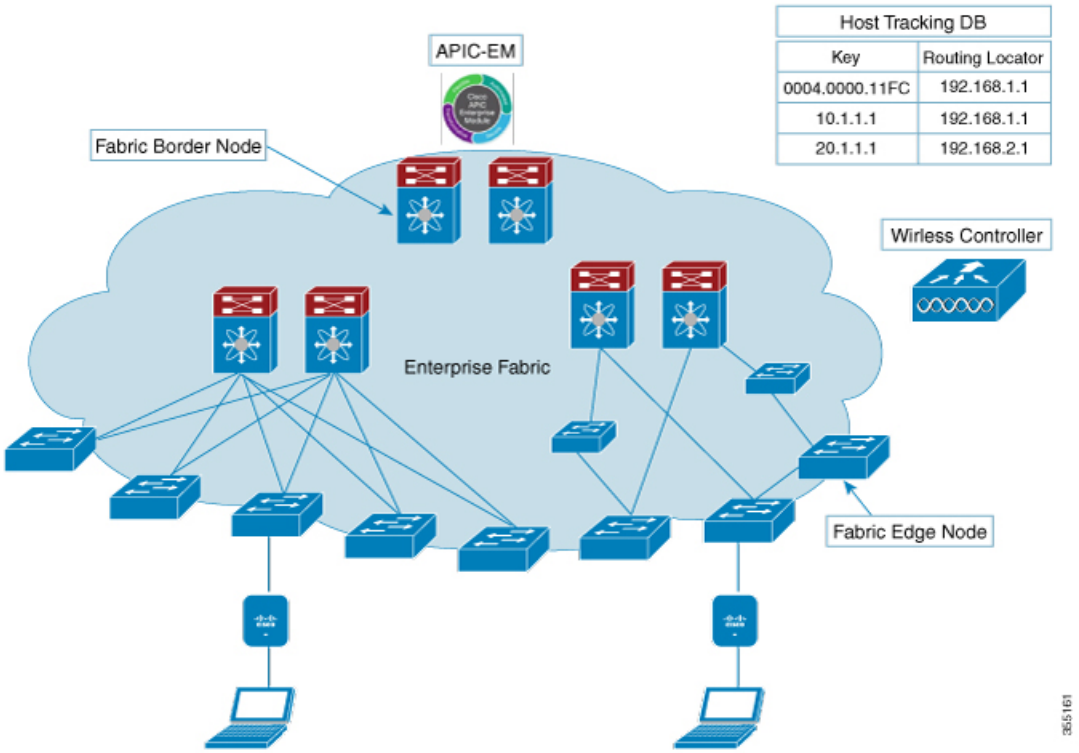
エンタープライズファブリックは、相互接続されたスイッチを介してトラフィックを転送するネットワーク トポロジであり、単一レイヤ2またはレイヤ3のデバイスの抽象化を行います。これにより、ファブリックのエッジでポリシーを適用し、強制することで、シームレスな接続が実現します。ファブリックは IP オーバーレイを使用します。これにより、クラスタリング テクノロジーを使用せずにネットワークが単一の仮想エンティティとして表示されます。

ファブリック ノードに使用される定義は次のとおりです。

- **エンタープライズ ファブリック**：相互接続スイッチを通じてトラフィックが渡され、単一レイヤ 2 またはレイヤ 3 のデバイスの抽象化を実行するネットワーク トポロジ。
- **ファブリック ドメイン**：ネットワークの独立した操作部。他のファブリック ドメインとは別に管理されます。
- **エンドポイント**：ファブリック エッジ ノードに接続されたホストまたはデバイスをエンドポイント（EP）といいます。エンドポイントはファブリック エッジ ノードに直接接続するかまたはレイヤ 2 ネットワークを通じて接続します。

次に、通常の SD-Access ワイヤレスのコンポーネントの図を示します。ファブリック ボーダー ノード（BN）、ファブリック エッジ ノード（EN）、ワイヤレス コントローラ（WLC）、Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）、およびホスト トラッキング データベース（HDB）から構成されています。

図 *1 : SD-Access* ワイヤレス



APIC-EM コントローラ：APIC-EM コントローラ上に開発されたファブリック サービスは、エンタープライズファブリックの管理とオーケストレーションを促進します。また、接続されているユーザとデバイスのポリシーのプロビジョニングも行います。

ホスト ID トラッキング データベース（マップ サーバと LISP のマップリゾルバ）：このデータベースにより、デバイスまたはユーザの場所をネットワークが判断できます。ホストの EP ID を学習すると、他のエンドポイントがホストの場所に関してデータベースにクエリを実行できます。トラッキングサブネットの柔軟性により、ドメイン間での集約が助長され、データベースのスケーラビリティが向上します。

ファブリック ボーダー ノード（プロキシ出力トンネル ルータ（PxTR または LISP の PITR/PETR））：これらのノードは従来のレイヤ 3 ネットワーク、またはさまざまなファブリック ドメインをエンタープライズ ファブリック ドメインに接続します。複数のファブリック ドメインがある場合、これらのノードは 1 つのファブリック ドメインを 1 つ以上のファブリック ドメインに接続しますが、それらのドメインのタイプは同じであることも、異なることもあります。これらのノードは、1 つのファブリック ドメインから別のドメインへのコンテキストの変換を担います。カプセル化が異なるファブリック ドメイン間で同じである場合、ファブリック コンテキストの変換は通常 1 対 1 となります。2 つのドメインのファブリック コントロール プレーンはこのデバイスを介した到達可能性とポリシー情報を交換します。

ファブリック エッジ ノード（出力トンネル ルータ（ETR）または LISP の入力トンネル ルータ（ITR））：これらのノードは EP からのトラフィックの承認、カプセル化またはカプセル化解除、および転送を担います。これらはファブリックを囲む境界にあり、ポリシーが適用さ

れる最初のポイントです。EPは、ファブリック ドメインの外側にある中間レイヤ2ネットワークを使用してファブリック エッジ ノードに直接または間接的に接続されることがあります。従来のレイヤ 2 ネットワーク、ワイヤレス アクセス ポイント、またはエンド ホストがファブリック エッジ ノードに接続されます。

ワイヤレス コントローラ：WLC は AP イメージと設定管理、クライアント セッション管理とモビリティを提供します。さらに、ワイヤレス クライアントの MAC アドレスをクライアント接続時にホスト トラッキング データベースに登録するとともに、クライアントのローミング時に場所を更新します。

アクセス ポイント：AP はすべてのワイヤレス メディアの固有の機能を適用します。たとえば、無線ポリシーと SSID ポリシー、WebAuth パント、ピアツーピア ブロッキングなどです。これで、CAPWAP 制御と WLC へのデータ トンネルを確立します。ワイヤレス クライアントからの 802.11 データ トラフィックを 802.3 に変換し、VXLAN カプセル化を使用してアクセス スイッチに送信します。

SDA では次を簡素化できます。

- ワイヤレス ネットワーク内でのアドレッシング
- ワイヤレス ネットワーク内でのモビリティ
- ゲスト アクセスとマルチ テナントに向けての移行
- ワイヤレス ネットワーク内でのサブネット拡張機能（拡張サブネット）の活用
- 一貫性のあるワイヤレス ポリシーの提供

AP 起動プロセス

次に、AP を起動する手順を示します。

- スイッチが AP に電源を投入します（PoE または UPoE）。
- AP は DHCP サーバから IP アドレスを取得します。
- スイッチは AP の IP アドレスをマップ サーバに登録します。
- AP は CAPWAP 検出により Cisco WLC を検出します。
- Datagram Transport Layer Security（DTLS）のハンドシェイク後、制御パケット用に CAPWAP 制御トンネルが AP と Cisco WLC 間に作成されます。CAPWAP データ トンネルが IEEE 802.11 管理フレーム用に作成されます。AP イメージがダウンロードされ、設定がコントローラから AP にプッシュされます。
- Cisco WLC は、登録された AP が背後にあるスイッチのマップ サーバ（RLOC IP）を照会します。
- Cisco WLC は、マップ サーバにダミーの MAC アドレスを登録します。
- マップ サーバは、AP に VXLAN トンネルを作成するスイッチにダミーの MAC アドレス通知を送信します。

- AP はクライアントを受け入れる準備が整います。

ワイヤレス クライアントのオンボーディング

次に、クライアントをオンボーディングする手順を示します。

- ワイヤレス クライアントがそれ自体を AP に関連付けます。
- クライアントは、CAPWAP データ トンネルを使用して Cisco WLC（設定されている場合）で IEEE 802.1x 認証を開始します。
- レイヤ 2 認証が完了すると、Cisco WLC はクライアントの MAC アドレスをマップ サーバに登録します。
- マップ サーバはクライアントの詳細を示した通知メッセージをスイッチに送信します。
- スイッチはクライアントの MAC をレイヤ 2 転送テーブルに追加します。
- クライアントは DHCP サーバから IP アドレスを取得します。
- AP は Cisco WLC にクライアントの IP アドレスを送信します。
- Cisco WLC はクライアントを RUN 状態に移行して、クライアントがトラフィックの送信を開始できるようにします。
- スイッチはクライアントの IP アドレスをマップ サーバに登録します。
- スイッチは VXLAN パケットのカプセル化を解除します。
- スイッチは DHCP パケットを DHCP サーバに転送するか、またはリレーします。
- スイッチはワイヤレス クライアントの DHCP ACK を受信します。スイッチはクライアントの IP アドレスを学習し、更新をマップ サーバに送信します。
- スイッチは DHCP ACK を AP 側 VXLAN トンネルを含めて、VLAN 内のすべてのポートにブロードキャストします。
- DHCP ACK が AP に到達し、その AP が ACK をクライアントに転送します。
- AP はクライアントの IP アドレスを WLC に送信します。
- Cisco WLC はクライアントを RUN 状態にします。

プラットフォーム サポート

表 *1:* サポートされる *AireOS* コントローラ

コントローラ	サポート
2504	なし

コントローラ	サポート
3504	あり
5508	なし
WiSM2	なし
8510	ローカルモードの AP のみでサポート
5520	ローカルモードの AP のみでサポート
8540	ローカルモードの AP のみでサポート
7510	なし
vWLC	なし

表 *2 : AP* のサポート

AP	サポート
802.11n	なし
802.11ac Wave 1	あり
802.11ac Wave 2	あり
メッシュ	非対応

表 *3 :* クライアント セキュリティ

セキュリティ	サポート
オープンおよび静的 WEP	なし
WPA-PSK	あり
802.1x（WPA/WPA2）	あり
MAC フィルタリング	あり
CCKM 高速ローミング	あり
ローカル EAP	あり。ただし、推奨しません。

セキュリティ	サポート
AAA オーバーライド	SGT、L2 VNID、ACL ポリシー、および QoS ポリシーでサポート
内部 WebAuth	IPv4 クライアント
外部 WebAuth	IPv4 クライアント
事前認証 ACL	IPv4 クライアント
FQDN ACL	なし

表 *4 : IPv6* のサポート

IPv6	**サポート**
IPv6 インフラ サポート	なし
IPv6 クライアント サポート	なし

表 *5 :* ポリシー、*QoS*、および機能サポート

機能	サポート
クライアントの IPv4 ACL	はい。AP での ACL の Flex ACL
クライアントの IPv6 ACL	なし
P2P ブロッキング	同じ AP 上のクライアント用スイッチのセキュリティ グループ タグ（SGT）およびセキュリティ グループ ACL（SGACL）を通じてサポート。
IP ソース ガード	スイッチ
AVC の可視性	AP
AVC QoS	AP
ダウンロード可能なプロトコル パックの更新	なし
デバイスのプロファイリング	なし
mDNS プロキシ	なし
MS Lync Server QoS の統合	なし
NetFlow エクスポータ	なし

機能	サポート
QoS	あり（メタルプロファイルおよびレート制限）
パッシブ クライアント/サイレント ホスト	なし
ロケーション トラッキング/HyperLocation	あり
ワイヤレス マルチキャスト	はい。ビデオ ストリーミングはサポートされていません。
URL フィルタリング	なし
HA	WLC から WLC へ

統合アクセスからの移行

次に、統合アクセスからファブリック ワイヤレスへの移行プロセスを示します。

1. イメージ対応のファブリック モードで WLC を起動します。
2. APIC-EM または CLI を使用して、適切なサブネットのファブリック モードでネットワークを設定します。これには、APIC-EM を使用することをお勧めします。
3. 新しい AP サブネットでの DHCP 検出がコントローラ対応のファブリック モードとなるように検出メカニズムを設定します。
4. AP が起動したら、DHCP 要求を実行して AP VLAN 内の IP アドレスを取得します。
5. AP は WLC を使用してコントロール プレーンの CAPWAP トンネルを作成します。
6. 設定に基づいて、WLC がファブリック モード用に AP をプログラムします。
7. この後は、AP はワイヤレス フローの SDA に従います。

（注） ファブリック SSID とファブリック以外の SSID 間のモビリティはサポートされていません。

（注） AP イメージとライセンスは Cisco WLC でホストされ、AP はその WLC からイメージとライセンスを直接取得します。APIC-EM は、Cisco WLC 上での AP ライセンスの管理を担います。

（注） WLC での TCP 接続フラップ後、接続を再確立するには 5 ～ 6 分かかります。この間に、アクセス トンネルはクライアントの参加時にリセットされます。

SD-Access ワイヤレスの設定（CLI）

WLAN でファブリックを設定するには、次の手順を実行します。

始める前に

- ファブリックをイネーブルにするように、ローカル モードで AP を設定します。

手順

ステップ 1 **config wlan fabric enable** *wlanid*

例：

```
config wlan fabric enable wlan1
```

WLAN でファブリックをイネーブルにします。

ステップ 2 **config wlan fabric vnid** *vnid wlanid*

例：

```
config wlan fabric vnid 10 wlan1
```

ファブリック WLAN で仮想拡張 LAN（VXLAN）ネットワーク識別子（VNID）を設定します。

ステップ 3 **config wlan fabric encap vxlan** *wlanid*

例：

```
config wlan fabric encap vxlan wlan1
```

ファブリック WLAN に VNID をマップします。

ステップ 4 **config wlan fabric switch-ip** *ip-address wlanid*

例：

```
config wlan fabric switch-ip 1.1.1.1 wlan1
```

VLAN ピア IP を WLAN に設定します。

ステップ 5 **config wlan fabric acl** *fabric-acl-name wlanid*

例：

```
config wlan fabric acl fabric-acl wlan1
```

WLC でフレックス ACL を設定して、ファブリック WLAN に関連付けます。

ステップ 6 **config wlan fabric avc-policy** *fabric-avc-policy wlanid*

例：

```
config wlan fabric fabric-avc-policy wlan1
```

AVC プロファイル名を設定して、ファブリック WLAN に関連付けます。

ステップ 7 **config wlan fabric controlplane guest-fabric enable** *wlanid*

例：

```
config wlan fabric controlplane guest-fabric enable wlan1
```

（任意）この WLAN のゲスト ファブリックをイネーブルにします。

ステップ 8 **show fabric summary**

例：

```
show fabric summary
```

（任意）リンク設定のサマリーを表示します。