DNAによるワイヤレスのソフトウェア定義型アクセスの実装

内容

はじめに

このドキュメントでは、ファブリック対応WLCおよびアクセスLAPに関連するワイヤレステクノロジーのSDAをCisco DNAに実装する方法について説明します.

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 9800ワイヤレスLANコントローラ(WLC)の設定
- Lightweightアクセスポイント(LAP)
- シスコのDNA

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9800-CL WLC Cisco IOS® XEバージョン17.9.3
- シスコアクセスポイント：9130AX、3802E、1832I
- Cisco DNAバージョン2.3.3.7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SD-Access

ソフトウェア定義のアクセス：動的なルールと自動セグメンテーションを使用してセキュリティポリシーを確立し、ネットワーク全体に自動的に適用します。また、エンドユーザは、ネットワークへの接続方法を制御および設定できます。SD-Accessは、接続された各エンドポイントとの初期レベルの信頼を確立し、継続的にモニタリングして信頼レベルを再検証します。エンドポイントが正常に動作しない場合、または扱いが検出された場合、エンドユーザは即座にそのエンドポイントを封じ込めて対策を講じることができます。これにより、侵害が発生する前に対策を講じ、ビジネスリスクを軽減し、リソースを保護できます。完全に統合されたソリューションで、新規および導入済みネットワークの両方に導入と設定が容易

SD-Accessは、従来のキャンパスネットワークを進化させたシスコのテクノロジーであり、Software-Defined Networking(SDN)コンポーネントを使用してインテントベースのネットワーキング(IBN)と中央集中型のポリシー制御を提供します。

SD-Accessの3本の柱：

1. ネットワークファブリック：ネットワーク自体を抽象化したもので、プログラマブルオーバーレイと仮想化をサポートします。ネットワークファブリックは、有線アクセスとワイヤレスアクセスの両方をサポートし、相互にセグメント化され、ビジネスの目的によって定義される複数の論理ネットワークをホストできます。
2. オーケストレーション：Cisco DNAは、SDAのオーケストレータエンジンです。Cisco

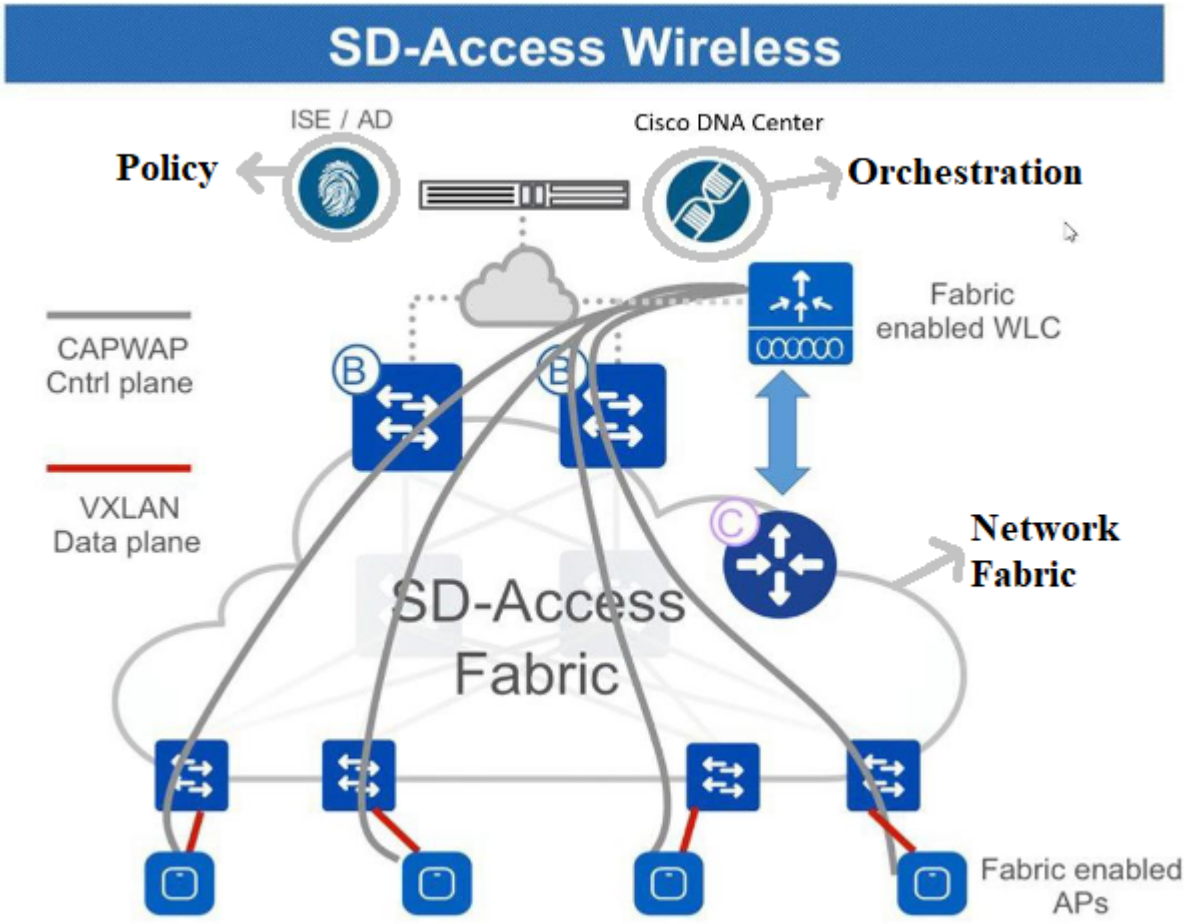
DNAはSDNコントローラのように機能します。ファブリック内にポリシーと設定変更を実装するまた、ネットワーク設計をサポートし、DNA Assuranceを通じてリアルタイムのネットワークテレメトリ操作とパフォーマンス分析をサポートするツールも組み込まれています。Cisco DNAの役割は、ネットワークファブリックをオーケストレーションして、セキュリティ、Quality of Service(QoS)、およびマイクロセグメンテーションに関するポリシー変更とネットワークの意図を提供することです。

3. ポリシー：Identity Services Engine(ISE)は、ネットワークポリシーを定義するツールです。ISEは、デバイスとノードを仮想ネットワークにセグメント化する方法を整理します。また、ISEは、アクセスデバイスがファブリックに入るユーザトラフィックをセグメント化するために使用する、スケーラブルなグループタグ(SGT)も定義します。SGRは、ISEによって定義されたマイクロセグメンテーションポリシーを適用する責任があります。

SDAは一元化されたオーケストレーション上に構築されます。プログラマブルオーケストレーションエンジンとしてのCisco DNA、ポリシーエンジンとしてのISE、および新世代のプログラマブルスイッチの組み合わせにより、ファブリックシステムの柔軟性と管理性が以前よりもはるかに向上しています。

注：このドキュメントでは、特にSDアクセスワイヤレスについて説明します。

ネットワークファブリックは、次の要素で構成されています。

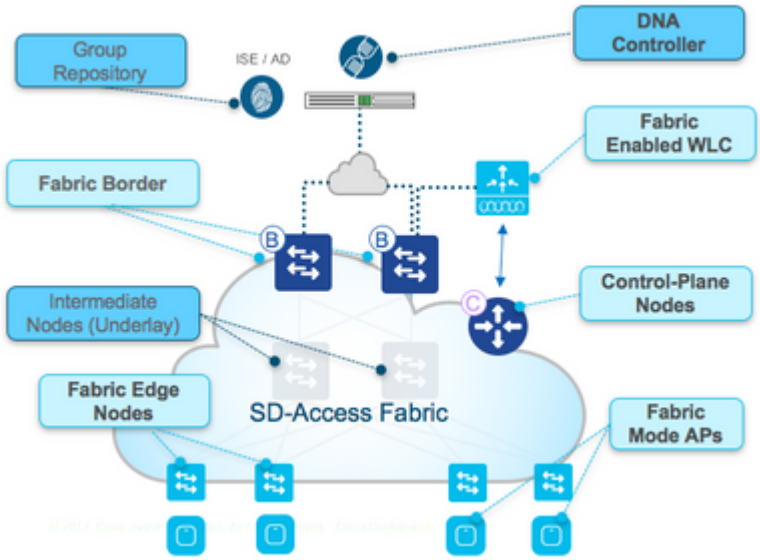


ネットワークファブリックの要素

ファブリックへのワイヤレス統合により、ワイヤレスネットワークにはいくつかの利点が得られます。たとえば、アドレッシングの簡素化、物理ロケーションにまたがる拡張されたサブネットによるモビリティ、有線ドメインと無線ドメインの両方で一貫した一元化されたポリシーによるマイクロセグメンテーションなどです。また、コントローラは、ワイヤレスネットワークの集中型サービスおよびコントロールプレーンとして機能し続けながら、データプレーンを解放して作業を転送することもできます。したがって、FlexConnectモデルと同様に、データプレーントラフィックを処理する必要がなくなるため、ワイヤレスコントローラのスケーラビリティが実際に向上します。

SD-Accessワイヤレスアーキテクチャ

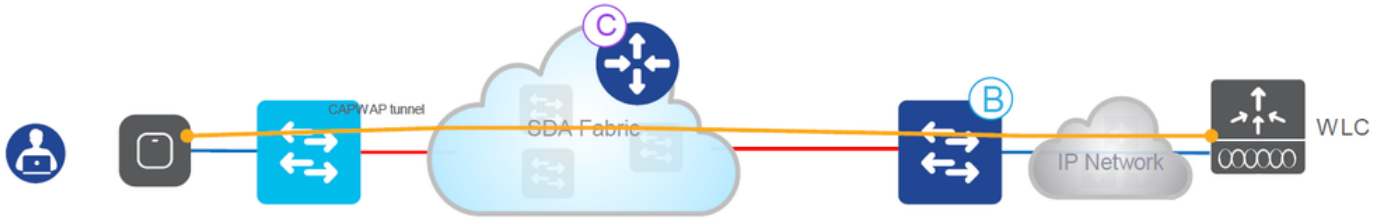
概要



SDAの概要

SDAでサポートされるワイヤレス導入モデルには、主に次の2つがあります。

1つはオーバーザトップ(OTT)方式で、ファブリック有線ネットワーク上に接続された従来のCAPWAP導入です。SDAファブリックは、CAPWAPコントロールトラフィックとデータプレーントラフィックをワイヤレスコントローラに転送します。

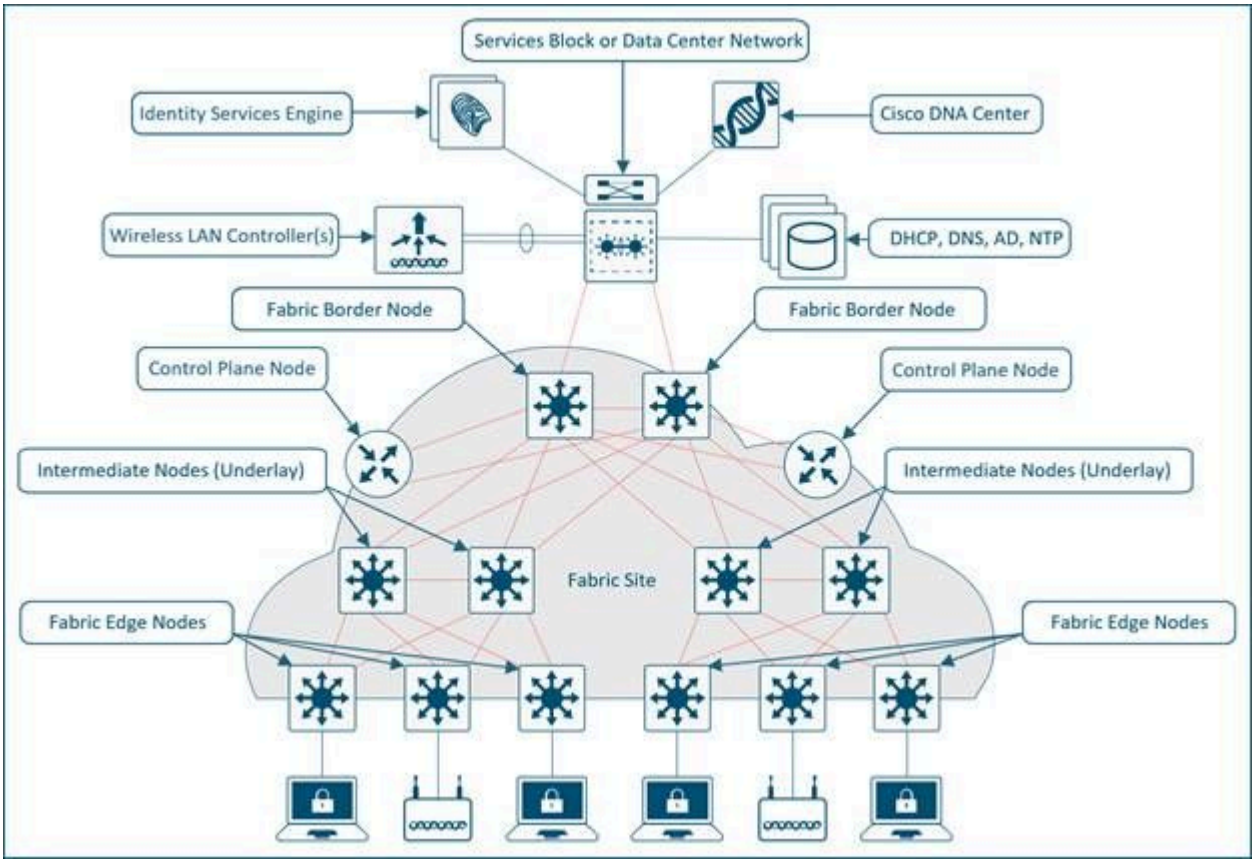


オーバーザトップ方式

この導入モデルでは、SDAファブリックはワイヤレストラフィックの転送ネットワークです（移行で導入されることが多いモデル）。 APの動作は従来のローカルモードと非常によく似ています。CAPWAPのコントロールプレーンとデータプレーンは両方ともコントローラで終端するため

、コントローラが直接ファブリックに参加することはありません。このモデルは、有線スイッチを初めてSDAファブリックに移行する際に、ワイヤレスネットワークのファブリックオーバーレイを完全に統合する準備が整っていない場合によく使用されます。

その他の導入モデルは、完全統合型のSDAモデルです。ワイヤレスネットワークはファブリックに完全に統合され、オーバーレイに参加します。これにより、異なるWLANを異なる仮想ネットワーク(VN)の一部にすることができます。 ワイヤレスコントローラはCAPWAPコントロールプレーン（APを管理するため）のみを管理し、CAPWAPデータプレーンはコントローラに到達しません。



完全統合型SDAモデル

ワイヤレスデータプレーンは有線スイッチと同様に処理され、各APはVXLANでデータをカプセル化してファブリックエッジノードに送信します。その後、ファブリックエッジノードを介して別のエッジノードに送信されます。ワイヤレスコントローラは、ファブリックコントローラとして設定する必要があります。これは、通常の動作からの変更です。

ファブリック対応コントローラはファブリックコントロールプレーンと通信し、レイヤ2クライアントMACアドレスとレイヤ2仮想ネットワーク識別子(VNI)情報を登録します。APはワイヤレスエンドポイントとの通信を行い、トラフィックのカプセル化とカプセル化解除を行うことでVXLANデータプレーンを支援します。

SDAの役割と用語

ネットワークファブリックは、次の要素で構成されています。

- コントロールプレーンノード：これは、Location Separator Protocol(LISP)コントロールプ

レーンの一部であるロケーションマッピングシステム（ホストデータベース）であり、エンドポイントIDとロケーションの関係（またはデバイスの関係）を管理します。 コントロールプレーンは、コントロールプレーン機能を提供する専用ルータにすることも、他のファブリックネットワークエレメントと共存させることもできます。

- ファブリックボーダーノード：通常は、外部ネットワークとSDAファブリックの境界で機能するルータで、ファブリック内の仮想ネットワークにルーティングサービスを提供します。外部レイヤ3ネットワークをSDAファブリックに接続する
- ファブリックエッジノード：スイッチ、AP、ルータなどの非ファブリックデバイスをSDAファブリックに接続するファブリック内のデバイス。これらは、仮想オーバーレイトンネルとVirtual eXtensible LAN(VXLAN)を使用したVNを作成し、ファブリックバウンドトラフィックにSGTを適用するノードです。ファブリックエッジの両側のネットワークは、SDAネットワーク内にあります。有線エンドポイントをSD-Accessファブリックに接続する
- 中間ノード：これらのノードはSDAファブリックのコア内部にあり、エッジノードまたはボーダーノードのいずれかに接続します。中継ノードは、複数の仮想ネットワークが含まれていることに気付かずに、SDAトラフィックをIPパケットとして転送するだけです。
- ファブリックWLC：ファブリック対応で、SDAコントロールプレーンに参加するが、CAPWAPデータプレーンを処理しないワイヤレスコントローラ。
- ファブリックモードAP：ファブリック対応のアクセスポイント。ワイヤレストラフィックはAPでVXLANカプセル化され、エッジノードを介してファブリックに送信できます。
- Cisco DNA(DNAC):Software Defined Access(SDA)ファブリックオーバーレイネットワーク用のエンタープライズSDNコントローラで、自動化タスクと保証タスクの両方を担当します。また、アンダーレイを形成する（SDAに関連しない）ネットワークデバイスの自動化タスクや関連タスクにも使用できます。
- ISE:Identity Services Engine(ISE)は、さまざまな役割と機能を提供できる拡張ポリシープラットフォームです。特に、認証、許可、アカウンティング(AAA)サーバの役割と機能は重要です。ISEは通常、Active Directory(AD)と通信しますが、小規模な導入では、ユーザをISE自体でローカルに設定することもできます。

注：コントロールプレーンはSDAアーキテクチャの重要なインフラストラクチャピースであるため、復元力のある方法で導入することをお勧めします。

アンダーレイネットワークとオーバーレイネットワーク

SDAアーキテクチャは、物理ネットワーク（アンダーレイネットワーク）上で動作するプログラム可能な仮想ネットワーク（オーバーレイネットワーク）をサポートするファブリックテクノロジーを利用します。

ファブリックはオーバーレイです。

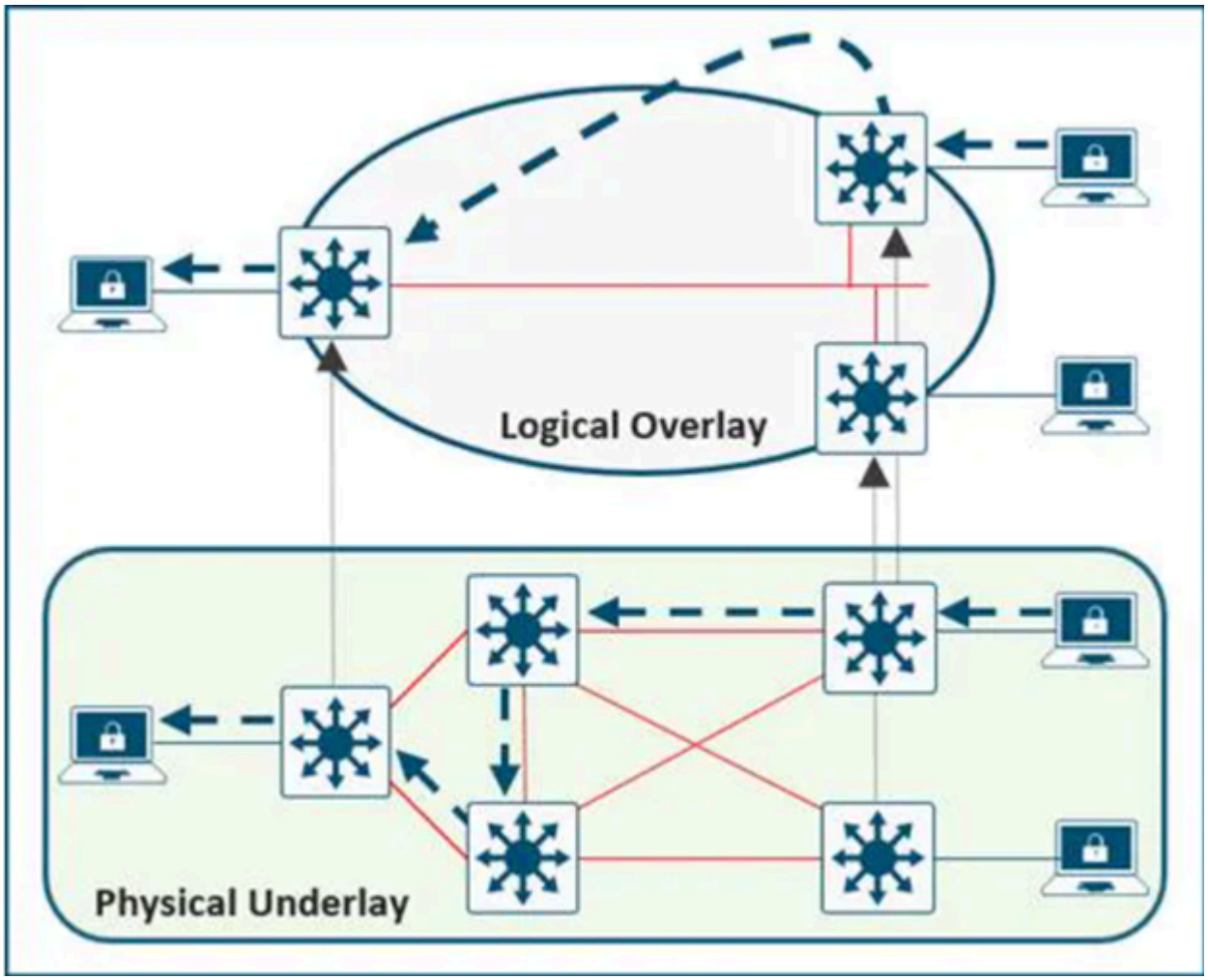
オーバーレイネットワークは、デバイスを仮想的に接続するために使用される論理トポロジで、任意の物理アンダーレイトポロジ上に構築されます。代替の転送属性を使用して、アンダーレイでは提供されない追加サービスを提供します。アンダーレイの上に作成され、1つまたは複数の仮想化されたセグメント化されたネットワークを作成します。オーバーレイはソフトウェア定義型であるため、物理的な接続の制約を受けることなく、非常に柔軟な方法で接続できます。オーバーレイは単一の物理的な出口ポイント（ファブリックボーダーノード）を持つようにプログラム可能であり、1つのファイアウォールをその背後にあるネットワークを保護するために使用できるため（配置できるかどうか）、セキュリティポリシーを適用するための簡単な方法です。 オーバーレイはVXLANを使用してトラフィックをカプセル化します。VXLANは、アンダーレイ全体を転送するために、レイヤ2フレーム全体をカプセル化します。各オーバーレイネットワークは、VXLANネットワーク識別子(VNI)で識別されます。 オーバーレイファブリックは複雑になる傾向があり、導入する新しい仮想ネットワークやセキュリティポリシーの実装には大量の管理者オーバーヘッドが必要になります。

ネットワークオーバーレイの例：

- GRE、mGRE
- MPLS、VPLS
- IPSec、DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

アンダーレイネットワークは、SDAネットワークの導入に使用されるスイッチ、ルータ、ワイヤレスAPなどの物理ノードによって定義されます。アンダーレイのすべてのネットワーク要素は、ルーティングプロトコルを使用してIP接続を確立する必要があります。アンダーレイネットワークでは、従来のアクセス、ディストリビューション、コアモデルを使用することはあまりありませんが、堅牢なパフォーマンス、スケーラビリティ、およびハイアベイラビリティを提供する、適切に設計されたレイヤ3基盤を使用する必要があります。

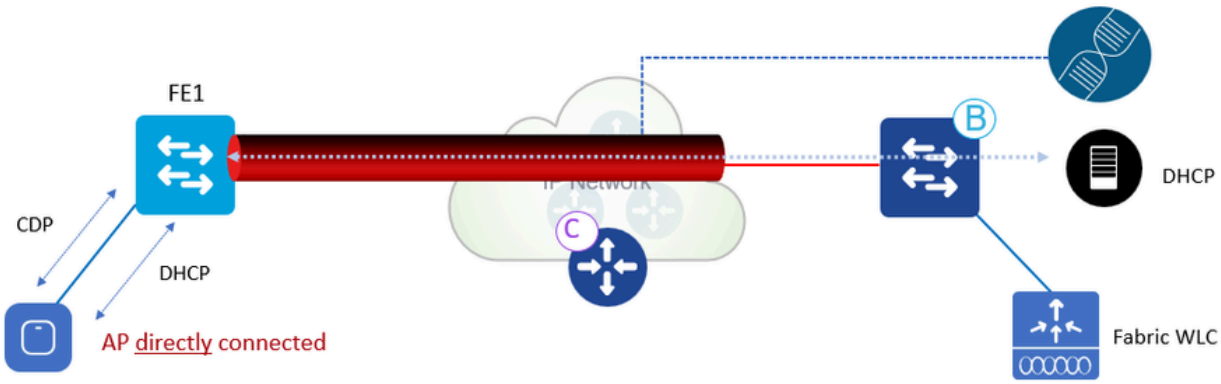
注:SDAは、アンダーレイネットワークではIPv4、オーバーレイネットワークではIPv4および/またはIPv6をサポートします。



アンダーレイネットワークとオーバーレイネットワーク

基本ワークフロー

AP加入



AP加入ワークフロー

AP加入ワークフロー：

1. 管理者がINFRA_VNのDNACでAPプールを設定します。Cisco DNAは、すべてのファブリック

エッジノード上の設定を事前プロビジョニングして、APを自動的にオンボーディングします。

2. APが接続され、電源がオンになっている。ファブリックエッジは、CDPを介してAPであることを検出し、マクロを適用して、スイッチポート（またはインターフェイステンプレート）に適切なVLANを割り当てます。

3. APはオーバーレイでDHCP経由でIPアドレスを取得します。

4. ファブリックエッジは、APのIPアドレスとMAC(EID)を登録し、コントロールプレーン(CP)を更新します。

5. APは従来の方法でWLCのIPを学習します。ファブリックAPはローカルモードAPとして加入します。

6. WLCは、それがファブリック対応（Wave 2またはWave 1 AP）かどうかを確認します。

7. APがファブリックでサポートされている場合、WLCはAPがファブリックに接続されているかどうかをCPに問い合せます。

8. コントロールプレーン(CP)がRLOCを使用してWLCに応答します。これは、APがファブリックに接続され、「Fabric enabled」と表示されていることを意味します。

9. WLCは、CPでAPのL2 LISP登録（つまり、APの「特別な」セキュアクライアント登録）を行います。 これは、重要なメタデータ情報をWLCからファブリックエッジに渡すために使用されます。

10. このプロキシ登録に応答して、コントロールプレーン(CP)はファブリックエッジに通知し、WLCから受信したメタデータ（APであることを示すフラグとAPのIPアドレス）を渡します。

11. ファブリックエッジは情報を処理し、それがAPであることを学習し、指定されたIPへのVXLANトンネルインターフェイスを作成します（最適化：スイッチ側はクライアントが参加できる状態です）。

debug/showコマンドを使用すると、AP加入ワークフローを確認および検証できます。

コントロール プレーン

debug lisp control-plane all（すべてのLISPコントロールプレーンをデバッグ）

show lisp instance-id <L3 instance id> ipv4 server（APが接続されているエッジスイッチによって登録されたAPのIPアドレスを示す必要があります）

show lisp instance-id <L2 instance id> ethernet server（AP無線に加えて、イーサネットMACアドレス、WLCによって登録されたAP無線、およびAPが接続されているエッジスイッチによってイーサネットMACを表示する必要があります。 ）

エッジスイッチ

debug access-tunnel all（トンネルモード）

debug lisp control-plane all（すべてのLISPコントロールプレーンをデバッグ）

show access-tunnel summary（トンネルの概要を表示）

show lisp instance < L2 instance id> ethernet database wlc access-points（ここでAP radio macを表示する必要があります）

WLC

show fabric ap summary（ダウンロード）

WLC LISPのデバッグ

set platform software trace wncd chassis active r0 lisp-agent-api debug

set platform software trace wncd chassis active r0 lisp-agent-db debug

set platform software trace wncd chassis active r0 lisp-agent-fsm debug

set platform software trace wncd chassis active r0 lisp-agent-internal debug

set platform software trace wncd chassis active r0 lisp-agent-lib debug

set platform software trace wncd chassis active r0 lisp-agent-lispmsg debug

set platform software trace wncd chassis active r0 lisp-agent-shim debug

set platform software trace wncd chassis active r0 lisp-agent-transport debug

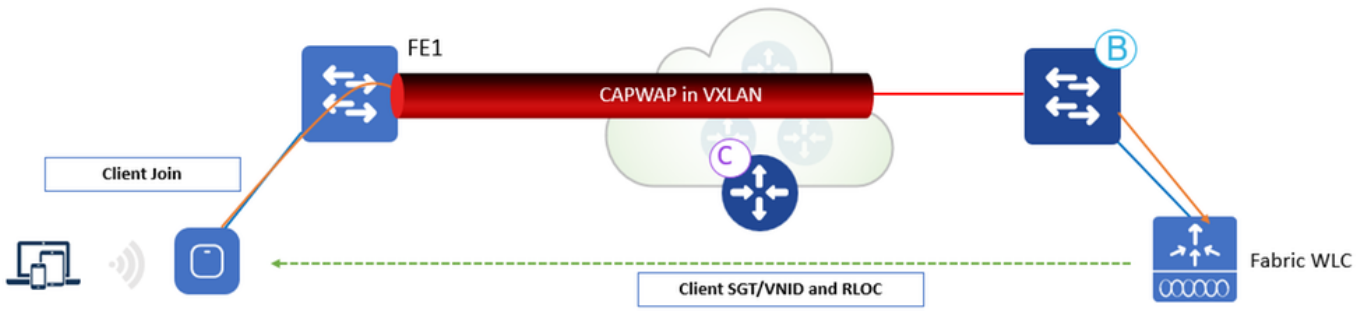
set platform software trace wncd chassis active r0 lisp-agent-ha debug

set platform software trace wncd chassis active r0 ewlc-infra-evq debug

アクセス ポイント

show ip tunnel fabric（すべてのインターフェイス）

クライアントオンボード



クライアントオンボードワークフロー

クライアントオンボードワークフロー：

1. クライアントはファブリック対応WLANに対して認証を行います。WLCはISEからSGTを取得し、クライアントL2VNIDとSGTを使用してAPをRLOC IPとともに更新します。WLCは、内部データベースからAPのRLOCを認識します。

2. WLCプロキシがクライアントL2情報をCPに登録します。これは、クライアントSGTなどの追加情報を渡すためにLISPで変更されたメッセージです。

3. ファブリックエッジはCPによって通知され、L2のクライアントMACを転送テーブルに追加し、クライアントSGTに基づいてISEからポリシーを取得します。

4. クライアントがDHCP要求を開始します。

5. APでは、L2 VNI情報を使用してVXLANにカプセル化します。

6. ファブリックエッジは、L2 VNIDをVLANインターフェイスにマッピングし、DHCPをオーバーレイで転送します（有線ファブリッククライアントと同じ）。

7. クライアントがDHCPからIPアドレスを受け取る。

8. DHCPスヌーピング（スタティックの場合はARP）は、ファブリックエッジによるCPへのクライアントEID登録をトリガーします。

debug/showコマンドを使用すると、クライアントオンボードワークフローを確認および検証できます。

コントロール プレーン

debug lisp control-plane all（すべてのLISPコントロールプレーンをデバッグ）

エッジスイッチ

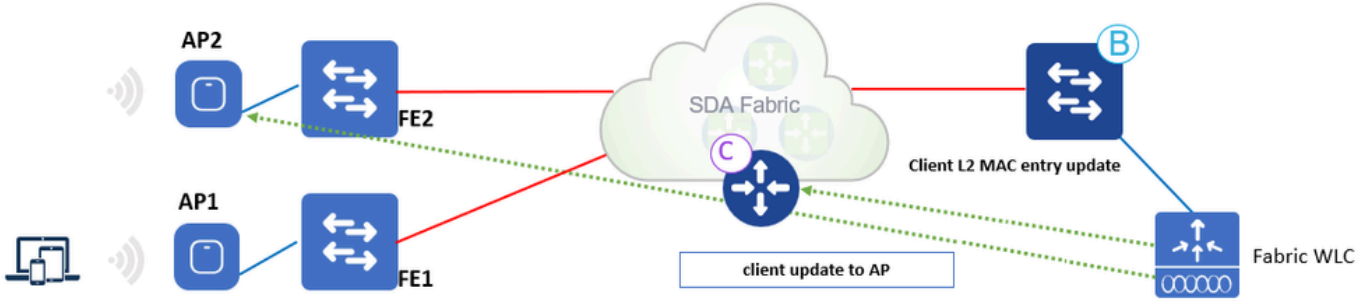
debug lisp control-plane all（すべてのLISPコントロールプレーンをデバッグ）

debug ip dhcp snooping packet/event（登録ユーザ専用）

WLC

LISP通信の場合、AP加入と同じデバッグです。

クライアントのローミング



クライアントローミングのワークフロー：

1. クライアントはFE2上のAP2にローミングします（スイッチ間ローミング）。 WLCはAPから通知を受け取ります。

2. WLCはクライアント情報(SGT、RLOC)を使用してAPの転送テーブルを更新します。

3. WLCが新しいRLOCファブリックエッジ2でCPのL2 MACエントリを更新します。

4. CPは次のように通知します。

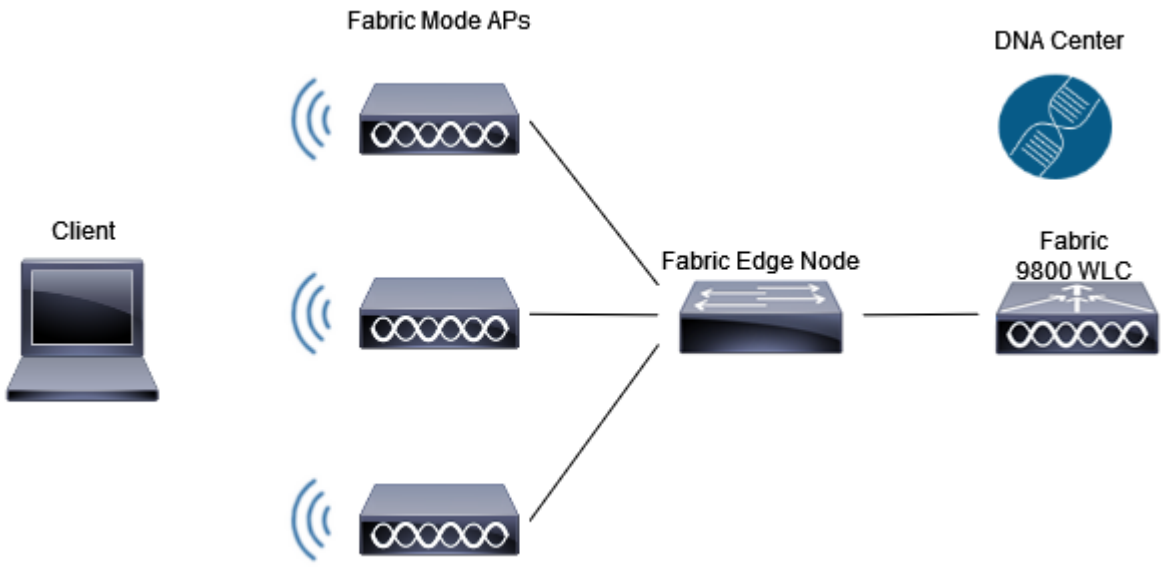
- VXLANトンネルを指す転送テーブルにクライアントMACを追加するファブリックエッジFE2（スイッチへのローミング）。
- ファブリックエッジFE1（ローミング元のスイッチ）：ワイヤレスクライアントのクリーンアップを実行します。

5. ファブリックエッジは、トラフィックを受信すると、CPデータベース内のL3エントリ(IP)を更新します。

6. ファブリックエッジ2は同じVLANインターフェイスを持つため（エニーキャストゲートウェイ）、ローミングはレイヤ2です。

設定

ネットワーク図



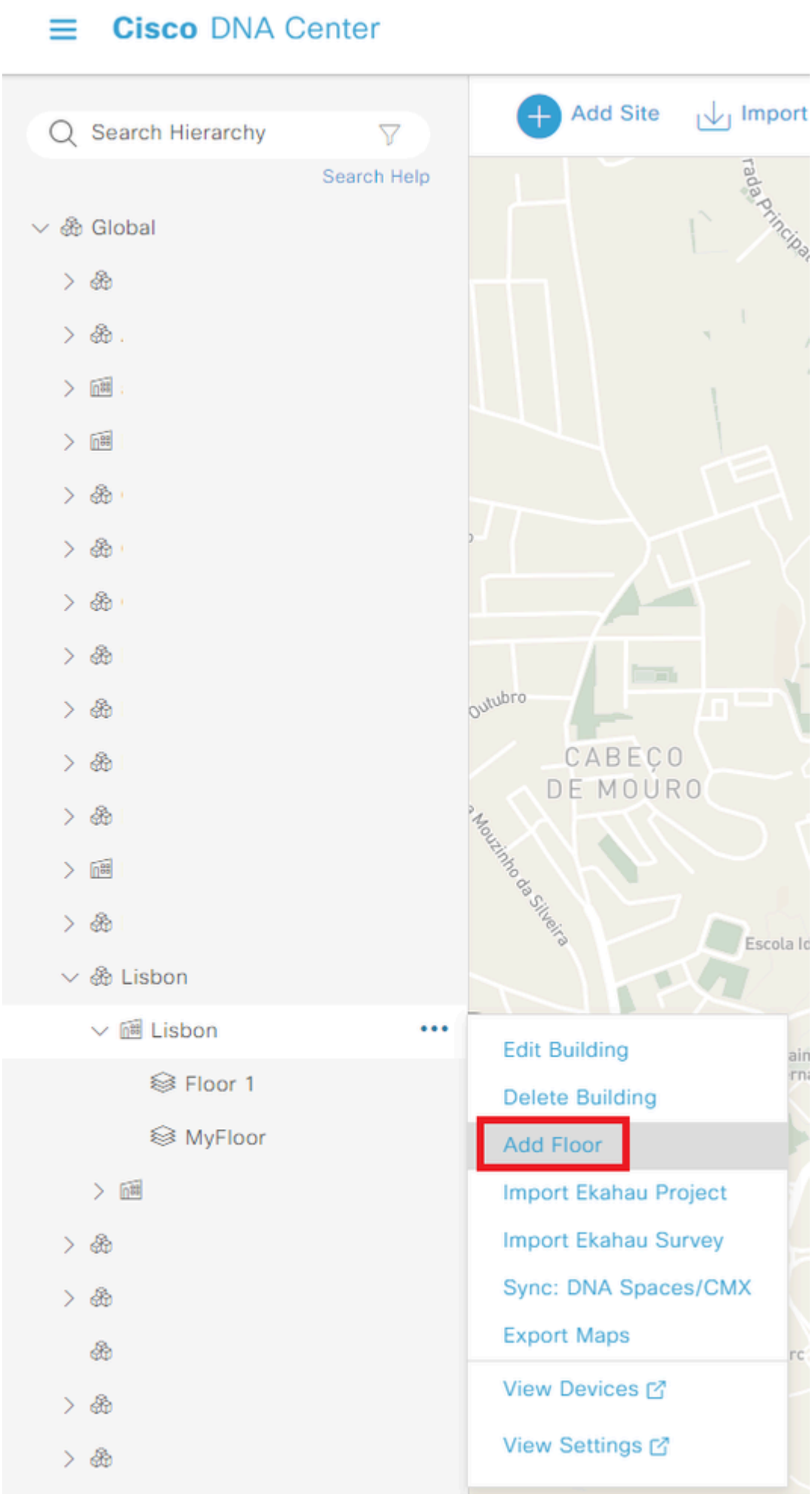
ネットワーク図

Cisco DNAにおけるWLCの検出とプロビジョニング

WLCの追加

ステップ 1：WLCを追加する場所に移動します。新しい建物/床を追加できます。

Design > Network Hierarchy に移動し、building/floorと入力するか、図に示すように新しいフロアを作成します。



新しいフロアの作成

ステップ 2：floorを追加します。また、床の植物の画像をアップロードすることもできます

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。