ソフトウェア定義アクセスでのIPv6の実装

内容

はじめに

このドキュメントでは、Cisco® Software-Defined Access(SD-Access)にIPv6を実装する方法について説明します。

背景説明

IPv4は1983年にリリースされ、現在でもインターネットトラフィックの大部分に使用されています。32ビットのIPv4アドレッシングでは、40億を超える一意の組み合わせが可能でした。ただし、インターネットに接続するクライアントの数が増加したため、一意のIPv4アドレスが不足しています。1990年代には、IPv4アドレッシングの枯渇は避けられないものになりました。
これを見越して、Internet Engineering Taskforce(IETF)はIPv6標準を導入しました。IPv6は128ビットを使用し、340澗（アンデシリオン）個の一意のIPアドレスを提供します。これは、拡大する接続デバイスのニーズに対応するのに十分な数です。デュアルスタックや単一のIPv6スタックをサポートするエンドポイントデバイスが増え続けているため、どのような組織でもIPv6の導入に備えることが重要です。つまり、インフラストラクチャ全体がIPv6に対応する準備ができている必要があります。Cisco SD-Accessは、従来のキャンパス設計から、組織の目的を直接実装するネットワークへと進化したものです。Cisco Software Defined Networks(SDN)は、デュアルスタック（IPv6デバイス）をオンボーディングする準備が整いました。

IPv6の導入に関する組織の主な課題は、従来のIPv4システムからIPv6への移行に伴う変更管理と複雑さです。このホワイトペーパーでは、Cisco SDNでのIPv6機能のサポート、戦略、および重要な穴埋めスポットについて詳しく説明します。これらは、Cisco Software Defined NetworkでIPv6を導入する際に対処する必要があります。

2019年8月、IPv6のサポートにより、Cisco Digital Network Architecture(DNA)Centerバージョン1.3が初めて導入されました。このリリースでは、Cisco SD-Accessキャンパスネットワークは、オーバーレイファブリックネットワークからのIPv4、IPv6、またはIPv4v6デュアルスタックの有線およびワイヤレスクライアントでホストIPアドレスをサポートしました。このソリューションは、あらゆる企業のIPv6を簡単にオンボーディングできる新機能を実現するために、継続的に進化するものです。

Cisco SD-Access with IPv6アーキテクチャ

SD-Accessに不可欠なファブリックテクノロジーは、設計の目的に合わせて、物理ネットワークで1つ以上の論理ネットワークをホストできる、プログラム可能なオーバーレイと簡単に導入できるネットワーク仮想化を有線およびワイヤレスキャンパスネットワークに提供します。ネットワークの仮想化に加え、キャンパスネットワークのファブリックテクノロジーによって通信の制御が強化され、ユーザIDとグループメンバーシップに基づいたソフトウェア定義のセグメント化とポリシー適用が可能になります。Cisco SDNソリューション全体は、ファブリックのDNA上で動作します。したがって、IPv6のサポートに関して、ソリューションの各柱を理解することが重要です。

- アンダーレイ：IPv6オーバーレイはIPv4アンダーレイIPアドレッシングを使用して、Locator/ID Separation Protocol(LISP)コントロールプレーンと仮想拡張LAN(VXLAN)データプレーントンネルを作成するため、オーバーレイのIPv6機能はアンダーレイに依存しています。アンダーレイルーティングプロトコルのデュアルスタックはいつでも有効にできます。SD-AccessオーバーレイLISPだけがIPv4ルーティングに依存します。
- オーバーレイ：オーバーレイに関して、SD-AccessはIPv6のみの有線エンドポイントとワイヤレスエンドポイントの両方をサポートします。そのIPv6トラフィックは、ファブリックボーダーノードに到達するまで、SDアクセスファブリック内でIPv4およびVXLANヘッダーにカプセル化されます。ファブリック境界ノードはIPv4およびVXLANヘッダーをカプセル化解除し、そこから通常のIPv6ユニキャストルーティングプロセスを実行します。
- コントロールプレーンノード：コントロールプレーンノードは、サブネット範囲内のすべてのIPv6ホストサブネットと/128ホストルートをマッピングデータベースに登録できるように設定されます。
- ボーダーノード：ボーダーノードで、FusionデバイスとのIPv6 BGPピアリングが有効になっています。ボーダーノードはファブリックの出力トラフィックからIPv4ヘッダーをカプセル化解除しますが、入力IPv6トラフィックもボーダーノードによってIPv4ヘッダーでカプセル化されます。
- ファブリックエッジ：ファブリックエッジに設定されているすべてのスイッチ仮想インターフェイス(SVI)は、IPv6である必要があります。この設定は、DNA Center Controllerによってプッシュされます。
- Cisco DNA Center：このドキュメントの公開時点では、Cisco DNA Centerの物理インターフェイスはデュアルスタックをサポートしていません。DNA Centerの管理インターフェイ

スまたはエンタープライズインターフェイスにのみ、IPv4またはIPv6のいずれかを使用して1つのスタックに導入できます。

- クライアント：Cisco SD-Accessは、デュアルスタック（IPv4およびIPv6）またはシングルスタック（IPv4またはIPv6）をサポートします。ただし、IPv6シングルスタックを導入する場合でも、DNA Centerはデュアルスタックプールを作成してIPv6専用クライアントをサポートする必要があります。デュアルスタックプール内のIPv4は、クライアントがIPv4アドレスを無効にするIPv6として期待されるため、ダミーアドレスのみです。

シスコのソフトウェア定義型アクセスにおけるIPv6オーバーレイアーキテクチャ

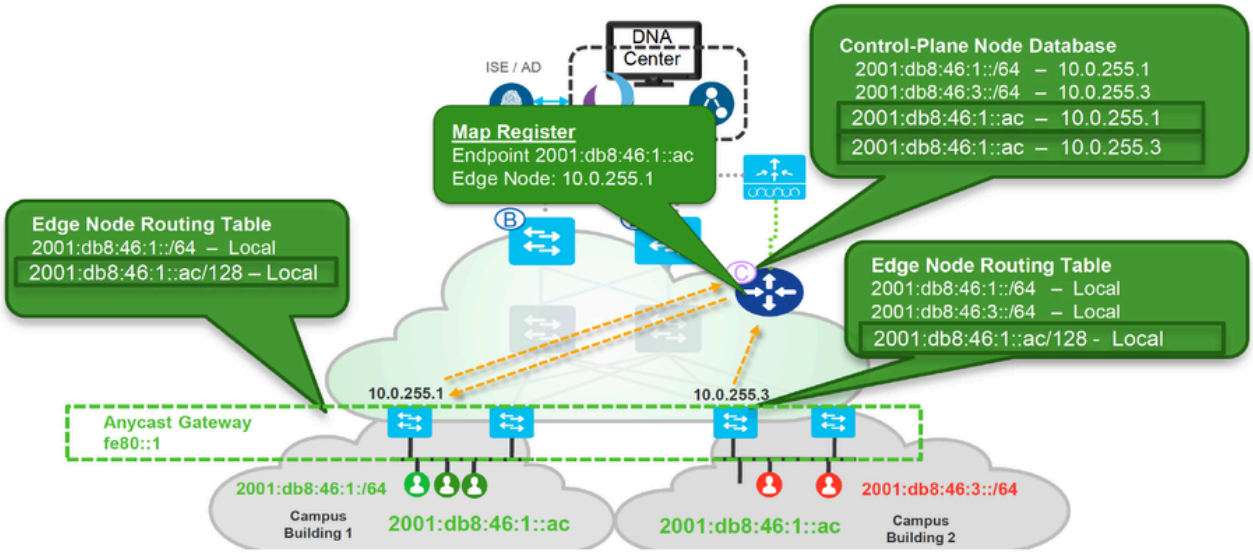


Figure 1.
IPv6 Overlay Architecture in Cisco Software Defined Access

IPv6オーバーレイアーキテクチャ

Cisco DNA-CenterによるIPv6の有効化

Cisco DNA CenterでIPv6プールを有効にするには、次の2つの方法があります。
1. 新しいデュアルスタックIPv4/v6プールを作成する：新規開拓
2. 既存のIPv4プールでIPv6を編集する – 既存環境への移行

DNA Centerの現在のリリース（最大2.3.x）はIPv6をサポートしていません。プールのみ（ユーザが単一/ネイティブのIPv6アドレス専用クライアントをサポートする予定の場合）ダミーのIPv4アドレスをIPv6プールに関連付ける必要があります。配置済みのIPv4プールのうち、関連付けられたサイトにすでに存在するものから、IPv6アドレスを持つプールを編集します。DNA Centerは、SDアクセスファブリックの移行オプションを提供します。このオプションでは、ユーザがそのサイトのファブリックを再プロビジョニングする必要があります。サイトが属するファブリックに警告インジケータが表示され、ファブリックで「ファブリックの再構成」が必要であることを示します。サンプルについては、次の図を参照してください。

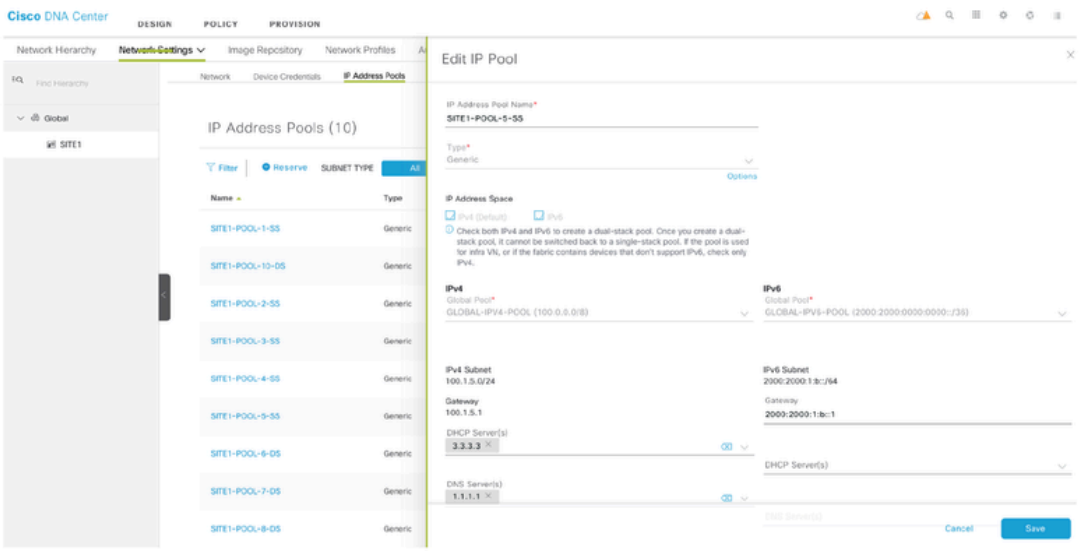


Figure 2.
Single IPv4 upgrade to Dual-Stack pool by edit existing IPv4 pool option

IPv4プールオプションの編集によるデュアルスタックプールへの単一IPv4プールアップグレード

Pool upgrade: Warning on fabric page

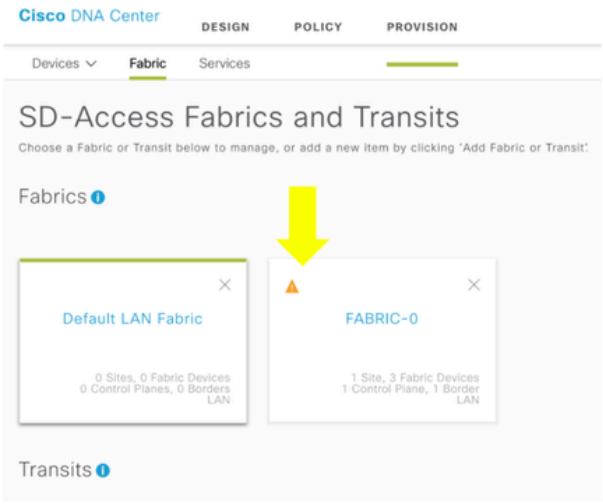


Figure 3.
Fabric has warning indicator which needs to 'reconfigure the fabric'

ファブリックには、「ファブリックの再構成」が必要な警告インジケータがあります。

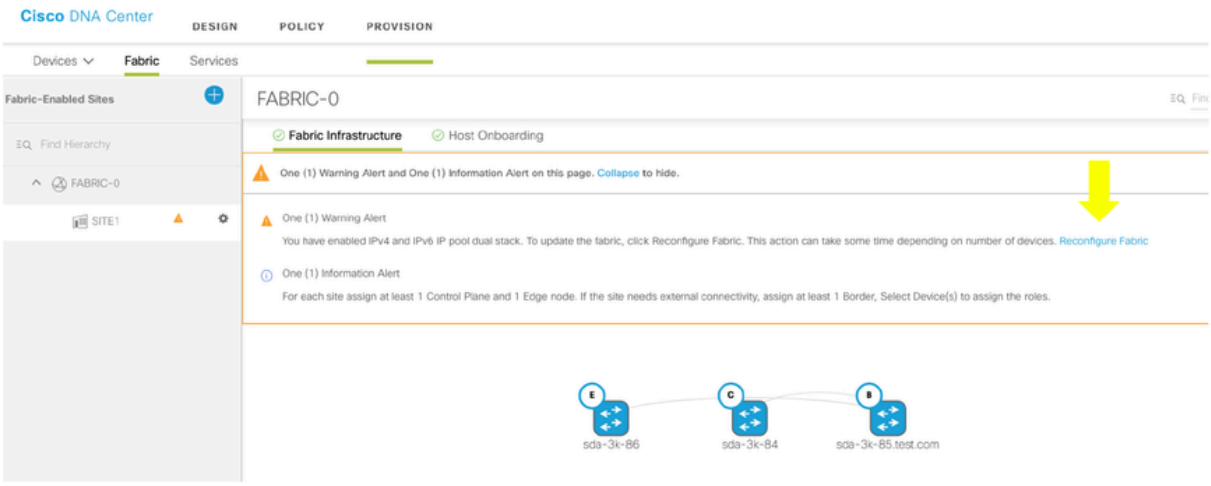


Figure 4.
User needs to click on 'reconfigure Fabric' to auto-reprovision the fabric nodes for the dual-stack information to take effect for the migration.

移行プロセスの一部としてデュアルスタック構成を有効にするには、「ファブリックの再構成」をクリックしてファブリックノードを自動的に再プロビジョニングする必要がある

Cisco SD-AccessにおけるIPv6の設計上の考慮事項

Cisco SD-Accessクライアントは、デュアルスタックまたはIPv6のみのネットワーク設定で実行できますが、DNA Center Switch(SW)バージョン2.3.x.xまでの現行のSD-Accessファブリック実装には、IPv6の導入に関する考慮事項がいくつかあります。

- Cisco SD-Accessは、IPv4アンダーレイルーティングプロトコルをサポートします。したがって、IPv6クライアントトラフィックは、IPv4ヘッダー内にカプセル化されたときに転送されます。これは、現在のLISPソフトウェアの導入に必要です。ただし、アンダーレイがIPv6ルーティングプロトコルを有効にできないという意味ではありません。SD-Accessオーバーレイ LISPだけが依存して実行されることはありません。
- ファブリックアンダーレイは現在IPv4のみであるため、IPv6ネイティブマルチキャストはサポートされていません。
- ゲストワイヤレスは、デュアルスタックでのみ実行できます。現在のIdentity Services Engine(ISE)リリース（3.2までなど）のため、IPv6ゲストポータルはサポートされていません。そのため、IPv6専用ゲストクライアントは認証されません。
- IPv6アプリケーションQoSポリシーの自動化は、現在のDNA Centerリリースではサポートされていません。このドキュメントでは、大規模なユーザの1つに導入されたCisco SD-Accessの有線およびワイヤレスデュアルスタッククライアントにIPv6 QoSを実装するために必要な手順について説明します。
- Service Set Identifier(SSID)またはポリシーに基づくクライアント単位のダウンストリームトラフィックおよびアップストリームトラフィックに対するワイヤレスクライアントレート制限機能は、IPv4(TCP/UDP)およびIPv6（TCPのみ）でサポートされています。 IPv6

UDPレート制限はまだサポートされていません。
- IPv4プールは、デュアルスタックプールにアップグレードできます。ただし、デュアルスタックプールをIPv4プールにダウングレードすることはできません。デュアルスタックプールを削除してIPv4シングルスタックプールに戻す場合は、デュアルスタックプール全体を解放する必要があります。
- 現在のDNA CenterではIPv4またはデュアルスタックプールしか作成できませんが、単一のIPv6はまだサポートされていません。
- Cisco IOS® XEのプラットフォームは、16.9.2以降の最小ソフトウェアバージョン要件です。
- IPv6ゲストワイヤレスはCisco IOS XEプラットフォームではまだサポートされていませんが、AireOS(8.10.105.0+)では回避策がサポートされています。
- アクセスポイント(AP)または拡張ノードプールだけを割り当てることができるINFRA_VNでは、デュアルスタックプールを割り当てることはできません。
- LANの自動化は、まだIPv6をサポートしていません。

前述の制限に加えて、SD-AccessファブリックをIPv6対応で設計する際は、各ファブリックコンポーネントの拡張性を常に念頭に置く必要があります。 エンドポイントに複数のIPv4またはIPv6アドレスがある場合、各アドレスは個別のエントリとしてカウントされます。

ファブリックホストのエントリには、アクセスポイントと、従来のノードおよびポリシーで拡張されたノードが含まれます。

ボーダーノードのスケールに関するその他の考慮事項：

/32(IPv4)または/128(IPv6)エントリは、ボーダーノードがファブリックの外部からファブリック内のホストにトラフィックを転送するときに使用されます。

Cisco Catalyst 9500シリーズハイパフォーマンススイッチおよびCisco Catalyst 9600シリーズスイッチを除くすべてのスイッチ：

- IPv4では、すべてのIPv4 IPアドレスに対して1つのTernary Content Addressable Memory(TCAM)エントリ（ファブリックホストエントリ）が使用されます。
- IPv6では、各IPv6 IPアドレスに対して2つのTCAMエントリ（ファブリックホストエントリ）が使用されます。

Cisco Catalyst 9500シリーズハイパフォーマンススイッチおよびCisco Catalyst 9600シリーズスイッチの場合：

- IPv4では、IPv4 IPアドレスごとに1つのTCAMエントリ（ファブリックホストエントリ）が使用されます。
- IPv6では、IPv6 IPアドレスごとに1つのTCAMエントリ（ファブリックホストエントリ）が使用されます。

また、IPv6アドレスの取得にステートレスアドレス自動設定(SLAAC)を使用するAndroid OSベースのスマートフォンなど、一部のエンドポイントはDHCPv6をサポートしていません。1つのエンドポイントが2つ以上のIPv6アドレスで終わる可能性があります。この動作により、各ファブリックノード、特にファブリックボーダーノードとコントロールノードで、より多くのハードウェア

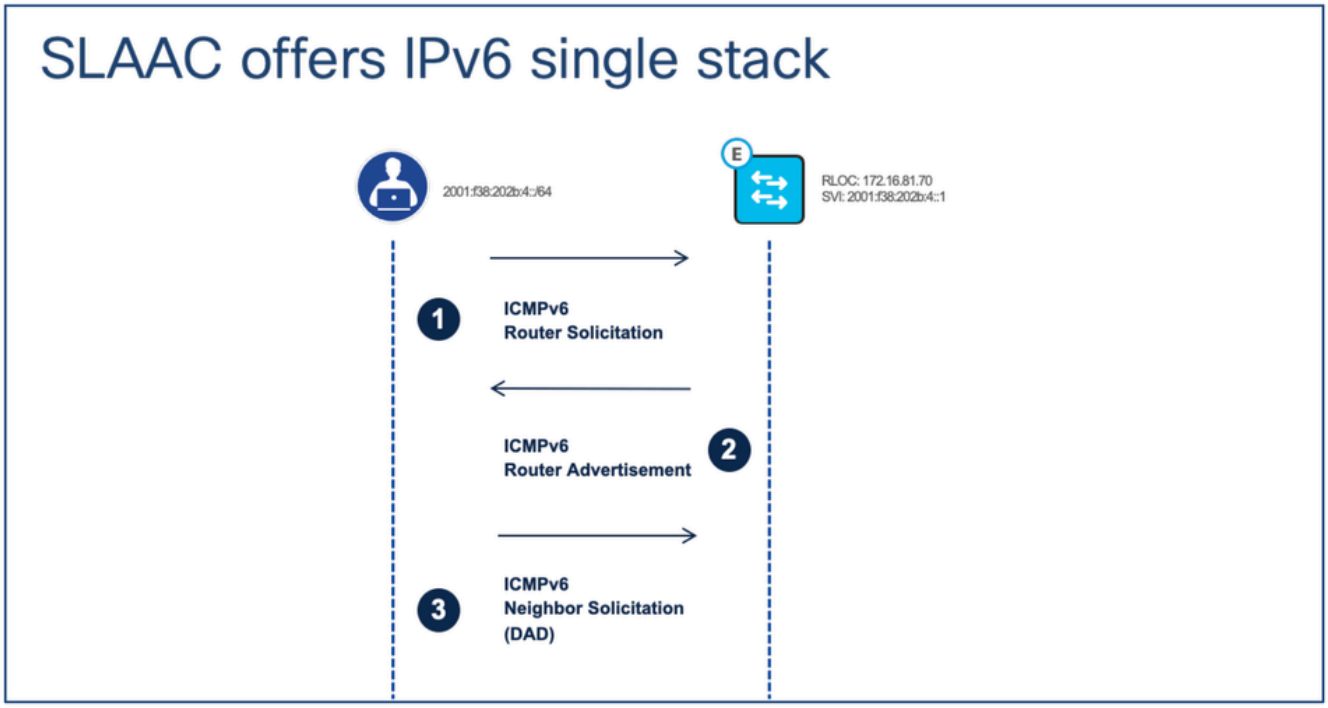
リソースが消費されます。たとえば、境界ノードが任意のエンドポイントのエッジノードにトラフィックを送信しようとするたびに、ホストルートがTCAMエントリにインストールされ、ハードウェア(HW)TCAMのVXLAN隣接関係エントリが書き込まれます。

有線およびワイヤレスクライアントの接続とコールフロー

クライアントをファブリックエッジに接続すると、さまざまな方法でIPv6アドレスを取得できます。このセクションでは、クライアントIPv6アドレッシングの最も一般的な方法であるSLAACおよびDHCPv6について説明します。

IPv6アドレスの割り当て – SLAAC

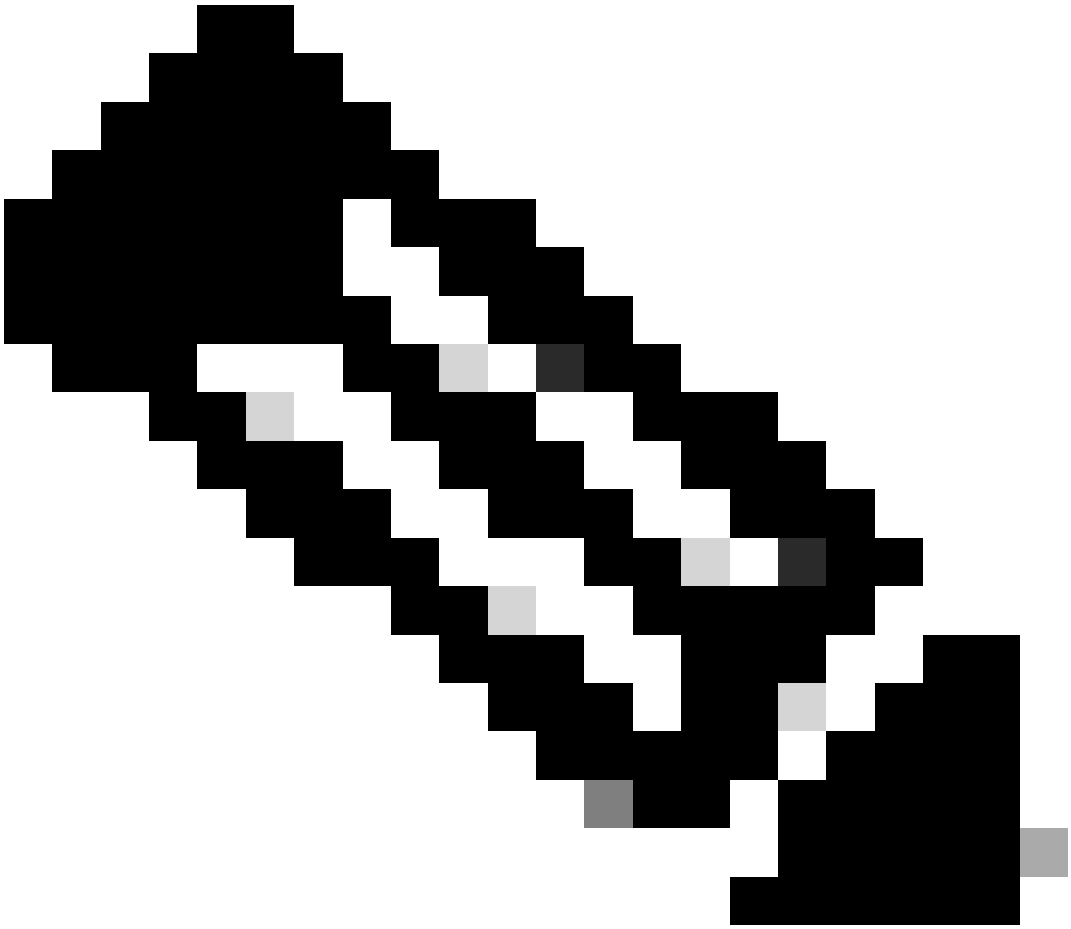
ソフトウェア定義アクセス(SDA)のSLAACは、標準のSLAACプロセスフローと異なりません。SLAACが適切に機能するためには、IPv6クライアントのインターフェイスにリンクローカルアドレスを設定する必要があります。クライアントがリンクローカルアドレスを使用して自動的に自身を設定する方法については、このドキュメントでは説明しません。



IPv6アドレスの割り当て – SLAAC

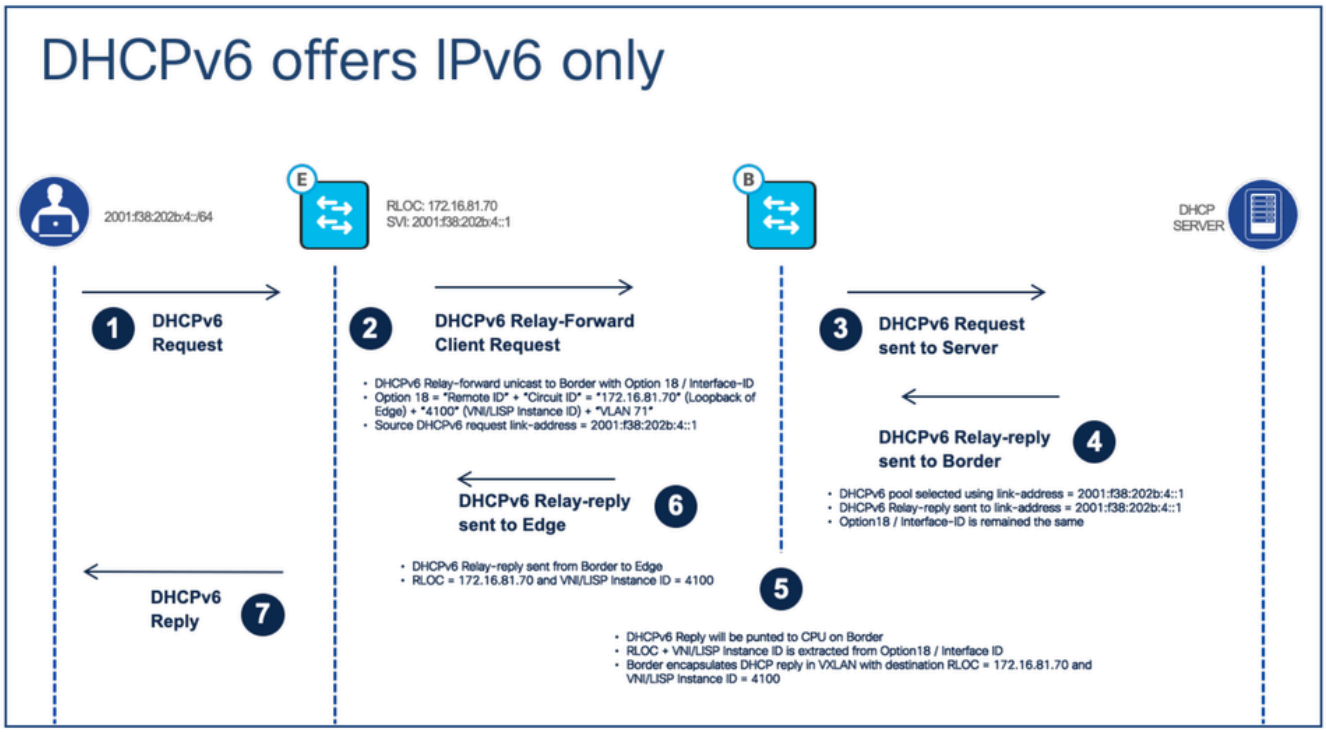
コールフローの説明：
ステップ 1：IPv6クライアントがIPv6リンクローカルアドレスを使用して自身を設定した後、クライアントはICMPv6ルータ要求(RS)メッセージをファブリックエッジに送信します。このメッセージの目的は、接続セグメントのグローバルユニキャストプレフィクスを取得することです。
ステップ 2：ファブリックエッジは、RSメッセージを受信すると、ICMPv6ルータアドバタイズメント(RA)メッセージで応答します。このメッセージには、グローバルIPv6ユニキャストプレフィックスとその長さが含まれています。
ステップ 3：クライアントはRAメッセージを受け取ると、一意のIPv6グローバルユニキャストアドレスを生成し、クライアントのセグメントに関連するファブリックエッジのSVIのリンクロー

カルアドレスにゲートウェイを設定するために、IPv6グローバルユニキャストプレフィックスとEUI-64インターフェイス識別子を組み合わせます。次に、クライアントはICMPv6ネイバー送信要求メッセージを送信して、重複アドレス検出(DAD)を実行し、取得するIPv6アドレスが一意であることを確認します。



注:SLAAC関連のすべてのメッセージは、クライアントおよびファブリックノードのSVIのIPv6リンクローカルアドレスでカプセル化されます。

IPv6アドレスの割り当て：DHCPv6

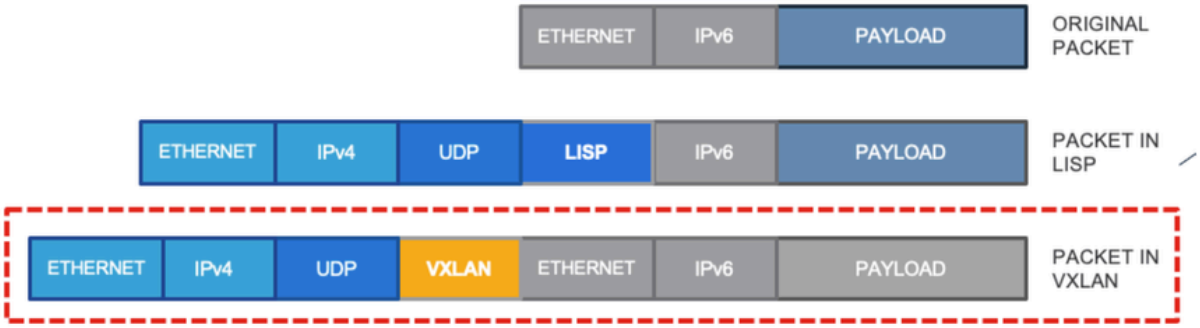


IPv6アドレスの割り当て：DHCPv6

コールフローの説明：
ステップ 1：クライアントはDHCPv6要求をファブリックエッジに送信します。
ステップ 2：ファブリックエッジがDHCPv6要求を受信すると、DHCPv6リレー転送メッセージを使用して、DHCPv6オプション18でファブリックボーダーに要求をユニキャストします。DHCPオプション82と比較すると、DHCPv6 Option 18は「回線ID」と「リモートID」の両方を同時にエンコードします。LISPインスタンスID/VNI、IPv4ルーティングロケータ(RLOC)、およびエンドポイントVLANは、内部でエンコードされます。
ステップ 3：ファブリックボーダーはVXLANヘッダーをカプセル化解除し、DHCPv6パケットをDHCPv6サーバにユニキャストします。
ステップ 4：DHCPv6サーバはリレー転送メッセージを受信し、メッセージの送信元リンクアドレス（DHCPv6リレーエージェント/クライアントゲートウェイ）を使用して、IPv6アドレスを割り当てるためにIPv6 IPプールを選択します。次に、DHCPv6リレー応答メッセージをクライアントゲートウェイアドレスに返信します。オプション18は変更されません。
ステップ 5：ファブリックボーダーは、リレー応答メッセージを受信すると、オプション18からRLOCおよびLISPインスタンス/VNIを抽出します。ファブリックボーダーは、オプション18から抽出した宛先を使用して、VXLANのリレー応答メッセージをカプセル化します。
手順 6：ファブリックボーダーは、クライアントが接続するファブリックエッジにDHCPv6リレー応答メッセージを送信します。
手順 7：ファブリックエッジがDHCPv6リレー応答メッセージを受信すると、メッセージのVXLANヘッダーのカプセル化を解除して、メッセージをクライアントに転送します。これにより、クライアントは割り当てられたIPv6アドレスを認識します。

Cisco SD-AccessでのIPv6通信

IPv6通信は、標準のLISPベースのコントロールプレーンとVXLANベースのデータプレーンの通信方法を使用します。Cisco SD-Access LISPおよびVXLANの現在の実装では、外部IPv4ヘッダーを使用して内部にIPv6パケットを伝送します。次の図に、このプロセスを示します。



IPv6パケットを内部に搬送する外部IPv4ヘッダー

つまり、すべてのLISPクエリはIPv4ネイティブパケットを使用しますが、コントロールプレーンノードテーブルには、エンドポイントのIPv6とIPv4の両方のIPアドレスを持つRLOCの詳細が含まれます。このプロセスは、次のセクションでワイヤレスエンドポイントの観点から詳しく説明します。

Cisco SD-Accessのワイヤレス IPv6通信

ワイヤレス通信は、一般的なCisco SDアクセスファブリックコンポーネントとは別に、アクセスポイントとワイヤレスLANコントローラという2つの特定のコンポーネントに依存します。ワイヤレスアクセスポイント(AP)は、ワイヤレスLANコントローラ(WLC)を使用して、Control and Provisioning of Wireless Access Points(CAPWAP)トンネルを作成します。 クライアントトラフィックがファブリックエッジに存在する間、無線統計情報を含むその他のコントロールプレーン通信はWLCによって管理されます。IPv6の観点からは、WLCとAPの両方にIPv4アドレスが必要で、すべてのCAPWAP通信はこれらのIPv4アドレスを使用します。非ファブリックWLCおよびAPはIPv6通信をサポートしますが、Cisco SD-Accessは、IPv4パケット内のクライアントIPv6トラフィックを伝送するすべての通信にIPv4を使用します。つまり、Infra VNの下で割り当てられたAPプールは、デュアルスタックのIPプールではマッピングできず、このマッピングを試みるとエラーがスローされます。Cisco SDA内のワイヤレス通信は、次の主要なタスクに分類できます。

- アクセスポイントオンボーディング
- クライアントオンボーディング

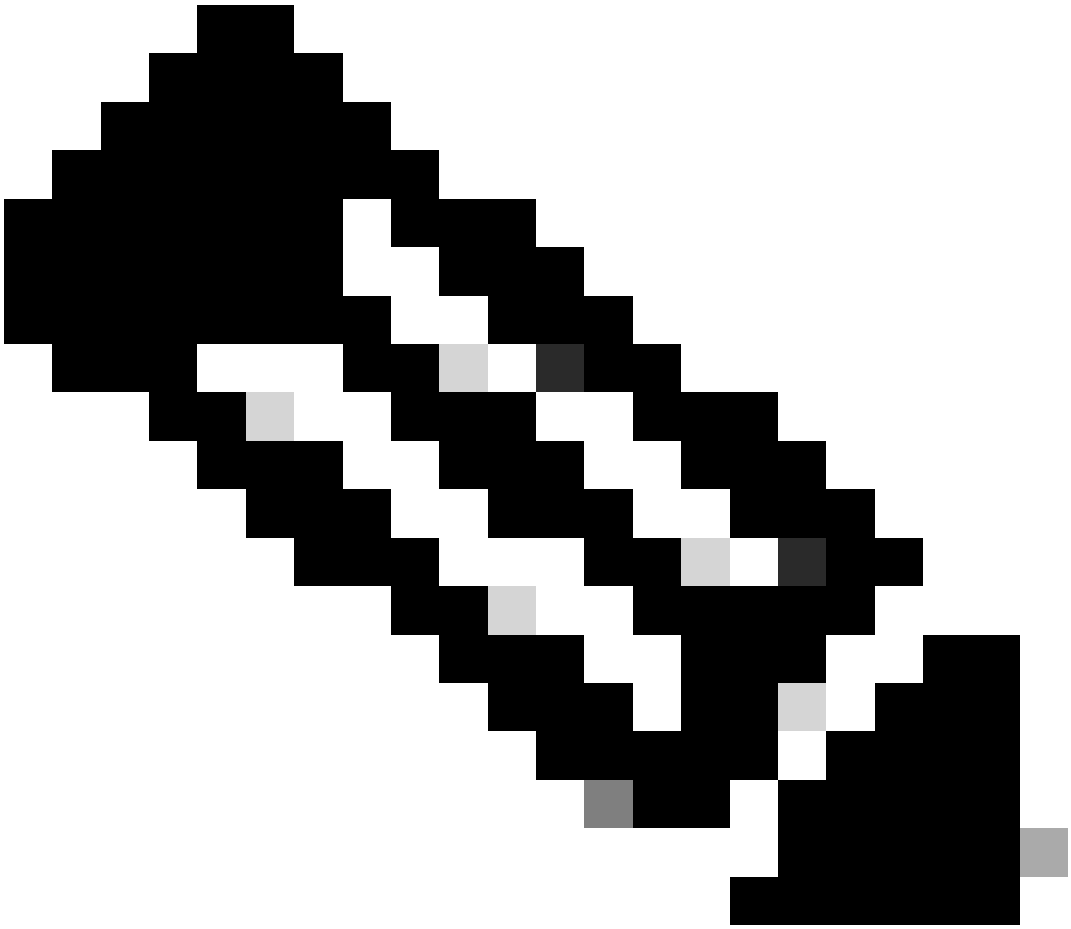
IPv6の観点からこれらのイベントを見てみましょう。

アクセスポイントオンボーディング

WLCとAPの両方にIPv4アドレスと手順が含まれているため、このプロセスはIPv6とIPv4で同じです。

1. ファブリックエッジ(FE)ポートがAPをオンボードするように設定されている。
2. APはFEポートに接続し、CDP AP経由でFEにその存在を通知します（これにより、FEは正しいVLANを割り当てることができます）。
3. APはDHCPサーバからIPv4アドレスを取得し、FEはAPを登録し、コントロールプレーン(コントロールプレーン(CP)ノード)をAPの詳細で更新します。
4. APは従来の方法（DHCPオプション43など）でWLCに参加します。
5. WLCは、APがファブリック対応かどうかを確認し、AP RLOC情報（たとえば、RLOC Requested/Response Received）をコントロールプレーンに照会します。
6. CPがAPのRLOC IPを使用してWLCに応答します。
7. WLCがAPメディアアクセス制御（アドレス）(MAC)をCPに登録します。
8. CPは、APに関するWLCからの詳細情報でFEを更新します（これにより、FEはAPとのVXLANトンネルを開始します）。

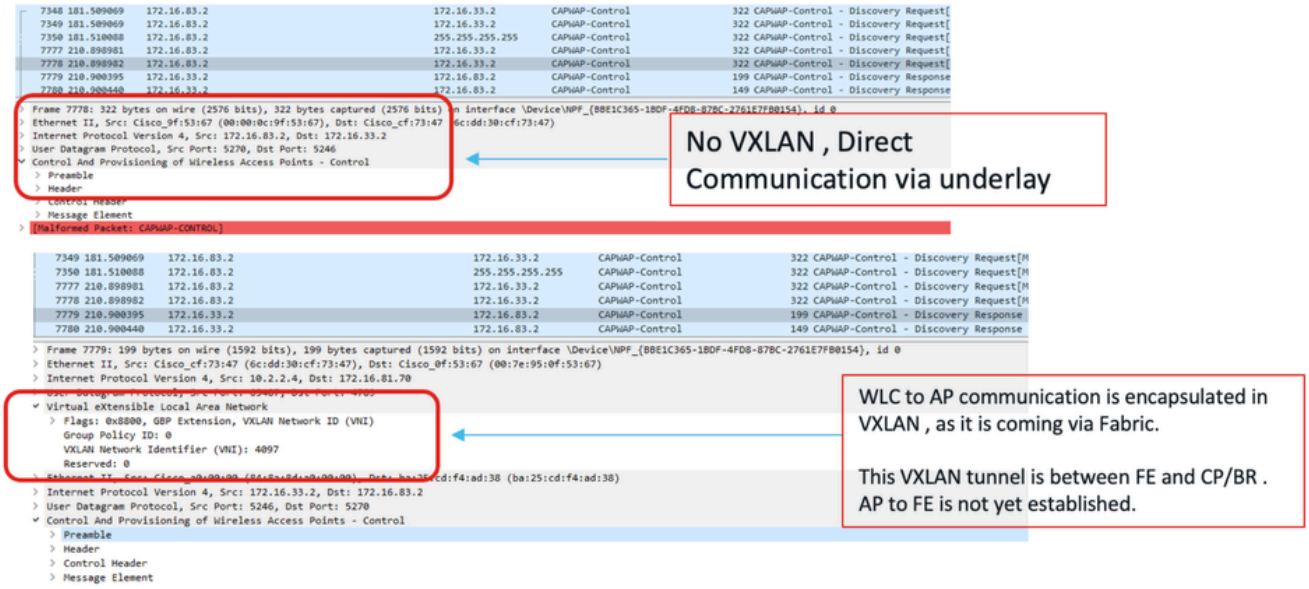
FEは情報を処理し、APとのVXLANトンネルを作成します。この時点で、APはファブリック対応SSIDをアドバタイズします。



注:APが非ファブリックSSIDをブロードキャストし、ファブリックSSIDをブロードキャストしない場合は、アクセスポイントとファブリックエッジノード間のVXLANトンネル

を確認してください。

また、APからWLCへの通信は常にアンダーレイCAPWAP経由で行われ、すべてのWLCからAPへの通信はオーバーレイ経由でVXLAN CAPWAPを使用することに注意してください。つまり、APからWLCに送信されるパケットをキャプチャする場合、CAPWAPが表示されるのは逆トラフィックにVXLANトンネルがある場合だけです。APとWLC間の通信については、次の例を参照してください。



APからWLCへのパケットキャプチャ（CAPWAPトンネル）とWLCからAPへのパケットキャプチャ（ファブリック内のVxLANトンネル）

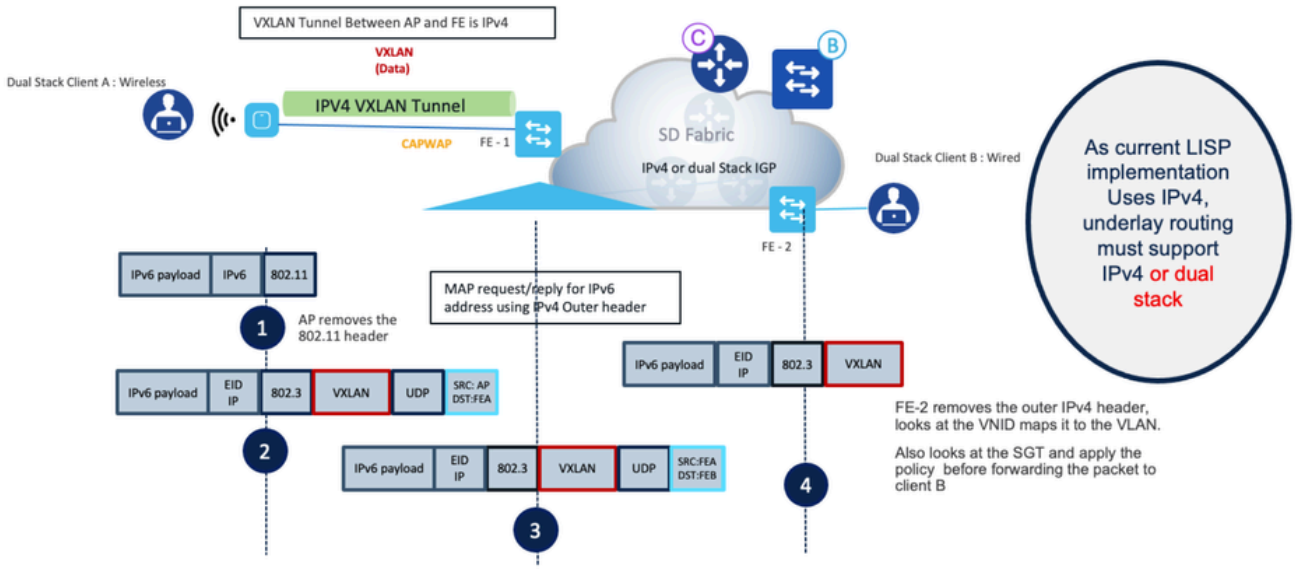
クライアントオンボーディング

デュアルスタック/IPv6クライアントのオンボーディングプロセスは同じですが、クライアントはSLAAC/DHCPv6などのIPv6アドレス割り当て方法を使用してIPv6アドレスを取得します。
1. クライアントがファブリックに参加し、APでSSIDを有効にします。
2. WLCはAPのRLOCを認識しています。
3. クライアントが認証し、WLCがクライアントL2の詳細をCPに登録して、APを更新します。
4. クライアントが、設定された方式(SLAAC/DHCPv6)からIPv6アドレス指定を開始します。
5. FEは、CP Host Tracking Database(HTDB)へのIPv6クライアント登録をトリガーします。
APからFE、およびFEから他の宛先は、VXLANおよびLISPのIPv6カプセル化をIPv4フレーム内で使用します。

IPv6を使用したクライアント間通信

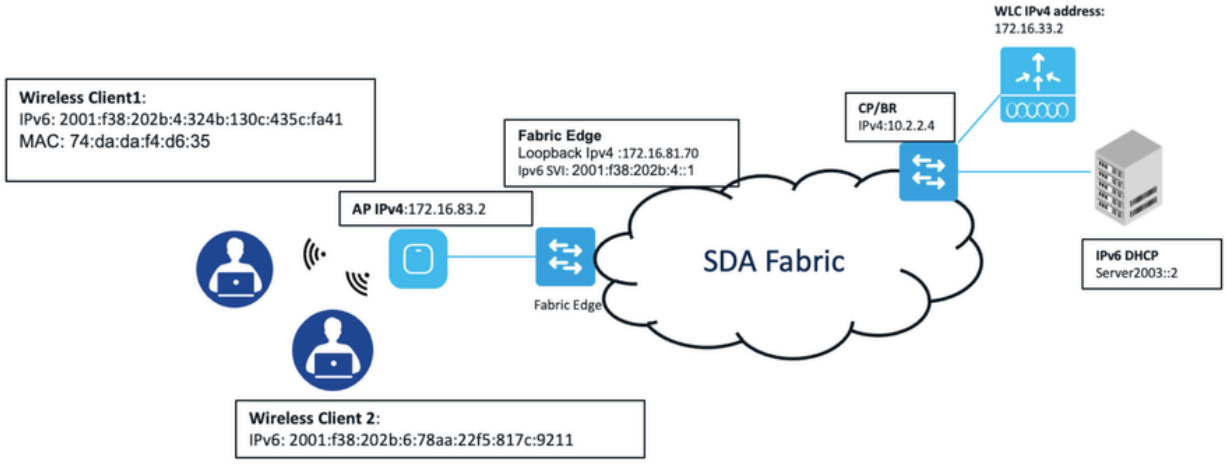
次の図は、別のIPv6有線クライアントとのIPv6ワイヤレスクライアント通信プロセスをまとめたものです。（これは、クライアントが認証され、設定された方法でIPv6アドレスを取得すること

を前提としています）。
1. クライアントはAPにIPv6ペイロードで802.11フレームを送信します。
2. APは802.11ヘッダーを削除し、IPv4 VXANトンネル内の元のIPv6ペイロードをファブリックエッジに送信します。
3. ファブリックエッジは、メッセージアクセスプロトコル(MAP)要求を使用して宛先を識別し、IPv4 VXLANを使用して宛先RLOCにフレームを送信します。
4. 宛先スイッチでは、IPv4 VXLANヘッダーが削除され、IPv6パケットがクライアントに送信されます。

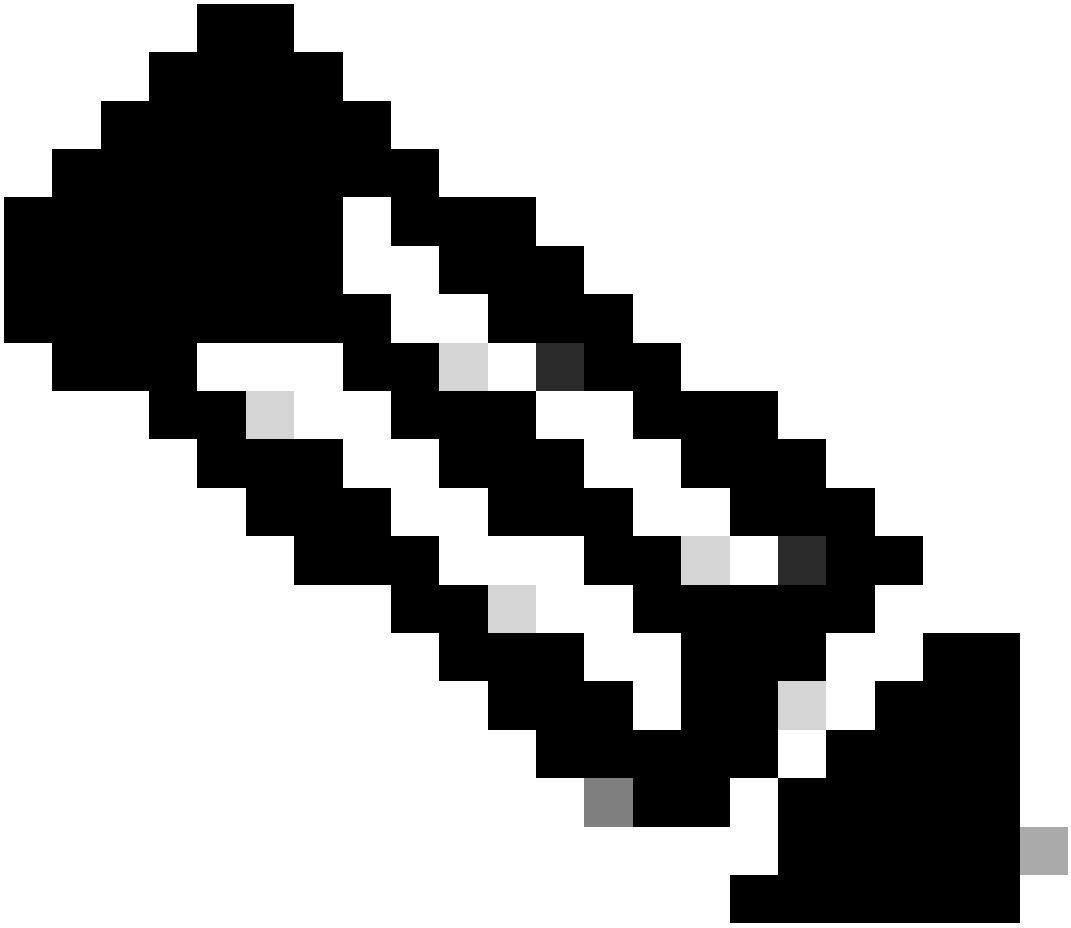


デュアルスタック無線クライアントからデュアルスタック有線クライアントへのパケットフロー

パケットキャプチャを使用してこのプロセスを詳しく調べ、IPアドレスとMACアドレスの詳細については図を参照してください。この設定では、同じアクセスポイントに接続されたデュアルスタッククライアントの両方を使用しますが、異なるIPv6サブネット(SSID)でマッピングされることに注意してください。

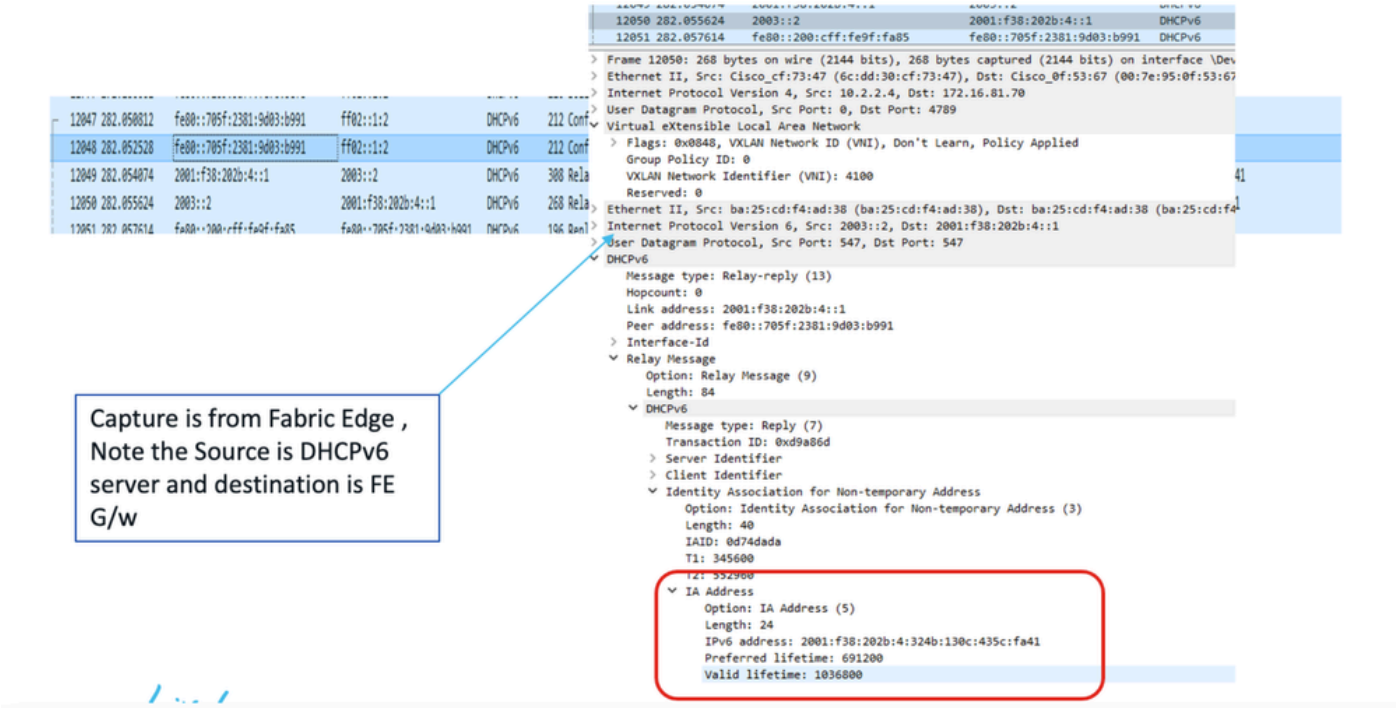


サンプルSDアクセスファブリックネットワークのIPアドレスとMACアドレスの詳細



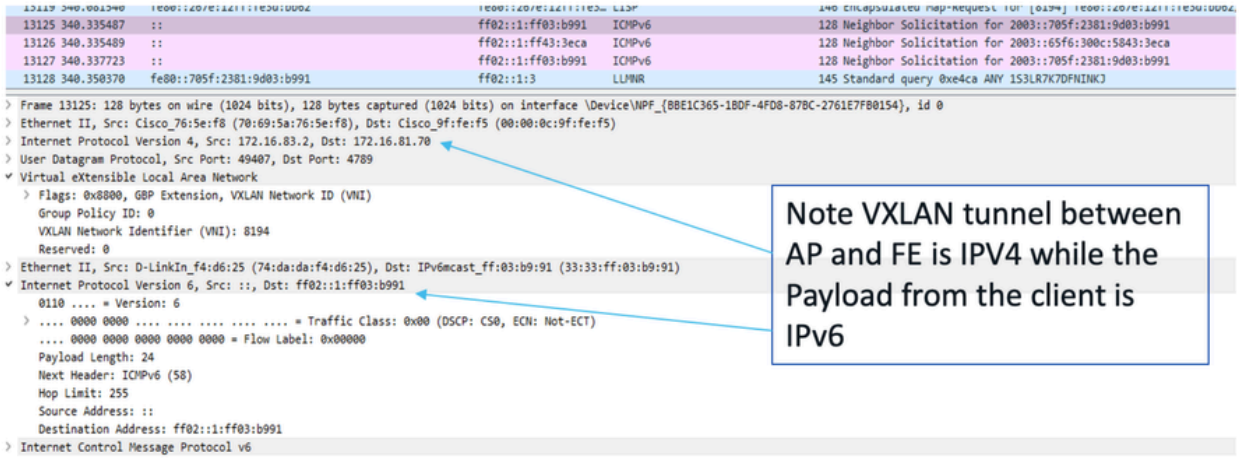
注:DHCP/DNSなど、ファブリック外のIPv6通信では、境界インフラストラクチャと非ファブリックインフラストラクチャの間でIPv6ルーティングを有効にする必要があります。

ステップ 1：クライアントが認証し、設定された方式からIPv6アドレスを取得します。



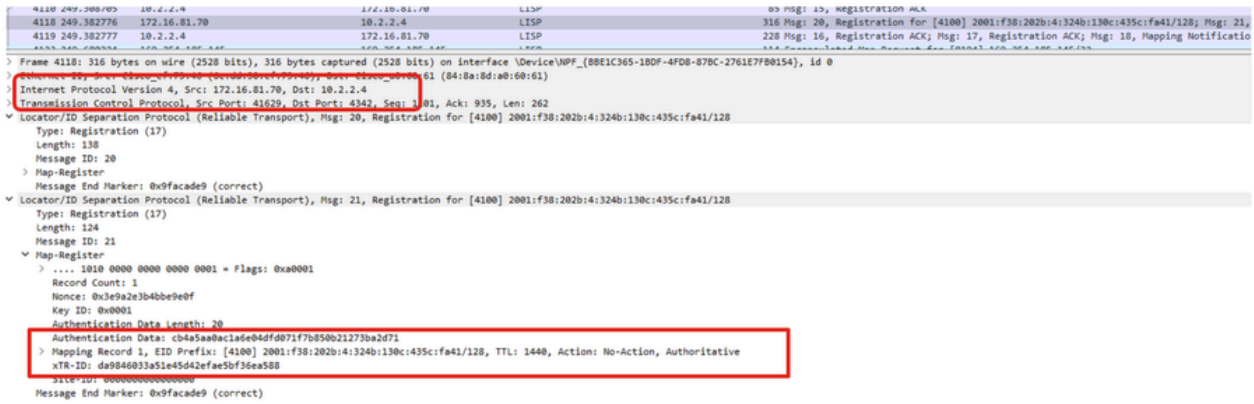
DHCPv6サーバからファブリックエッジノードへのパケットキャプチャ

ステップ 2：ワイヤレスクライアントは、IPv6ペイロードを含む802.11フレームをアクセスポイントに送信します。
ステップ 3：アクセスポイントはワイヤレスヘッダーを削除し、パケットをファブリックエッジに送信します。アクセスポイントはIPv4アドレスを持つため、これはIPv4ベースのVXLANトンネルヘッダーを使用します。



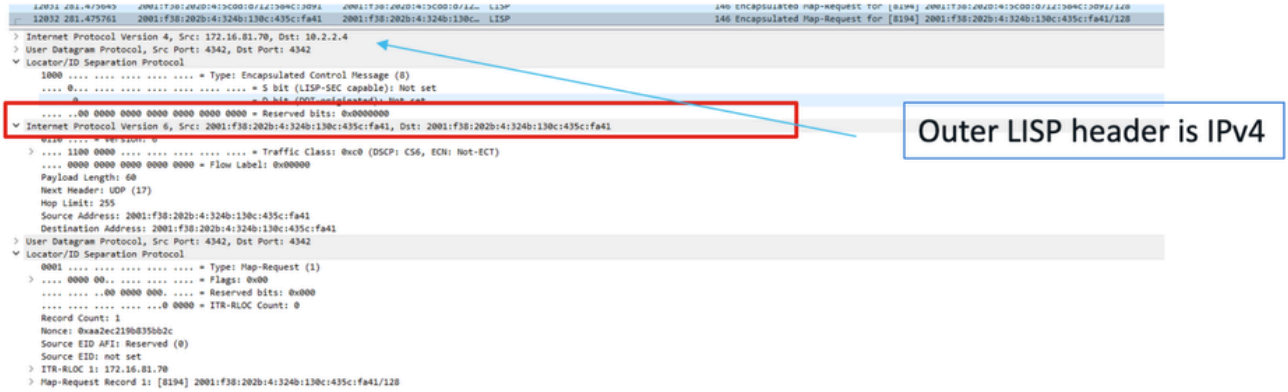
FEとAP間のVxLANトンネルのパケットキャプチャ

ステップ 3.1：ファブリックエッジは、IPv6クライアントをコントロールプレーンに登録します。これは、内部のIPv6クライアントの詳細とIPv4登録方式を使用します。



IPv6クライアント用コントロールプレーンを使用したFEレジスタのパケットキャプチャ

ステップ 3.2：FEは、宛先RLOCを識別するために、コントロールプレーンにMAP要求を送信します。



MAP登録メッセージを使用したFEからCPへのパケットキャプチャ

ファブリックエッジは、次の図に示すように、既知のIPv6クライアントのMAPキャッシュも維持します。

```
Pod2-Edge-2#sh lisp eid-table vrf Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries

::/0, uptime: 6w4d, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:3::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:4::/64, uptime: 3w1d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2001:F38:202B:4:324B:130C:435C:FA41/128, uptime: 00:00:05, expires: 23:59:54, via map-reply, self, complete
  Locator       Uptime    State     Pri/Wgt     Encap-IID
  172.16.81.70  00:00:05  up, self   10/10        -
2001:F38:202B:6::/64, uptime: 1w2d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
2002::/15, uptime: 05:57:20, expires: 00:14:34, via map-reply, forward-native
  Encapsulating to proxy ETR
Pod2-Edge-2#
```

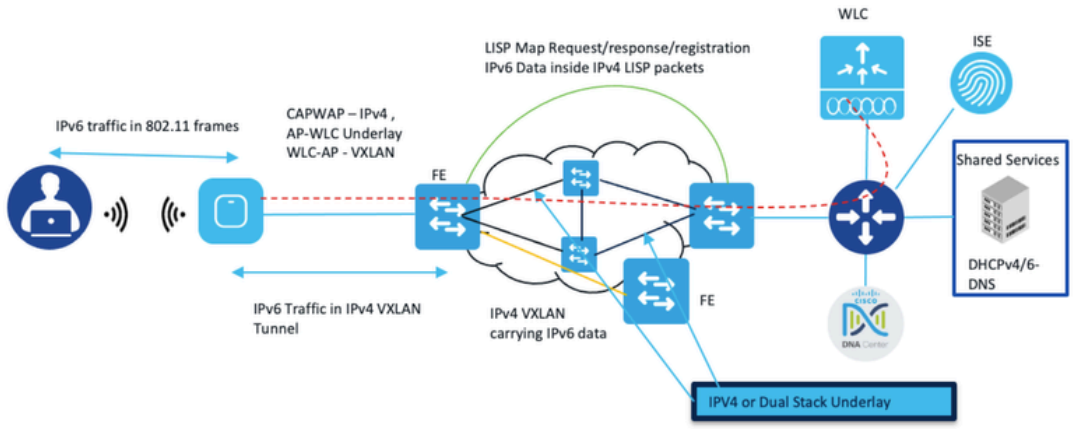
IPv6オーバーレイマップキャッシュ情報のファブリックエッジ画面出力

ステップ 4：パケットは、元のIPv6ペイロードを内部に伝送するIPv4 VXLANを使用して宛先RLOCに転送されます。両方のクライアントが同じAPに接続されているため、IPv6 pingはこのパスを使用します。

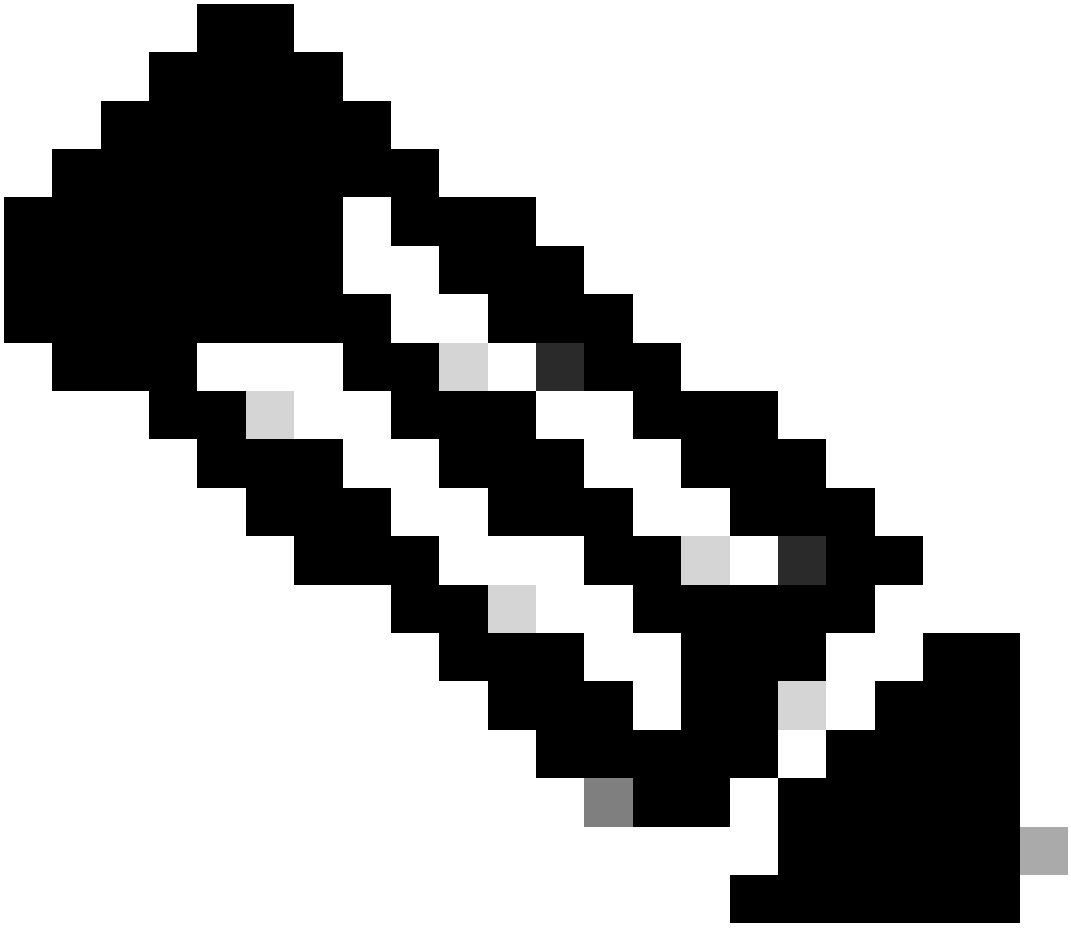
```
    71 3.392805     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=63
    72 3.392836     2001:f38:202b:4:324b:130c:435c:fa41   2001:f38:202b:6:78aa:22f5:817c:9211 ICMPv6      144 Echo (ping) request id=0x0001, seq=148, hop limit=64
    73 3.398939     2001:f38:202b:6:78aa:22f5:817c:9211   2001:f38:202b:4:324b:130c:435c:fa41 ICMPv6      144 Echo (ping) reply id=0x0001, seq=148, hop limit=64 (
    74 3.398941     2001:f38:202b:6:78aa:22f5:817c:9211   2001:f38:202b:4:324b:130c:435c:fa41 ICMPv6      144 Echo (ping) reply id=0x0001, seq=148, hop limit=63

> Frame 72: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface \Device\NPF_{BBE1C365-1BDF-4FD8-87BC-2761E7FB0154}, id 0
> Ethernet II, Src: Cisco_76:5e:f8 (70:69:5a:76:5e:f8), Dst: Cisco_9f:fe:f5 (00:00:0c:9f:fe:f5)
> Internet Protocol Version 4, Src: 172.16.83.2, Dst: 172.16.81.70
> User Datagram Protocol, Src Port: 49407, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 8194
    Reserved: 0
> Ethernet II, Src: D-LinkIn_f4:d6:25 (74:da:da:f4:d6:25), Dst: Cisco_9f:fa:85 (00:00:0c:9f:fa:85)
> Internet Protocol Version 6, Src: 2001:f38:202b:4:324b:130c:435c:fa41, Dst: 2001:f38:202b:6:78aa:22f5:817c:9211
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x036f [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 148
    [Response In: 73]
  > Data (32 bytes)
```

同じAPに登録されている2つのワイヤレスクライアント間でのIPv6 pingのパケットキャプチャ

この図は、ワイヤレスクライアントの観点からIPv6通信をまとめたものです。



図は、ワイヤレスクライアントの観点からIPv6通信を要約しています



注:ISEの制限により、Cisco Identity ServicesによるIPv6ゲストアクセス（Webポータル）はサポートされません。

依存関係マトリックス

Cisco SD-Accessの一部であるさまざまなワイヤレスコンポーネントからのIPv6の依存関係とサポートに注意することが重要です。このイメージの表は、この機能マトリクスをまとめたものです。

C9800 IPv6 Features by Release

Feature		AireOS	16.12	17.1
Infra IPv6 (CAPWAP over IPv6)				
	Local	YES	YES	YES
	Flex	YES	YES	YES
	Fabric	NO	YES	YES
Infra IPv6 (WLC Platforms)				
	Hardware Wireless Controller	YES	YES	YES
	Wireless Controller in the switches	NO	YES	YES
	Public Cloud: AWS	NO	NO	NO
	Public Cloud: GCP	NO	NO	NO
	Private Cloud: ESXi	YES	YES	YES
	Private Cloud: KVM	YES	YES	YES
	Private Cloud: NFVIs	NO	YES	YES
Interop IPv6 support				
	C9800 <-> DNA-C (Infra IPv6)	NO	TBD	NO
	C9800 <-> CMX (Infra IPv6)	NO	TBD	YES
	C9800 <-> ISE (Infra IPv6)	NO	TBD	YES
	WLC<->PI(Infra IPv6)	YES(Over SNMP)	YES	YES
	OpenDNS(Infra iPv6)	NO	YES	YES
	Netflow over IPv6	NO	YES	YES
	ETA for IPv6	NO	NO	YES

リリース別Cat9800 WLC IPv6機能

IPv6のコントロールプレーンの監視

IPv6を有効にすると、マップサーバ(MS)/マップリゾルバ(MR)サーバにホストIPv6に関する追加エントリが表示されるようになります。ホストは複数のIPv6 IPアドレスを持つことができるため、MS/MRルックアップテーブルにすべてのIPアドレスのエントリがあります。これは、すでに存在するIPv4テーブルと組み合わされます。
すべてのエントリを確認するには、デバイスのCLIにログインし、次のコマンドを発行する必要があります。

```
Pod2-Border#sh lisp site

LISP Site Registration Information

* = Some locators are down or unreachable

# = Some registrations are sourced by reliable transport


Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4097     172.16.83.0/24
               2w1d      yes#   172.16.81.70:41629   4097     172.16.83.2/32
```

```
              never     no     --                  4099     172.16.79.0/24

              never     no     --                  4100     172.16.71.0/24

              never     no     --                  4100     172.16.72.0/24

              never     no     --                  4100     172.16.78.0/24

              never     no     --                  4100     2001:F38:202B:3::/64

              1w0d      yes#   172.16.81.65:16775  4100     2001:F38:202B:3:5B84:C9B0:1271:D4B/128

              1w0d      yes#   172.16.81.70:41629  4100     2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128

              never     no     --                  4100     2001:F38:202B:4::/64

              6d14h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:324B:130C:435C:FA41/128

              6d15h     yes#   172.16.81.70:41629  4100     2001:F38:202B:4:705F:2381:9D03:B991/128

              14:10:42  yes#   172.16.81.70:41629  4100     2001:F38:202B:4:B8AE:8711:5852:BE6A/128

              never     no     --                  4100     2001:F38:202B:6::/64
```

```
Pod2-Border#sh lisp site summary

                    ----------- IPv4 ----------- ----------- IPv6 ----------- ----------- MAC -----------

Site name           Configured Registered Incons Configured Registered Incons Configured Registered Incons

site_uci                     5          1      0          3          5      0          5          5      0



Site-registration limit for router lisp 0:              0

Site-registration count for router lisp 0:             11

Number of address-resolution entries:                  14

Number of configured sites:                             1

Number of registered sites:                             1

Sites with inconsistent registrations:                  0

IPv4

  Number of configured EID prefixes:                    5

  Number of registered EID prefixes:                    1

  Maximum MS entries allowed:                       81920

IPv6

  Number of configured EID prefixes:                    3
```

```
  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920

MAC

  Number of configured EID prefixes:                5

  Number of registered EID prefixes:                5

  Maximum MS entries allowed:                   81920
```

アシュアランスを介してホストIPv6の詳細を確認することもできます。

Cisco SD-AccessでのIPv6 QoSの実装

現在のCisco DNA Centerリリース（最大2.3.x）では、IPv6 QoSアプリケーションポリシーの自動化はサポートされていません。ただし、ユーザは手動でIPv6有線およびワイヤレステンプレートを作成し、QoSテンプレートをファブリックエッジノードにプッシュできます。DNA Centerは、適用後にすべての物理インターフェイスでIPv4 QoSポリシーを自動化するため、テンプレートを使用して「class-default」の前にクラスマップ(IPv6アクセスコントロールリスト(ACL)に一致する)を手動で挿入できます。

DNA Centerで生成されたポリシー設定と統合された有線IPv6 QoS対応テンプレートの例を次に示します。

```
!
interface GigabitEthernetx/y/z
service-policy input DNA-APIC_QOS_IN
class-map match-any DNA-APIC_QOS_IN#SCAVENGER <<< Provisioned by DNAC
match access-group name DNA-APIC_QOS_IN#SCAVENGER__acl
match access-group name IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
!
ipv6 access-list IPV6_QOS_IN#SCAVENGER__acl <<< Manually add
sequence 10 permit icmp any any
!
Policy-map DNA-APIC_QOS_IN
class IPV6_QOS_IN#SCAVENGER__acl <<< manually add
set dscp cs1
For wireless QoS policy, Cisco DNA Center with current release (up to 2.3.x) will provision IPv4 QoS on
and apply IPv4 QoS into the WLC (Wireless LAN Controller). It doesn't automate IPv6 QoS.
© 2021 Cisco and/or its affiliates. All rights reserved. Page 20 of 24
Below is the sample wireless IPv6 QoS template. Please make sure to apply the QoS policy into the wirel
interface from the wireless VLAN:
ipv6 access-list extended IPV6_QOS_IN#TRANS_DATA__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#REALTIME
remark ### a placeholder ###
```

```
!
ipv6 access-list extended IPV6-QOS_IN#TUNNELED__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#VOICE
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#SCAVENGER__acl
permit icmp any any
!
ipv6 access-list extended IPV6_QOS_IN#SIGNALING__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BROADCAST__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#BULK_DATA__acl
permit tcp any any eq ftp
permit tcp any any eq ftp-data
permit tcp any any eq 21000
permit udp any any eq 20
!
ipv6 access-list extended IPV6_QOS_IN#MM_CONF__acl
remark ms-lync
permit tcp any any eq 3478
permit udp any any eq 3478
permit tcp range 5350 5509
permit udp range 5350 5509
!
ipv6 access-list extended IPV6_QOS_IN#MM_STREAM__acl
remark ### a placeholder ###
!
ipv6 access-list extended IPV6_QOS_IN#OAM__acl
remark ### a placeholder ###
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
!
class-map match-any IPV6_QOS_IN#TRANS_DATA
match access-group name IPV6_QOS_IN#TRANS_DATA__acl
!
class-map match-any IPV6_QOS_IN#REALTIME
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#TUNNELED
match access-group name IPV6_QOS_IN#TUNNELED__acl
!
class-map match-any IPV6_QOS_IN#VOICE
match access-group name IPV6_QOS_IN#VOICE
!
class-map match-any IPV6_QOS_IN#SCAVENGER
match access-group name IPV6_QOS_IN#SCAVENGER__acl
!
class-map match-any IPV6_QOS_IN#SIGNALING
match access-group name IPV6_QOS_IN#SIGNALING__acl
class-map match-any IPV6_QOS_IN#BROADCAST
match access-group name IPV6_QOS_IN#BROADCAST__acl
!
class-map match-any IPV6_QOS_IN#BULK_DATA
match access-group name IPV6_QOS_IN#BULK_DATA__acl
!
class-map match-any IPV6_QOS_IN#MM_CONF
```

```
match access-group name IPV6_QOS_IN#MM_CONF__acl
!
class-map match-any IPV6_QOS_IN#MM_STREAM
match access-group name IPV6_QOS_IN#MM_STREAM__acl
!
class-map match-any IPV6_QOS_IN#OAM
match access-group name IPV6_QOS_IN#OAM__acl
!
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
policy-map IPV6_QOS_IN
class IPV6_QOS_IN#VOICE
set dscp ef
class IPV6_QOS_IN#BROADCAST
set dscp cs5
class IPV6_QOS_IN#REALTIME
set dscp cs4
class IPV6_QOS_IN#MM_CONF
set dscp af41
class IPV6_QOS_IN#MM_STREAM
set dscp af31
class IPV6_QOS_IN#SIGNALING
set dscp cs3
class IPV6_QOS_IN#OAM
set dscp cs2
class IPV6_QOS_IN#TRANS_DATA
set dscp af21
class IPV6_QOS_IN#BULK_DATA
set dscp af11
class IPV6_QOS_IN#SCAVENGER
set dscp cs1
class IPV6_QOS_IN#TUNNELED
class class-default
set dscp default
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
interface Vlan1xxx < = = (wireless VLAN)
service-policy input IPV6_QOS_IN
end
```

Cisco SD-AccessのIPv6のトラブルシューティング

SDアクセスのトラブルシューティングIPv6はIPv4と非常によく似ており、同じ目標を達成するために異なるキーワードオプションで同じコマンドを常に使用できます。ここでは、SDアクセスのトラブルシューティングによく使用されるコマンドを示します。

```
Pod2-Edge-2#sh device-tracking database
Binding Table has 24 entries, 12 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHC
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match 0002:Orig trunk 0004:Orig access
0008:Orig trusted trunk 0010:Orig trusted access 0020:DHCP assigned

0040:Cga authenticated 0080:Cert authenticated 0100:Statically assigned
Network Layer Address Link Layer Address Interface vlan prlvl age state Time left
DH4 172.16.83.2 7069.5a76.5ef8 Gi1/0/1 2045 0025 5s REACHABLE 235 s(653998 s)
```

```
L 172.16.83.1 0000.0c9f.fef5 Vl2045 2045 0100 22564mn REACHABLE
ARP 172.16.79.10 74da.daf4.d625 Ac0 71 0005 49s REACHABLE 201 s try 0
L 172.16.79.1 0000.0c9f.f886 Vl79 79 0100 22562mn REACHABLE
L 172.16.78.1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
DH4 172.16.72.101 000c.29c3.16f0 Gi1/0/3 72 0025 9803mn STALE 101187 s
L 172.16.72.1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
L 172.16.71.1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
ND FE80::7269:5AFF:FE76:5EF8 7069.5a76.5ef8 Gi1/0/1 2045 0005 12s REACHABLE 230 s
ND FE80::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 107s REACHABLE 145 s try 0
L FE80::200:CFF:FE9F:FA85 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
L FE80::200:CFF:FE9F:FA09 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
L FE80::200:CFF:FE9F:F886 0000.0c9f.f886 Vl79 79 0100 87217mn DOWN
L FE80::200:CFF:FE9F:F1AE 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
ND 2003::B900:53C0:9656:4363 74da.daf4.d625 Ac0 71 0005 26mn STALE 451 s
ND 2003::705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 49 s try 0
ND 2003::5925:F521:C6A7:927B 74da.daf4.d625 Ac0 71 0005 3mn REACHABLE 47 s try 0
L 2001:F38:202B:6::1 0000.0c9f.fa09 Vl78 78 0100 9546mn REACHABLE
ND 2001:F38:202B:4:B8AE:8711:5852:BE6A 74da.daf4.d625 Ac0 71 0005 83s REACHABLE 164 s try 0
ND 2001:F38:202B:4:705F:2381:9D03:B991 74da.daf4.d625 Ac0 71 0005 112s REACHABLE 133 s try 0
DH6 2001:F38:202B:4:324B:130C:435C:FA41 74da.daf4.d625 Ac0 71 0024 107s REACHABLE 135 s try 0(985881 s)
L 2001:F38:202B:4::1 0000.0c9f.fa85 Vl71 71 0100 22562mn REACHABLE
DH6 2001:F38:202B:3:E6F4:68B3:D2A6:59E6 000c.29c3.16f0 Gi1/0/3 72 0024 9804mn STALE 367005 s
L 2001:F38:202B:3::1 0000.0c9f.f1ae Vl72 72 0100 22562mn REACHABLE
Pod2-Edge-2#sh lisp eid-table Campus_VN ipv6 database
LISP ETR IPv6 Mapping Database for EID-table vrf Campus_VN (IID 4100), LSBs: 0x1
Entries total 5, no-route 0, inactive 1
© 2021 Cisco and/or its affiliates. All rights reserved. Page 23 of 24
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, dynamic-eid InfraVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:324B:130C:435C:FA41/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:705F:2381:9D03:B991/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
2001:F38:202B:4:ACAF:7DDD:7CC2:F1B6/128, Inactive, expires: 10:14:48
2001:F38:202B:4:B8AE:8711:5852:BE6A/128, dynamic-eid ProdVLAN-IPV6, inherited from default locator-set
0ed275d1fc01
Locator Pri/Wgt Source State
172.16.81.70 10/10 cfg-intf site-self, reachable
Pod2-Edge-2#show lisp eid-table Campus_VN ipv6 map-cache
LISP IPv6 Mapping Cache for EID-table vrf Campus_VN (IID 4100), 6 entries
::/0, uptime: 1w3d, expires: never, via static-send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:3:E6F4:68B3:D2A6:59E6/128, uptime: 00:00:04, expires: 23:59:55, via map-reply, self, comp
Locator Uptime State Pri/Wgt Encap-IID
172.16.81.70 00:00:04 up, self 10/10 -
2001:F38:202B:4::/64, uptime: 5w1d, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2001:F38:202B:6::/64, uptime: 6d15h, expires: never, via dynamic-EID, send-map-request
Encapsulating to proxy ETR
2002::/15, uptime: 00:05:04, expires: 00:09:56, via map-reply, forward-native
© 2021 Cisco and/or its affiliates. All rights reserved. Page 24 of 24
Encapsulating to proxy ETR
```

ボーダーノードからオーバーレイDHCPv6サーバpingを確認するには、次の手順を実行します。

```
Pod2-Border#ping vrf Campus_VN 2003::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2003::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Cisco SD-Accessを使用したIPv6設計に関するFAQ

Q. Cisco Software Defined Network(SDN)は、アンダーレイおよびオーバーレイネットワークのIPv6をサポートしていますか。
A.このドキュメントの作成時点では、現在のリリース(2.3.x)ではオーバーレイのみがサポートされています。

Q. Cisco SDNは、有線クライアントとワイヤレスクライアントの両方でネイティブIPv6をサポートしていますか。
A. あります。これには、クライアントがIPv4 DHCP要求を無効にし、IPv6 DHCPまたはSLAACアドレスのみが提供されるため、IPv4がダミープールである一方でDNA Centerで作成されたデュアルスタックプールが必要です。

Q. Cisco SDアクセスファブリックで、ネイティブのIPv6専用キャンパスネットワークを使用できますか。
A.現在のリリース（2.3.xまで）ではサポートされていません。 ロードマップに掲載されています。

Q. Cisco SD-AccessはL2 IPv6ハンドオフをサポートしていますか。
A.現時点ではサポートされていません。L2 IPv4ハンドオフまたはL3デュアルスタックハンドオフのみがサポートされています。

Q. Cisco SD-AccessはIPv6のマルチキャストをサポートしていますか。
A.はい。ヘッドエンドレプリケーションマルチキャストを使用するオーバーレイIPv6のみがサポートされます。ネイティブIPv6マルチキャストはまだサポートされていません。

Q. Cisco SD-Access Fabric Enabled Wirelessはデュアルスタックのゲストをサポートしていますか。
A. Cisco IOS XE(Cat9800)WLCではまだサポートされていません。AireOS WLCは、回避策によってサポートされます。回避策の実装の詳細については、シスコカスタマーエクスペリエンスチームにお問い合わせください。

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。