Cisco Network Plug and Play ソリューション ガイド

初版:2015/11/23

最終更新日:2016/05/25

マニュアルの構成

このマニュアルは、以下の項で構成されています。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	表示
bold フォント	コマンド、キーワード、およびユーザが入力するテキストは、**bold** フォントで記載されます。
italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで記載されます。
[ ]	角カッコの中の要素は、省略可能です。

表記法	表示
{x | y | z }	いずれか 1 つを選択しなければならない必須キーワードは波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

注: *読者に留意していただきたいことを示しています。*役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意: ***注意が必要なことを示しています。*機器の損傷またはデータ損失を予防するための注意事項が記述されています。**

ソリューションの概要

エンタープライズおよびキャンパス規模の環境では、データセンター、ブランチ ネットワーク、およびキャンパス全体に多数のネットワーク デバイスを設置および展開するため、コストが大きく膨らみます。通常、熟練した設置技術者が各デバイスを事前にステージングし、コンソール接続での CLI によりロードして、ネットワークに接続する必要があります。このプロセスは、コストと時間がかかり、エラーが生じやすい作業です。一方、お客様はセキュリティ上の問題を招くことなく、展開時間が短縮され、複雑さが軽減されることを望んでいます。

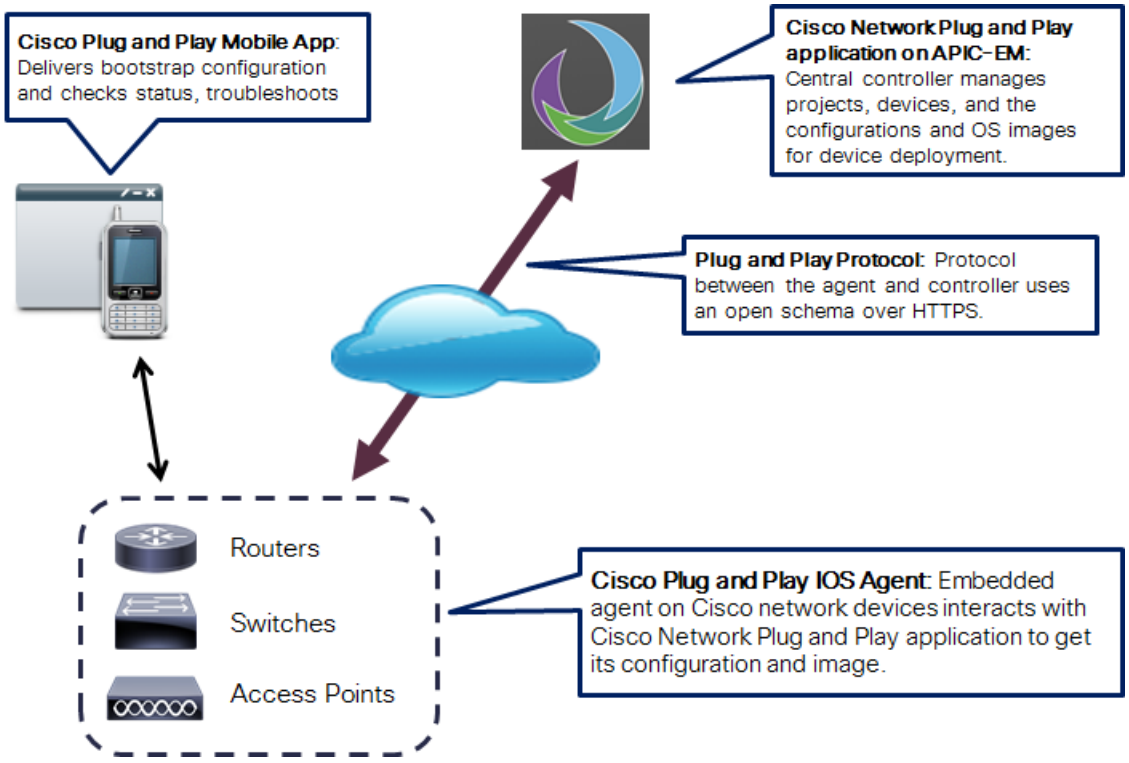
Cisco Network Plug and Play ソリューションは、エンタープライズ ネットワークを利用するお客様にシンプルかつセキュアなユニファイド/統合オファリングを提供することで、新しいブランチ/キャンパス デバイスのロールアウトや、既存ネットワーク向けの更新のプロビジョニングを簡易化します。このソリューションは統合的なアプローチを採用しており、ほぼゼロタッチの展開エクスペリエンスで、シスコのルータ、スイッチ、およびワイヤレス デバイスで構成されるエンタープライズ ネットワークのプロビジョニングを実現します。

また、新規デバイスの展開プロセスを大幅に簡素化することで、企業の負担を軽減します。CLI の知識がなくてもサイトのインストーラで新しいデバイスを展開でき、ネットワーク管理者はデバイス設定を一元管理できます。

Cisco Network Plug and Play ソリューションは、次のような特長を備えています。

- シスコ ネットワーク デバイスの簡単かつ一貫性のある展開
- Cisco Application Policy Infrastructure Controller エンタープライズ モジュール(APIC-EM)による、リモート デバイス展開の自動化と集中管理
- シスコのルータ、スイッチ、およびワイヤレス アクセス ポイントデバイス向けの統合ソリューション
- 最大 9 つのメンバーを持つスイッチ スタックのサポート。Cisco Network Plug and Play は、1 つのメンバー スイッチの識別に基づいてスタック メンバーをインテリジェントに検出し、スタック全体を 1 つの単位としてプロビジョニングできます。各スタック メンバーを個別にプロビジョニングする必要はありません。
- デバイスは、DHCP、DNS、プロキシ サーバを介して自動的に APIC-EM コントローラを検出します。また、デバイスがオンラインになったときに、事前定義の設定やイメージをそれらのデバイスにプッシュできます
- iOS または Android 用のモバイル アプリケーションを使用すると、リモート サイトからデバイス インストーラによりデバイスをブートしたり、インストールをモニタしたりできます。
- Secure Unique Device Identifier(SUDI)と Cisco マネージド Trustpool バンドルに格納されている証明書を使用して、デバイスの認証と通信を保護します。この Trustpool バンドルは、信頼できる認証局により署名され、Cisco InfoSec によって発行された証明書専用のストアです。セキュリティの詳細および管理方法については、セキュアな接続(9 ページ)を参照してください。

図 1　Cisco Network Plug and Play アーキテクチャの概要



ソリューションのコンポーネント

Cisco Network Plug and Play ソリューションは、以下のコンポーネントから構成されています。

- **Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）**：Cisco APIC-EM は、エンタープライズ ネットワーク（アクセス、キャンパス、WAN、およびワイヤレス）向けの Cisco SDN コントローラです。プラットフォームは複数のアプリケーション（SDN アプリケーション）をホストし、それらのアプリケーションでは、コア ネットワーク自動化ソリューションを推進するオープンなノースバウンド REST API が使用されます。このプラットフォームはさまざまなサウスバウンド プロトコルもサポートしています。これらのプロトコルにより、プラットフォームはお客様の環境に導入済みの各種ネットワーク デバイスと通信し、新規および既存のいずれの環境にも SDN の利点を活かすことができます。
- **Cisco Network Plug and Play アプリケーション**：この Cisco APIC-EM アプリケーションはプレインストールされており、シスコ デバイスからプラグ アンド プレイ要求を受信して、事前定義のルールと条件に基づいてデバイスをプロビジョニングします。
- **Cisco Plug and Play IOS エージェント**：このエージェントはシスコ デバイスに組み込まれており、デバイスの展開時に HTTPS によるオープン プラグ アンド プレイ プロトコルを使用して Cisco Network Plug and Play アプリケーションと通信します。
- **iOS および Android デバイス用の Cisco Plug and Play モバイル アプリケーション**：iOS および Android デバイス用のモバイル アプリケーションを使用して、シスコ デバイスにブートストラップ コンフィギュレーションを設定し、リモート ブランチでの展開を開始できます。このアプリケーションは、3G/4G/WiFi 接続で Cisco Network Plug and Play アプリケーションと通信して、事前定義のデバイス ブートストラップ コンフィギュレーションを取得し、それを物理接続の特殊なシリアル ケーブルを使用してシスコ ネットワーク デバイスに配布します。

- **Cisco SMI プロキシ**：このオプションのコンポーネントは、新しい Cisco Plug and Play IOS エージェントがない旧バージョンの IOS（IOS-XE3.6.3E および IOS 15.2(2) E3 よりも前の IOS）を搭載しているシスコ スイッチを展開する場合に必要です。SMI プロキシは、新しいプラグ アンド プレイ プロトコルを使用する Cisco Network Plug and Play アプリケーションと古いシスコ スイッチとの間でプロキシとして機能します。このプロキシはルーティング プラットフォームではサポートされません。
- **汎用 HTTP プロキシ**：Cisco APIC-EM が DMZ ゾーンの背後にあるため、リモート デバイスから直接到達できない場合は、このオプションのコンポートネントを使用してリモート ブランチを展開します。汎用 HTTP リバース プロキシを DMZ 内で APIC-EM の前に配置して、デバイスとコントローラの間でメッセージを中継させることができます。また、汎用プロキシを使用しないで VPN を介してコントローラに到達できるように、プライベート VPN リンクを設定することもできます。

ソリューションのワーク フロー

ここでは、以下の一般的な使用例のワークフローについて説明します。

- リモート ブランチ/サイトの展開（4 ページ）（モバイル アプリケーションを使用）
- キャンパス/LAN の展開（6 ページ）（DHCP または DNS による自動検出を使用）
- 計画外のデバイスの展開（7 ページ）

前提条件として、Cisco Network Plug and Play アプリケーションを搭載した Cisco APIC-EM コントローラが稼動している必要があります。

リモート ブランチ/サイトの展開

以下に、Cisco Network Plug and Play を使用してリモート ブランチ/サイトにシスコ ネットワーク デバイスを展開する手順の概要を示します。

前提条件：シスコ ネットワーク デバイスで、Cisco Plug and Play IOS エージェントをサポートしている Cisco IOS イメージが実行されていること。

1. APIC-EM コントローラで、ネットワーク管理者は Cisco Network Plug and Play アプリケーションを使用して、リモート サイトとデバイスの情報をアプリケーションに事前プロビジョニングします。この操作には、インストールする各デバイスのデバイス情報の入力と、ブートストラップ コンフィギュレーション、すべてのコンフィギュレーション、IOS イメージの設定が含まれます。ブートストラップ コンフィギュレーションは Plug and Play エージェントを有効化し、通常は、使用するデバイス インターフェイスの指定およびインターフェイスのスタティック IP アドレスの設定を行います。Cisco Network Plug and Play アプリケーションの詳しい使用方法については、『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』を参照してください。
2. （任意）。中央ネットワーク オペレーション センターが DMZ の背後にある場合は、リモート サイトのデバイスで Cisco Plug and Play IOS エージェントが Cisco Network Plug and Play アプリケーションと通信できるように、ネットワーク管理者は汎用 HTTP プロキシまたはネットワーク オペレーション センターへの VPN リンクを設定する必要があります。これは一度だけ実行するタスクです。一度設定すると、以降のリモート サイトにおけるすべてのデバイス展開にプロキシまたは VPN を使用できるようになるからです。HTTP プロキシの設定の詳細については、汎用 HTTP プロキシの設定（11 ページ）を参照してください。
3. リモート サイトで、デバイス インストーラを使用し、シスコ ネットワーク デバイスをインストールして電源を投入します。次に、特別なシリアル ケーブルを使用して、シスコ ネットワーク デバイスのコンソール ポートにモバイル デバイスを接続します。

   注：シスコ ワイヤレス アクセス ポイント デバイスの場合は、ブートストラップ コンフィギュレーションがサポートされないので、このステップおよび Cisco Plug and Play Mobile App モバイル アプリケーションは不要です。

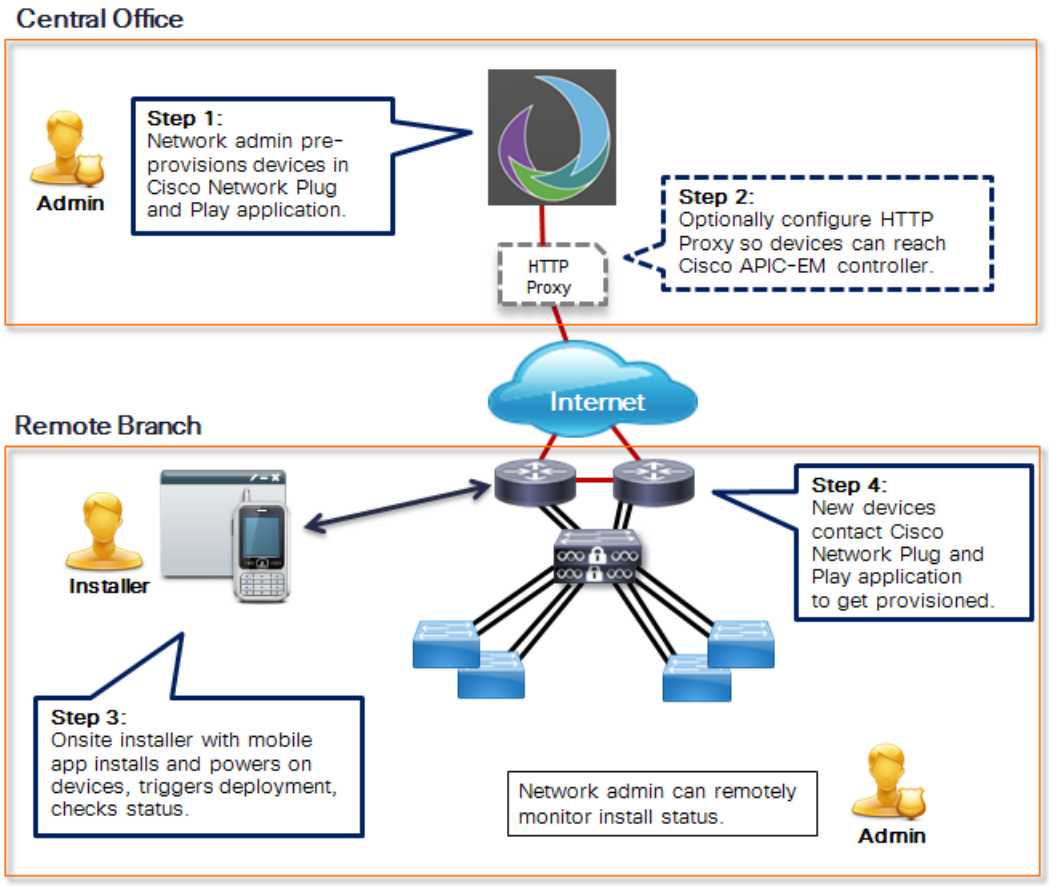
   デバイス インストーラは、Cisco Plug and Play モバイル アプリケーションの [デバイスの展開（Deploy Devices）] 機能を使用して、ブートストラップ コンフィギュレーションをシスコ ネットワーク デバイスに配信し、展開をトリガーします。Cisco Plug and Play モバイル アプリケーションを使用してデバイスを展開する方法については、モバイル アプリケーションのオンライン ヘルプを参照してください。

注:デバイスが USB フラッシュ ドライブをサポートしている場合は、Cisco Plug and Play モバイル アプリケーションの代わりに USB フラッシュ ドライブを使用して、シスコのルータやスイッチにブートストラップ コンフィギュレーションを配布できます。

4. ネットワーク デバイスは、APIC-EM コントローラ上の Cisco Network Plug and Play アプリケーションに接続して、シリアル番号により自己証明を行い、自身の設定をすべてダウンロードします。また、必要に応じて、ネットワーク管理者により事前プロビジョニングされた IOS イメージもダウンロードします。

注:電源が投入されると、シスコ ネットワーク デバイスは DHCP または DNS を使用して自動的に APIC-EM を検出し、自身の設定をすべてダウンロードします。この場合、Cisco Plug and Play モバイル アプリケーションは必要ありません。DHCP を使用するには、Cisco APIC-EM コントローラとのレイヤ 3 接続が確立され、DHCP サーバに Cisco Network Plug and Play オプション 43 が設定されている必要があります。これに該当しない場合、Cisco Network Plug and Play IOS エージェントは、DNS を使用して APIC-EM コントローラを検出できます。リモート サイトの展開ではこれらの要件が満たされない場合があります。そのため、この使用例では Cisco Plug and Play モバイル アプリケーションの使用に重点を置いています。DHCP の設定の詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定(13 ページ)を参照してください。

図 2　自動ブランチ展開



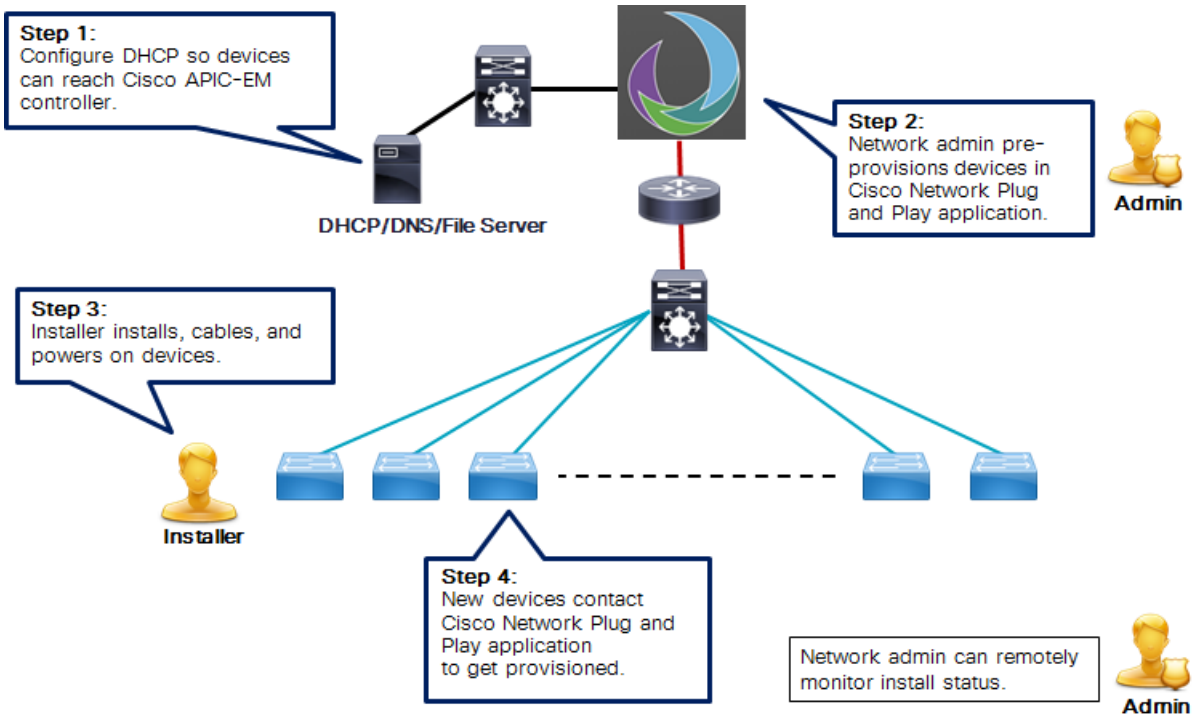
キャンパス/LAN の展開

以下に、Cisco Network Plug and Play を使用して、キャンパス/LAN にシスコ ネットワーク デバイスを展開する手順の概要を示します。この場合、ネットワーク デバイスは Cisco APIC-EM コントローラを自動的に検出できます。

前提条件: シスコ スイッチで、Cisco Plug and Play IOS エージェントをサポートしている Cisco IOS イメージが実行されていること。スイッチで古い Cisco IOS イメージが実行されている場合は、SMI プロキシを使用する必要があります。詳細は、SMI プロキシの設定（10 ページ）を参照してください。

1. ネットワーク管理者は、DHCP オプション 43 によるクライアント検出要求に応答するために、ネットワークに DHCP サーバを設定します。DHCP オプション 43 には APIC-EM コントローラの IP アドレスとポート情報が含まれています。または、DNS を使用してコントローラを検出することができます。DHCP および DNS の設定の詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定（13 ページ）を参照してください。
2. ネットワーク管理者は Cisco Network Plug and Play アプリケーションを使用して、リモート サイトとデバイスの情報を事前プロビジョニングします。この操作には、インストールする各デバイスのデバイス情報の入力と、ブートストラップ コンフィギュレーション（任意）、すべてのコンフィギュレーション、IOS イメージの設定が含まれます。ブートストラップ コンフィギュレーションは Cisco Plug and Play エージェントを有効化し、通常は、使用するデバイス インターフェイスの指定およびインターフェイスのスタティック IP アドレスの設定を行います。Cisco Network Plug and Play アプリケーションの詳しい使用方法については、『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』を参照してください。
3. デバイス インストーラによって、シスコ ネットワーク デバイスがインストールされ、電源が投入されます。
4. デバイスは、DHCP または DNS を使用して APIC-EM コントローラを自動検出し、Cisco Network Plug and Play アプリケーションに対してシリアル番号により自己証明し、自身の設定をすべてダウンロードします。また、必要に応じて、ネットワーク管理者により事前プロビジョニングされた IOS イメージもダウンロードします。

図 3　キャンパスの展開



計画外のデバイスの展開

小規模サイトや事前プロビジョニングが不要な場合など、場合によっては、Cisco Network Plug and Play アプリケーションで事前設定せずにデバイスを展開し、その後、デバイスを要求して設定することができます。

以下に、Cisco Network Plug and Play を使用して、計画外デバイス オプションによりシスコ ネットワーク デバイスを展開する手順の概要を示します。

前提条件: シスコ ネットワーク デバイスで、Cisco Plug and Play IOS エージェントをサポートしている Cisco IOS イメージが実行されていること。

1. ネットワーク管理者は、DHCP オプション 43 によるクライアント検出要求に応答するために、ネットワークに DHCP サーバを設定します。DHCP オプション 43 には APIC-EM コントローラの IP アドレスとポート情報が含まれています。または、DNS を使用してコントローラを検出することができます。DHCP および DNS の設定の詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定（13 ページ）を参照してください。
2. デバイス インストーラによって、シスコ ネットワーク デバイスがインストールされ、電源が投入されます。
3. デバイスが DHCP または DNS を使用して APIC-EM コントローラを自動検出します。デバイスは、計画外のデバイスとして Cisco Network Plug and Play アプリケーションのリストに記載され、IP アドレスと製品 ID によって識別されます。
4. ネットワーク管理者は Cisco Network Plug and Play アプリケーションを使用してデバイスを要求し、デバイスに新しい設定と IOS イメージを設定します。Cisco Network Plug and Play アプリケーションの詳しい使用方法については、『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』を参照してください。

Cisco Network Plug and Play ソリューションの展開

ここでは、Cisco Network Plug and Play ソリューションの展開について説明します。

前提条件

Cisco Network Plug and Play ソリューションを使用するための前提条件は、以下のとおりです。

- Cisco Network Plug and Play アプリケーションを搭載した APIC-EM が展開され、動作していること。詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。
- 展開するシスコ ネットワーク デバイスで、Cisco Plug and Play IOS エージェントをサポートしている IOS リリースが実行されていること（サポート対象のプラットフォームとソフトウェア リリースについては、『*Release Notes for Cisco Network Plug and Play*』を参照してください）。
- 展開するシスコ ネットワーク デバイスが工場出荷時のデフォルト状態になっており、サポートされているイメージによって自動起動可能であること。以前に設定された（またはステータスが不明な）ネットワーク デバイスを使用している場合は、ネットワーク デバイスのトラブルシューティング（13 ページ）でリセットの詳細を参照してください。
- シスコ スイッチ スタックのすべてのメンバーは、同じ IOS リリースを実行している必要があります。また、プラグ アンド プレイ プロビジョニングには、スイッチを電源投入して APIC-EM に接続する前に正しく接続されている必要があります。
- Cisco Plug and Play モバイル アプリケーション（iOS または Android 版）がデバイス インストーラで使用されるモバイル デバイスにインストールされており、特別なシリアル コンソール ケーブルを使用できること。

  注: Cisco Plug and Play モバイル アプリケーションは、シスコ ワイヤレス アクセス ポイント デバイスの展開には使用されません。他のデバイスの展開に対しては任意です。
- 新しい Cisco Plug and Play IOS エージェントがない旧バージョンの IOS（IOS-XE3.6.0E、IOS15.2(2)E よりも前の IOS）を搭載したシスコ スイッチを展開する場合は、必要に応じて、Cisco SMI プロキシをネットワークにインストールします。詳細は、SMI プロキシの設定（10 ページ）を参照してください。

- 展開するリモート デバイスがパブリック インターネットを使用して APIC-EM コントローラと通信する必要があり、コントローラが DMZ の背後にある場合は、必要に応じて、汎用 HTTP プロキシをネットワークにインストールします。詳細は、汎用 HTTP プロキシの設定（11 ページ）を参照してください。また、汎用プロキシを使用しないで VPN を介してコントローラに到達できるように、プライベート VPN リンクを設定することもできます。VPN 接続は、モバイル アプリケーションによってデバイスに配布されるブートストラップ コンフィギュレーションで設定できます。
- Cisco Plug and Play モバイル アプリケーションを使用していて、APIC-EM コントローラがファイアウォールの背後にある場合、ファイアウォールを介したポート 80 および 443 のトラフィックを許可する必要があります。

ガイドライン

Cisco Network Plug and Play ソリューションを展開する際は、次の推奨事項に従ってください。

- DHCP サーバにオプション 43 を設定して、シスコ ネットワーク デバイスによる APIC-EM コントローラの自動検出を有効にします。DHCP および DNS の設定の詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定（13 ページ）を参照してください。
- 展開するすべての新規デバイスに対して、Cisco Network Plug and Play アプリケーションにデバイス設定を事前プロビジョニングします。これには、デバイス シリアル番号、ブートストラップ コンフィギュレーション、すべてのコンフィギュレーション、IOS イメージをサイトのとそのデバイスに設定することも含まれます。詳細については、『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』を参照してください。ただし、[計画外デバイス（Unplanned Device）] 展開オプションを使用する場合は、事前プロビジョニングは必要ありません。
- trustpool セキュリティ機能を使用するには、既知の認証局（CA）から発行された有効な証明書を APIC-EM コントローラにインストールする必要があります。デフォルトの自己署名証明書では trustpool セキュリティを使用できません。また、DHCP オプション 43 の文字列に HTTPS トランスポート オプション（K5）を設定する必要があります。詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定（13 ページ）を参照してください。
- デバイスの起動順序：通常は、ルーティング デバイスとアップストリーム デバイスを最初に起動する必要があります。ルータとすべてのアップストリーム デバイスが起動してプロビジョニングされたら、スイッチとダウンストリーム デバイスを起動できます。Cisco Network Plug and Play IOS エージェントは、デバイスの初回起動時にのみ、APIC-EM コントローラの自動検出を試みます。この時点で、デバイスがコントローラに接続できないと、デバイスのプロビジョニングに失敗するため、最初にアップストリーム デバイスをプロビジョニングする必要があります。
- Cisco ルータ トランク/アクセス ポートの設定：一般的なブランチ ネットワークにはルータとスイッチが含まれています。1 つ以上のスイッチが WAN ルータに接続され、IP Phone やアクセス ポイントなどの他のエンドポイントはスイッチに接続されます。スイッチをアップストリーム ルータに接続する場合、Cisco Network Plug and Play では次の展開モデルがサポートされます。
  - ルータのスイッチ ポートを使用してダウンストリーム スイッチをルータに接続する。このタイプの接続では、ルータのスイッチ ポートをアクセス ポートとして設定する必要があります。ルータのスイッチ ポートをトランク ポートとして設定すると、スイッチに対して Cisco Network Plug and Play プレイ ソリューションが機能しません。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグ アンド プレイ プロセス中、スイッチはそのポートを自動的にトランク ポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。
- デフォルトでは、非 VLAN 1 設定の Cisco Network Plug and Play は、VLAN 1 を使用してデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリーム デバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリーム デバイスに「**pnp startup vlan *x***」グローバル CLI コマンドを設定して、以降のプラグアンドプレイ デバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、以降のプラグ アンド プレイ デバイス上のすべてのアクティブ インターフェイスは、指定された VLAN に変更されます。このガイドラインはルータとスイッチの両方に該当します。

重要:非 VLAN 1 機能を使用する場合は、すべてのネイバー スイッチ デバイスが、3.6.0、3.6.1 や 3.6.2 リリースではなく、Cisco IOS XE リリース 3.6.3 以降を実行していることを確認してください。以前のリリースに含まれていた関連の注意事項 CSCut25533 の詳細については、『*Release Notes for Cisco Network Plug and Play*』の「Caveats」の項を参照してください。

セキュアな接続

Cisco Network Plug and Play ソリューションでは、ネットワーク デバイスと APIC-EM コントローラ間で HTTPS 接続が使用されます。このセキュアな接続は、DHCP オプションで指定された転送タイプに応じて、2 種類の方法のいずれかで実行されます。DHCP の設定の詳細については、APIC-EM コントローラの自動検出に対する DHCP の設定（13 ページ）を参照してください。

DHCP オプション 43 の文字列の K パラメータで指定された転送タイプに応じて、セキュア接続は次の方法で実装されます。

- HTTP が転送プロトコル（デフォルト）として指定され、セキュア接続はトラストポイントに基づきます。

  トラストポイントに基づくセキュア接続は、APIC-EM コントローラにデフォルトでインストールされる自己署名証明書を信頼します。この自己署名証明書を使用して、ネットワーク デバイスにデフォルトのトラストポイントが作成されます。これにより、デバイスは HTTPS を介して APIC-EM コントローラに安全に接続できるようになります。HTTP が転送プロトコルとして指定されているにもかかわらず、HTTPS が APIC-EM コントローラとの通信に使用されます。

- HTTPS が転送プロトコルとして指定され、セキュア接続は trustpool に基づきます。

  trustpool に基づくセキュア接続では、さらに、APIC-EM コントローラの自己署名証明書を各自の CA 署名付き証明書と置き換える必要があります。trustpool は、信頼できる認証局により署名され、Cisco InfoSec によって発行された証明書の特別なストアです。シスコ ネットワーク デバイスは、APIC-EM コントローラに接続するとただちに trustpool バンドルをインポートします。これにより、デバイスはコントローラの証明書を検証してルート CA トラストポイントを作成できるので、固有の署名付き証明書を使用して HTTPS 経由で安全に通信できます。

  T パラメータを使って DHCP オプション 43 に場所を指定することで、ネットワークの別の場所に trustpool バンドルをホストすることもできます。その場合、ネットワーク デバイスは、APIC-EM にインストールされているデフォルトの trustpool ではなく、ユーザの trustpool バンドルを取得します。

セキュリティ、証明書のインポート、および trustpool バンドルの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』の「Cisco APIC-EM Security」の章を参照してください。

SUDI 認証

一部の次世代シスコ ネットワーク デバイス（Cisco ISR 4000 シリーズ ルータなど）は、SUDI 証明書によるセキュアなデバイス識別と認証をサポートしています。セキュア ユニーク デバイス識別子（SUDI）証明書は、出荷時にデバイス ハードウェアにインストールされます。デバイスは、SSL ハンドシェイク時にこの SUDI 証明書を APIC-EM コントローラに送信します。APIC-EM コントローラが SUDI 証明書を検証してデバイスを認証するように指定できます。

SUDI 認証をサポートしているデバイスで SUDI 認証を要求するには、Cisco Network Plug and Play アプリケーションの [プロジェクト（Projects）] タブに一覧表示されているデバイスの横にある [認証（Authentication）] チェックボックスをオンにします。SUDI 認証をサポートしてないデバイスでこのボックスをオンにすると、認証およびプロビジョニングに失敗して認証エラーが発生するので、そのデバイスで操作を続行するにはこのボックスをオフにする必要があります。詳細については、『*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*』を参照してください。

SUDI 認証をサポートしているデバイスのリストについては、『*Release Notes for Cisco Network Plug and Play*』を参照してください。

モバイル アプリケーションの設定

APIC-EM コントローラを自動検出できない場合は、デバイス インストーラで Cisco Plug and Play モバイル アプリケーション（iOS または Android 版）を使用して、シスコ デバイスにブートストラップ コンフィギュレーションを設定し、リモート ブランチの展開を開始することができます。このモバイル アプリケーションは、3G/4G/WiFi 接続で Cisco Network Plug and Play アプリケーションと通信して、事前定義されたデバイス ブートストラップ コンフィギュレーションを取得し、デバイスのコンソール ポートに物理的に接続している特別なケーブルを使用して、シスコ ネットワーク デバイスにブートストラップ コンフィギュレーションを配布します。

モバイル アプリケーションは次の App Store から入手できます。

- iOS：https://itunes.apple.com/WebObjects/MZStore.woa/wa/viewSoftware?id=1050793709&mt=8
- Android：https://play.google.com/store/apps/details?id=com.cisco.ciscopnpandroid

注：iOS 向け Cisco Plug and Play アプリケーションでは、IOS バージョン 7 以降が必要です。Android 向けアプリケーションでは、Android バージョン 4.1 以降が必要です。

注：Cisco Plug and Play モバイル アプリケーションは、シスコ ワイヤレス アクセス ポイント デバイスの展開には使用されません。

デバイスが iOS デバイスであるか Android デバイスであるかに応じて、次のコンソール ケーブルが必要です。

- iOS デバイス：Lightening（8 ピン）コネクタ付き iOS デバイスの場合は、Redpark Lightning コンソール ケーブル（L2-RJ45V）。従来の 30 ピン コネクタ付き iOS デバイスの場合は、Redpark コンソール ケーブル（C2-RJ45V）。
- Android デバイス：Airconsole Bluetooth アダプタ

Cisco Plug and Play モバイル アプリケーションを初めて使用する場合は、事前に APIC-EM コントローラの URL とクレデンシャルをアプリケーションに設定しておく必要があります。これらの設定は一度セットアップすると保存されます。

コントローラ情報をセット アップするには、次の手順を実行します。

1. Cisco Plug and Play モバイル アプリケーションを起動し、メニューから [設定（Settings）] を選択します。
2. [サーバURL（Server URL）] フィールドに、APIC-EM コントローラの IP アドレスを入力します。
3. [ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、インストーラ ロールを持つ APIC-EM ユーザ アカウントのユーザ名とパスワードのクレデンシャルを入力します。ユーザ アカウントおよびロールの設定の詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の「Managing Users and Roles」の章を参照してください。
4. [テスト接続（Test Connection）] をタップして、コントローラとの接続をテストし、ステータスを表示します。
5. 接続に成功した場合は、右上の [保存（Save）] をタップし、次に左上の [完了（Done）] をタップしてメイン画面に戻ります。

注：コンソール ケーブルをネットワーク デバイスから切断した後で別のネットワーク デバイスに接続する場合は、新しいデバイスに接続するときに、先に手動でモバイル アプリケーションを更新して、正しいステータスを反映させる必要があります。

重要：Redpark ケーブル付きの iOS モバイル デバイスを使用しており、複数のネットワーク デバイスを展開する場合は、1 台のデバイスで作業が完了したら、モバイル デバイスとネットワーク デバイスの両方から Redpark ケーブルを外してシリアル接続を閉じる必要があります。モバイル デバイスからケーブルを外さないと、シリアル セッションが終了せず、以降のデバイスに誤った設定が展開される可能性があります。

SMI プロキシの設定

Smart Install（SMI）プロキシは、新しい Cisco Plug and Play IOS エージェントがない旧バージョンの IOS（IOS-XE3.6.3E および IOS 15.2(2) E3 よりも前の IOS）を搭載しているシスコ スイッチの Smart Install 機能を活用します。SMI プロキシは、そのようなスイッチと新しいプラグ アンド プレイ プロトコルを使用する Cisco Network Plug and Play アプリケーションとの間でプロキシとして機能します。

SMI プロキシは、Smart Install Director 機能をサポートしているスイッチング プラットフォームにのみ適用され、ルーティング プラットフォームではサポートされません。

SMI プロキシの設定の詳細については、『*Smart Install Configuration Guide*』の「Configuring SMI Proxy」の章を参照してください。

注:お客様が Cisco Network Plug and Play ソリューションのメリットをすべて享受するには、新しい IOS イメージへのアップグレードを検討する必要があります。SMI プロキシは、新しい Cisco Network Plug and Play IOS エージェントの全機能を備えているわけではないので、Cisco Network Plug and Play IOS エージェントを備えた IOS イメージを展開するまでの暫定的なソリューションと見なす必要があります。

汎用 HTTP プロキシの設定

展開するリモート ネットワーク デバイスがパブリック インターネットを使用して APIC-EM コントローラと通信する必要があり、コントローラが DMZ の背後にある場合は、ネットワーク デバイスが APIC-EM コントローラと通信できるように、ネットワークに汎用 HTTP プロキシをインストールする必要があります。汎用 HTTP リバース プロキシ(Apache リバース プロキシなど)を DMZ 内で APIC-EM コントローラの前に配置して、ネットワーク デバイスと APIC-EM コントローラの間でメッセージを中継させることができます。

リバース プロキシを使用するには、既知の認証局(CA)から発行されたのと同じ証明書を Apache HTTP プロキシ サーバ、APIC-EM、および展開するネットワーク デバイスにインストールする必要があります。この証明書によって、すべてのデバイスで信頼できる通信を確立できます。APIC-EM コントローラは、ネットワーク デバイスに証明書をインストールします。

APIC-EM に証明書をインポートするには、[設定(Settings)] > [プロキシゲートウェイ証明書(Proxy Gateway Certificate)] GUI コマンドを使用します(『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』の「Configuring the Cisco APIC-EM Settings」の章を参照)。

注:自己署名証明書をコントローラで使用したり、コントローラにインポートすることはお勧めしません。既知の認証局(CA)から有効な X.509 証明書をインポートすることをお勧めします。

Cisco Network Plug and Play ソリューションは、Ubuntu 上で Apache HTTP Server バージョン 2.4.7 を使用してテストされています。Apache コンフィギュレーション ファイルの下記の行は、Apache でリバース プロキシを有効にする方法を示しています。コマンド内の *APIC-EM-ip-address* を APIC EM コントローラの IP アドレスに置き換えてください。

```
<VirtualHost *:80>
        ProxyRequests Off
        ProxyPreserveHost On
        ProxyPass / http://apic-em-ip-address/
        ProxyPassReverse / http://apic-em-ip-address/
        ServerName your-server-name
        ServerAdmin webmaster@localhost
        SSLCertificateChainFile /etc/apache2/sites-available/Your-IntermediateCA-file.crt
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
<VirtualHost *:443>
        SSLProtocol ALL
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine On
        SSLCertificateFile /etc/apache2/sites-available/your-certificate-file.crt
        SSLCertificateKeyFile /etc/apache2/sites-available/your-certificate-key-file.key
        SSLProxyEngine On
        SSLProxyVerify none
        SSLProxyCheckPeerCN Off
        SSLProxyCheckPeerExpire Off
        SSLProxyCheckPeerName Off
        SSLProxyProtocol all -SSLv2
```

```
    <Location />
        ProxyPass https://apic-em-ip-address/ retry=1 acquire=3000 timeout=600 KeepAlive=On
        ProxyPassReverse https://apic-em-ip-address/
    </Location>
        <Proxy *>
        Order allow,deny
        Allow from all
        </Proxy>
        ProxyPreserveHost On
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
        SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
        SSLOptions +StdEnvVars
        </Directory>
        BrowserMatch "MSIE [2-6]" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
```

トラブルシューティングのヒント

この項では、展開時に生じる可能性がある一般的なセルフ ヘルプ トピックや問題を扱います。

注: 本製品をシスコのリセラーから購入された場合は、テクニカル サポートについて直接リセラーにお問い合わせください。本製品をシスコから直接購入された場合は、次の URL からシスコ テクニカル サポートにご連絡ください: http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

APIC-EM コントローラのトラブルシューティング

APIC-EM コントローラのトラブルシューティングの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』のトラブルシューティングに関する章を参照してください。

[ホーム(Home)] 画面に移動して、左側のナビゲーション ペインで [Network Plug and Play] をクリックすると、APIC-EM GUI で Cisco Network Plug and Play アプリケーションのステータスを確認できます。アプリケーションが実行中の場合は、アプリケーションが開きます。

[ホーム(Home)] 画面に移動して、左側のナビゲーション ペインで [ログ(Logs)] をクリックすると、Cisco Network Plug and Play アプリケーション上のログを表示できます。Cisco Network Plug and Play アプリケーションのログだけをフィルタリングするには、[サービス(Service)] ドロップダウン メニューで [pnp-service] を選択します。

ネットワーク デバイスのステータスが Cisco Network Plug and Play アプリケーションで表示されるステータスと同期していない場合は、ネットワーク デバイスのプロビジョニング ステータスをリセットできます。[サイト(Sites)] タブでデバイスを選択して [リセット(Reset)] ボタンをクリックし、次に確認ダイアログで [OK] をクリックします。デバイスをリセットすると、そのデバイスは再びプロビジョニング処理されます。デバイスは APIC-EM コントローラに再び接続して、自身の設定をすべてダウンロードし、必要に応じて IOS イメージもダウンロードします。

モバイル アプリケーションのトラブルシューティング

ブートストラップ コンフィギュレーション ファイルを取得するために、Cisco Plug and Play モバイル アプリケーションは 3G/4G/WIFI で APIC-EM コントローラに接続する必要があります。

以前にアプリケーションをコントローラに接続して、ブートストラップ コンフィギュレーションをデバイスに配信した場合は、アプリケーションをオフライン モードで使用してブートストラップを配信することもできます。ブートストラップ コンフィギュレーション ファイルはアプリケーションに残っているので、同じタイプのデバイスへのオフライン配信に使用できます。

Cisco Plug and Play モバイル アプリケーションには、アプリケーション操作とシリアル接続との相互作用に関する詳細なログが保持されます。メイン画面で [トラブルシューティング(Troubleshooting)] を選択して、[ログの表示(View Logs)] または [ログのメール送信(Email Logs)] を選択すると、ログを表示したりメール送信することができます。

ネットワーク デバイスのトラブルシューティング

展開するシスコ ネットワーク デバイスを工場出荷時のデフォルト状態に戻す必要があります。以前に設定された（またはステータスが不明な）ネットワーク デバイスを使用している場合は、次のようにして、デバイスを工場出荷時のデフォルト状態に戻してください。

- 以前に設定された（またはステータスが不明な）シスコ ルータやスイッチを使用している場合は、次の CLI コマンドを実行して、デバイスを工場出荷時のデフォルト状態に戻します。

```
configure terminal
crypto key zeroize
no crypto pki certificate pool
no pnp profile pnp-zero-touch
end
delete nvram:*.cer
delete stby-nvram:*.cer (if the device has stack members)
write erase
reload
```

- 以前に設定された（またはステータスが不明な）シスコ アクセス ポイント デバイスを使用している場合は、次の CLI コマンドを実行して、デバイスを工場出荷時のデフォルト状態に戻します。

```
debug capwap console cli
conf t
boot system flash:/ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx (3700、2700、1700、3600、2600 プラットフォームの場合)
boot system flash:/ap1g2-rcvk9w8-mx/ap1g2-rcvk9w8-mx (1600 プラットフォームの場合)
boot system flash:/ap1g1-rcvk9w8-mx/ap1g1-rcvk9w8-mx (700 プラットフォームの場合)
end
clear capwap private-config
reload [yes][confirm] yes
```

シスコ ネットワーク デバイスの Cisco Plug and Play IOS エージェントと APIC-EM コントローラ間には IP 接続が必要です。ネットワーク デバイスが APIC-EM コントローラを ping できることを確認してください。

次のようにして、Cisco Plug and Play IOS エージェントのアクティブな接続を表示できます。

```
Router# show pnp tech-support
```

必要な場合は、次のようにデバッグ情報を有効化して、Cisco Plug and Play IOS エージェントの出力をキャプチャできます。

```
Router> enable
Router> debug pnp all
Router> ter mon
```

注：debug cns all コマンドを使用すると、Cisco Networking Services（CNS）に関する詳細なデバッグ情報をキャプチャできます。通常、このコマンドを実行すると大量の出力が生成されるので、ログ バッファが十分にあることを確認してください。

Cisco Plug and Play IOS エージェントに関連するコマンドの詳細なヘルプについては、『*Cisco Open Plug-n-Play Agent Configuration Guide*』を参照してください。

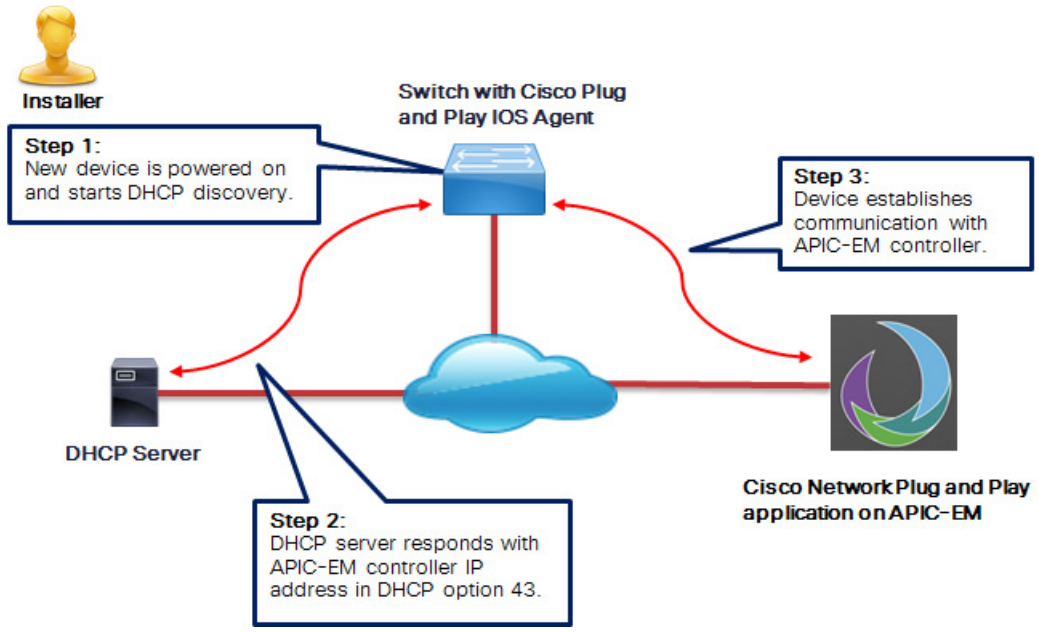
APIC-EM コントローラの自動検出に対する DHCP の設定

スタートアップ コンフィギュレーションがないシスコ ネットワーク デバイスは、Cisco Plug and Play IOS エージェントをトリガーして DHCP 検出プロセスを開始します。これにより、DHCP サーバから APIC-EM コントローラの IP アドレスを取得できます。この自動検出プロセスでは、APIC-EM コントローラに関する追加情報を含むベンダー固有のオプション 43 を、DHCP サーバに設定する必要があります。

文字列「ciscopnp」を含むオプション 60 付きの DHCP 検出メッセージを受信すると、DHCP サーバはオプション 43 情報を含む応答を返して、デバイスに応答します。

Cisco Plug and Play IOS エージェントは応答から APIC-EM コントローラの IP アドレスを取得し、そのアドレスを使用してコントローラと通信します。

図 4　DHCP による Cisco APIC-EM コントローラの検出



DHCP 自動検出方式の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバに到達できる
- DHCP サーバに Cisco Network Plug and Play 用のオプション 43 が設定されている

DHCP オプション 43 は、DHCP サーバとして動作するシスコ ルータの CLI で次のように設定された文字列値から構成されます。

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0     <-- Range of IP addresses assigned to clients
default-router 192.168.1.1            <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80"     <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分を変更する必要はありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）
- I *xxx.xxx.xxx.xxx*;（APIC-EM コントローラの IP アドレスまたはホスト名（大文字 I の後））。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*（APIC-EM コントローラへの接続に使用するポート番号）。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。

- K4;(Cisco Plug and Play IOS エージェントとサーバ間で使用される転送プロトコル)。
  - K4 = HTTP(デフォルト)
  - K5 = HTTPS
- T*rustpoolBundleURL*:デフォルト(APIC-EM コントローラ)以外の別の場所から trustpool バンドルを取得する場合は、このオプション パラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラ は、Cisco InfoSec Cloud(http://www.cisco.com/security/pki/)からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Ttftp://10.30.30.10/ios.p7b」と指定します。

  trustpool セキュリティを使用しており、T パラメータを指定しない場合、デバイスは APIC-EM コントローラから trustpool バンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;(NTP サーバの IP アドレス)。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

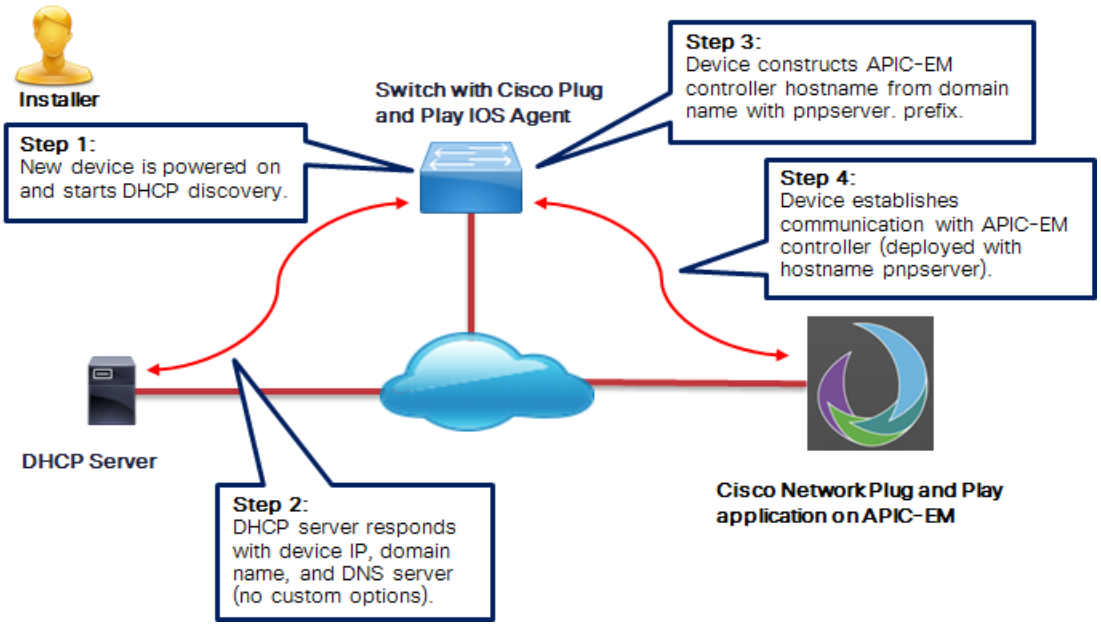
DHCP 設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DNS を使用した APIC-EM コントローラの自動検出

DHCP による検出で APIC-EM コントローラの IP アドレスを取得できない場合(たとえば、オプション 43 が設定されていない場合など)、Cisco Plug and Play IOS エージェントは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワーク ドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、APIC-EM コントローラの完全修飾ドメイン名(FQDN)を作成します。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、Cisco Plug and Play IOS エージェントは「pnpserver.customer.com」という FQDN を作成します。次に、ローカル ネーム サーバを使用して、この FQDN の IP アドレスを解決します。

図 5　DNS による Cisco APIC-EM コントローラの検出



DNS 自動検出方式の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバに到達できる
- APIC-EM コントローラがホスト名「pnpserver」で展開されている

関連資料

- 『Release Notes for Cisco Network Plug and Play』:Cisco Network Plug and Play ソリューションのリリース ノート。
- 『Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM』:APIC-EM で Network Plug and Play アプリケーションを使用してシスコ ネットワーク デバイスを設定する方法が記載されています。
- 『Cisco Open Plug-n-Play Agent Configuration Guide』:Cisco IOS または IOS-XE デバイス上で実行される、Cisco Open Plug-n-Play Agent ソフトウェア アプリケーションの設定方法が記載されています。
- 『Mobile Application User Guide for Cisco Network Plug and Play』:Cisco Network Plug and Play モバイル アプリケーションの使用方法が記載されています。
- 『Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide』:Cisco APIC-EM の展開方法とトラブルシューティング方法が記載されています。
- 『Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide』:Cisco APIC-EM の設定方法が記載されています。
- 『Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module』:Cisco APIC-EM のリリース ノート。
- 『*Cisco APIC-EM Quick Start Guide*』:APIC-EM のクイック スタート ガイド。関連資料のリストが含まれています(APIC-EM GUI で利用可能)。
- 『Open Source Used In Cisco APIC-EM』:Cisco APIC-EM で使用されるオープン ソース コードのリスト。
- 『*Open Source Used In Cisco IWAN App Release 1*』:APIC-EM 向け Cisco IWAN と Cisco Network Plug and Play アプリケーションで使用されるオープン ソース コードのリスト。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool(BST)の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。

シスコの新規および改訂版のテクニカル コンテンツを直接受信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

関連資料