Cisco Network Plug and Play エージェント

この章は、次の項で構成されています。

Cisco Network Plug and Play エージェントの前提条件

- Cisco Network Plug and Play（PnP）の展開方法は、お客様が必要とする検出プロセスのタイプによって異なります。
- PnP を起動する前に、DHCP サーバ検出プロセスか、またはドメインネームサーバ（DNS）検出プロセスのいずれかの検出メカニズムを展開します。
- PnP を展開する前に DHCP サーバまたは DNS サーバを設定します。
- PnP サーバが PnP エージェントと通信できることを確認します。
- Cisco Network PnP エージェント が PnP サーバと接続していることを確認します。Cisco Network PnP エージェントはサーバに ping できる必要があります。
- PnP エージェントは、どの要求についてもユーザ クレデンシャルを送信するよう PnP サーバに求めます。Cisco では、HTTP Secure（HTTPS）プロトコルの使用を推奨しています。

（注）

- このガイドでは、Cisco Network Plug and Play と PnP という用語は区別なく使用されており、すべて同じ意味です。
- このガイドでは、PnP エージェント、エージェント、および展開エージェントという用語は区別なく使用されており、すべて同じ意味です。
- このガイドでは、PnP サーバ、サーバ、および展開サーバという用語は区別なく使用されており、すべて同じ意味です。

Cisco Network Plug and Play エージェントの制約事項

- Cisco Network Plug and Play（PnP）エージェントは、サーバとの HTTP と HTTPS トランスポートベースの通信を促進します。
- 暗号化対応イメージがサポートされていないプラットフォームでは、HTTPS を使用することはできません（また、暗号化対応のイメージが使用されている場合も、セキュアソケットレイヤ（SSL）プロトコルや Transport Layer Security（TLS）プロトコルを使用しません）。
- 非 VLAN 1 設定 - デフォルトでは、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 Plug and Play 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 Plug and Play 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。

（注）

PNP プロセス中にファームウェア アップグレードを実行するときは、ルータ上の古いイメージを削除して、間違ったイメージがロードされないようにすることをお勧めします。

詳細については、CSCwd68868 を参照してください。

Cisco Network Plug and Play エージェントに関する情報

Cisco Network Plug and Play 展開ソリューション

Cisco Network PnP エージェントは、Cisco Network Plug and Play ソリューションに含まれています。シスコ主導の Network Plug and Play（PnP）展開ソリューションではリダイレクトの概念がサポートされており、PnP エージェント、PnP サーバ、およびその他のコンポーネントが含まれています。シスコのデバイスの簡素化された展開プロセスは、運用タスク関連の次の展開を自動化します。

- デバイスの初期ネットワーク接続を確立する
- デバイス設定を配信する
- ソフトウェアおよびファームウェアのイメージを配信する
- ライセンスを配信する
- 導入スクリプト ファイルを配信する
- ローカル クレデンシャルをプロビジョニングする
- 導入関連のイベントについて他の管理システムに通知する

簡素化された展開により、コストと複雑さが軽減され、展開の速度とセキュリティが向上します。

Cisco Network Plug and Play（PnP）エージェントは、Cisco IOS または IOS-XE デバイスで実行されているソフトウェアアプリケーションです。PnP エージェントと PnP 展開サーバは、労力のかからない展開サービスを提供します。デバイスに最初に電源を投入すると、PnP エージェントプロセスがデバイスコンソールにスタートアップ コンフィギュレーションやユーザ入力なしで起動し、PnP サーバのアドレスを検出しようとします。PnP エージェントは DHCP、ドメインネームシステム（DNS）他の方式を使用して、PnP サーバの目的の IP アドレスを取得します。PnP エージェントが IP アドレスを正常に取得すると、サーバとの長期間の双方向レイヤ 3 接続を開始し、サーバからのメッセージを待ちます。PnP サーバアプリケーションは、デバイスで実行される情報とサービスを要求するメッセージをエージェントに送信します。

PnP エージェントは、既存のソリューションを統合エージェントに統合し、現在のソリューションを強化する機能を追加します。PnP エージェントの主な目的は次のとおりです。

- すべての展開シナリオに一貫した Day 1 展開ソリューションを提供する。
- 既存のソリューションを改善するための新機能を追加する。
- Day 2 の管理フレームワークを、主に設定およびイメージのアップグレードとの関連で提供する。

Cisco Network Plug and Play の機能

次に、Cisco Network Plug and Play エージェントが提供する一部の機能を示します。

- Day 0 ブートストラップ：設定、イメージ、ライセンス、およびその他のファイル
- Day 2 管理：Simple Network Management Protocol（SNMP）と syslog メッセージの設定およびイメージのアップグレードと継続的なモニタリング
- オープン通信プロトコル — 顧客およびパートナーがアプリケーションを作成することが可能
- サーバとエージェント間の HTTP を介した XML ベースのペイロード。
- セキュリティ：管理アプリとエージェント間の認証と暗号化された通信チャネル
- ファイアウォールとネットワークアドレス変換（NAT）の背後にあるデバイスの展開と管理
- 1 対 1 および 1 対多の通信サポート
- ポリシー ベースの導入サポート（デバイスの製品 ID またはロケーション）
- 一意 ID（一意のデバイス ID（UDI）または MAC）に基づく導入
- Cisco のさまざまなプラットフォームを通じての統一ソリューション（IOS Classic を含む）
- さまざまな導入シナリオとユース ケースのサポート
- 可能ならゼロタッチ、必要ならロータッチ

Cisco Network Plug and Play エージェントのサービスと機能

Cisco Network Plug and Play エージェントのサービスと機能は次のとおりです。

1. Backoff
2. CLI の実行
3. 設定のアップグレード
4. デバイス情報
5. ファイル転送
6. イメージのインストール
7. ライセンスのインストール
8. PnP タギング
9. スクリプトの実行
10. トポロジ情報

（注） PnP サーバは、PnP エージェントによるイメージのインストールと設定のアップグレードサービス要求で使用されるオプションのチェックサムタグを提供します。チェックサムが要求に含まれている場合、イメージのインストールプロセスはそのチェックサムを実行中の現在のイメージのチェックサムと比較します。

チェックサムが同じである場合、インストールまたはアップグレードされるイメージは、デバイスで実行されている現在のイメージと同じです。このシナリオでは、イメージのインストールプロセスは他の操作を実行しません。

チェックサムが同じでない場合、新しいイメージがローカルファイルシステムにコピーされ、チェックサムが再度計算されて、要求で指定されたチェックサムと比較されます。同じ場合は、新しいイメージのインストールまたはデバイスの新しいイメージへのアップグレードが続行されます。チェックサムが異なる場合、プロセスはエラーで終了します。

Backoff

PnP プロトコル（HTTP トランスポートを使用）をサポートする Cisco IOS デバイスでは、PnP エージェントが PnP サーバに継続的に作業要求を送信する必要があります。PnP サーバに、PnP エージェントが実行するスケジュール済みまたは未処理の PnP サービスがない場合は、連続的な no operation 作業要求によってネットワーク帯域幅とデバイスリソースの両方が使い果たされます。この PnP バックオフサービスにより、PnP サーバは PnP エージェントに指定された時間だけ休止し、後でコールバックするように通知できます。

CLI の実行

Cisco IOS は、EXEC モードとグローバル コンフィギュレーション モードの 2 つのコマンド実行モードをサポートしています。EXEC コマンドのほとんどは、**show** コマンド（現在のコンフィギュレーション ステータスを表示）、**clear** コマンド（カウンタまたはインターフェイスを消去）などのように、一回限りのコマンドです。EXEC コマンドは、デバイスをリブートするときには保存されません。コンフィギュレーションモードでは、ユーザが実行コンフィギュレーションを変更できます。設定を保存すると、これらのコマンドはデバイスの再起動後も保存されます。

（注） **show** コマンドの要求と応答の詳細、およびすべての PnP 設定コマンドについては、『*Cisco Network Plug and Play Agent Command Reference*』を参照してください。

設定のアップグレード

シスコのデバイスで実行する可能性がある設定のアップグレードは 2 種類あります。1 つはスタートアップ コンフィギュレーションへの新しいコンフィギュレーション ファイルのコピー、もう 1 つは実行コンフィギュレーションへの新しいコンフィギュレーション ファイルのコピーです。

スタートアップ設定への新しい設定ファイルのコピー：新しいコ設定ファイルは **copy** コマンドを使用してファイルサーバからデバイスにコピーされ、ファイルの有効性を確認するためにファイルチェックが実行されます。ファイルが有効な場合、そのファイルがスタートアップ設定にコピーされます。使用可能なディスク領域が十分にある場合は、以前の設定ファイルのバックアップが実行されます。デバイスを再度リロードすると、新しい設定が表示されます。

実行コンフィギュレーションへの新しいコンフィギュレーションファイルのコピー：新しいコンフィギュレーション ファイルは、**copy** コマンドまたは **configure replace** コマンドを使用してファイルサーバからデバイスにコピーされます。ロールバックが効率的に実行されると、コンフィギュレーションファイルの置換とロールバックによってシステムが不安定な状態のままになることがあります。したがって、ファイルをコピーして設定をアップグレードすることをお勧めします。

デバイス情報

PnP エージェントは、要求に応じてデバイスインベントリとその他の重要な情報を PnP サーバに抽出する機能を提供します。次の 5 種類のデバイスプロファイル要求がサポートされています。

1. all：固有のデバイス識別子（UDI）、イメージ、ハードウェア、およびファイルシステムのインベントリデータを含む完全なインベントリ情報を返します。
2. filesystem：ファイルシステムの名前とタイプ、ローカルサイズ（バイト単位）、空きサイズ（バイト単位）、読み取りフラグ、書き込みフラグなど、ファイルシステムのインベントリ情報を返します。
3. hardware：ホスト名、ベンダー文字列、プラットフォーム名、プロセッサタイプ、ハードウェアリビジョン、メインメモリサイズ、I/O メモリサイズ、ボード ID、ボードリワーク ID、プロセッサリビジョン、ミッドプレーンリビジョンおよび場所など、ハードウェアインベントリ情報を返します。
4. image：バージョン文字列、イメージ名、ブート変数、rommon への復帰理由、ブートローダ変数、コンフィギュレーション レジスタ、次回ブート時のコンフィギュレーション レジスタ、およびコンフィギュレーション変数など、イメージインベントリ情報を返します。バージョン文字列、イメージ名、ブート変数、rommon への復帰理由、ブートローダ変数、コンフィギュレーション レジスタ、次回ブート時のコンフィギュレーション レジスタ、およびコンフィギュレーション変数など、
5. UDI：デバイス UDI を返します。

ファイル転送

PnP ファイルサーバは、ネットワーク内の展開デバイスによってコピーできるファイルをホストします。ファイルサーバは、ファイルをホストする専用サーバ、または PnP サーバをホストするデバイスの一部にすることができます。PnP エージェントは、標準のファイル転送プロトコルを使用して、リモートファイルサーバからデバイスにファイルをコピーします。デバイスが暗号化イメージを実行している場合は、SFTP、SCP、HTTPS などのセキュアなファイル転

送プロトコルがサポートされます。非暗号化イメージを実行するデバイスの場合、PnP エージェントは FTP、TFTP、HTTP などのセキュアでないコピープロトコルをサポートします。

イメージのインストール

イメージインストールサービスを使用すると、PnP 対応デバイスが PnP サーバから要求を受信した時点でイメージのアップグレードを実行できます。

スタンドアロン デバイス

スタンドアロンデバイス上の PnP エージェントが PnP サーバから要求を受信すると、エージェントは XML ペイロードを解析し、その要求をイメージアップグレード要求として識別します。次に、エージェントは ImageInstall プロセスを作成します。このプロセスは、スタンドアロンイメージ インストール要求として識別されます。PnP エージェントは、ImageInstall サービスによって定義されたデータ構造を入力し、それを ImageInstall サービスに渡します。

その後、イメージ インストール サービスは次の操作を実行して、新しいイメージをデバイスに正常にロードします。

1. ファイルサーバからローカルディスクにイメージをコピーします（ファイルサーバ情報は、要求で PnP サーバによって提供されます）。
2. **boot system** コマンドを実行して、次回のリロード時に新しいイメージをロードするようにデバイスを設定します。
3. デバイスをリロードし、PnP サーバにメッセージを送信します。

PnP タギング

Cisco IOS は、すべてのシスコのデバイスをより適切にグループ化および追跡するために、デバイスにタグを割り当てる機能を提供します。PnP エージェントは、デバイスでタグ情報を設定し、Cisco Discovery Protocol（CDP）を使用してネットワーク内でタグ情報を伝達するための XML サービスを提供します。このサービスの目的は、PnP エージェントがタグ情報を認識し、要求に応じてこの情報を PnP サーバに渡すことです。

トポロジ情報

デフォルトでは、ネットワーク上のすべてのシスコのデバイスが Cisco Discovery Protocol（CDP）を実行します。ネットワーク内のデバイスは、CDP を介して直接のネイバーを検出し、プロトコルを介して学習または取得した属性をデータベースに入力します。このネイバー情報はデータベースに保存され、デバイスが PNP サーバに対してオンデマンドで使用できます。一般的なネイバー情報には、ネイバーデバイス ID、ソフトウェアバージョン、ハードウェア プラットフォーム、インターフェイス IP、および CDP メッセージが送受信されるポートが含まれます。

ソフトウェア メンテナンス アップグレード

ソフトウェア メンテナンス アップグレード（SMU）は特定の障害の修正やリリース済みのイメージに対するセキュリティの解決策を含むパッケージです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。SMU はルータ動作に大きく影響を及ぼ

すことはありません。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンス バージョンに同期されます。

ソフトウェア メンテナンス アップ グレード パッケージをインストールし、アクティブ化するには、次の手順を実行します。

ステップ 1 **install add** <*filename*> コマンドを使用してパッケージ ソフトウェア ファイルを解凍し、それを起動デバイス（通常は disk0）にコピーします。ファイルがリモートソースにある場合は、tftp/ftp オプションを使用してファイルをデバイスにコピーします。

ファイルがデバイスにコピーされると、パッケージ内の情報を使用して、対象カードとの互換性と、他のアクティブなソフトウェアとの互換性が確認されます。パッケージの互換性とアプリケーション プログラム インターフェイス（API）の互換性が確認された場合に限り、実際のアクティブ化が実行されます。

ステップ 2 パッケージをアクティブ化するには、**install activate** <*filename*> コマンドを使用します。アクティブ化操作により互換性チェックが実行され、ソフトウェア メンテナンス アップグレード パッケージがインストールされます。リロード ソフトウェア メンテナンス アップグレードの場合は、自動的にリロードが開始されます。

ステップ 3 **install commit** コマンドを使用して変更をコミットします。

ステップ 4 パッケージを非アクティブ化するには、**install deactivate** <*filename*> コマンドを使用します。

ステップ 5 以前のパッケージセットの方が現在アクティブなパッケージセットよりも適切であることがわかった場合は、**install rollback to committed** コマンドを使用して、以前アクティブだったパッケージ セットを再びアクティブにできます。

ステップ 6 インストールされているバージョンを削除するには、**install remove** <*filename*> コマンドを使用します。

次に、ソフトウェア メンテナンス アップグレード パッケージをデバイスにインストールし、削除する例を示します。

```
install add <filename>
install activate <filename>
install commit
install rollback to committed
install remove <filename>
```

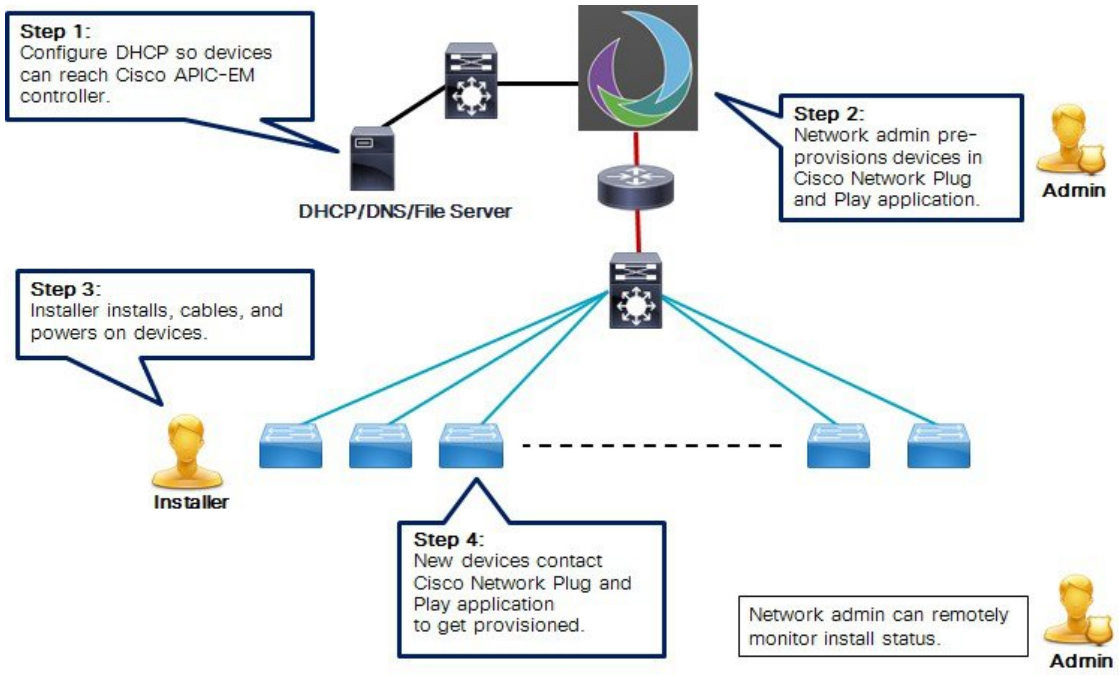
Cisco Network Plug and Play エージェント

Cisco Network Plug and Play エージェントは、シスコのネットワーク デバイスのうち、簡素化された展開アーキテクチャをサポートするものすべてに含まれている組み込みソフトウェア コンポーネントです。PnP エージェントが認識し、対話する対象は PnP サーバのみです。PnP エージェントはまず、通信可能な PnP サーバの検出を試みます。サーバが検出されて接続が確立されると、エージェントはサーバと通信し、設定、イメージ、ライセンス、ファイル更新などの展開関連のアクティビティを実行します。また、アウトオブバウンドの設定変更やインターフェイス上の新しいデバイス接続などの対象のすべての展開関連イベントをサーバに通知します。

Cisco Network Plug and Play サーバ

Cisco Network Plug and Play サーバは、導入するデバイスの展開情報（イメージ、設定、ファイル、およびライセンス）の管理や配布のロジックを符号化する中央サーバです。このサーバは、特定の展開プロトコルを使用することで、簡素化された展開プロセスをサポートするデバイス上のエージェントと通信します。

図 *1* : 簡素化された展開サーバ



PnP サーバは、スマートフォンと PC の導入アプリケーションなどのプロキシサーバ、Neighbor Assisted Provisioning Protocol（NAPP）として動作する他の PnP エージェント、および VPN ゲートウェイのようなその他のタイプのプロキシ導入サーバと通信します。

PnP サーバは、エージェントを別の展開サーバにリダイレクトできます。リダイレクトの一般的な例は PnP サーバによるリダイレクトで、ブートストラップ設定を NAPP サーバを介して送信した後に直接通信するデバイスをリダイレクトします。PnP サーバは企業がホストできます。このソリューションでは、シスコが提供するクラウドベースの展開サービスが可能です。この場合、デバイスはシスコのクラウドベースの展開サービスを検出して通信し、初期導入を実行します。その後、お客様の展開サーバにそのデバイスをリダイレクトできます。

デバイスとの通信に加え、サーバは認証、承認、アカウンティング（AAA）システム、プロビジョニングシステム、その他の管理アプリケーションなどのさまざまな外部システムと連動します。

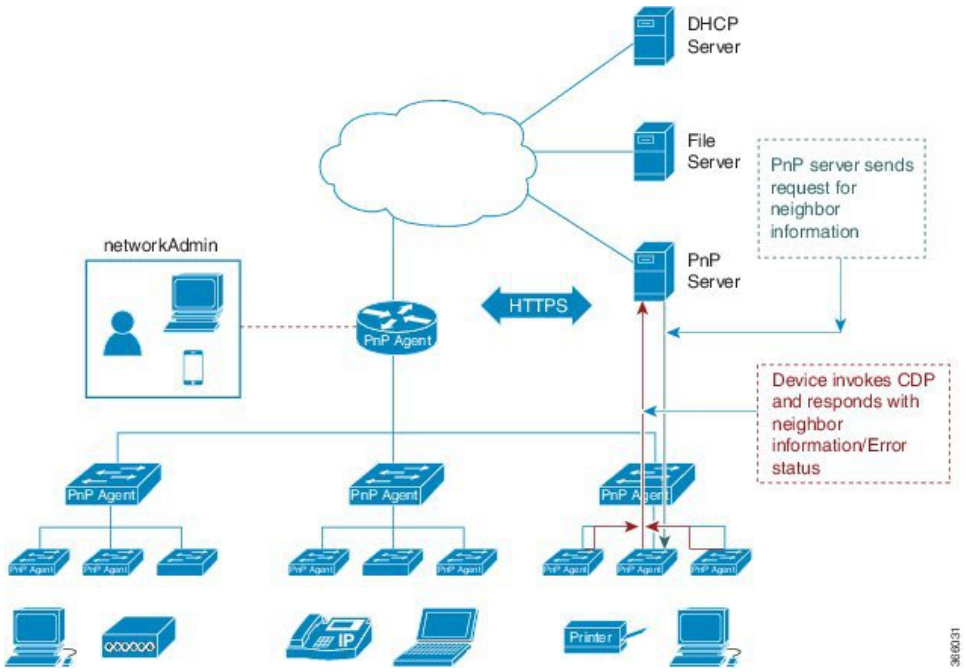
Cisco Network Plug and Play エージェントの展開

次に、シスコのデバイスでの Cisco Network Plug and Play エージェントの展開手順を示します。

1. PnP エージェントを備えているシスコのデバイスは PnP サーバに問い合わせタスクを要求します。つまり、PnPエージェントは作業の要求とともに、一意のデバイス識別子（UDI）を送信します。
2. デバイスのタスクがある場合は、PnP サーバは作業要求を送信します。たとえば、イメージのインストール、設定のアップグレードなどです。
3. PnP エージェントが作業要求を受信すると、タスクを実行し、タスクのステータス、成功かエラーかと要求された対応する情報に関する応答を PnP サーバに返します。

Cisco Network Plug and Play エージェントのネットワークトポロジ

図 *2 : Cisco Network Plug and Play* エージェントの展開のネットワークトポロジ



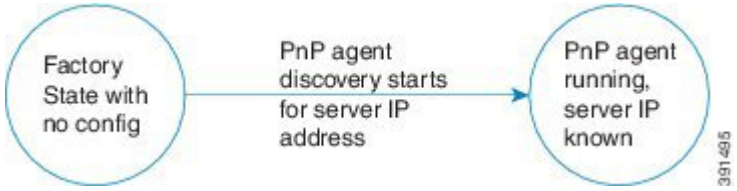
Cisco Network Plug and Play エージェントの初期化

Cisco Network Plug and Play エージェントソフトウェアは現在すべての Cisco IOS XE プラットフォームで使用でき、デフォルトで有効になっています。PnPエージェントは次の方法でデバイス上で開始できます。

スタートアップ コンフィギュレーションなし

新しいシスコのデバイスは、デバイスのNVRAMの中にスタートアップ コンフィギュレーションファイルのない状態でお客様に出荷されます。新しいデバイスがネットワークに接続され、電源が投入された時点でスタートアップ コンフィギュレーションとユーザ入力ファイルがデバイス上にない場合は、Cisco Network Plug and Play エージェントが自動的に起動され、PnP サーバの IP アドレスを検出します。

図 *3 :* スタートアップ コンフィギュレーションなしの *PnP* トリガーの状態図



Open Plug-n-Play エージェントの CLI 設定

ネットワーク管理者は CLI 設定を使用すると Plug-n-Play（PnP）エージェントプロセスをいつでも開始できます。CLI を介して PnP プロファイルを設定することによって、ネットワーク管理者はデバイス上で PnP エージェントを開始したり停止したりできます。CLI を使用して PnP プロファイルを設定すると、デバイスは PnP エージェントプロセスを開始し、次にそのプロセスが PnP プロファイル内の IP アドレスを使用して PnP サーバとの接続を開始します。

図 *4 : CLI* 設定 *PnP* プロファイルによる *PnP* トリガーの状態図

Cisco Network Plug and Play エージェントの展開ソリューション

この項では、デバイスの導入と管理のために PnP サーバに公開される Cisco Network Plug and Play エージェントの機能について説明します。PnP エージェントの展開ソリューションは、エージェント、デバイス、エージェント、およびサーバ間の通信、ならびに PnP エージェントサービスによって開始される検出プロセスで構成されています。PnP ソリューションについては、次の項で詳しく説明します。

Cisco Network Plug and Play エージェント検出プロセス

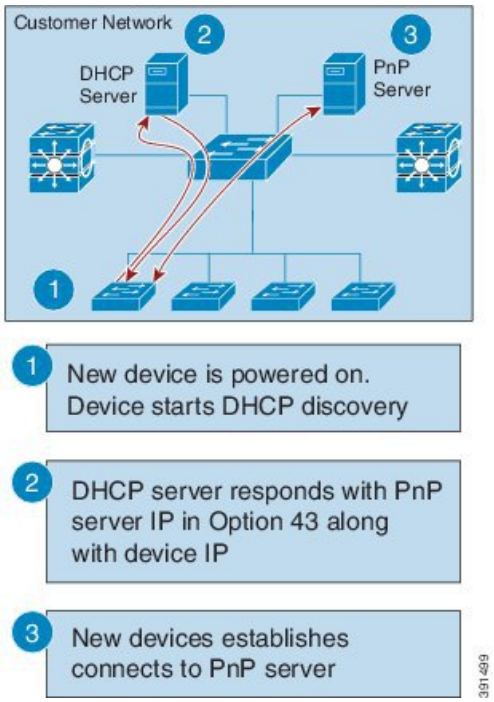
デバイスが起動すると、NVRAM のスタートアップコンフィギュレーションのいずれかがない場合は PnP 検出エージェントによって PnP サーバの IP アドレスが取得されます。PnP サーバの IP アドレスを取得するため、PnP エージェントは次の検出機能のうちの 1 つを実行します。

1. DHCP サーバによる PnP の検出
2. DHCP スヌーピングによる PnP の検出
3. DNS ルックアップによる PnP の検出
4. レイヤ 2 およびレイヤ 3 デバイスの PnP プロキシ
5. PnP 導入アプリケーション

DHCP サーバを介した Cisco Network Plug and Play 検出

NVRAM にスタートアップ コンフィギュレーションのないデバイスは、Cisco Network Plug and Play エージェントを起動し、DHCP サーバからデバイスに必要な IPv4 設定を取得する DHCP 検出プロセスを開始します。DHCP サーバは、文字列「cisco pnp」のあるデバイスからオプション 60 を受信した時点でベンダー固有のオプション 43 を使用して追加の情報を挿入し、PnP サーバの IPv4 アドレスまたはホスト名を要求側のデバイスに渡します。デバイスが DHCP 応答を受信すると、PnP エージェントは応答からオプション 43 を抽出して、PnP サーバの IP アドレスまたはホスト名を取得します。PnP エージェントは、PnP サーバと通信するためにこの IPv4 アドレスまたはホスト名を使用します。

図 *5 : PnP* サーバの *DHCP* 検出プロセス



前提条件：

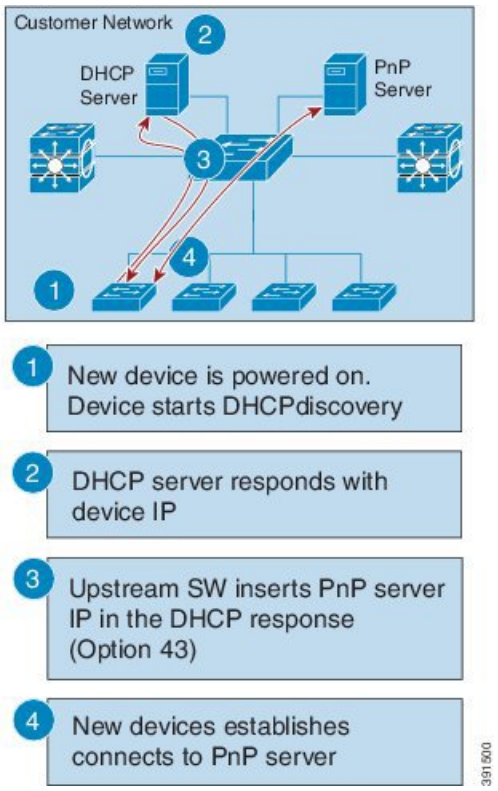
- 新しいデバイスが DHCP サーバに到達できる
- お客様がネットワークデバイスの DHCP サーバを設定する意思がある

DHCP スヌーピングによる Plug-n-Play 検出

ベンダー固有のオプションを挿入するようにサードパーティ製DHCP サーバを設定することができない場合、DHCP 応答にスヌーピングし、PnP サーバの IP アドレスを持つ PnP 固有のオプション 43 を挿入するように、既存の Cisco Open Plug-n-Play（PnP）対応デバイスを設定できます。

オプション 43 を挿入する前に、スヌーピング エージェントにより、DHCP メッセージがネットワーク内のシスコデバイスからのものかどうかが確認されます。DHCP 検出プロセスの残りの部分は、前のセクションで説明したものと同じです。

図 *6 : PnP* サーバによる *DHCP* スヌーピング



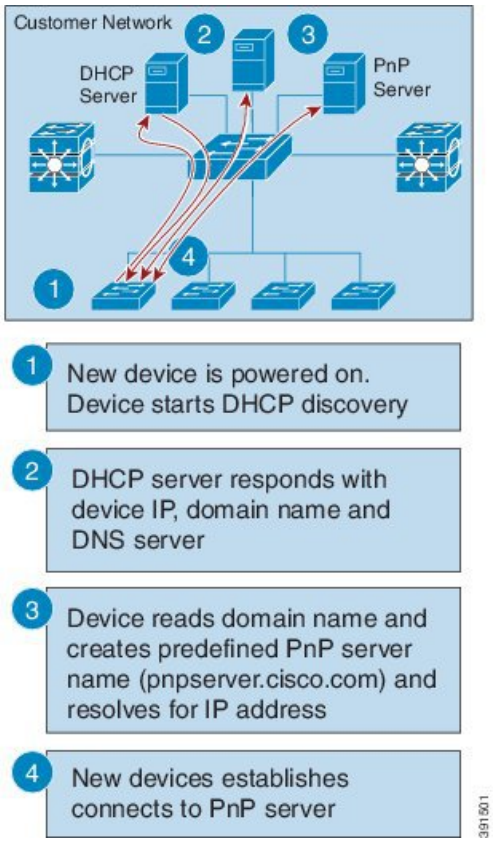
前提条件：

- 新しいデバイスが DHCP サーバに到達できる
- 新しいデバイスが DNS サーバに到達できる
- お客様がネットワークデバイスの DHCP サーバを設定することを希望していない
- DHCP をスヌーピングし、PnP サーバ IP を挿入するようにアップストリームスイッチ（SW）が設定されている

DNS ルックアップによる Cisco Network Plug and Play 検出

DHCP 検出で Cisco Network Plug and Play サーバの IP アドレスが取得できないと、エージェントは ドメインネームシステム（DNS）ルックアップ方式にフォールバックします。次に、PnP エージェントはプリセットの展開サーバ名を使用します。エージェントは、DHCP応答から顧客のネットワークのドメイン名を取得し、完全修飾ドメイン名（FQDN）を形成します。次の FQDN は、DHCP応答のプリセットの展開サーバ名とドメイン名情報（*deployment.customer.com*）を使用して PnP エージェントによって構成されます。次に、エージェントは、ローカル ネーム サーバでの検索を実行し、前述の FQDN の IP アドレスの解決を試みます。

図 *7 : deployment.customer.com* の *DNS* ルックアップ



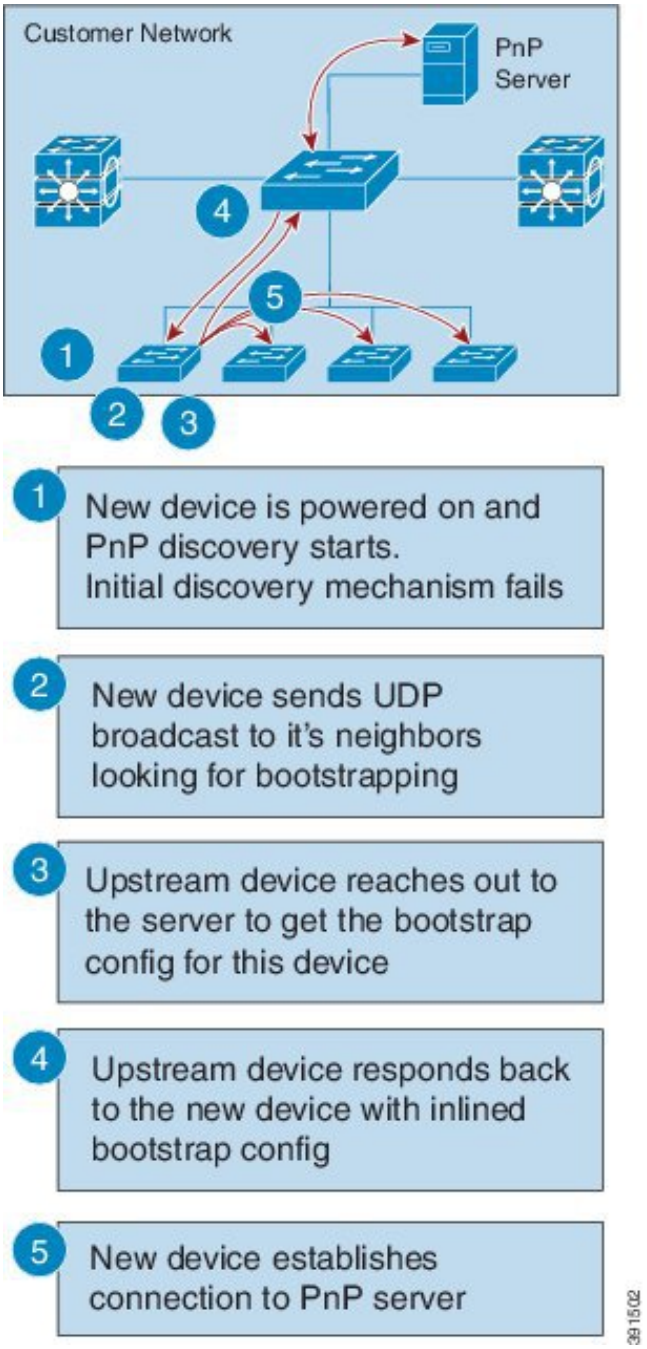
前提条件：

- 新しいデバイスが DHCP サーバに到達できる
- 「pnpserver」という名前でお客様がネットワークに PnP サーバを展開した

レイヤ 3 デバイスとレイヤ 2 デバイス用の Cisco Network Plug and Play プロキシサーバ

このデバイスは、特定のポートで PnP 着信メッセージをリッスンします。PnP デバイスとしての登録を試みるシスコ デバイスは、ネットワークに UDP ブロードキャスト メッセージを 30 分ごとに 10 回送信します。したがって、デバイスが応答を受信しない場合、ブロードキャストは 300 分後に停止します。

図 *8 :* レイヤ *3* デバイスとレイヤ *2* デバイスの *DNS* ルックアップ



プロキシ サーバ プロセスのホスト デバイスが着信ブロードキャストを受信すると、要求中のバージョン フィールドを検証し、バージョンの検証が成功すると、PnP サーバに要求を転送します。また、プロキシ サーバ プロセスは、PnP サーバに要求を転送する前に、着信データグラムにより要求元クライアントの Unique Device Identifier（UDI）をキャッシュに入れます。

プロキシ サーバは PnP サーバからコンフィグレット データグラムを受信すると、UDI キャッシュ内のエントリを使用して、着信データグラムの UDI の検証を実行します。検証が成功すると、プロキシ サーバ プロセスはそのデータグラムを、プロキシ クライアント プロセスがデータグラムを受信するために予約されている特定のポート番号にブロードキャストします。

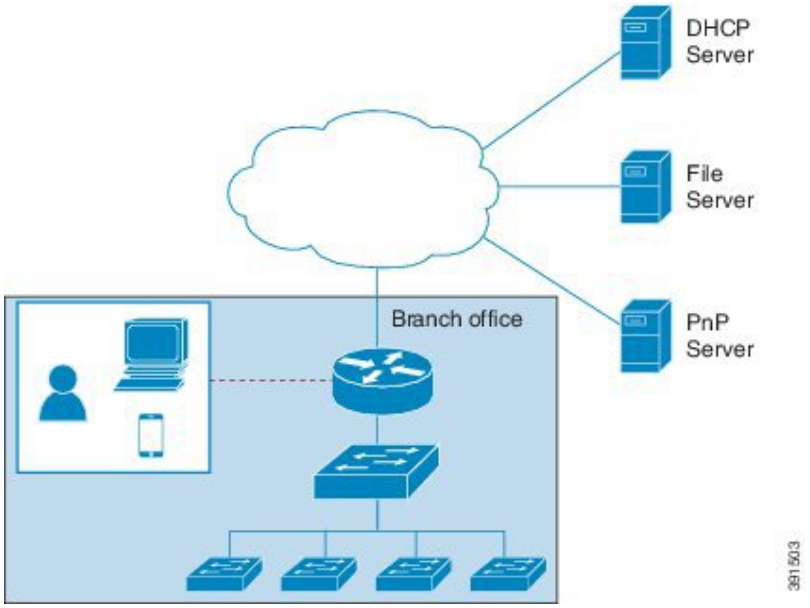
そのデータグラムを受信すると、プロキシクライアントプロセスを実行するデバイスは、ターゲット UDI を得るため着信データグラムを解析します。そのデータグラムのターゲット UDI がデバイスの UDI と一致すると、プロキシ クライアント プロセスは、フレーミング、エラー制御、およびコンフィグレットの設定に進みます。

データグラムのターゲット UDI がデバイスの UDI と一致しない場合、パケットはドロップされます。

Plug-n-Play エージェント展開アプリケーション

また、シスコのデバイスは、PC またはスマートフォンで実行されている展開アプリケーションを使用してネットワーク管理者が手動で設定することができます。PC またはスマートフォンは、USB またはイーサネットケーブルを使用してデバイスに接続できます。

図 *9:* 手動で設定された *PnP* エージェント



Plug-n-Play エージェント展開プロトコル

展開はさまざまなトランスポートを介して実行できます。これらのトランスポートには、イーサネットと Transport Layer Security（TLS）を使用した IP が含まれます。レイヤ 2 トランスポートは通常、展開エージェントと、展開アプリケーションなどのプロキシ展開サーバ間、またはプロキシとして機能する展開エージェントとして使用されます。エージェントとサーバ間のトランスポートは、セキュリティのために TLS を使用した IP 接続を介して行われます。プロキシ展開サーバと展開サーバ間のトランスポートも、TLS を使用した IP を介して行われます。

Plug-n-Play エージェント アプリケーション プロトコル

Cisco Open Plug-n-Play（PnP）エージェント アプリケーション プロトコルは、ネットワークデバイスをリモートアプリケーションでモニタおよび制御可能なメカニズムを定義するXMLベースのプロトコルです。PnPエージェントは、シスコのデバイスで実行するソフトウェアモジュールです。PnP サーバは、ネットワークデバイスをリモートで管理するネットワークマネージャとして実行するアプリケーションです。PnP プロトコルの主な機能は次のとおりです。

1. HTTP プロトコルをサポート
2. HTTP の Transport Level Security（TLS）ベースの暗号化をサポート
3. TLS ハンドシェイクに HTTP セキュア（HTTPS）証明書を使用

イーサネットトランスポートによる Plug-n-Play

Cisco Open Plug-n-Play（PnP）エージェントは、次の 2 つのシナリオでイーサネットベースのトランスポートを使用します。

- **PC 上の展開アプリケーションと通信する展開エージェント**：この場合、PCはイーサネットケーブルを使用して展開されるデバイスに接続されます。展開アプリケーションは、イーサネットトランスポートをサポートする展開サーバとしてそれ自体をアドバタイズします。
- **展開エージェントがプロキシ展開サーバとして機能する、すでに展開されているデバイスと通信している場合**：この場合、展開する新しいデバイスには、すでに展開されているデバイスへのイーサネット接続が備わっています。展開されたデバイス上の展開エージェントは検出要求に応答し、新しいデバイスのプロキシ展開サーバとして機能します。

検出が完了すると、展開エージェントはイーサネットを介して展開サーバとのセキュアでないXML ストリームを開始します。このプロトコルは、このために Ethertype（0xXX TBD）を予約します。展開エージェントとサーバは、拡張可能認証プロトコル/トランスポート層セキュリティ（EAP-TLS）を使用して通信を保護し、EAP-TLS セッションの確立を完了します。次に、展開サーバはHTTPセキュア（HTTPS）証明書またはその他のサポートされているメカニズムを使用してデバイスを認証します。

IP を介した Plug-n-Play トランスポート

Cisco Network Plug-n-Play（PnP）エージェントでは、展開エージェントが展開サーバへの TCP 接続を開き、メッセージの XML ストリームを開始します。サーバはこの時点で Transport Layer Security（TLS）の使用を要求できます。エージェントは既存の XML ストリームを閉じ、サーバへの TLS 接続を開始してから XML ストリームを再起動します。サーバは TLS 接続を介してエージェント認証を要求できます。

Plug-n-Play エージェントのセキュリティ

すべての Cisco Open Plug-n-Play（PnP）デバイスに対するセキュリティは、トランスポートレベルとアプリケーションレベルの両方で提供されます。以降の項では、セキュリティメカニズムについて詳しく説明します。

Plug-n-Play トランスポートレイヤ 3 セキュリティ

非暗号化または非暗号化対応イメージの場合、TLS セキュリティを選択することはできません。代わりとなるもう 1 つの最小セキュリティは、指定した信頼できる PnP サーバへの接続を PnP エージェントがポート 5222 で開始することです。

Plug-n-Play エージェントとサーバ間の認証と承認

Cisco Open Plug-n-Play（PnP）展開エージェントが PnP サーバを検出すると、エージェントは Transport Layer Security（TLS）ハンドシェイクを実行します。サーバに対してそのエージェント自体を認証するために、エージェントは HTTP セキュア（HTTPS）証明書を提示します。PnP サーバの管理者は、特定の展開に受け入れられるデバイス認証メカニズムを設定します。

展開サーバは、エージェントがサーバを認証できるように、展開エージェントに証明書を提示します。エージェントがサーバ証明書を確認できるかどうかに関係なく、エージェントは TLS 後の認証交換で展開サーバを使用します。この交換で、エージェントはサーバにサーバ認証トークンの提示を要求します。この要求に応じて、サーバはシスコから取得した認証トークンを提示します。エージェントは認証トークンの署名を確認します。認証トークンが Unique Device Identifier（UDI）に固有の場合、エージェントはその UDI が認証トークンのリストに存在していることも確認します。この手順の最後に、展開エージェントとサーバ間にセキュアな通信チャネルが確立されます。このセキュアな通信チャネルは、展開情報をエージェントに送信するためにサーバが活用します。

PnP 検出プロセスのセキュリティ方式

このセクションでは、PnP エージェント サーバ通信をさまざまなシナリオで保護するために使用する方法について説明します。セキュリティオプションは、ゼロタッチ PnP サーバ検出時に PnP エージェントによって使用されます。

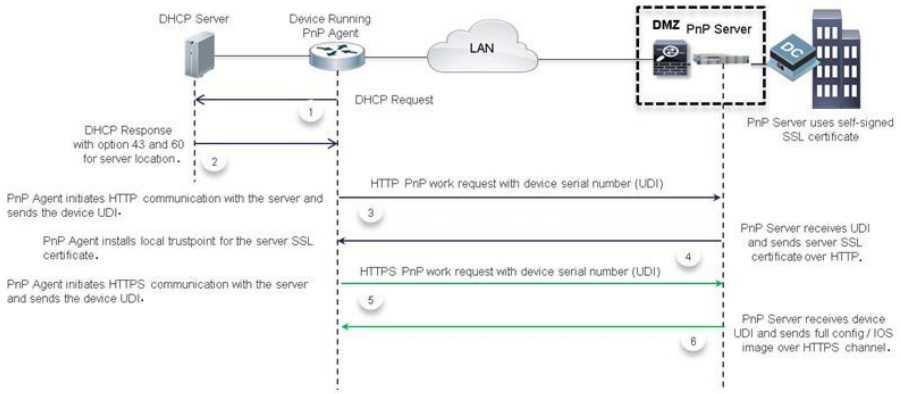
自己署名証明書ベースの認証

PnP サーバには、サーバ側の認証に自己署名 SSL 証明書を使用するオプションがあります。PnP サーバが自己署名証明書を使用する場合、PnP 検出を使用してエージェントからサーバへのセキュアな通信を自動的に開始することはできません。デバイスは通常の PnP 検出メカニズムを通過し、サーバが検出されると、エージェントは HTTP 経由で作業要求を送信します。サーバは PnP 証明書インストールサービスを使用してサーバの自己署名証明書をインストールして HTTPS を介してサーバに自動的に再接続するようにエージェントに指示する必要があります。

ソリューションのセキュリティを確保するには、サーバの非セキュアなポート 80 を使用して、1 回限りの証明書のインストールをデバイスに配信することを推奨します。他のすべてのサービスは、セキュアなポートを介して送信する必要があります。

次の図に、自己署名サーバ SSL 証明書を使用したエンドツーエンドのセキュアな PnP ワークフローを示します。

図 *10* : 自己署名証明書を使用した *PnP* の展開

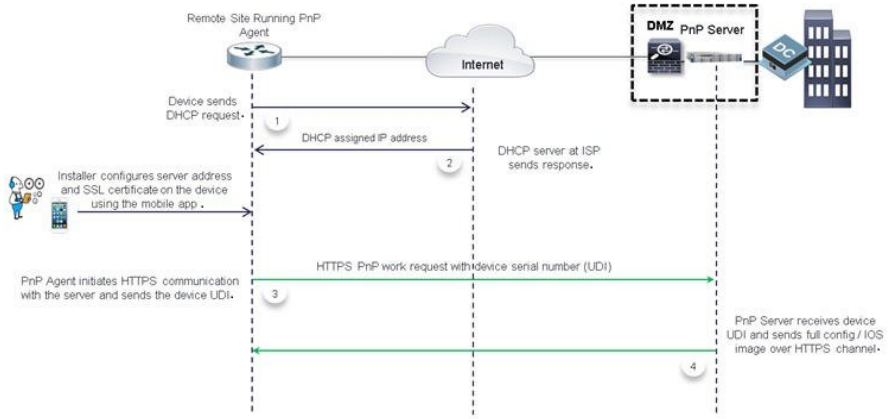


モバイルデバイスベースのセキュアなインストール

このソリューションの一部として、モバイルデバイス用のアプリケーションを使用してデバイスにブートストラップを設定できます。モバイルアプリケーションを使用して、他のブートストラップ設定とともに各デバイスにサーバ証明書を直接インストールし、PnP エージェントがサーバとのセキュアな通信を開始できるようにすることができます。この方法では、サーバは証明書インストール用のセキュアでないポートを開きません。

次の図に、モバイルデバイスでアプリケーションを使用するエンドツーエンドのセキュアな PnP ワークフローを示します。

図 *11* : モバイルアプリケーションによるセキュアな *PnP* 展開



CA 署名付き証明書ベースの認証

シスコでは、署名機関によって署名された証明書を .tar ファイル形式で配布し、シスコの認証局（CA）の署名を使用してバンドルに署名します。この証明書バンドルは、cisco.com でのパブリックダウンロード向けに Cisco infoSec によって提供されます。

このバンドルの証明書は、SSL ハンドシェイク時にサーバ側の検証用 Cisco IOS デバイスにインストールできます。サーバでは、バンドルで使用可能な CA のいずれかによって署名された証明書を使用するものとします。

PnP エージェントは、組み込み PKI 機能を使用して証明書バンドルを検証します。バンドルはシスコの CA によって署名されるため、エージェントはデバイスに証明書をインストールする前に、改ざんされたバンドルを特定できます。エージェントによってバンドルの整合性が確認されると、デバイスに証明書がインストールされます。証明書がデバイスにインストールされると、サーバから追加手順を実行しなくても PnP エージェントがサーバへの HTTPS 接続を開始します。次のメカニズムは PnP エージェントがゼロタッチのセキュアな通信を開始するのに役立ちます。

IPv4 ネットワークを介した DHCP オプションベースの検出

DHCP オプション 43 とオプション 60 は、PnP サーバを検出して接続するために PnP エージェントが使用するベンダー固有の識別子です。複数のベンダーをサポートするために、シスコのデバイスの PnP エージェントは DHCP 検出時にオプション 60 文字列として大文字と小文字を区別して「ciscopnp」を送信します。DHCP サーバは各ネットワークデバイスからの異なるオプション 60 文字列と一致する複数のクラスで設定できます。オプション 60 の文字列が一致すると、DHCP サーバは対応するオプション 43 の文字列をデバイスに送り返します。次に、PnP 展開のオプション 43 を定義するための形式を示します。

*option 43 ascii "5A;K5;B2;I10.30.30.10;J443;**Ttftp://10.30.30.10/ ios.p7b**;Z10.30.30.1*

PnP 文字列のフィールド「T」は、ネットワーク管理者がローカルまたはリモートのファイルサーバでホストできる証明書バンドルの場所を指定するためのオプションを提供します。

指定された場所で証明書バンドルが使用可能な場合、エージェントは次の処理を実行します。

1. ファイルサーバからデバイスにバンドルをダウンロードします。
2. ダウンロードしたバンドルの署名を調べて、正規のシスコの署名があることを確認します。
3. デバイスに証明書をインストールします。

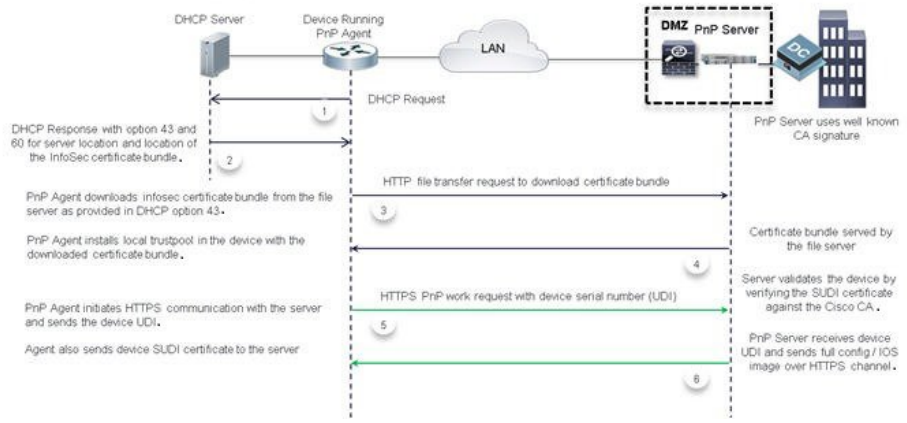
「T」オプションが指定されておらず、トランスポートメカニズムがオプション 43 文字列で HTTPS として指定されている場合、PnP エージェントは同じサーバ（*http://10.30.30.10:443/certificates/default/cert.p7b*）のデフォルトフォルダでシスコの署名付き証明書バンドルを検索します。

証明書がデフォルトの場所にある場合、エージェントは上記の手順を実行して証明書をインストールします。

証明書がインストールされ、サーバ検出が完了すると、エージェントは追加設定なしでサーバとの HTTPS 接続を開始します。HTTPS ハンドシェイク時に、デバイスはバンドルからインストールされた証明書を使用してサーバ証明書を検証します。

次に、CA バンドルベースの証明書を使用した、S エンドツーエンドのセキュアな PnP ワークフローの図を示します。

図 *12* : トラストプールによるセキュアな *PnP* 展開



このフローは、バンドルで使用可能な既知の署名機関のいずれかによって署名された証明書をサーバが使用している場合にのみ機能します。サーバがバンドルに含まれていない証明書を使用する場合、HTTPS ハンドシェイクは失敗します。トランスポートオプションとして HTTPS を使用してオプション 43 の文字列を指定し、バンドルのダウンロードが失敗した場合、サーバが到達可能であっても、エージェントはセキュアでない通信プロトコルにフォールバックしません。トランスポートオプションが HTTP として有効な証明書バンドルの場所を指すパラメータ「T」を使用して指定されている場合、エージェントは転送オプション HTTP をオーバーライドし、セキュアな通信を確保するために HTTPS に変更します。通常、エージェントは使用可能なオプションから最もセキュアな通信を選択します。

証明書バンドルファイルを見つけるために DHCP オプション 43 で指定されたパスは絶対 URL または相対 URL のいずれかです。相対 URL を指定すると、エージェントはオプション 43 の文字列で指定されているサーバの IP アドレスまたはホスト名を使用して完全な URL を形成し、ファイル転送プロトコルとして HTTP を使用します。

また、証明書をインストールするために、エージェントはデバイスのシステムクロックが更新されていると想定しています。DHCP サーバを最初に設定するため、DHCP サーバで現在時刻を指定することはできません。このようなシナリオでは、IP アドレスまたは URL をオプション 43 の代替パラメータとしてプレフィックス「Z」を付けて指定できます。これにより、デバイスは NTP サーバをポイントできます。エージェントは、デバイスのクロックを NTP サーバと同期し、証明書をインストールします。

IPv6 ネットワークを介した DHCP オプションベースの検出

Cisco Network PnP は、IPv6 DHCP 検出プロセスに DHCP オプション 16 とオプション 17 を使用します。オプション 16 とオプション 17 はベンダー固有の識別子です。これらは、Cisco Network PnP エージェントが Cisco Network PnP サーバを検出して接続するために使用されます。DHCP サーバはベンダー固有のオプション 17 を使用して追加情報を挿入するように設定できます。DHCP サーバが文字列 *cisco pnp* を含むオプション 16 をデバイスから受信し、オプション 17 の文字列と一致する場合、サーバは要求元のデバイスに Cisco PnP サーバの IP アドレスまたはホスト名を渡します。デバイスが DHCPv6 応答を受信すると、Cisco Network PnP エージェントは応答からオプションを抽出し、Cisco PnP サーバの IPv6 アドレスを識別します。Cisco PnP エージェントはこの IPv6 アドレスを使用して Cisco PnP サーバと通信します。

証明書を取得してインストールするには、「IPv4 ネットワークを介した DHCP オプションベースの検出」の項で説明したのと同じプロセスを使用します。

次に、ベンダー固有のオプションを使用してプール（DHCPv6-pool）を設定する例を示します。

```
ipv6 dhcp pool dhcpv6-pool
 address prefix 2003::/64 lifetime infinite infinite
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;K4;B3;IFE80::2E0:81FF:FE2D:3799;J6088"
```

DNS ベースの検出

DNS ベースの検出では、DHCP サーバはカスタマーネットワークのドメイン名を受け取ります。ドメイン名は、*pnpserver.<domain_name>* などの PnP 固有の完全修飾ドメイン名（FQDN）の作成に使用されます。この方法では、カスタマーネットワークはこの URL を有効な PnP サーバの IP アドレスに解決します。証明書の場所を指定するメカニズムがないため、エージェントは HTTPS 接続を開始するサーバ証明書を見つけます。手動での介入は必要ありません。

システムの起動時に、デバイスはドメイン名とともに IP ネットワーク情報を DHCP サーバから取得します。お客様固有のドメイン名を使用して、Cisco PnP エージェントは URL *pnpserver.<domain_name>* を作成し、シスコの署名付き証明書バンドルをサーバのデフォルトフォルダ *<domain_name>/ca/trustpool/cabundle.p7b* で検索します。

指定された場所で証明書バンドルが使用可能な場合、エージェントは次の処理を実行します。

1. ファイルサーバからデバイスにバンドルをダウンロードします。
2. ダウンロードしたバンドルの署名を調べて、正規のシスコの署名があることを確認します。
3. デバイスに証明書をインストールします。

指定した場所で証明書バンドルが使用できない場合、PnP エージェントは事前定義された URL *pnpcertserver.<domain_name>* を使用してサーバのデフォルトフォルダ *<domain_name>/ca/trustpool/cabundle.p7b* でシスコの署名付き証明書バンドルを検索します。

指定された場所に証明書がある場合、エージェントは証明書をインストールするために上記の手順を実行します。

証明書がインストールされ、サーバの検出が完了すると、設定を追加することなく、エージェントは URL *pnpserver.<domain_name >* でサーバとの HTTPS 接続を開始します。HTTPS ハンドシェイク時にデバイスはバンドルからインストールされた証明書を使用してサーバ証明書を検証します。

また、証明書をインストールするために、エージェントはデバイスのシステムクロックが更新されていると想定しています。DHCP サーバを最初に設定するため、DHCP サーバで現在時刻を指定することはできません。このようなシナリオでは、エージェントは事前に設定された URL *pnpntpserver.<domain_name>* を使用します。この URL は証明書をインストールする前に NTP サーバにマッピングしてデバイス上のクロックと同期させる必要があります。

ただし、証明書がどちらの URL にも存在しない場合、Cisco PnP エージェントはフォールバックし、作成した FQDN pnpserver.<domain_name> を使用してサーバへの HTTP 接続を確立します。このワークフローでは、エージェントはサーバが証明書インストールサービスを使用して自己署名証明書をインストールし、プロビジョニング手順を開始すると想定しています。

IPv6 ネットワークを介した DNS ベースの検出

IPv6 ネットワークを介した DNS ベースの検出を有効にするには、次の手順を実行します。

ステップ 1 IPv6 オプションを使用して DNS サーバを設定します。Cisco Network PnP DNS 検出を有効にするには、次の例のように DNS サーバを設定します。

```
ip host pnpntpserver.domain.com 2001::1
ip host pnptrustpool.domain.com 2001::2
ip host pnpserver.domain.com   2001::3
```

ステップ 2 DHCPv6 サーバは、DHCP ブートストラッププロセスによって検出されます。次に、DHCP サーバを設定する例を示します。

```
ipv6 unicast routing
ipv6 cef

ipv6 dhcp pool test
dns-server 2001::4
domain-name example.com
```

デバイスは、IPv6 ネットワークを介して DHCPv6 パケットをサーバに送信します。DHCPv6 パケットを受信すると、DNS サーバ情報とドメイン名がそれぞれオプション 23 とオプション 24 としてデバイスに返されます。

ステップ 3 NTP サーバを設定します。次に、NTP サーバを設定する例を示します。

```
ntp master 1
```

（注） 同様に、デバイスの NTP 設定では NTPv4 オプションを使用する必要があります。

ステップ 4 IPv6 ネットワークでトラストプールサーバをホストします。トラストプールは、DHCP オプション T と Z でのみサポートされています。オプション T が設定されている場合は、トラストプール CA バンドルの URL を指定します。オプション Z が設定されている場合は、NTP サーバの IP アドレスを指定します。

（注） Cisco Network PnP エージェントが IPv6 オプションを使用して HTTP 経由でトラストプールバンドルをダウンロードしようとすると、トラストプールサーバは IPv6 ネットワーク経由の HTTP をサポートする必要があります。また、トラストプールを設定する前にクロックを同期する必要があります。

ステップ 5 IPv6 ネットワークで Cisco Network PnP サーバをホストします。

IPv4 および IPv6 ネットワークを介した Cisco Cloud リダイレクト

Cisco Cloud リダイレクトサービスは、Cisco Network PnP ゼロタッチ検出をサポートしています。IPv4 および IPv6 ベースの Cisco Cloud 検出でサポートされています。

（注） 一部の Cisco PnP デバイスには、デバイスにルート証明書が組み込まれている場合があります。これらのデバイスは、最初から HTTPS を使用して CCO サーバと通信します。デバイスに組み込み証明書がない場合は、レガシー動作が開始されます。

デバイスがスタートアップコンフィギュレーションまたは認証証明書なしで起動し、DHCP および DNS 検出が失敗した場合、デバイスは *devicehelper.cisco.com* の Cisco Cloud サーバに接続しようとします。

devicehelper.cisco.com に到達できる場合、Cisco Network PnP エージェントはトラストプールバンドルをダウンロードし、Cisco Cloud リダイレクトサービスとのセキュアな HTTP 接続を確立します。デバイスが Cisco Cloud 検出を初めて試行すると、Cisco Network PnP エージェントは、この場所（*devicepooler.cisco.com/ca/trustpool*）からトラストプールをダウンロードし、ローカルフラッシュメモリに保存します。この場所は、トラストプールのインストール用の公開キーインフラストラクチャと共有されます。Cisco Cloud 検出が失敗した場合、トラストプールバンドルはフラッシュメモリ内に保持され、Cisco Network PnP はローカルデバイスのフラッシュメモリ内の trustpool バンドルのコピーを確認します。コピーがローカルフラッシュメモリで使用できない場合は、この場所（*devicehelper.cisco.com/ca/trustpool download*）からトラストプールバンドルのダウンロードを再試行します。

Cisco Network PnP エージェントは、HTTPS hello メッセージを Cisco Cloud に送信します。Cisco Cloud サーバで実行されている Cisco Network PnP リダイレクトサービスは、HTTP 要求に応答します。次の例に示すように、Cisco Cloud サーバの PnP プロファイルがデバイスに作成されます。

```
pnp profile pnp_cco_profile
transport https host devicehelper.cisco.com port 443
```

Cisco Cloud プロファイルが作成された後、デバイスは一意のデバイス識別子情報を含む作業情報メッセージを Cisco Cloud サーバに送信します。Cisco Cloud リダイレクトサービスは、Cisco Network PnP サーバ情報とともにリダイレクト非バックオフ PnP 要求を送信します。IPv4 アドレス、IPv6 アドレス、またはホスト名を指定できます。リダイレクトが成功すると、次のリダイレクトプロファイルがデバイスに設定されます。

```
pnp profile pnp_redirection_profile
transport https ipv4 172.19.153.133 port 443
```

非バックオフ PnP 要求をデフォルトの待機時間内に受信しなかった場合、Cisco Network PnP 検出プロセスは次の検出メカニズムを続行します。

4G インターフェイスを介した Cisco Network PnP 検出

4G インターエイスを介した Cisco Network PnP は、4G NIM を搭載し、Cisco IOS XE を実行しているプラットフォームで使用できます。アクティブになっている SIM カードを搭載したデバイスが起動すると、4G インターフェイスがアクティブになり、Cisco Network PnP クラウド検出プロセスに使用されます。SIM カードがアクティブになっていないデバイスが起動すると、検出プロセスには4G以外のインターフェイスが優先されます。4Gインターフェイスを介した Cisco Network PnP クラウド検出は、4G 以外のインターフェイスを使用できない場合や、4G 以外のインターフェイスで Cisco Network PnP 検出が成功しない場合に試行されます。デバ

イスにアクティブなSIMカードを備えた複数の4Gインターフェイスがある場合、Cisco Network PnP は、いずれかが成功するまで、すべての 4G インターフェイスでクラウド検出を試行します。

（注） Cisco Network PnP 検出に 4G インターフェイスを使用するには、4G NIM にアクティブ化された SIM カードが必要です。

4G インターフェイスを介した Cisco Network PnP クラウド検出は、すべての 4G インターフェイスがデバイス起動時にデフォルトでアクティブになっている場合に機能します。スタートアップ コンフィギュレーションがない場合、デバイスはデフォルトで4Gインターフェイスを起動しようとし、クラウドを介して Cisco PnP を試行します。デバイスがリダイレクトされると、デバイスは Cisco Network PnP サーバに接続し、適切なイメージと設定をデバイスにダウンロードします。

（注） DNS サーバは4Gネットワークの一部として使用でき、クラウドポータルはデバイスをプロビジョニングするために適切な Cisco Network PnP サーバに発信側デバイスをリダイレクトするようにプログラムする必要があります。現在、4G インターフェイスを介した Cisco Network PnP のサポートでは、IPv4 ネットワークのみが使用されます。

Cisco Network PnP サーバを介してプッシュされた設定に、4Gインターフェイスを介した Cisco Network PnP サーバへのルートが含まれていることを確認します。これはデフォルトルートである可能性があり、プロビジョニングが完了した後も 4G インターフェイス上で動作するように、Cisco Network PnP エージェントとサーバの通信を維持する必要があります。

管理インターフェイスを介した Cisco Network PnP 検出

Cisco Network PnP Agent は、デフォルトの VPN ルーティング/転送（VRF）を使用し、管理インターフェイスを介して検出と4方向ハンドシェイクをサポートします。VRFインターフェイスを介して DHCP トラフィックを送受信するには、IOS DHCP サーバを設定する必要があります。この機能は、管理インターフェイスのみがアクティブな場合に、新しいデバイスが Cisco Network PnP 機能にアクセスするのに役立ちます。

デバイスが起動すると、デフォルトの VRF 管理インターエイスに IP アドレスが DHCP を介して割り当てられます。このインターフェイスは Cisco Network PnP サーバへの接続を確立し、デバイス上の Cisco Network PnP エージェントがこの情報（VRF 名と送信元インターフェイス）を記録します。この情報は Cisco Network PnP サーバとの今後の PnP 通信に使用されます。この場合、デバイスで作成される Cisco PnP プロファイルには追加のキーワード **VRF** が付加されます。

EtherChannel を介した Cisco PnP

Cisco Network Plug and Play を使用してアクセススイッチを展開する場合、プロビジョニングされたスイッチ（トランクとして動作）に LACP EtherChannel が存在するため、デバイスを設定できません。アクセスデバイスが LACP を使用して L2 EtherChannel を介してプロビジョニン

グされたスイッチ経由で接続しようとすると、接続が切断されます。設定がアクセスデバイスに存在しないため、アクセスデバイスはスイッチでEtherChannelを起動できません。これにより、EtherChannel ポートが中断状態になり、L2 接続が切断されます。Cisco Network PnP エージェントは、EtherChannelの存在を検出し、デバイスのEtherChannelを自動設定して、Day-Zero設定のレイヤ 2 接続を自動的に起動します。

PnP 検出プロセス完了後のセキュリティ方式

この項では、Cisco PnP エージェントによって提供される、検出プロセスの完了後のクライアント/サーバ通信を保護するために Cisco PnP サーバで使用できる方法について説明します。ここでは、次の内容について説明します。

• 証明書インストールサービス （26 ページ）

証明書インストールサービス

Cisco PnP エージェントは、Cisco PnP サーバに証明書インストールサービスを提供することで、デバイス上の SSL 証明書を管理するメカニズムを提供します。certificate-install サービスは、HTTPS接続を開始する前に、サーバの自己署名証明書またはデバイスの標準CA証明書によって署名された証明書をインストールするためのシンプルな XML を提供します。certificate-install サービスには、クライアントの SSL 証明書をインストールし、次のデバイス認証プロセス時に同じSSL証明書を使用するようにデバイスに指示するオプションもあります。

SUDI ベースの PnP アプリケーションレベルの認証

SSL 通信はサーバとデバイス間で交換されるデータパケットを確実に暗号化しますが、デバイスを認証するためのソリューションは提供しません。

サーバが正規のシスコのデバイスと通信していることを確認するために、エージェントはデバイスに組み込みまれている Secure Unique Device Identifier（SUDI）証明書サポートを使用します。SUDI は製造時にデバイスの安全なチップ（ACT2）に書き込まれた X.509 準拠のデバイス証明書です。SUDI 証明書には、デバイスのシリアル番号、秘密/公開キー、および Cisco CA の署名が含まれています。エージェントは、サーバがデバイスを正規のシスコのデバイスとして認証するのに使用できる次のメカニズムを提供します。

• SUDI ベースのクライアント証明書の検証 （26 ページ）
• SUDI ベースのシリアル番号 （27 ページ）

SUDI ベースのクライアント証明書の検証

エージェントがサーバとの HTTPS 接続を開始する前に、エージェントはデバイスに組み込みの SUDI 証明書があるかどうかを確認します。デバイスに証明書がある場合は、エージェントは検証のための SSL ハンドシェイク時に SUDI 証明書をクライアントに送信します。必要に応じて、HTTPS サーバは、SSL ハンドシェイク時に SUDI 証明書を使用してデバイスを検証する

こともできます。検証後、HTTPS サーバはデバイスがサーバに接続できるようにします。デバイスの SUDI 証明書を検証するには、サーバが Cisco CA を使用して検証を完了する必要があります。

SUDI ベースのシリアル番号

デバイスに SUDI 証明書がロードされている場合、PnP エージェントは SUDI 証明書からシリアル番号を読み取り、サーバとのすべての通信の作業要求の本文に同じ情報を追加タグとして提示します。これを実現するために、次のオプションのタグが作業情報メッセージに追加されます。これは、すべての作業要求でデバイスから送信されます。このフィールドはオプションであり、SUDI 証明書がないデバイスには表示されません。

シャーシインベントリから読み取られる既存の UDI メカニズムに変更はありません。プライマリ識別子としてシャーシ UDI を送信することで、エージェントは引き続き下位互換性を維持します。サーバは追加で提供された SUDI ベースのシリアル番号を使用してデバイスを認証するとプライマリ UDI を引き続き使用できます。SUDI 証明書のないデバイスの場合、エージェントはこの追加の SUDI ベースのシリアル番号を送信しません。したがって、サーバは認証とそれ以降の通信のためにプライマリ UDI を継続する必要があります。

メンバーハードウェアから SUDI ベースのシリアル番号の読み取りに使用できるメカニズムはなく、スタック または HA ユニットの他のメンバーからの UDI の読み取り方法に変更はありません。エージェントは引き続き、現在のようにすべてのハードウェアユニットから UDI を読み取ります。

SUDI ベースのデバイス認証

SUDI ベースのデバイス認証では、エージェントは起動時にデバイスに組み込みの SUDI 証明書があるかどうかを確認します。デバイスに SUDI 証明書がロードされている場合、エージェントは新しい PnP サービスを提供します。これにより、サーバがデバイスを識別できるようになります。この新しいサービスが利用できるかどうかは SUDI 証明書の存在によって異なり、エージェントの機能サービスのリストに表示されます。

上記の capability-service の変更に伴い、エージェントは device-info 応答の hardware-info セクションに新たなフィールドを追加し、SUDI 証明書がデバイスに組み込まれているかどうかを特定して確認します。

その後、エージェントはサーバとの HTTPS 接続を開始し、作業要求を送信します。サーバはデバイス認証サービスをチャレンジ要求/応答に使用できる必要があります。デバイス認証サービスでは、サーバが文字列を生成するために少なくとも 1 つのフィールドが必要です。オプションで、サーバはサポート可能な暗号化方式とハッシュ方式のリストを送信できます。エージェントは、サーバによって指定されたリストの暗号化方式のいずれかを使用する機能があるかどうかを確認し、暗号化方式を使用してサーバに通知を送信します。サーバで指定されたいずれの方法もエージェントが使用できない場合、エージェントはエラーメッセージで応答します。

サーバがデバイス認証サービス要求をエージェントに送信すると、エージェントは次の処理を実行します。

1. 指定された暗号化方式とハッシュ方式のいずれかを使用します。

2. 指定された暗号化方式およびハッシュ方式のいずれかを使用する機能がエージェントにない場合、エージェントはエラーメッセージで応答します。
3. PKI API を使用して、秘密キーを使用してサーバから提供されたチャレンジ文字列を暗号化します。
4. 次の応答を返します。
    1. 暗号テキスト
    2. 暗号に使用される方法
    3. 証明書（SUDI またはクライアントインストール証明書）

その後、サーバはデバイスから上記の応答を受信すると、次の処理を実行します。

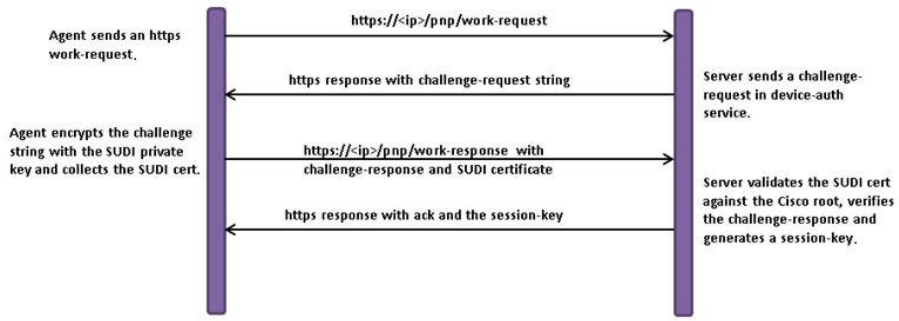
1. シスコまたはカスタマー CA に対して SUDI またはクライアント証明書を確認します。
2. SUDI またはクライアント証明書で使用可能な公開キーを使用して暗号文字列を復号します。
3. 復号された文字列が元のバージョンと一致するかどうかを確認します。
4. セッションキー（文字列）を生成し、確認応答としてデバイスに送り返します。

エージェントは、セッションキーを含む最終確認応答をサーバから受信すると、対応するプロファイルを提供されたセッションキーに関連付け、それをエージェントが送信する後続のすべてのメッセージのルート PnP セクションの属性としてサーバに送信します。

サーバは、デバイスからメッセージを送信する前にセッションキーを検証します。必要に応じて、サーバはセッションキーのタイマーを保持し、タイマーが期限切れになると無効ステータスに移行します。エージェントが期限切れのセッションキーを含むメッセージを送信すると、サーバはデバイス認証プロセスを繰り返し、新しいセッションキーを生成してから同じデバイスに再度送信します。デバイスがセッションキーを使用せずに要求を送信すると、サーバはデバイス認証プロセスを実行し、新しいセッションキーを生成してから同じデバイスに送信します。

次の図に、SUDI証明書を使用してデバイス認証を行うための、エージェントとサーバ間のメッセージシーケンスを示します。

図 *13 :* メッセージ シーケンス



Cisco Network Plug and Play エージェントの設定方法

Cisco Network Plug and Play エージェントのプロファイルの設定

Cisco Network Plug and Play エージェントのプロファイルを作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Network Plug and Play エージェントデバイスの設定

Cisco Network Plug and Play エージェントのデバイスを作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**device** {**username** *username* } {**password {0 | 7}** *password*} 例： `Device(config-pnp-init)# device username sjohn password 0 Tan123`	デバイス上に PnP エージェントを設定します。 • ユーザ名とパスワードに基づく認証システムを確立します。 • *username*：ユーザ ID • *password*：ユーザが入力したパスワード • **0**：非暗号化パスワードまたは秘密キー（設定による）が後に続くことを指定します。 • **7**：暗号化パスワード（非表示）が後に続くことを指定します。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の再接続要因の設定

固定インターバルバックオフ、指数バックオフ、ランダム指数バックオフのいずれかのモードでのセッション再接続を試みる前に、待機する時間を設定するために、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**reconnect** [*pause-time* [*exponential-backoff-factor* [**random**]]] 例： `Device(config-pnp-init)# reconnect 100 2 random`	PnP エージェント イニシエータ プロファイルがセッション再接続を試行するまでの待機時間を指定します。 • pause-time 値は、接続が失われてから再接続するまで待機する時間（秒数）です。範囲は 1 ～ 2000000 です。デフォルトは 60 です。 • exponential-backoff-factor 値は、再接続試行を指数的にトリガーする値です。範囲は 2 ～ 9 です。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の HTTP トランスポートプロファイルの設定

Cisco Plug and Play エージェントの HTTP トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

PnP サーバ IP 設定には、IPv4 アドレスと IPv6 アドレスの両方を使用できます。また、PnP サーバに接続するため、設定の中でホスト名を使用することもできます。

どのプロファイルにも、1 つのプライマリ サーバと 1 つのバックアップ サーバの設定が可能です。Cisco PnP エージェントは、まずプライマリサーバとの接続の開始を試み、それが失敗した場合にはバックアップサーバを試します。バックアップサーバで障害が発生すると、Cisco PnP エージェントは再びプライマリサーバへの接続を試みます。サーバのうちの 1 つとの接続が確立されるまでこれが続行されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**transport http host** *host-name* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# transport http host hostname-1 port 1 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。 • host の値はサーバのホスト名、ポート、および発信元を指定します。 • port-number の値は使用するポートを指定します。 • interface-type の値はエージェントのサーバへの接続に使用されるインターフェイスを指定します。
ステップ 5	**transport http ipv4** *ipv4-address* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。
ステップ 6	**transport http ipv6** *ipv6-address* [**port** *port-number*] [**source** *interface-type interface-number*] 例： `Device(config-pnp-init)# transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の HTTPS トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントの HTTP Secure（HTTPS）トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**transport https host** *host-name* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。 • *localcert* の値は、Transport Layer Security（TLS）ハンドシェイク時にクライアント側の認証用に使用するトラストポイントを指定します。 • *remotecert* の値は、サーバ証明書の検証に使用されるトラストポイントを指定します。 （注） **crypto pki trustpoint** コマンドを使用した trustpoint-name の設定

	コマンドまたはアクション	目的
ステップ 5	**transport https ipv4** *ipv4-address* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。
ステップ 6	**transport https ipv6** *ipv6-address* [**port** *port-number*][**source** *interface-type interface-number*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップデバイスの設定

バックアッププロファイルを作成し、デバイス上で Cisco Network Plug and Play エージェントを手動で有効または無効にするには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例：	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# pnp profile test-profile-1`	• PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup device** {**username** *username* } {**password {0 | 7}** *password*} 例： `Device(config-pnp-init)# backup device username sjohn password 0 Tan123`	デバイス上に PnP エージェント バックアップ プロファイルを設定します。 • ユーザ名とパスワードに基づく認証システムを確立します。 • *username* - ユーザ ID • *password* - ユーザが入力するパスワード • 0：非暗号化パスワードまたは秘密キー（設定による）が後に続くことを指定します。 • 7 — 非表示パスワードが後に続くことを指定します。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ再接続要因の設定

固定インターバルバックオフ、指数バックオフ、またはランダム指数バックオフのいずれかの方法で、サーバに Cisco Network Plug and Play（PnP）エージェントのバックアップ再接続を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup reconnect** [*pause-time* [*exponential-backoff-factor* [**random**]]] 例： `Device(config-pnp-init)# backup reconnect 100 2 random`	PnP エージェントイニシエータ プロファイルがセッション再接続を試行するまでの待機時間を指定します。 • pause-time 値は、接続が失われてから再接続するまで待機する時間（秒数）です。範囲は 1 ～ 2000000 です。デフォルトは 60 です。 • exponential-backoff-factor 値は、再接続試行を指数的にトリガーする値です。範囲は 2 ～ 9 です。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ HTTP トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントのバックアップ HTTP トランスポートプロファイルをデバイス上に手動で作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup transport http host** *host-name* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# backup transport http host hostname-1 port 1 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。 • host の値はサーバのホスト名、ポート、および発信元を指定します。 • port-number の値は使用するポートを指定します。 • interface-type の値はエージェントのサーバへの接続に使用されるインターフェイスを指定します。
ステップ 5	**backup transport http ipv4** *ipv4-address* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# backup transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。
ステップ 6	**backup transport http ipv6** *ipv6-address* [**port** *port-number*] [**source** *interface-type interface-number*] 例： `Device(config-pnp-init)# backup transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ HTTPS トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントのバックアップ HTTPS トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup transport https host** *host-name* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。 • *localcert* の値は、Transport Layer Security（TLS）ハンドシェイク時にクライアント側の認証用に使用するトラストポイントを指定します。 • *remotecert* の値は、サーバ証明書の検証に使用されるトラストポイントを指定します。
ステップ 5	**backup transport https ipv4** *ipv4-address* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。

	コマンドまたはアクション	目的
ステップ 6	**backup transport https ipv6** *ipv6-address* [**port** *port-number*][**source** *interface-type interface-number*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play エージェント タグの設定

Cisco Network Plug and Play エージェントのタグ情報を作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pnp tag** *tag-name* 例： `Device(config)# pnp tag xyz`	デバイスにタグを設定するには、**pnp tag** コマンドを使用します。Cisco のネイバー デバイスは Cisco Discovery Protocol（CDP）を通じてこのタグ情報を受信します。 （注） デバイスに既存のタグがある場合、タグ名を変更できるのは、タグ名の変更のために xml スキーマが PnP サーバにより送信される場合のみです。タグ名は上書きできません。

	コマンドまたはアクション	目的
		• PnP エージェント タグの名前を指定する英数字文字列。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングとデバッギング

Cisco Network Plug and Play サーバでデバッグを実行する（サーバを起動する）には、PnP プロファイルと PnP トランスポートを設定します。たとえば、PnP エージェントと PnP サーバ間でのサービスの連携動作を開始します。

debug pnp service コマンドを実行することでデバッグをキャプチャできます。問題を報告する場合は、ガイドに従って PnP エージェントフラッシュ内のすべての pnp を収集します。

（注） Cisco Plug and Play サーバのログを収集するには、『Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide』を参照してください。

デバイス、サーバ、および Cisco PnP エージェントのトラブルシューティングを行うには、次のコマンドを使用します。

表 *1:* デバイス、サーバ、および *Cisco PnP* エージェントのトラブルシューティング

コマンド	説明
dir nvram	デバイスに証明書が残っていないことを確認するには、このコマンドを使用します。
ping vrf interface-name *<controller_ip>*	デバイスがコントローラを ping できることを確認するには、このコマンドを使用します。
show auto install trace	自動インストールのトレースログを表示するには、このコマンドを使用します。
show boot	BOOTLDR 変数の現在の値を表示するには、このコマンドを使用します。
show cdp neighbor	すべての CDP ネイバーを表示するには、このコマンドを使用します。

コマンド	説明
Show crypto pki trustpoint	PKI トラストポイントを表示するには、このコマンドを使用します。
Show crypto pki trustful	信頼できる PKI を表示するには、このコマンドを使用します。
show ip interface brief	ルータインターフェイスの概要を表示するには、このコマンドを使用します。
show ipv6 interface brief	IPv6 インターフェイスを表示するには、このコマンドを使用します。
show run | inc pnp	1 つの PnP プロファイルのみがインストールされていることを確認するには、このコマンドを使用します。
show pnp trace	デバイスにスタートアップ コンフィギュレーションがないことを確認するには、このコマンドを使用します。
show pnp tech	Cisco Plug and Play IOS エージェントのアクティブな接続を表示するには、このコマンドを使用します。
show vlan	VLAN 情報を表示するには、このコマンドを使用します。
show ntp status	NTP ステータスを表示するには、このコマンドを使用します。
show version	デバイスが最新の CCO イメージを実行していることを確認するには、このコマンドを使用します。

用語集

PnP エージェント：展開プロセスを自動化するためのデバイス上の組み込みエージェント

PnP ヘルパーアプリケーション：スマートフォンやパーソナルコンピュータ上の展開を容易にするアプリケーション。PnP ヘルパーアプリケーションは、お客様またはデバイスに固有ではなく、どのような展開シナリオでも使用できます。限られたシナリオで必要になることがあります。

PnP プロトコル：PnP エージェントと PnP サーバ間のプロトコル。これは、PnP サーバのサードパーティ開発を可能にするオープンプロトコルです。

PnP サーバ：展開するデバイスの展開情報（イメージ、設定、ファイル、およびライセンス）を管理し、配布する中央サーバ。Cisco Network Plug and Play サーバは、管理アプリケーションにノース バウンド インターフェイスを提供し、PnP プロトコルを使用してデバイス上の PnP エージェントと通信します。

Open Plug-n-Play エージェントのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
PnP コマンド：コマンドシンタックスの詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	Cisco IOS PnP Command Reference
Cisco Network Plug and Play ソリューション	Solution Guide for Cisco Network Plug and Play
APIC-EM で Cisco Network Plug and Play を使用してシスコのネットワークデバイスを設定する方法	Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM
APIC-EM の展開方法	Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide
APIC-EM を使用する前に	Cisco APIC-EM Quick Start Guide

MIB

MIB	MIB のリンク
• CISCO-BULK-FILE-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-PROCESS-MIB • Expression-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

翻訳について
このドキュメントは、米国シスコ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。