Cisco プラグ アンド プレイ機能ガイド

シスコ サービス

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイ機能ガイド

目次

目次

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイ機能ガイド

はじめに

はじめに

Cisco® プラグ アンド プレイ ソリューションは、安全性が高くスケーラブルかつシームレスな、統一されたゼロタッチ導入エクスペリエンスを提供する統合ソリューションです。

企業がキャンパスや支店における導入の一部としてさまざまなネットワーク デバイスを設置して導入するには、大きな運用コストがかかります。多くの場合、事前にすべてのデバイスのそれぞれについて準備作業をしておかなければならず、そのために、Cisco IOS® ソフトウェアのイメージをコピーし、コンソール接続を通じて設定を手動で適用する操作を何度も繰り返すことになります。デバイスの事前準備が終了したなら、それらを最終的に使用する現場に発送して設置します。サポート サイトの設置では、設定のトラブルシューティング、ブートストラップ、または変更のために熟練した設置作業者が必要になることがあります。そのプロセスは、全体として、コストと時間がかかり、エラーが発生しがちです。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 プラグ アンド プレイのコンポーネント

Cisco プラグ アンド プレイ(PnP)導入には、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。

このシンプル導入プロセスにより、シスコ デバイスに対する、次のような導入関連の運用手順が自動化されます。

- 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

プラグ アンド プレイ エージェント

Cisco のプラグ アンド プレイ(PnP)エージェントは、Cisco ネットワーク デバイスのうちシンプル導入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のソフトウェア 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、DHCP や DNS などの方法を使用することにより、通信相手の PnP サーバの IP アドレスの取得を試みます。サーバが検出され、接続が確立されると、エージェントは PnP サーバと通信して導入関連のさまざまなアクティビティを実行します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

また、アウトオブバ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の接続など、関係する導入関連イベントすべてをサーバに通知します。

主なメリット

Cisco プラグ アンド プレイ(PnP)エージェントには、次のメリットがあります。

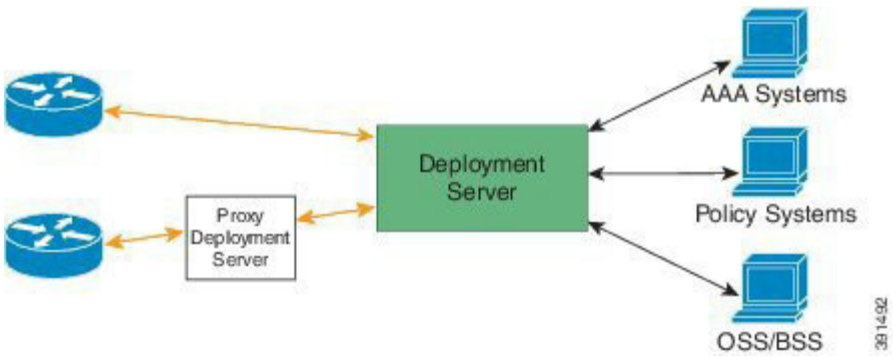
- 0 日目のブートストラップ - 設定、イメージ、ライセンス、およびその他のファイル
- 2 日目の管理 - SNMP および syslog メッセージの設定およびイメージのアップグレードと継続的なモニタリング
- オープン通信プロトコル - 顧客およびパートナーがアプリケーションを作成することが可能
- サーバとエージェントの間の、HTTP および Extensible Messaging and Presence Protocol(XMPP)上の XML ベースのペイロード
- セキュリティ - 管理アプリとエージェントとの間の認証と暗号化通信チャネル
- ファイアウォールおよびネットワーク アドレス変換(NAT)の背後にあるデバイスの導入と管理
- 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

プラグ アンド プレイ サーバ

Cisco プラグ アンド プレイ(PnP)サーバは、導入するデバイスの導入情報(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、特定の導入プロトコルを使用することにより、シンプル導入プロセスをサポートするデバイス上にインストールされるエージェントと通信します。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

図1:シンプル導入サーバ



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。

Cisco PnP ではリダイレクトがサポートされています。たとえば、PnP サーバは、NAPP サーバ経由でブートストラップ設定を送信した後に、デバイスにリダイレクトして直接通信することが可能です。Cisco が提供するクラウド ベースの導入サービスを活用する企業によって PnP サーバがホストされている場合、デバイスは、初期導入用に Cisco のクラウド ベース導入サービスを検出し、それと通信します。その後、PnP サーバは、顧客の導入サーバにデバイスをリダイレクトします。

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。

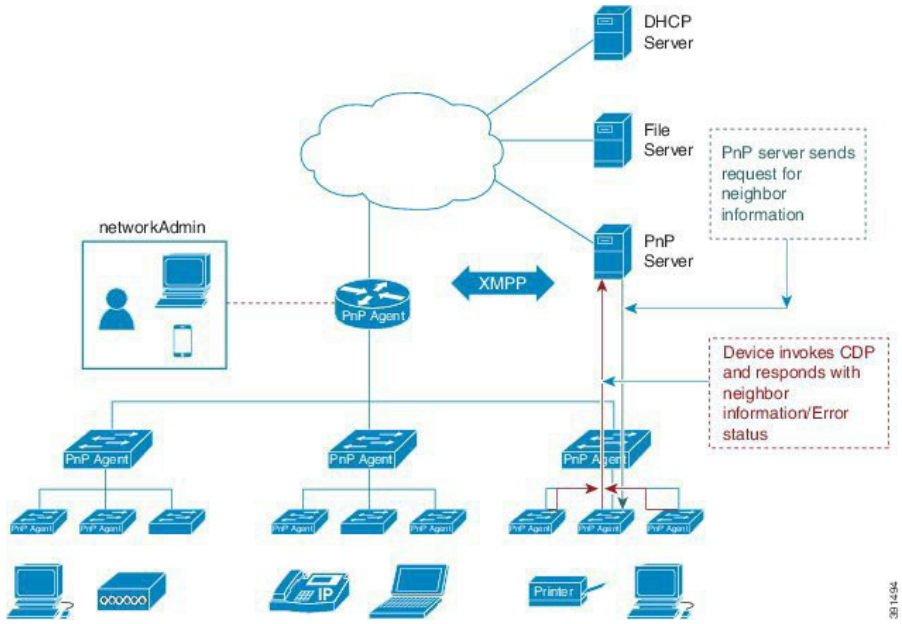
Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

シスコ デバイスでの Cisco プラグ アンド プレイの仕組み

シスコ デバイス上でのプラグ アンド プレイ(PnP)展開手順の詳細を以下に示します。

1. PnP エージェントがインストールされているシスコ デバイスは、PnP サーバと連絡を取って、作業要求と共に Unique Device Identifier(UDI)を送信することにより、操作を要求します。
2. PnP サーバは、デバイスに対して実行可能な手順がある場合、PnP エージェントが実行しなければならない処理の種類を示す作業要求を送り返します。たとえば、イメージのインストールやアップグレード設定などの処理です。
3. PnP エージェントは作業要求を受信すると、その手順を実行し、その手順のステータスを示す応答を PnP サーバに返します。

図 2 :Cisco プラグ アンド プレイ導入のネットワークトポロジ



Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイ機能ガイド

はじめに

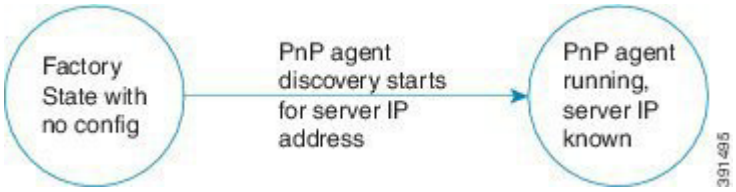
プラグ アンド プレイ エージェントの初期化のシナリオ

Cisco プラグ アンド プレイ(PnP)エージェントは、デバイスにおいてデフォルトで有効になっています。PnP エージェントは、デバイス上で次のように開始できます。

起動設定のないデバイス上での PnP 自動開始

新しいシスコ デバイスは、デバイスの NVRAM の中に起動設定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、デバイス上に起動設定ファイルがないと、Cisco プラグ アンド プレイ(PnP)エージェントが自動的に開始され、PnP サーバ IP アドレスを検出します。

図 3 : 起動設定なしでの PnP トリガーのワークフロー



CLI 使用による PnP エージェントの初期化

ネットワーク管理者は、コマンドライン インターフェイス(CLI)を使用することにより、プラグ アンド プレイ(PnP)のエージェント プロセスをいつでも開始できます。CLI で PnP プロファイルを設定することにより、デバイス上の 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 プロファイルが設定されると、デバイスは PnP エージェント プロセスを開始し、そのプロセスにより、PnP プロファイルの IP アドレスを使用して PnP サーバとの接続が開始されます。

図 4 : CLI で PnP プロファイルを設定する場合の PnP トリガーのワークフロー

Cisco プラグ アンド プレイの前提条件

- PnP エージェントを起動する前に、DHCP サーバ検出プロセスか、ドメイン ネーム サーバ(DNS)のいずれかの検出メカニズムを導入します。
- PnP エージェントを導入する前に、DHCP サーバまたは DNS サーバを設定します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

- PnP エージェントが PnP サーバに到達できることを確認します。
- 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。

制限事項とガイドライン

- Cisco プラグ アンド プレイ(PnP)エージェントにより、PnP サーバとの間での HTTP、Extensible Messaging and Presence Protocol(XMPP)、HTTP Secure(HTTPS)転送ベースの通信が容易なものとなります。
- 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。暗号化対応イメージを使用する場合、Secure Sockets Layer(SSL)と Transport Layer Security(TLS)プロトコルは、いずれも使用しないでください。
- Cisco ネットワーク プラグ アンド プレイでは、VLAN 1 を使用するデバイスがデフォルトでサポートされています。VLAN 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、サポートされている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 コマンドを設定して、プラグ アンド プレイ デバイスにこの設定を適用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、そのデバイスでは VLAN メンバーシップは変更されません。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。

(注)

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 デバイスで、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 が実行され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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイの導入シナリオ

デバイスのブート時に、NVRAM 上に起動設定が欠如している場合、PnP 検出エージェントにより 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。

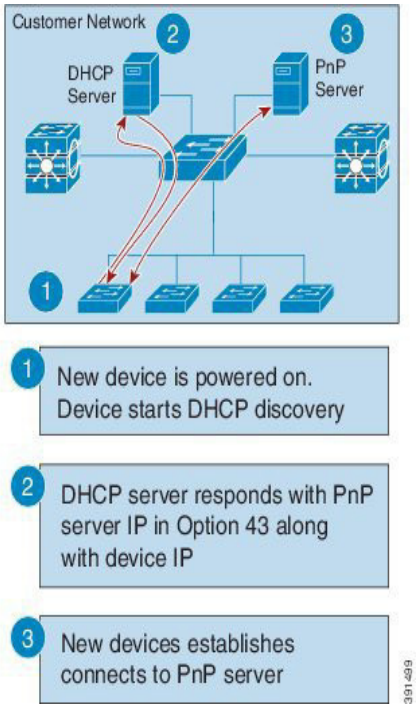
- DHCP サーバによる PnP の検出
- DHCP スヌーピングによる PnP の検出
- DNS ルックアップによる PnP の検出
- レイヤ 2 およびレイヤ 3 デバイスの PnP プロキシ
- PnP 導入アプリケーション

DHCP サーバによるプラグアンドプレイ検出

NVRAM に起動設定がないデバイスは、デバイスに必要な IP アドレスを DHCP サーバから要求する DHCP 検出プロセスを開始するよう、Cisco プラグ アンド プレイ（PnP）エージェントを起動します。DHCP サーバは、デバイスから文字列「cisco pnp」を伴うオプション 60 を受信した時点でベンダー固有のオプション 43 を使用して追加情報を挿入するように設定できます。これは、PnP サーバの IP アドレスまたはホスト名を要求元デバイスに渡すためです。

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 IP アドレスまたはホスト名を使用します。

図 5 :PnP のための DHCP 検出プロセス



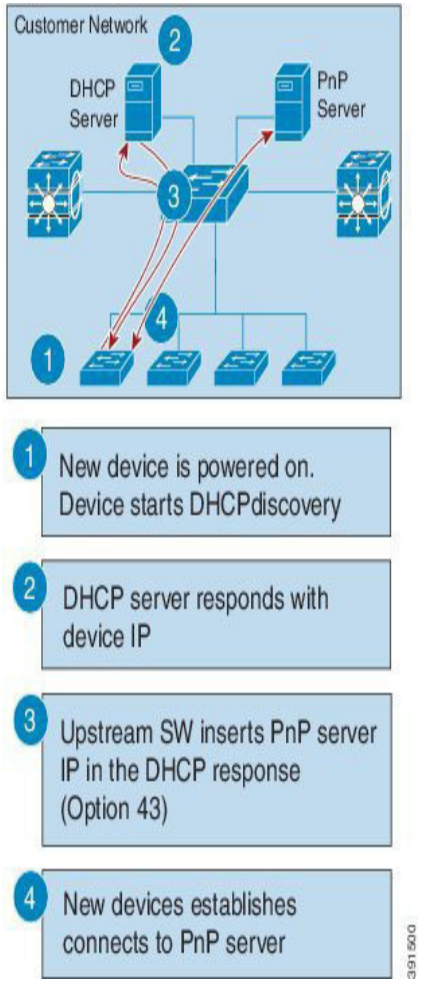
Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

DHCP スヌーピングによるプラグ アンド プレイ検出

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の 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 IP アドレスを伴う PnP 固有のオプション 43 を挿入するように、既存のプラグ アンド プレイ(PnP)対応デバイスを設定できます。

DHCP 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

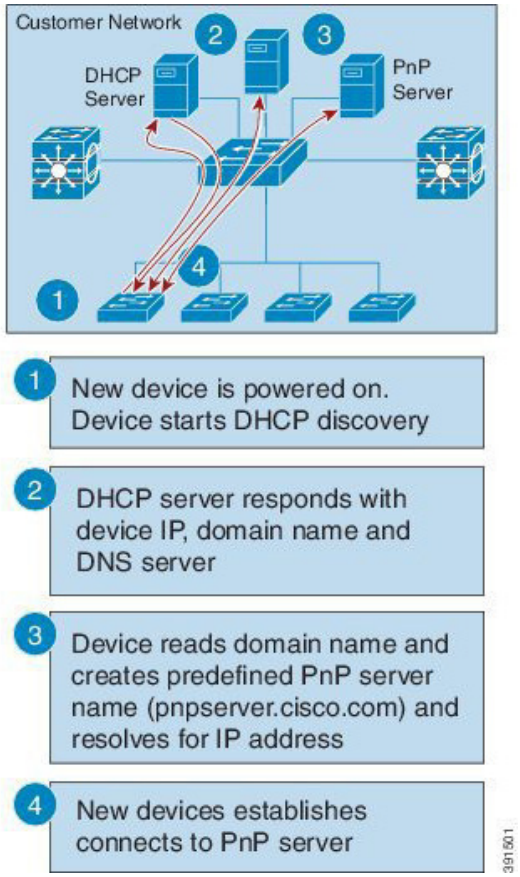


Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

DNS ルックアップによるプラグ アンド プレイ検出

DHCP 検出機能による Cisco プラグ アンド プレイ(PnP)サーバの IP アドレスの取得に失敗した場合、エージェントは、フォールバックとしてドメイン ネーム システム(DNS)ルックアップ方式を実行します。PnP エージェントは、プリセットされた導入サーバの名前を使用します。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。プリセットされた導入サーバ名と DHCP 応答のドメイン名の情報を使用して、PnP エージェントによって、FQDN *<pnpservername>.cisco.com* が構成されます。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



Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

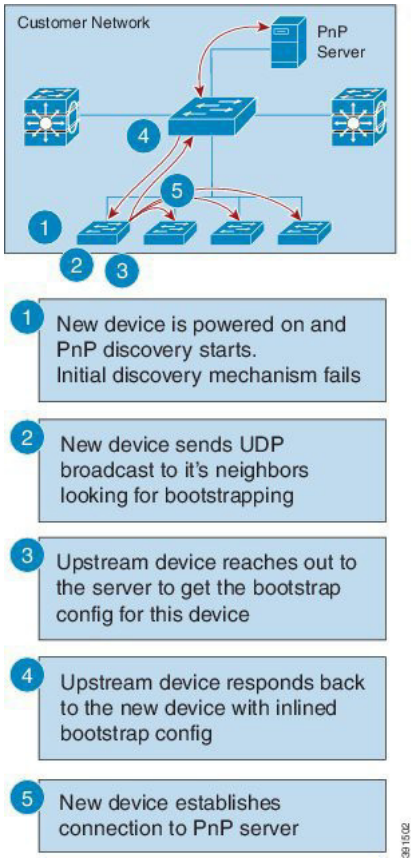
レイヤ 3 およびレイヤ 2 デバイス用のプラグ アンド プレイ プロキシ サーバ

DHCP サーバもドメイン ネーム システム(DNS)サーバも存在しない場合、PnP Neighbor Assisted Provisioning Protocol(NAPP)サーバとして機能するように、隣接ネットワークにある運用中の既存のプラグ アンド プレイ(PnP)対応デバイスを設定することができます。

NAPP サーバは PnP 検出フェーズの一部です。このサーバは、PnP 自律型ネットワーキングに基づく検出、DHCP、DNS、Cisco クラウド サービス検出機能で PnP サーバに接続できない場合に起動されます。

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 およびレイヤ 2 のデバイスでの DNS 検索



| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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。

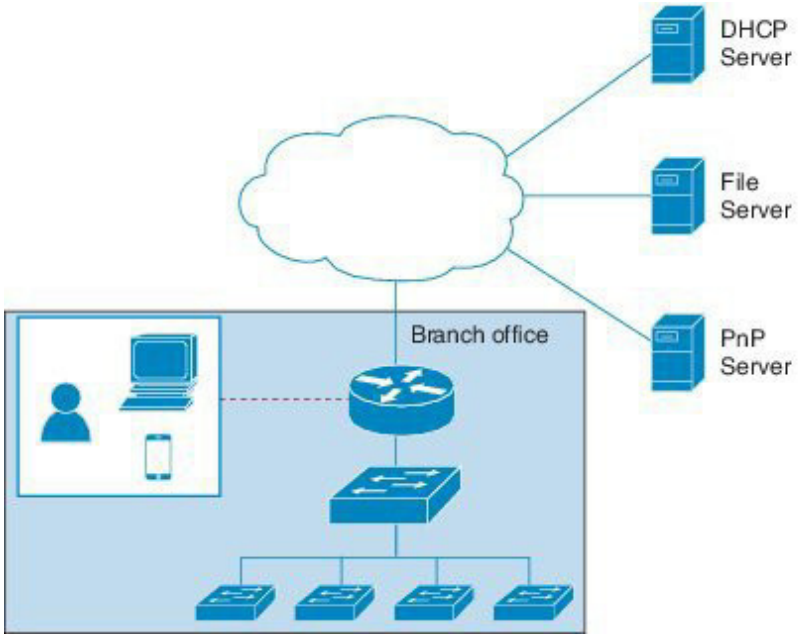
そのデータグラムを受信すると、プロキシ クライアント プロセスを実行するデバイスは、ターゲット UDI を得るため着信データグラムを解析します。そのデータグラムのターゲット UDI がデバイスの UDI と一致すると、プロキシ クライアント プロセスは、フレーミング、エラー制御、およびコンフィグレットの設定に進みます。

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。

導入アプリケーション使用によるプラグ アンド プレイ エージェントの導入

別の方法として、ネットワーク管理者は、コンピュータやスマートフォンで実行される導入アプリケーションを使用して手動でデバイスを設定することができます。コンピュータまたはスマートフォンは、USB またはイーサネット ケーブルを介してデバイスに接続できます。

図 9 :PnP エージェントの手動設定



Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイの設定

デバイス上に Cisco プラグ アンド プレイ（PnP）を設定するには、次の手順を実行します。

Cisco プラグ アンド プレイ エージェント プロファイルの設定

Cisco プラグ アンド プレイ（PnP）エージェント プロファイルを作成するには、次の手順を実行します。

	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 モードをイネーブルにします。 • 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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

プラグ アンド プレイ エージェント デバイスの設定

Cisco プラグ アンド プレイ（PnP）エージェント デバイスを作成するには、次の手順を実行します。

	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 モードをイネーブルにします。 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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

	コマンドまたはアクション	目的
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(設定に依存)を伴うことを指定します。 • **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。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

プラグ アンド プレイ再接続の係数の設定

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、次の手順を実行します。

	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 モードをイネーブルにします。 • 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`	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 1002 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。

Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 プラグ アンド プレイ HTTP 転送プロファイルの設定

デバイス上にプラグ アンド プレイ(PnP)エージェントの HTTP 転送プロファイルを手動で作成するには、以下の手順を実行します。

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 サーバの構成が可能です。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 サーバを試みます。バックアップ サーバで障害が発生すると、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。

	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 モードをイネーブルにします。 • 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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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:**	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 転送設定を作成します。 • 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。
ステップ 5	**transport http ipv4** *ipv4-address* [**port** *port-number*] [**source** *interface-type*] **例:**	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 転送設定を作成します。
ステップ 6	**transport http ipv6** *ipv6-address* [**port** *port-number*] [**source** *interface-type interface-number*] **例:**	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 転送設定を作成します。
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 プラグ アンド プレイ HTTPS 転送プロファイルの設定

デバイス上に Cisco プラグ アンド プレイ（PnP）エージェントの HTTP Secure（HTTPS）転送プロファイルを手動で作成するには、以下の手順を実行します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

	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 モードをイネーブルにします。 • 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 転送設定を作成します。 • *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** トラストポイント名を設定するには **crypto pki trustpoint** コマンドを使用します。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 転送設定を作成します。
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 転送設定を作成します。
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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

Cisco プラグ アンド プレイ XMPP 転送プロファイルの設定

デバイス上に手動で Cisco プラグ アンド プレイ（PnP）エージェントの Extensible Messaging and Presence Protocol（XMPP）転送プロファイルを作成するには、次の手順を実行します。

	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 モードをイネーブルにします。 • 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。

Cisco プラグ アンド プレイ機能ガイド| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

ステップ 4	**transport xmpp socket** {**host** *host-name* | **ipv4** *ipv4-address*| **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# transport xmpp socket host example.com port 231 sasl plain server-jid cisco123`	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 XMPP 転送設定を作成します。
ステップ 5	**transport xmpp starttls** {**host** *host-name* | **ipv4** *ipv4-address*| **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**localcert** *trustpoint-name*} {**remotecert** *trustpoint-name*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# transport xmpp starttls 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 XMPP 転送設定を作成します。 • *localcert* の値は Transport Layer Security（TLS）ハンドシェイク中のクライアント側の認証に使用され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 6	**transport xmpp tls** {**host** *host-name* | **ipv4** *ipv4-address*| **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**localcert** *trustpoint-name*} {**remotecert** *trustpoint-name*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# transport xmpp tls ipv6 2001:DB8:1::1 port 221 source gigabitEthernet 0/0/0`	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 XMPP 転送設定を作成します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

バックアップ Cisco プラグ アンド プレイ 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 プラグ アンド プレイ エージェントを手動で有効または無効にするには、次の手順を実行します。

	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 モードをイネーブルにします。 • 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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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(設定に依存)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。

バックアップ Cisco プラグ アンド プレイ再接続の係数の設定

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方法で、サーバに Cisco プラグ アンド プレイ(PnP)エージェントのバックアップ再接続を設定するには、次の手順を実行します。

	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 モードをイネーブルにします。 • パスワードを入力します(要求された場合)。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 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。

バックアップ Cisco プラグ アンド プレイ HTTP 転送プロファイルの設定

デバイス上に Cisco プラグ アンド プレイ(PnP)エージェントのバックアップ HTTP 転送プロファイルを手動で作成するには、以下の手順を実行します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

	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 モードをイネーブルにします。 • 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 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 転送設定を作成します。 • 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。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 転送設定を作成します。
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 転送設定を作成します。
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。

バックアップ Cisco プラグ アンド プレイ HTTPS 転送プロファイルの設定

デバイス上に Cisco プラグ アンド プレイ（PnP）エージェントのバックアップ HTTPS 転送プロファイルを手動で作成するには、以下の手順を実行します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

	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 モードをイネーブルにします。 • 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 転送設定を作成します。 • *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。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 転送設定を作成します。
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 転送設定を作成します。
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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

バックアップ Cisco プラグ アンド プレイ XMPP 転送プロファイルの設定

デバイス上に手動で Cisco プラグ アンド プレイ（PnP）エージェントのバックアップ Extensible Messaging and Presence Protocol（XMPP）転送プロファイルを作成するには、次の手順を実行します。

	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 モードをイネーブルにします。 • 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。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

ステップ 4	**backup transport xmpp socket** {**host** *host-name* | **ipv4** *ipv4-address*| **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# backup transport xmpp socket host example.com port 231 sasl plain server-jid cisco123`	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 XMPP 転送設定を作成します。
ステップ 5	**backup transport xmpp starttls** {**host** *host-name* | **ipv4** *ipv4-address* | **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**localcert** *trustpoint-name*} {**remotecert** *trustpoint-name*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# backup transport xmpp starttls 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 XMPP 転送設定を作成します。 • *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 6	**backup transport xmpp tls** {**host** *host-name* | **ipv4** *ipv4-address* | **ipv6** *ipv6-address*} {**port** *port-number*} {**source** *interface-type interface-number*} {**localcert** *trustpoint-name*} {**remotecert** *trustpoint-name*} {**sasl plain server-jid** *xmpp-jabber-id*} **例:** `Device(config-pnp-init)# backup transport xmpp tls ipv6 2001:DB8:1::1 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 IPv6 アドレスに基づいて、PnP エージェント プロファイルの XMPP 転送設定を作成します。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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 プラグ アンド プレイ エージェント タグの設定

Cisco プラグ アンド プレイ(PnP)エージェント タグ情報を作成するには、次の手順を実行します。

	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 モードをイネーブルにします。 • 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`	**pnp tag** コマンドは、デバイスのタグを設定する場合に使用します。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。 • PnP エージェント タグの名前を指定する英数字文字列。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

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。

| © 2014-2015 Cisco and/or its affiliates. All rights reserved.

トラブルシューティング

デバイス情報の表示

Cisco プラグ アンド プレイ（PnP）サーバ上でデバッグを実行するには、サーバを起動して、PnP プロファイルおよび PnP 転送を設定します。つまり、PnP エージェントと PnP サーバの間のサービス対話を開始します。デバッグ情報を収集するには、**debug pnp service** コマンドを実行します。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

リソースおよびサポート情報

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*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技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。

 © 2014-2015 Cisco and/or its affiliates. All rights reserved.

TOMORROW
starts here.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)