Solution Guide for Cisco Network Plug and Play

First Published: 2015-11-23

Last Modified: 2018-05-17

Solution Guide for Cisco Network Plug and Play

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Monospace font`	Terminal sessions and information the system displays appear in `monospace` font.
`Bold monospace font`	Bold monospace font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Solution Overview

Enterprises and campus deployments incur major costs to install and deploy the large number of networking devices that go into their data center, branch networks and campus rollout. Typically, every device has to be pre-staged by a skilled installer and loaded, through a console connection, with a CLI configuration that allows it to connect to the rest of the network. This process is costly, time consuming, and error-prone. At the same time, customers would like to increase the speed and reduce complexity of the deployment without compromising the security.

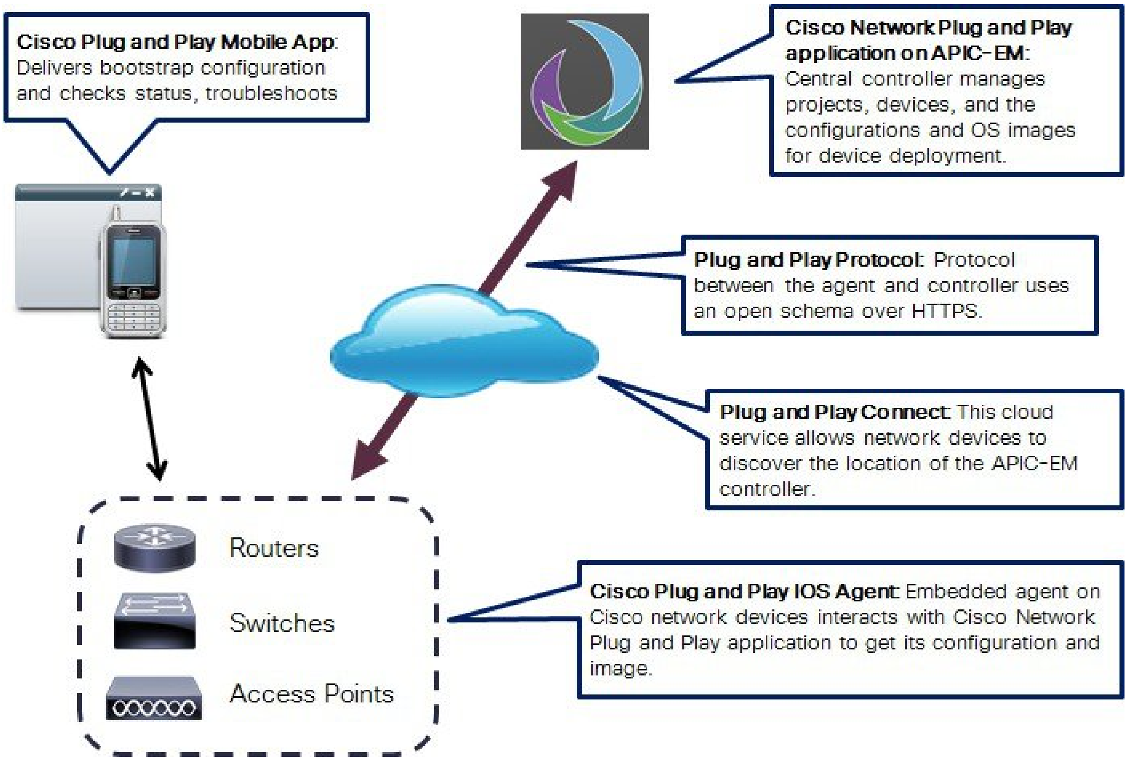
The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new branch or campus device rollouts or for provisioning updates to an existing network. The solution provides a unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless devices with a near zero touch deployment experience.

It reduces the burden on enterprises by greatly simplifying the process of deploying new devices. An installer at the site can deploy a new device without any CLI knowledge, while a network administrator centrally manages device configuration.

The Cisco Network Plug and Play solution offers these features:

- Simplified and consistent deployment of Cisco network devices
- Automated and centrally managed remote device deployment from the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)
- Converged solution for Cisco routers, switches, and wireless access point devices
- Support for switch stacks with up to 9 members in Cisco Network Plug and Play version 1.2 and later. Cisco Network Plug and Play intelligently discovers stack members based on identifying a single member switch and allows provisioning of the whole stack as one unit, without needing to provision each stack member individually.
- Devices can automatically discover the APIC-EM controller through DHCP, DNS, a proxy server, or the cloud through Plug and Play Connect, and predefined configurations and images can be pushed out as devices come online.
- Configuration templates allow an administrator to define a template of CLI commands that can be used to consistently configure multiple network devices, reducing deployment time. Configuration templates are supported in Cisco Network Plug and Play version 1.3 and later.
- Mobile iOS or Android application helps the device installer to bootstrap devices and monitor installation from remote site
- Secure device authentication and communication using secure unique device identifiers (SUDI), and certificates stored in a Cisco managed trustpool bundle, which is a special store of certificates signed by trusted certificate authorities and published by Cisco InfoSec. For more details on security and how it is managed, see Secure Connectivity, on page 14.

Figure 1: Cisco Network Plug and Play Architectural Overview


Cisco Plug and Play Mobile App: Delivers bootstrap configuration and checks status, troubleshoots
Cisco Network Plug and Play application on APIC-EM: Central controller manages projects, devices, and the configurations and OS images for device deployment.
Plug and Play Protocol: Protocol between the agent and controller uses an open schema over HTTPS.
Plug and Play Connect: This cloud service allows network devices to discover the location of the APIC-EM controller.
Routers
Switches
Access Points
Cisco Plug and Play IOS Agent: Embedded agent on Cisco network devices interacts with Cisco Network Plug and Play application to get its configuration and image.

Solution Components

The Cisco Network Plug and Play solution includes the following components:

- **Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)**—Cisco APIC-EM is Cisco's SDN Controller for Enterprise Networks (Access, Campus, WAN, and Wireless). The platform hosts multiple applications (SDN apps) that use open Northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.
- **Cisco Network Plug and Play application**—This preinstalled Cisco APIC-EM application receives plug and play requests from Cisco devices and provisions devices based on predefined rules and criteria.
- **Cisco Plug and Play IOS Agent**—This agent is embedded in Cisco devices and communicates to the Cisco Network Plug and Play application using the open plug and play protocol over HTTPS during device deployments.
- **Cisco Plug and Play Mobile App for iOS and Android devices**—Mobile application for iOS and Android devices that helps configure Cisco devices with a bootstrap configuration and triggers remote branch deployments. The app communicates with the Cisco Network Plug and Play application over 3G/4G/WiFi connections to get the predefined device bootstrap configuration, and delivers it to a Cisco network device by using a special serial cable that is physically connected to the device.
- **Cisco SMI Proxy**—Optional component needed to deploy Cisco switches that have older IOS versions without the new Cisco Plug and Play IOS Agent (older than IOS-XE3.6.3E and IOS15.2(2)E3). SMI

Proxy acts as a proxy between older Cisco switches and the Cisco Network Plug and Play application using the newer plug and play protocol. This proxy is not supported on routing platforms.

- **Generic HTTP Proxy**—Optional component for remote branch deployments where the Cisco APIC-EM is not reachable directly by remote devices because it is behind a DMZ zone. A generic HTTP reverse proxy can be placed before the APIC-EM in the DMZ, to relay messages between devices and the controller. Alternately, you can choose to set up a private VPN link so that the controller is reachable via VPN, without using a generic proxy.

- **Plug and Play Connect**—Optional cloud component for automatic PNP server discovery if the DHCP or DNS methods are not available. The PNP Server is the backend part of the Cisco Network Plug and Play application in the APIC-EM. The Cisco network device contacts the Cisco Plug and Play Connect cloud service at devicehelper.cisco.com to obtain the IP address of the appropriate PNP server that is defined for your organization.

Solution Workflows

This section describes workflows for the following typical use cases:

- Remote Branch/Site Deployment, on page 5
- Campus/LAN Deployment, on page 7
- Unplanned Device Deployment, on page 8
- Plug and Play Connect Device Deployment, on page 9

A prerequisite is an operating Cisco APIC-EM controller with the Cisco Network Plug and Play application.

Remote Branch/Site Deployment

The following steps summarize how to use Cisco Network Plug and Play to deploy a Cisco network device in a remote branch or site.

Before you begin

Cisco network devices are running Cisco IOS images that support the Cisco Plug and Play IOS Agent.

Procedure

Step 1 On the APIC-EM controller, the network administrator uses the Cisco Network Plug and Play application to pre-provision the remote site and device information in the application.

This includes entering device information and setting up a bootstrap configuration, full configuration, and IOS image for each device to be installed. The bootstrap configuration enables the Plug and Play Agent and typically specifies the device interface to be used and configures a static IP address for it. For details on using the Cisco Network Plug and Play application, see the *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*.

Step 2 (Optional). If the central network operations center is behind a DMZ, the network administrator should configure a generic HTTP proxy or a VPN link to the network operations center so that the Cisco Plug and Play IOS Agent in devices at remote sites can communicate with the Cisco Network Plug and Play application.

This is a one-time task, because once set up, the proxy or VPN can be used for all subsequent device deployments at remote sites. For details on setting up an HTTP proxy, see Generic HTTP Proxy Set Up, on page 16.

Step 3 At the remote site, the device installer installs and powers up the Cisco network device, then connects their mobile device to the console port of the Cisco network device with the special serial cable.

Note For Cisco wireless access point devices, the bootstrap configuration is not supported, so this step and the Cisco Plug and Play Mobile App is not needed.

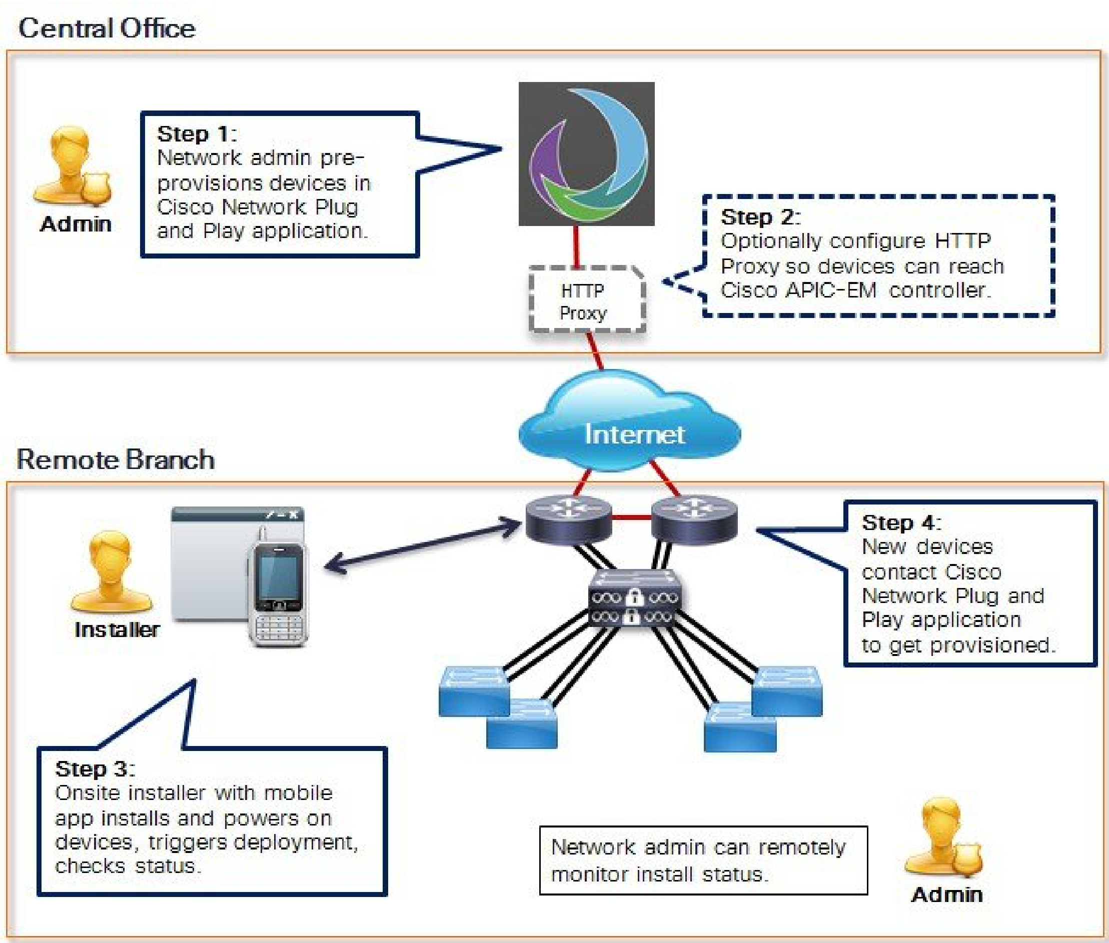
The device installer uses the Deploy Devices function in the Cisco Plug and Play Mobile App to deliver the bootstrap configuration to the Cisco network device and trigger deployment. For details on using the Cisco Plug and Play Mobile App to deploy devices, see the online help in the mobile app.

Note You can also deliver the bootstrap configuration to a Cisco router or switch by using a USB flash drive, however, USB autoinstall is a platform dependent feature. For details on using a USB flash drive, see Overview of Cisco 800 Series ISR Deployment. For platforms that do not support USB (such as the Cisco Catalyst 2000 Series and 3000 Series switches), we recommend using the Cisco Plug and Play Mobile App.

Step 4 The network device connects to the Cisco Network Plug and Play application on the APIC-EM controller, identifies itself by serial number, and downloads its full configuration and, optionally, an IOS image, which were pre-provisioned by the network administrator.

Note By using DHCP or DNS, Cisco network devices can automatically discover the APIC-EM and download their full configurations when powered on, and the Cisco Plug and Play Mobile App is not needed in such cases. Using DHCP requires that there is layer 3 connectivity to the Cisco APIC-EM controller and a DHCP server is configured with Cisco Network Plug and Play option 43. Alternately, the Cisco Plug and Play IOS Agent can find the Cisco APIC-EM controller by using DNS. Sometimes, these requirements are not met in a remote site deployment, so this use case focuses on using the Cisco Plug and Play Mobile App. For DHCP configuration details, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.

Figure 2: Automated Branch Deployment


Central Office
Admin
Step 1: Network admin pre-provisions devices in Cisco Network Plug and Play application.
Step 2: Optionally configure HTTP Proxy so devices can reach Cisco APIC-EM controller.
HTTP Proxy
Internet
Remote Branch
Installer
Step 4: New devices contact Cisco Network Plug and Play application to get provisioned.
Step 3: Onsite installer with mobile app installs and powers on devices, triggers deployment, checks status.
Network admin can remotely monitor install status.
Admin

Campus/LAN Deployment

The following steps summarize how to use Cisco Network Plug and Play to deploy a Cisco network device in a campus or LAN, where network devices can auto-discover the Cisco APIC-EM controller.

Before you begin

Cisco switches are running Cisco IOS images that support the Cisco Plug and Play IOS Agent. If any switches are running older Cisco IOS images, you must use the SMI Proxy. For details, see SMI Proxy Set Up, on page 16.

Procedure

Step 1 The network administrator sets up a DHCP server in the network to respond to client discover requests with DHCP option 43, which contains the APIC-EM controller IP address and port information.

Alternatively, DNS can be used to locate the controller. For DHCP and DNS configuration details, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.

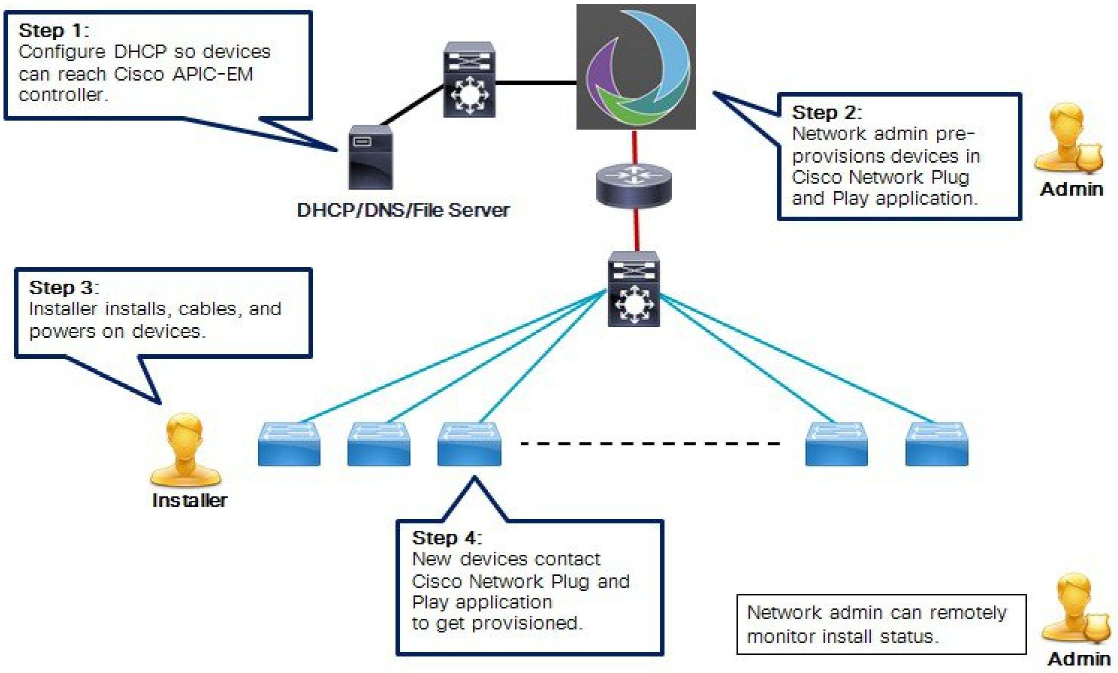
Step 2 The network administrator uses the Cisco Network Plug and Play application to pre-provision the remote site and device information.

This includes entering device information and setting up a bootstrap configuration (optional), full configuration, and IOS image for each device to be installed. The bootstrap configuration enables the Cisco Plug and Play IOS Agent and typically specifies the device interface to be used and configures a static IP address for it. For details on using the Cisco Network Plug and Play application, see the *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*.

Step 3 The device installer installs and powers up the Cisco network device.

Step 4 The device auto-discovers the APIC-EM controller by using DHCP or DNS, identifies itself by serial number to the Cisco Network Plug and Play application, and downloads its full configuration and, optionally, an IOS image, which were pre-provisioned by the network administrator.

Figure 3: Campus Deployment


Step 1:
Configure DHCP so devices can reach Cisco APIC-EM controller.
DHCP/DNS/File Server
Step 2:
Network admin pre-provisions devices in Cisco Network Plug and Play application.
Admin
Step 3:
Installer installs, cables, and powers on devices.
Installer
Step 4:
New devices contact Cisco Network Plug and Play application to get provisioned.
Network admin can remotely monitor install status.
Admin

Unplanned Device Deployment

In some cases, such as small sites or where pre-provisioning is not needed, devices can be deployed without prior set up on the Cisco Network Plug and Play application and then claimed and configured later.

The following steps summarize how to use Cisco Network Plug and Play to deploy a Cisco network device by using the unplanned device option.

Before you begin

Cisco network devices are running Cisco IOS images that support the Cisco Plug and Play IOS Agent.

Procedure

Step 1 The network administrator sets up a DHCP server in the network to respond to client discover requests with DHCP option 43, which contains the APIC-EM controller IP address and port information.

Alternatively, DNS can be used to locate the controller. For DHCP and DNS configuration details, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.

Step 2 The device installer installs and powers up the Cisco network device.

Step 3 The device auto-discovers the APIC-EM controller by using DHCP or DNS.

The device is listed as an unplanned device in the Cisco Network Plug and Play application, identified by IP address and product ID.

Step 4 The network administrator uses the Cisco Network Plug and Play application to claim the device and configure it with a new configuration and IOS image.

For details on using the Cisco Network Plug and Play application, see the *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*.

Plug and Play Connect Device Deployment

In situations where automatic APIC-EM discovery is desired but using the DHCP or DNS discovery methods is not an option, Plug and Play Connect allows devices to discover the IP address of APIC-EM controller.

When the network device boots up, if it cannot locate the APIC-EM controller through DHCP or DNS, then it tries Plug and Play Connect by contacting devicehelper.cisco.com to obtain the IP address of the appropriate APIC-EM controller that is defined for your organization. To secure the communications, the first thing that the device does when contacting Plug and Play Connect is to download and install the Cisco trustpool bundle.

The following steps summarize how to use Cisco Network Plug and Play to deploy a Cisco network device by using Plug and Play Connect.

Before you begin

Cisco network devices are running Cisco IOS images that support the Cisco Plug and Play IOS Agent and have connectivity to the Cisco Plug and Play Connect service.

Procedure

Step 1 The network administrator configures the controller profile for the appropriate APIC-EM controller for your organization with Plug and Play Connect.

This can be done through the Cisco Smart Account, Plug and Play Connect web portal or through the Cisco Network Plug and Play application. For details, see the appropriate documentation.

Step 2 If you order plug and play network devices through Cisco Commerce Workspace (CCW), these network devices are automatically registered with Plug and Play Connect as long as a Cisco Smart Account is assigned to the order and you include the NETWORK-PNP-LIC option for each device that you want to use with Cisco Network Plug and Play.

This option causes the device serial number and PID to be automatically registered in your Smart Account for plug and play. If you have specified a default controller, then the devices are automatically assigned to that controller when the order is processed.

Step 3 If you want to be able to manually add other devices in Plug and Play Connect, you can request access to this functionality by sending an email to Pnp-access-request@cisco.com.

Step 4 When you manually add a device in the Plug and Play Connect web portal, you can optionally associate the device with a configuration or configuration template that you have uploaded to the web portal by using the Configurations or Configuration Templates tabs. The configuration is applied to the device when it contacts the Plug and Play Connect web portal.

Note This feature is in Beta release and can be used with Cisco network devices that support SUDI. You must enter the SUDI serial number of the device in the Plug and Play Connect web portal. You cannot use this feature of defining a configuration in Plug and Play Connect at the same time as redirecting devices to your own APIC-EM controller.

Step 5 In the Cisco Network Plug and Play application in the APIC-EM controller, click the **Settings** tab, choose Smart Accounts and register your APIC-EM as the default controller for your Smart Account.

This step is required if you order plug and play network devices through CCW and these network devices are automatically registered with Plug and Play Connect through your Smart Account. For details on using the Cisco Network Plug and Play application, see the Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM.

Step 6 In the Cisco Network Plug and Play application in the APIC-EM controller, choose the **Devices** > **Cloud Synced** tab, and click the **Sync** button.

Devices registered in the Plug and Play Connect web portal are synced to the controller, appear in the list, and can be moved to a project by selecting them and clicking Move to Project.

Note This step is not necessary for devices that you have manually added and associated with a configuration as described in Step 4.

Step 7 Pre-provision the devices by going to Projects, choosing the project, and editing the newly added devices to assign a configuration and image.

You can assign a bootstrap configuration (optional), full configuration, and IOS image for each device to be installed. The bootstrap configuration enables the Cisco Plug and Play IOS Agent and typically specifies the device interface to be used and configures a static IP address for it.

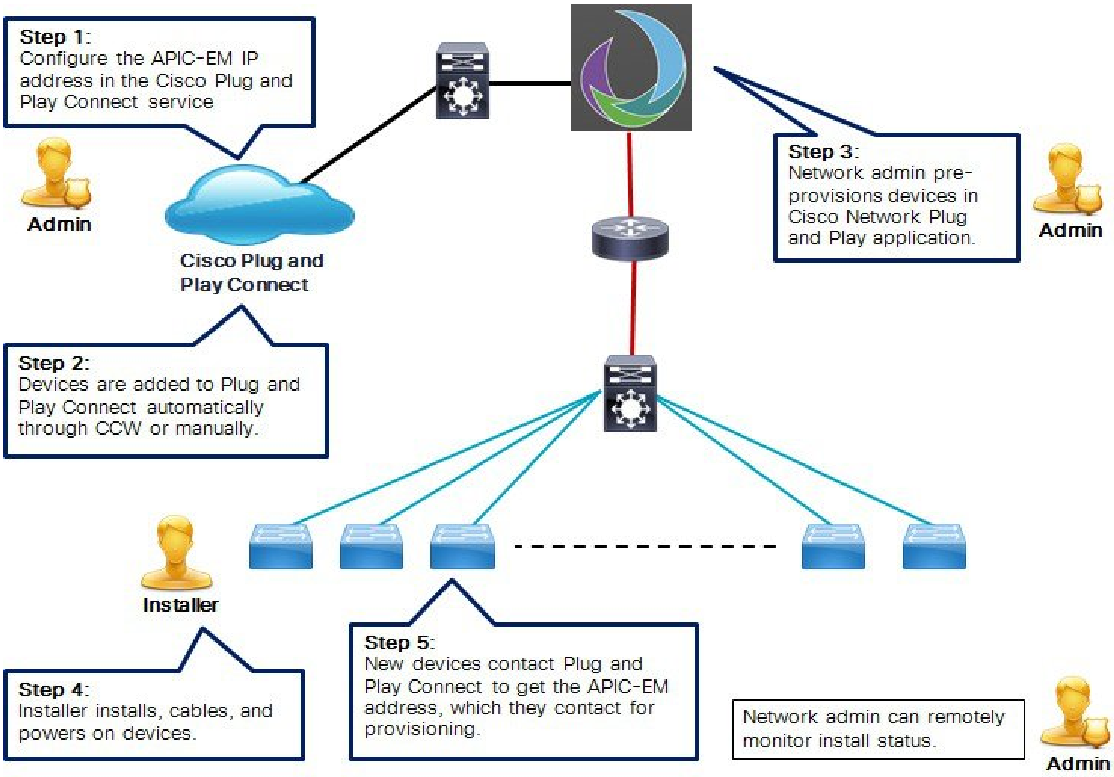
Note This step is not necessary for devices that you have manually added and associated with a configuration as described in Step 4.

Step 8 The device installer installs and powers up the Cisco network device.

Step 9 The device discovers the APIC-EM controller by querying the Plug and Play Connect service, then identifies itself by serial number to the Cisco Network Plug and Play application, and downloads its full configuration and, optionally, an IOS image, which were pre-provisioned by the network administrator.

Note The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers **time-pnp.cisco.com** or **pool.ntp.org**. To resolve this problem, either unblock NTP traffic to these two host names, or map these two NTP host names to local NTP server addresses on the DNS server.

Figure 4: Plug and Play Connect Device Deployment


Step 1:
Configure the APIC-EM IP address in the Cisco Plug and Play Connect service
Admin
Cisco Plug and Play Connect
Step 2:
Devices are added to Plug and Play Connect automatically through CCW or manually.
Step 3:
Network admin pre-provisions devices in Cisco Network Plug and Play application.
Admin
Installer
Step 4:
Installer installs, cables, and powers on devices.
Step 5:
New devices contact Plug and Play Connect to get the APIC-EM address, which they contact for provisioning.
Network admin can remotely monitor install status.
Admin

Deploying the Cisco Network Plug and Play Solution

This section discusses deploying the Cisco Network Plug and Play solution.

Prerequisites

The following are prerequisites for using the Cisco Network Plug and Play solution:

- APIC-EM with the Cisco Network Plug and Play application is deployed and operational. For details, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .
- Cisco network devices to be deployed are running IOS releases that support the Cisco Network Plug and Play IOS Agent (for supported platforms and software releases, see the *Release Notes for Cisco Network Plug and Play*).
- The Cisco network devices to be deployed are in a factory default state and can be auto-booted with the supported image. If you are using a network device that was previously configured or is in an unknown state, see the reset details in Network Device Troubleshooting, on page 18.

- All members of a Cisco switch stack must be running the same IOS release and must be properly connected before powering up the switches and connecting to the APIC-EM for Plug and Play provisioning.
- The Cisco Plug and Play Mobile App (iOS or Android version) is installed on the mobile device being used by the device installer and the special serial console cable is available.

Note The Cisco Plug and Play Mobile App is not used for deploying Cisco wireless access point devices and is optional for other devices.

- The Cisco SMI Proxy is optionally installed in the network if deploying Cisco switches that have older IOS versions, without the new Cisco Plug and Play IOS Agent (older than IOS-XE3.6.0E, IOS15.2(2)E). For details, see SMI Proxy Set Up, on page 16.
- A generic HTTP Proxy is optionally installed in the network if the remote devices to be deployed will need to contact the APIC-EM controller by using the public Internet and the controller is behind a DMZ. For details, see Generic HTTP Proxy Set Up, on page 16. Alternately, you can choose to set up a private VPN link so that the controller is reachable via VPN, without using a generic proxy. A VPN connection could be configured in the bootstrap configuration delivered by the mobile app to the device.
- If you are using the Cisco Plug and Play Mobile App and the APIC-EM controller is behind a firewall, you must allow traffic on ports 80 and 443 through the firewall.
- If you are using Cisco Plug and Play Connect, the IP address of the appropriate controller for your organization is defined in the Plug and Play Connect web portal in your Cisco Smart Account, and network devices are using a supported IOS software release. For details on device and software release support, see the Release Notes for Cisco Network Plug and Play.

Guidelines

Follow these recommendations when deploying the Cisco Network Plug and Play solution:

- Configure a DHCP server with option 43 to allow Cisco network devices to auto-discover the APIC-EM controller. For DHCP and DNS configuration details, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.
- Pre-provision the device configuration in the Cisco Network Plug and Play application for all new devices to be deployed. This includes setting up the site and devices in it with the device serial numbers, bootstrap configuration, full configuration, and IOS image. For details, see the *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*. Note that pre-provisioning is not needed if you plan to use the Unplanned Device deployment option.
- To use the trustpool security feature, a valid certificate from a well-known certificate authority (CA) must be installed on the APIC-EM controller. The default self-signed certificate does not allow the use of trustpool security. Additionally, the DHCP option 43 string must be configured with the HTTPS transport option (K5); for details, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.
- Device bring up order—In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Cisco Network Plug and Play IOS Agent attempts to auto-discover the APIC-EM controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.

- Cisco Router Trunk/Access Port Configuration—Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, the following deployment models are supported for Cisco Network Plug and Play:
  - Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router can be configured as a trunk or access port.

    Note If the upstream router is a Cisco 4000 Series ISR router, this functionality is impacted by caveat CSCut77951 , which is resolved in software release 15.5(3)S4.

  - Downstream switch is connected to the router using a routed port on the router. In this case, the routed port can support multiple VLANs using sub-interfaces. During the Plug and Play process the switch would automatically configure its port as a trunk port. In a large branch scenario, it becomes necessary to carry multiple VLANs between the router and the downstream switch. To support this use case, the switch must be connected to a routed port.

- Non-VLAN 1 configuration-Cisco Network Plug and Play supports devices using VLAN 1 by default. To use a VLAN other than 1, adjacent upstream devices must use supported releases and configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp startup vlan** *x* . When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, all the active interfaces on the upcoming Plug and Play device are changed to the specified VLAN. This guideline applies to both routers and switches.

Note When using the non-VLAN 1 feature, ensure that all the neighboring switch devices are running Cisco IOS XE Release 3.6.3 or later, and not the 3.6.0, 3.6.1, or 3.6.2 releases. For more information about related caveat CSCut25533 that exists in these previous releases, see the Caveats section in the *Release Notes for Cisco Network Plug and Play* .

Using VRF with Cisco Network Plug and Play

During Cisco Network Plug and Play configuration provisioning, the configuration file is applied to the running configuration of the device. If the device is using Virtual Route Forwarding (VRF), or it has multiple IP interfaces in the final configuration, the source IP address used to contact the APIC-EM controller could change after the final configuration is applied. This IP address change could result in the loss of connectivity to the controller and the device status will show a provisioning error because the controller fails to receive a successful response from the device.

For example, for a router deployment, the initial source IP address that the router uses to contact the APIC-EM controller is its WAN IP address. After the controller pushes the configuration to the router, the router could use any IP address (such as the tunnel IP address) to contact the controller. If there is no IP connectivity from the tunnel IP address to the controller, it will cause a health check error on the controller.

To avoid this issue, use the **ip http client source-interface** *interface* command in the final provisioning configuration. Since the plug and play protocol uses HTTP/HTTPS, this command tells the device to use the same interface for a response as was initially used for contacting the controller before configuration provisioning, regardless of VRF. For a router deployment scenario, you can specify the same WAN interface as the source interface.

Secure Connectivity

The Cisco Network Plug and Play solution uses HTTPS connections between network devices and the APIC-EM controller. This secure connectivity is implemented in one of two ways, depending on the type of transport you specify in the DHCP option. For details on configuring DHCP, see Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20.

Depending on the transport specified in the K parameter in the DHCP option 43 string, secure connectivity is implemented in the following ways:

- HTTP is specified as the transport protocol (default) and secure connectivity is based on trustpoint.

  Trustpoint based secure connectivity relies on the self-signed certification that is installed by default on the APIC-EM controller. This self-signed certificate is used to create a default trustpoint on network devices, which allows devices to connect securely over HTTPS to the APIC-EM controller. HTTPS is used for communications with the APIC-EM controller, despite the fact that HTTP is specified as the transport protocol.

- HTTPS is specified as the transport protocol and secure connectivity is based on trustpool.

  Trustpool based secure connectivity additionally requires that you replace the self-signed certification on the APIC-EM controller with your own CA signed certificate. A trustpool is a special store of certificates signed by trusted certificate authorities and published by Cisco InfoSec. A Cisco network device imports the trustpool bundle immediately upon contacting the APIC-EM controller and this allows it to validate the controller certificate and create root CA trustpoints, enabling secure communications over HTTPS with its own signed certificate.

You can choose to host the trustpool bundle in a different location in your network, which you can specify in the T parameter to DHCP option 43. In this case, network devices would obtain your trustpool bundle instead of the default one that is installed in the APIC-EM.

For more details on security, importing certificates, and the trustpool bundle, see the “Cisco APIC-EM Security” chapter in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

SUDI Authentication

Some of the next generation of Cisco network devices (such as the Cisco ISR 4000 Series routers) support secure device identification and authentication using a secure unique device identifier (SUDI) certificate that is factory installed in the device hardware. The device sends this SUDI certificate to the APIC-EM controller during the SSL handshake. You can specify that the APIC-EM controller must validate the SUDI certificate to authenticate the device.

To require SUDI authentication on devices that support it, check the Authentication check box next to the device listed in the Projects tab of the Cisco Network Plug and Play application. If you check this box for a device that does not support SUDI authentication, then authentication and provisioning fails with an authentication error and you should uncheck the box to continue with the device. For details, see the Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM.

Note Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). You must enter the SUDI serial number in the Serial Number field when adding a device that uses SUDI authentication.

For a list of devices that support SUDI authentication, see the Release Notes for Cisco Network Plug and Play.

Using the Mobile App

The Cisco Plug and Play Mobile App (iOS or Android version) can be used by the device installer to help configure Cisco devices with a bootstrap configuration and trigger remote branch deployments, if auto-discovery of the APIC-EM controller is not possible. The mobile app communicates with the Cisco Network Plug and Play application over 3G/4G/WiFi connections to get the predefined device bootstrap configuration, and delivers it to a Cisco network device by using a special cable that is physically connected to the device console port.

The mobile apps are available at the following app stores:

- 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

Note The Cisco Plug and Play app for iOS requires iOS version 7 or later. The Android app requires Android version 4.1 or later.

Note The Cisco Plug and Play Mobile App is not used for deploying Cisco wireless access point devices.

The following console cable is needed, depending on whether the device is an iOS or Android device:

- iOS device: Redpark Lightning Console Cable (L2-RJ45V), for iOS devices with the Lightening (8-pin) connector, or Redpark Console Cable (C2-RJ45V), for iOS devices with the older 30-pin connector.
- Android device: Airconsole bluetooth adapter

Note After disconnecting the console cable from the network device, if you want to connect it to a different network device, you must first manually refresh the mobile app to reflect the correct status when connecting to the new device.

Note If you have an iOS mobile device with a Redpark cable and are deploying multiple network devices, after you are done with one device, you must unplug the Redpark cable from both your mobile device and the network device to close the serial connection. If you do not disconnect the cable from your mobile device, the serial session is not closed and the wrong configuration could be deployed on the next device.

Setting Up the Mobile App

Before using the Cisco Plug and Play Mobile App for the first time, you must configure it with the URL and credentials for the APIC-EM controller. These settings are saved once set up.

To set up the controller information, follow these steps:

Procedure

Step 1 Launch the Cisco Plug and Play Mobile App and choose **Settings** from the menu.

Step 2 In the Server URL field, enter the IP address of the APIC-EM controller.

Step 3 In the Username and Password fields, enter the username and password credentials for an APIC-EM user account that has the installer role.

For details on setting up user accounts and roles, see the chapter “Managing Users and Roles” in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 4 Tap **Test Connection** to test the controller connection and show the status.

Step 5 If the connection is successful, tap **Save** in the upper right corner, then **Done** in the upper left corner, to return to the main screen.

SMI Proxy Set Up

The Smart Install (SMI) Proxy leverages Smart Install functionality that exists in Cisco switches that have older IOS versions without the new Cisco Plug and Play IOS Agent (older than IOS-XE 3.6.3E and IOS 15.2(2)E3). SMI Proxy acts as a proxy between the switches and the Cisco Network Plug and Play application using the newer plug and play protocol.

The SMI proxy is applicable only to switching platforms that support Smart Install Director functionality and is not supported on routing platforms.

For details on configuring SMI Proxy, see the “Configuring SMI Proxy” chapter of the *Smart Install Configuration Guide* .

Note Customers should consider upgrading to newer IOS images to get full benefit of the Cisco Network Plug and Play Solution. The SMI Proxy does not provide all of the capabilities of the newer Cisco Plug and Play IOS Agent and it should be considered only as an interim solution until deployment of an IOS image with the newer Cisco Plug and Play IOS Agent.

Generic HTTP Proxy Set Up

If the remote network devices to be deployed need to contact the APIC-EM controller by using the public Internet, and the controller is behind a DMZ, a generic HTTP proxy must be installed in the network so that the network devices can contact the APIC-EM controller. A generic HTTP reverse proxy, such as the Apache reverse proxy, can be placed before the APIC-EM controller in the DMZ, to relay messages between network devices and the APIC-EM controller.

To use a reverse proxy, the same certificate from a well known certificate authority (CA) must be installed on the Apache HTTP proxy server, the APIC-EM, and the network device that is being deployed. The certificate allows all devices to establish trusted communications. The APIC-EM controller installs the certificate on the network device.

To import the certificate on the APIC-EM, use the **Settings** > **Proxy Gateway Certificate** GUI command as described in the chapter “Configuring the Cisco APIC-EM Settings” in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

Note Cisco recommends against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended.

The Cisco Network Plug and Play solution has been tested with Apache HTTP Server version 2.4.7 on Ubuntu. The following lines from the Apache configuration file show an example of how to enable the reverse proxy in Apache. Substitute the IP address of the APIC-EM controller in place of *APIC-EM-ip-address* in the commands below:

```
<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>
```

Troubleshooting Tips

Refer to this section for common self-help topics or issues that may come up during deployment.

Note If you purchased this product through a Cisco reseller, contact the reseller directly for technical support. If you purchased this product directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

APIC-EM Controller Troubleshooting

For details on troubleshooting the APIC-EM controller, see the troubleshooting chapter in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

You can check the Cisco Network Plug and Play application status in the APIC-EM GUI by going to the Home screen and clicking on **Network Plug and Play** in the left navigation pane. If the application is running, it will open.

You can view logs on the Cisco Network Plug and Play application by going to the Home screen and clicking on **Logs** in the left navigation pane. In the Service drop-down menu, choose pnp-service to filter on logs only for the Cisco Network Plug and Play application.

You can reset the provisioning status of a network device if its state gets out of synchronization with the status shown in the Cisco Network Plug and Play application. Select the device in the Sites tab and click the **Reset** button, then click **OK** in the confirmation dialog. Resetting a device causes it to go through the provisioning process again. It recontacts the APIC-EM controller and downloads its full configuration and, optionally, an IOS image.

Mobile App Troubleshooting

The Cisco Plug and Play Mobile App requires 3G/4G/WIFI connectivity to the APIC-EM controller to retrieve the bootstrap configuration file for a device.

The app can also be used in offline mode for bootstrap delivery, if it was previously connected to the controller and a bootstrap configuration was delivered to a device. The bootstrap configuration file stays in the app and can be used again for offline delivery to the same type of device.

The Cisco Plug and Play Mobile App keeps detailed logs on app operations and serial connection interactions. You can view or email logs by choosing **Troubleshooting** from the main screen, then **View Logs** or **Email Logs**.

Network Device Troubleshooting

Cisco network devices to be deployed must be in a factory default state. If you are using a network device that was previously configured or is in an unknown state, you must reset it to the factory default condition, as follows:

- If you are using a Cisco router or switch that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
config terminal
no pnp profile pnp-zero-touch
no crypto pki certificate pool
config-register 0x2102   (for non-default ROMMON only)
end
delete /force vlan.dat   (for Switch platforms only)
delete /force nvram:*.cer
delete /force stby-nvram:*.cer  (for HA system only)
write erase  (answer no when asked to save)
reload
```

- If you are using a Cisco Aironet 3700, 3600, 2700, 2600, 1700, 1600, or 700 Series Access Point device that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
debug capwap console cli
config terminal
no crypto pki certificate pool
boot system flash:/ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx  (for 3700, 2700, 1700, 3600, 2600
 platforms)
boot system flash:/ap1g2-rcvk9w8-mx/ap1g2-rcvk9w8-mx  (for 1600 platforms)
boot system flash:/ap1g1-rcvk9w8-mx/ap1g1-rcvk9w8-mx  (for 700 platforms)
end
clear capwap private-config
delete /force flash:capwap*
delete /force flash:private-multiple-fs
delete /force flash:lwapp*
write erase
reload
```

- If you are using a Cisco Aironet 3800, 2800, or 1800 Series Access Point device that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
capwap ap erase all
reload
```

IP connectivity between the Cisco Plug and Play IOS Agent in the Cisco network device and the APIC-EM controller is required. Ensure that the network device is able to ping the APIC-EM controller.

You can view active connections for the Cisco Plug and Play IOS Agent as follows:

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

If needed, you can enable debug information and capture the output for the Cisco Plug and Play IOS Agent as follows:

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

Note You may also want to use the **debug cns all** command to capture additional debug information about the Cisco Networking Service (CNS). This command typically produces a lot of output, so ensure that you have a large enough log buffer.

See the *Cisco Open Plug-n-Play Agent Configuration Guide* for detailed help with any of the commands related to the Cisco Plug and Play IOS Agent.

Controller Discovery

Devices can automatically discover the APIC-EM controller through DHCP, DNS, a proxy server, or the cloud through Plug and Play Connect. This section contains the following topics related to controller discovery:

- Configuring DHCP for APIC-EM Controller Auto-Discovery, on page 20
- Using DNS for APIC-EM Controller Auto-Discovery, on page 21
- Configuring Server Identity, on page 22

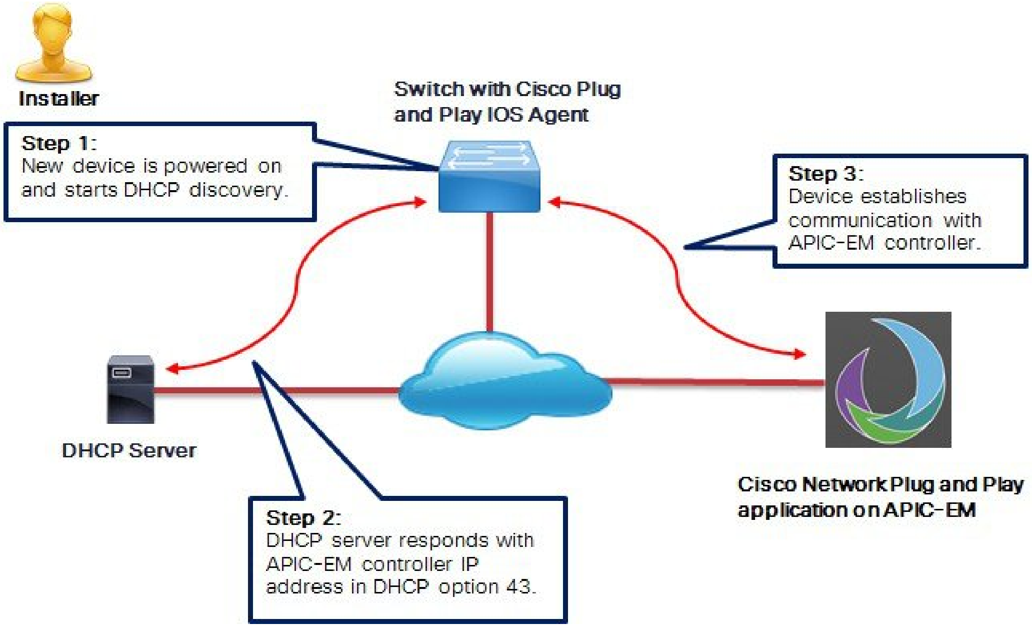
Configuring DHCP for APIC-EM Controller Auto-Discovery

A Cisco network device with no startup configuration triggers the Cisco Plug and Play IOS Agent to initiate a DHCP discovery process, which can acquire the APIC-EM controller IP address from the DHCP server. This auto-discovery process requires that the DHCP server be configured with the vendor specific option 43 that contains additional information about the APIC-EM controller.

When the DHCP server receives a DHCP discover message with option 60 that contains the string “ciscopnp”, it responds to the device by returning a response that contains the option 43 information.

The Cisco Plug and Play IOS Agent extracts the APIC-EM controller IP address from the response and uses this address to communicate with the controller.

Figure 5: DHCP Discovery of Cisco APIC-EM Controller


Installer
Switch with Cisco Plug and Play IOS Agent
Step 1: New device is powered on and starts DHCP discovery.
Step 3: Device establishes communication with APIC-EM controller.
DHCP Server
Cisco Network Plug and Play application on APIC-EM
Step 2: DHCP server responds with APIC-EM controller IP address in DHCP option 43.

The prerequisites for the DHCP auto-discovery method are as follows:

- New devices can reach the DHCP server
- The DHCP server is configured with option 43 for Cisco Network Plug and Play

DHCP option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

```
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
```

The option 43 string has the following components, delimited by semicolons:

- 5A1N;—Specifies the DHCP suboption for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2;—IP address type:
  - B1 = hostname
  - B2 = IPv4 (default)
- I*xxx.xxx.xxx.xxx*;—IP address or hostname of the APIC-EM controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
- J*xxxx*—Port number to use to connect to the APIC-EM controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- K4;—Transport protocol to be used between the Cisco Plug and Play IOS Agent and the server:
  - K4 = HTTP (default)
  - K5 = HTTPS
- T*trustpoolBundleURL*;—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the default, which is the APIC-EM controller, which gets the bundle from the Cisco InfoSec cloud (http://www.cisco.com/security/pki/). For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Ttftp://10.30.30.10/ios.p7b

  If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the APIC-EM controller.
- Z*xxx.xxx.xxx.xxx*;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

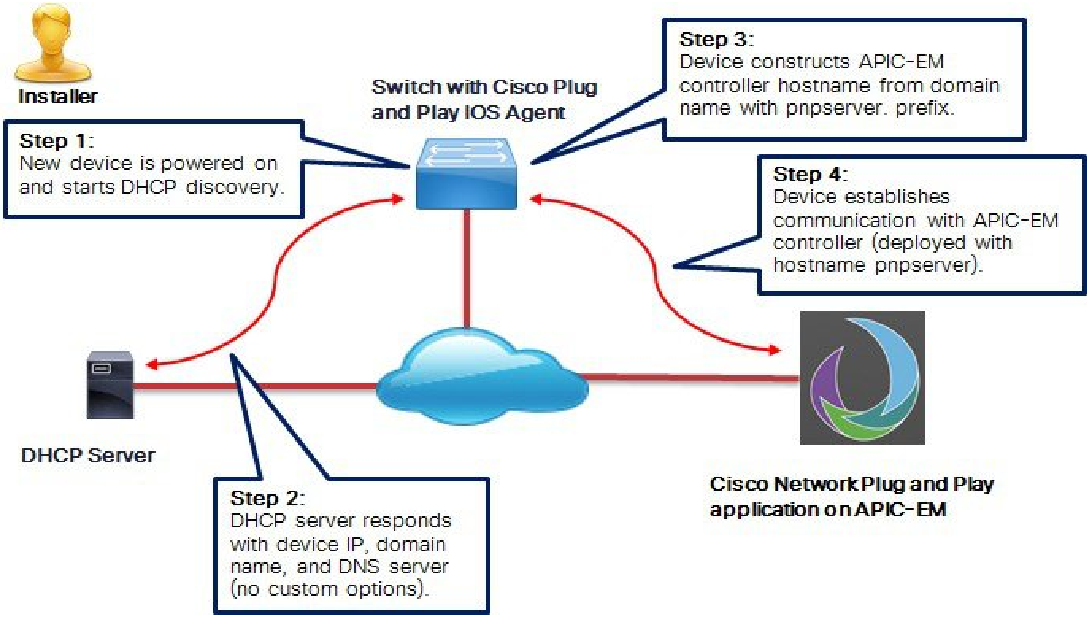
See the *Cisco IOS Command Reference* for additional details on DHCP configuration.

Using DNS for APIC-EM Controller Auto-Discovery

If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play IOS Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the APIC-EM controller, using the preset hostname pnpserver. The NTP server name is based on the preset hostname pnpntpserver.

For example, if the DHCP server returns the domain name “customer.com”, the Cisco Plug and Play IOS Agent constructs the APIC-EM controller FQDN of pnpserver.customer.com. It then uses the local name server to resolve the IP address for this FQDN. The NTP server name FQDN would be pnpntpserver.customer.com.

Figure 6: DNS Discovery of Cisco APIC-EM Controller


Installer
Step 1:
New device is powered on and starts DHCP discovery.
Switch with Cisco Plug and Play IOS Agent
Step 3:
Device constructs APIC-EM controller hostname from domain name with pnpserver. prefix.
Step 4:
Device establishes communication with APIC-EM controller (deployed with hostname pnpserver).
DHCP Server
Step 2:
DHCP server responds with device IP, domain name, and DNS server (no custom options).
Cisco Network Plug and Play application on APIC-EM

The prerequisites for the DNS auto-discovery method are as follows:

- New devices can reach the DHCP server.
- The APIC-EM controller is deployed with the hostname “pnpserver”.
- The NTP server is deployed with the hostname pnpntpserver.

Configuring Server Identity

To ensure successful controller discovery by Cisco devices running newer IOS releases, the server SSL certificate offered by the controller during the SSL handshake must contain an appropriate Subject Alternate Name (SAN) value, so that the Cisco Plug and Play IOS Agent can verify the server identity. This may require the controller administrator to upload a new server SSL certificate, which has the appropriate SAN values, to the controller. This requirement applies to all controllers that implement the Plug and Play server.

This requirement applies to devices running the following Cisco IOS releases:

- Cisco IOS Release 15.2(6)E2 and later
- Cisco IOS Release 15.6(3)M4 and later
- Cisco IOS Release 15.7(3)M2 and later
- Cisco IOS XE Denali 16.3.6 and later
- Cisco IOS XE Everest 16.5.3 and later
- Cisco IOS Everest 16.6.3 and later
- All Cisco IOS releases from 16.7.1 and later

The value of the SAN field in the controller certificate must be set according to the type of discovery being used by devices, as follows:

- For DHCP option-43/option-17 discovery using an explicit IPv4 or IPv6 address, set the SAN field to the specific IPv4/IPv6 address of the controller.
- For DHCP option-43/option-17 discovery using a hostname, set the SAN field to the controller hostname.
- For DNS discovery, set the SAN field to the hostname of the controller, in the form of pnpserver.*domain*.
- For Cisco Plug and Play Connect cloud portal discovery, set the SAN field to the controller IP address, if the IP address is used in the Plug and Play Connect profile. If the profile uses the controller hostname, then the SAN field must be set to the fully qualified domain name (FQDN) of the controller.

If the controller IP address that is used in the Plug and Play profile is a public IP address that is assigned by a NAT router, then this public IP address must be included in the SAN field of the server certificate.

If an HTTP proxy server is used between the devices and the controller, ensure that the proxy certificate has the same SAN fields with the appropriate IP address or hostname.

It is recommended to include multiple SAN values in the certificate, in case discovery methods vary. For example, you can include both the controller FQDN and IP address (or NAT IP address) in the SAN field. If you do include both, set the FQDN as the first SAN value, followed by the IP address.

If the SAN field in the controller certificate does not contain the appropriate value, the device will not be able to successfully complete the plug and play process.

Note The Cisco Plug and Play IOS Agent checks only the certificate SAN field for the server identity. It does not check the common name (CN) field.

Related Documentation

- Release Notes for Cisco Network Plug and Play—Release Notes for the Cisco Network Plug and Play solution.
- Release Notes for Cisco Plug and Play Connect—Release Notes for the Cisco Plug and Play Connect cloud service.
- Plug and Play Connect website—Documentation for the Cisco Plug and Play Connect cloud service.
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM—Describes how to use the Network Plug and Play application in the APIC-EM to configure Cisco network devices.
- Cisco Open Plug-n-Play Agent Configuration Guide—Describes how to configure the Cisco Open Plug-n-Play Agent software application that runs on a Cisco IOS or IOS-XE device.
- Mobile Application User Guide for Cisco Network Plug and Play—Describes how to use the Cisco Network Plug and Play mobile application.
- Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide—Describes how to deploy and troubleshoot the Cisco APIC-EM.
- Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide—Describes how to configure settings for the Cisco APIC-EM.
- Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module—Release Notes for the Cisco APIC-EM.

- Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)—Release Notes for Cisco IWAN.
- Software Configuration Guide for Cisco IWAN on APIC-EM—Configuration Guide for Cisco IWAN.
- *Cisco APIC-EM Quick Start Guide* Guide to getting started with the APIC-EM and including a list of related documentation (available in the APIC-EM GUI).
- Open Source Used In Cisco APIC-EM—List of open source code used in the Cisco APIC-EM.
- Open Source Used In Cisco IWAN App Release 1—List of open source code used in the Cisco IWAN and Cisco Network Plug and Play applications for APIC-EM.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.