Network Simplification

Network Plug and Play for Day-0 Deployments

René and Per, Cisco DK SEs
Cisco Network Plug and Play (PnP) Solution Overview
Simple & Secure & Consistent Device Onboarding

Network Plug-n-Play
Simple, Secure & Consistent device on-boarding for Enterprise platforms

Simple
- Zero-Touch provisioning of Campus & Branch deployments
- GUI Based workflows
- Robust Discovery Mechanisms for all deployment types (DHCP, DNS, Mobile App, USB)
- Cloud Redirect Service for automated branch deployments (Roadmap)

Secure
- SUDI based device authentication
- CA based server (APIC-EM) authentication
- HTTPS for image & config. Downloads
- Installer has no access to device configuration
- Unplanned device workflow – Admin selects device

Consistent
- Support for end-to-end Enterprise platforms – **Switches, Routers, AP**
- **Consistent workflows** for all platforms
- **Backward compatible** w/ Smart-Install (Switches Only)
- Integrated w/ PI3.x workflows

Switches (Catalyst)  Routers (ISR/ASR)  Wireless AP
Network PnP with the Cisco APIC-EM Automates Device Provisioning

Pre-Provision Projects and Sites
- Policies
- Match rules
- Configurations, images
- IP addressing

Remote Installer
- Mount and cable devices
- Power on

The network admin remotely monitors the installation status while in progress
Booting devices call home to the PnP server, and request instructions

Unskilled Installer
- GUI-Based
- Consistent for Devices and Pin (Campus, Branch)
- Highly Secure
- End to End
- Greenfield and Brownfield
Network Plug and Play - Components

1. **PnP Agent**
   - Runs on Cisco® switches, routers, and wireless access points
   - Automates the deployment process

2. **PnP Protocol**
   - Runs between Agent and Server
   - Open schema

3. **PnP Helper App**
   - Delivers bootstrap status and troubleshooting checks

4. **PnP Server**
   - Central server - APIC-EM
   - Manages sites, devices, images, licenses
   - Provides northbound REST APIs
Cisco APIC EM: PnP Server Workflow-Based and REST API

- Pre-provisioning
- Ad-hoc and unclaimed devices

Customer’s Existing Automation Framework

Device Repository and Database

Python

Automation Framework (i.e. Python script, configuration generator)

PnP REST API

APIC-EM API

Enterprise Applications and Orchestration Layer

Network PnP Application UI

IWAN App

Topology Discovery

APIC-EM Controller

REST API

Cisco® Devices
Catalyst®, ISR, ASR, Access Points

CLI, PnP Protocol

Python

Cisco® Devices

CLI, PnP Protocol

APIs

Cisco APIC EM: PnP Server Workflow-Based and REST API

- Pre-provisioning
- Ad-hoc and unclaimed devices

Customer’s Existing Automation Framework

Device Repository and Database

Python

Automation Framework (i.e. Python script, configuration generator)

PnP REST API

APIC-EM API

Enterprise Applications and Orchestration Layer

Network PnP Application UI

IWAN App

Topology Discovery

APIC-EM Controller

REST API

Cisco® Devices
Catalyst®, ISR, ASR, Access Points

CLI, PnP Protocol

Python

Cisco® Devices

CLI, PnP Protocol

APIs
Cisco PnP Agent
Device Capabilities
## PnP Server Discovery Options

<table>
<thead>
<tr>
<th>Switches (Catalyst®)</th>
<th>Routers (ISR, ASR)</th>
<th>Wireless Access Points</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td><strong>DHCP</strong></td>
<td><strong>172.19.45.222</strong></td>
</tr>
<tr>
<td>DHCP with options 60 and 43</td>
<td>**PnP string: 5A1D;B2;K4;</td>
<td><strong>172.19.45.222;J80</strong></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td><strong>DNS</strong></td>
<td><strong>172.19.45.222</strong></td>
</tr>
<tr>
<td>DNS lookup</td>
<td><strong>pnpserver.localdomain</strong></td>
<td><strong>(PnP Server)</strong></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>Cloud re-direction - roadmap (Q3CY2016)</strong></td>
<td><strong><a href="https://devicehelper.cisco.com/device-helper">https://devicehelper.cisco.com/device-helper</a></strong> re-directs to 172.19.45.22</td>
</tr>
<tr>
<td>USB-based bootstrapping</td>
<td><strong>Manual - using the Cisco® Installer App</strong></td>
<td><strong>iPhone, iPad, Android, (roadmap - Windows mobile and PC)</strong></td>
</tr>
</tbody>
</table>
Agent Services

Services add intelligence to the workflow and encapsulate the platform complexities from the server.

Standard Services:
- Image installation
- Configuration upgrade
- License management
- TCL script execution
- Certification installation
- Configuration CLI
## Cisco Automated Device Deployment Solution Comparison

<table>
<thead>
<tr>
<th>Customer Reqs for Day 1 Provisioning</th>
<th>Auto Install (all ENG)</th>
<th>Smart Install (Cat 2k/3k,4k*)</th>
<th>CNS/CE (Routers, switches)</th>
<th>PnP Solution PI 2.0 (Routers, Switches)</th>
<th>Network PnP Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support unskilled installers (NO CLI)</td>
<td>✓</td>
<td>✓</td>
<td>Partial</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure deployment</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Support any Place-in-Network (Campus/Branch)</td>
<td>Partial</td>
<td>Partial</td>
<td>✓</td>
<td>Partial</td>
<td>✓</td>
</tr>
<tr>
<td>GUI based</td>
<td>X</td>
<td>X</td>
<td>Partial</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Consistent for all IOS devices</td>
<td>Partial</td>
<td>X</td>
<td>Partial</td>
<td>Partial</td>
<td>✓</td>
</tr>
<tr>
<td>RMA Use Case</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Complete automation for branch deployments</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
Pre-Provisioning Workflow
What Is Needed to Start a Campus Deployment

Step 1
Configure the Linux DHCP server with the PnP-specific option 43

```
sudo apt-get install isc-dhcp-server
sudo vi /etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;
option space CISCO_PNP;
option CISCO_PNP.pnpserver code 43 = string;

option subnet-mask 255.255.255.0;
option broadcast-address 10.30.30.255;

subnet 10.30.30.0 netmask 255.255.255.0 {
  range 10.30.30.2 10.30.30.255;
}
class "ciscopnp" {
  match if option vendor-class-identifier = "ciscopnp";
  option vendor-class-identifier "ciscopnp";
  vendor-option-space CISCO_PNP;
  option CISCO_PNP.pnpserver "5A;B2;K4;I172.19.210.215;J80";
}
service isc-dhcp-server start
```
What Is Needed to Start a Campus Deployment

Step 1a
- A localized, Cisco IOS® Software-based DHCP server with the PnP-specific option 43

```bash
ip dhcp excluded-address 10.1.1.1 !
ip dhcp pool pnp_device_pool
  network 10.1.1.0 255.255.255.0
default-router 10.1.1.1
option 43 ascii
"5A1D;B2;K4;I172.19.45.222;J80"
!```

- The sample configuration uses 10.1.1.0/24 as the DHCP pool
- The DHCP server IP is 10.1.1.1
- DHCP option 43 is set with 172.19.45.222 as the PnP Server IP address
What Is Needed to Start a Campus Deployment

**Step 1b**
Configure the Linux DHCP server for a domain name (DNS)

```bash
sudo vi /etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 10.30.30.255;
option domain-name-servers 10.30.30.1;
option domain-name "cisco.com";
```

Network admin configures the DHCP server to a server domain name.

Network Admin

```bash
subnet 10.30.30.0 netmask 255.255.255.0 {
 range 10.30.30.2 10.30.30.255;
}
service isc-dhcp-server start
```
APIC-EM PnP Login Screen
Workflow on the APIC-EM

Log in to the APIC EM and click on Cisco® Network Plug and Play

Click on “Projects” to add a new site

Step 2. The network admin creates a site for any new deployment on the APIC-EM PnP app
Workflow on APIC-EM

Step 2. The network admin creates a site for any new deployment on the Cisco® APIC-EM PnP app

Name the site and click “Create”
Workflow on APIC-EM

Step 2a. The network admin uploads the needed images

“Upload” allows to save the image in APIC-EM. Once uploaded, the image is available across sites.

“Images” tab allows to upload/manage images for the devices

All available images, previous uploads, and new uploads will be listed here.
Workflow on APIC-EM

"Upload" saves the configuration in APIC-EM. Once uploaded, the configuration is available across sites.

"Configurations" tab allows to upload/manage the configurations for the devices.

Step 2b. The network admin uploads the needed configurations

All available configurations, previous uploads, and new uploads will be listed here.
Workflow on the APIC-EM

Step 3. Add devices

If any external TFTP server is used for configurations and images, for a given site information must be entered here. This is not recommended.

Select the image from an available list already loaded into the APIC-EM.

Drag and drop the device configuration here as a txt file or select from uploaded configurations.
Device Deployment - DHCP-Based Server Discovery

- **DHCP Server**: The device receives PnP Server-specific metadata information configured in DHCP option 43.

- **Switch running PnP Agent**: The device validates the server’s location and establishes communication with the server.

- **Remote Installer**:
  - Mount and cable devices
  - Power on

- **PnP Server**: The network admin remotely monitors the status of installation while in progress.

- **Installer**
Device Deployment - DNS-Based Server Discovery

The device receives the DHCP configuration, including the domain name and DNS server.

The network admin remotely monitors the status of installation while in progress.

The device reads the domain name and creates a predefined PnP Server name, such as pnpserver.cisco.com, and resolves it with the DNS server.

Installer

Remote Installer
- Mount and cable devices
- Power on

DNS Server

PnP Server

Installer

Remote Installer
- Mount and cable devices
- Power on
Campus - Site Bring-Up

Day 0
Pre-Provision Projects and Sites
- Policies
- Rules
- Configs, image
- IP addressing

Day 1: The network admin remotely monitors the status of installation while in progress

Remote Installer
- Mount and cable devices
- Power on

Installer

Network Admin

PnP Server

DHCP, DNS, File Server

Campus - Building 1

Campus - Building 3
Step 4. Verify installation of devices

Click on “Details” to see full workflow details in APIC-EM

Once devices get config, image, and certificates, the APIC-EM will show the device as provisioned.
Unplanned Device Deployment
Campus - Site: Unplanned Device

In some cases when a ad-hoc device joins, is not part of any site-specific list, or has been missed for any reason, it will show up in the “Unplanned Devices” view. This is also true in scenarios where a rogue device tries to join the network. Administrators can either claim the device or reject it.

- Claim, ignore, or delete the device once selected
- "Unplanned Devices" tab allows admin to take action on unclaimed/unplanned devices
- Time and current status will be shown here. Unclaimed devices will always appear in “Error”

Device information - click to get all information about the device
Mobile Application-Based Bootstrapping
Network PnP: Installer App

- Redpark
  - RJ45 to Apple 8pin
  - RJ45 to Apple 30pin

- Get Console
  - Airconsole 2.0
  - Bluetooth Adapter

Option

* Tested with Network-PnP Solution
Installer App - Workflow

Remote Installer
- Mount and cable devices
- Power on

APIC-EM PnP-Server

Wi-Fi, 3G, 4G

iPad to console cable, Bluetooth

Deliver bootstrap

HTTP Proxy

PnP Server - Sites and Devices

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Product ID</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR1004-Bridge-Condii</td>
<td>ASR1004</td>
<td>00110</td>
</tr>
<tr>
<td>3650-Level1</td>
<td>WS-C3650-12S</td>
<td>0123</td>
</tr>
<tr>
<td>3650-Level 2</td>
<td>WS-C3650-48P</td>
<td>0321</td>
</tr>
<tr>
<td>3650-Level3</td>
<td>WS-C3650-48P</td>
<td>091231</td>
</tr>
</tbody>
</table>

- WAN link up
- VPN up (Internet)

Custom WAN Configuration

! interface GigabitEthernet0/0
description To Corp Network
ip address 171.71.223.88 255.255.254.0
no shutdown

! PnP Server Config
pnp profile pnp-wan
transport https ipv4 172.19.45.222 port 443
Installer App: Home Screen

- App used by remote installer
- Runs on an iPad or iPhone

App provides:
- Bootstrap configuration delivery
- PnP devices status
- Notes for the installer
- Device registration for a site
- Device installation troubleshooting
The installer app needs to communicate with the Cisco® APIC-EM, and needs to authenticate itself. The app provides a setting where this information can be added.

The APIC-EM URL and passwords can be added here. The app can be pre-provisioned by admins so that installers don’t need to add this information.

Similarly, device credentials can be added for the app to connect to the console, without sharing information with installers, if that security is required.
The installer can help install and provision new devices that are unplanned. A barcode can be scanned or a serial number can be added manually. If the registration is successful, the device will show in the APIC-EM and can be provisioned accordingly. A device at a time can be registered through the app.
Installer App: Site Status

Installer per-device status for the site

Click on “Site Provisioning” to see the device status

“Deployed Devices” shows devices that completed the installation process

“Not Deployed” shows devices that have not started installation or are in progress for installation
The installer gets details on a device as it is installed. You can view:

- Device details
- A log of install events and messages

If the device has any issues during this process, there are a few troubleshooting methods available on the app itself.
The installer can perform more troubleshooting steps after checking physical connections and power.

- Check and view if the PnP Server on the APIC-EM is reachable and can be authenticated using the credentials provided in settings.
- Check and view if the PnP Agent on the device is executing correctly.
- Verbose logs are available for debugging by the admin to check failure symptoms.

Verbose logs are available for debugging by the admin to check failure symptoms.
Logs can be emailed by the installer to the admin for instant troubleshooting. The per-device per-provisioning instance is saved.
Installer App-Based Automated Installation with PnP Server
Zero-Touch Configuration for the Installer

0) Pre-provision site

1) Installer connects the ISR console cable with the app

2) Installer clicks the “Deploy Device” option and the Installer App connects to the PnP Server over 3G, 4G, or Wi-Fi

3) The PnP Server validates the credentials of the installer

4) The PnP Server registers the serial number of that device and sends the ISR bootstrap configuration

5) The app receives the bootstrap configuration (WAN config + Agent config) from the PnP Server

6) The app installs the server certificate (through the console) and applies the bootstrap configuration to the ISR

7) The ISR connects to the server using https and requests its image and full configuration

The network admin preconfigures the bootstrap prior to the installer onsite. The bootstrap configuration is available for all ISRs supporting the agent. The installer app is supported on iPhones and iPads.
Smart Install Proxy
PnP Support with SMI Proxy

- Smart Install Proxy (SMI Proxy) runs on the device with the PnP Agent
- SMI Proxy translates the SMI to PnP
  - Represents SMI client to the PnP Server
- SMI Proxy must be explicitly enabled
- The PnP Server can manage legacy Cisco IOS® Software images on Cisco Catalyst® switches
- Catalyst 3000 and 4000 Series Switches with a minimum IP base support SMI Proxy
SMI Proxy: Caveats

- Non-PnP Agent images do not get all the benefits of PnP Agent support
- Caveats to a solution with older Cisco IOS® Software clients:
  - Cisco® APIC-EM discovery
  - SMI Proxy device must be explicitly enabled
    - Must be an SMI director-capable switch or release
  - Not managed by the APIC-EM as a special device
  - Scale and performance limits
PnP Support for SMI Proxy

Integrated Branch Director (IBD) Configuration Snippet

vstack vlan 1
vstack config tftp://10.30.30.10/cfg_new.txt
vstack group custom test product-id
cfg tftp://10.30.30.10/cfg_new.txt
match WS-C3560C-12PC-S
vstack dhcp-localserver smi
address-pool 10.30.30.116 255.255.255.0
file-server 10.30.30.10
default-router 10.30.30.193
vstack director 10.30.30.193
vstack basic
vstack startup-vlan 1
no vstack backup

Sample configuration for IBD and SMI proxy to enable PnP

Sample XML payload sent from the device to the APIC-EM, enabled through SMI Proxy

```xml
<pnp xmlns="urn:cisco:pnp" version="1.0" udi="PID:7206VXR,VID:,SN:34835437">
  <info xmlns="urn:cisco:pnp:work-info" correlator="CiscoPnP-1.0-15-1B64AE4">
    <deviceid>
      <udi>PID:7206VXR,VID:,SN:34835437</udi>
    </deviceid>
    <hostname>Switch.viaProxy.PID:7206VXR,VID:,SN:34835437</hostname>
    <authRequired>false</authRequired>
    <viaProxy>true</viaProxy>
  </info>
</pnp>
```
Bulk Import and Export
Bulk Import is used when there are more than 10 devices to add across sites. A CSV file can be pre-populated with device information and uploaded to the APIC-EM to enable the import process to add devices in one instance, instead of adding devices one by one.

A sample is provided, which can be downloaded to create a template for bulk imports. Any import can later be exported. Bulk Import works across sites, so caution should be used to specify the correct site name.

All the files being used for bulk imports are listed here. Corresponding to each file, import information is populated. Sites and devices that are added skipped, or failed are displayed.

“Bulk Import” tab is used to reach the import screen.
Bulk Import

New slide
Sample Bulk Import File

All information about devices to be added can be filled in here. If the TFTP server needs to be used for a configuration or image download, the path needs to be specified here as well. Otherwise, the system assumes the configuration and image are available in the APIC-EM system. The file is then added using the import button in the APIC-EM Bulk Import screen.
PnP Security Workflow
PnP Deployment for Campus - Self-Signed Certificate Method

1. DHCP Request
   - DHCP response with options 43 and 60 for server location

2. DHCP Request
   - PnP Agent initiates HTTP communication with the server and sends the device UDI

3. HTTP PnP work request with device serial number (UDI)
   - PnP Agent installs the local trust point for the server SSL certificate

4. HTTPS PnP work request with device serial number (UDI)
   - PnP Server receives device UDI and sends the full configuration and Cisco IOS® Software image over the HTTPS channel

5. HTTPS PnP work request with device serial number (UDI)

6. HTTPS PnP work request with device serial number (UDI)
   - PnP Server receives device UDI and sends the full configuration and Cisco IOS® Software image over the HTTPS channel
Secured PnP Deployment for Campus - Trust Pool Method

1. DHCP response with options 43 and 60 for server location and location of the InfoSec certificate bundle.
2. PnP Agent downloads the InfoSec certificate bundle from the file server, as provided in DHCP option 43.
3. HTTP file transfer request to download certificate bundle.
5. HTTPS PnP work request with device serial number (UDI).
6. Server validates the device by verifying the SUDI certificate against the Cisco® CA.

PnP Server receives device UDI and sends the full configuration and Cisco IOS® Software image over the HTTPS channel.
Secured PnP Deployment for a Branch with the Mobile App

1. DHCP assigned IP address
2. DHCP server at ISP sends response
3. HTTPS PnP work request with device serial number (UDI)
4. PnP Server receives the device UDI and sends the full configuration and Cisco IOS® Software image over the HTTPS channel

The installer configures the server address and SSL certificate on device using the mobile app.

Remote Site Running PnP Agent

Device sends DHCP request

PnP Agent initiates HTTPS communication with the server and sends the device UDI

DMZ

APIC PnP Server

Internet

DC
PnP Security - Secure Connection Enablement

Phase 1

- Server certificate not authenticated
- PnP Agent on device accepts certificate from the server
  - The server certificate is NOT authenticated
- Installer App downloads the PnP Server certificate to the PnP Agent
  - App contains server certificate prior to delivering to the Agent
  - The server certificate is NOT authenticated

Phase 2

- HTTPS is always used
- Server certificate is authenticated
- PnP Agent has a built-in list of CA servers from the PKI trust pool
- PnP Agent authenticates the server certificate in the trust pool
- PnP Server follows the process to import the CA certificate
- It is a similar process to wireless LAN controllers
Key Takeaways
Summary

- Cisco® Network PnP is a simple, highly secure, and scalable automated network device deployment solution
- The agent is supported on end-to-end Cisco IOS® Software products
- The Cisco APIC-EM is the central server for the solution
- Programmability: The APIC-EM allows scripting (REST API) to automate server workflows
- Python server reference implementation in DevNet: Give link here
- Open-source protocol available: Customers and partners can adapt the PnP server into their own processes or build their own server based on open protocols (The schema is proprietary, even if using XMPP)

Solution Summary

- No pre-staging of devices
- Unskilled installer at remote sites
- GUI-based workflows
- Highly secure and scalable

Benefits
# NG Plug-N-Play – Supported Platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>PnP Agent Support on Products</th>
<th>Recommended Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Switches</strong></td>
<td><strong>Cisco Catalyst 4500E Switches (Sup8-E, 7-E/7L-E, 6-E/6L-E)</strong>&lt;br&gt;<strong>Cisco Catalyst 3850, 3650 Series Switches</strong>&lt;br&gt;<strong>Cisco Catalyst 4500-X, 4900 Series Switches</strong>&lt;br&gt;<strong>Cisco Catalyst 3750-X, 3560-X Series Switches</strong>&lt;br&gt;<strong>Cisco Catalyst 2960-C, 3560-C Series Compact Switches</strong>&lt;br&gt;<strong>Cisco Catalyst 2960-S/SF, 2960-X/XR Series Switches</strong></td>
<td><strong>IOS-XE 3.6.3E</strong>&lt;br&gt;<strong>IOS 15.2.2E3</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Catalyst 3850XU/XS Series Switches</strong>&lt;br&gt;<strong>Cisco Catalyst 2960-CX, 3560-CX Series Compact Switches</strong></td>
<td><strong>IOS-XE 3.7.2E</strong>&lt;br&gt;<strong>IOS 15.2.3E2</strong></td>
</tr>
<tr>
<td><strong>Core Switches</strong></td>
<td><strong>Cisco Catalyst 6500 Series Switches: Sup2T/Sup720</strong>&lt;br&gt;<strong>Cisco Catalyst 6880-X, 6807-XL Series Switches</strong></td>
<td><strong>IOS 15.2(2)SY1 (Mar2016)</strong></td>
</tr>
<tr>
<td><strong>Access Routers</strong></td>
<td><strong>Cisco 4300/4400 Integrated Services Router</strong>&lt;br&gt;<strong>Cisco ASR 1000 Series Aggregation Services Routers, Cisco CSR 1000v</strong>&lt;br&gt;<strong>Cisco Cloud Services Router 1000V Series</strong>&lt;br&gt;<strong>Cisco 800, 1900, 2900, 3900 Series Integrated Services Routers (ISR G2)</strong></td>
<td><strong>IOS-XE 3.16.S (ED)</strong>&lt;br&gt;<strong>IOS 15.5.3M (ED)</strong></td>
</tr>
<tr>
<td><strong>Industrial Ethernet Switches</strong></td>
<td><strong>Cisco Industrial Ethernet 2000, 3000 Series Switches</strong></td>
<td><strong>IOS 15.2.2E3</strong></td>
</tr>
<tr>
<td><strong>Indoor Access Points</strong></td>
<td><strong>Gen2 802.11n AP 1600, 2600, 3600, 702-W/I 802.11ac Wave1 - 1700, 2700, 3700, Wave 2 802.11ac &amp; Outdoor AP support (Roadmap)</strong>&lt;br&gt;<strong>WLC Supported: AireOS and IOS-XE</strong></td>
<td><strong>Nov2015</strong></td>
</tr>
</tbody>
</table>