



# 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



**Network Admin**

## Pre-Provision Projects and Sites

- Policies
- Match rules
- Configurations, images
- IP addressing



**Installer**

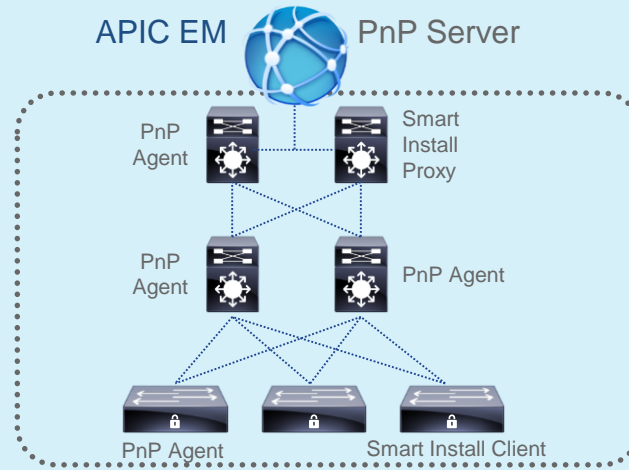
## Remote Installer

- 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

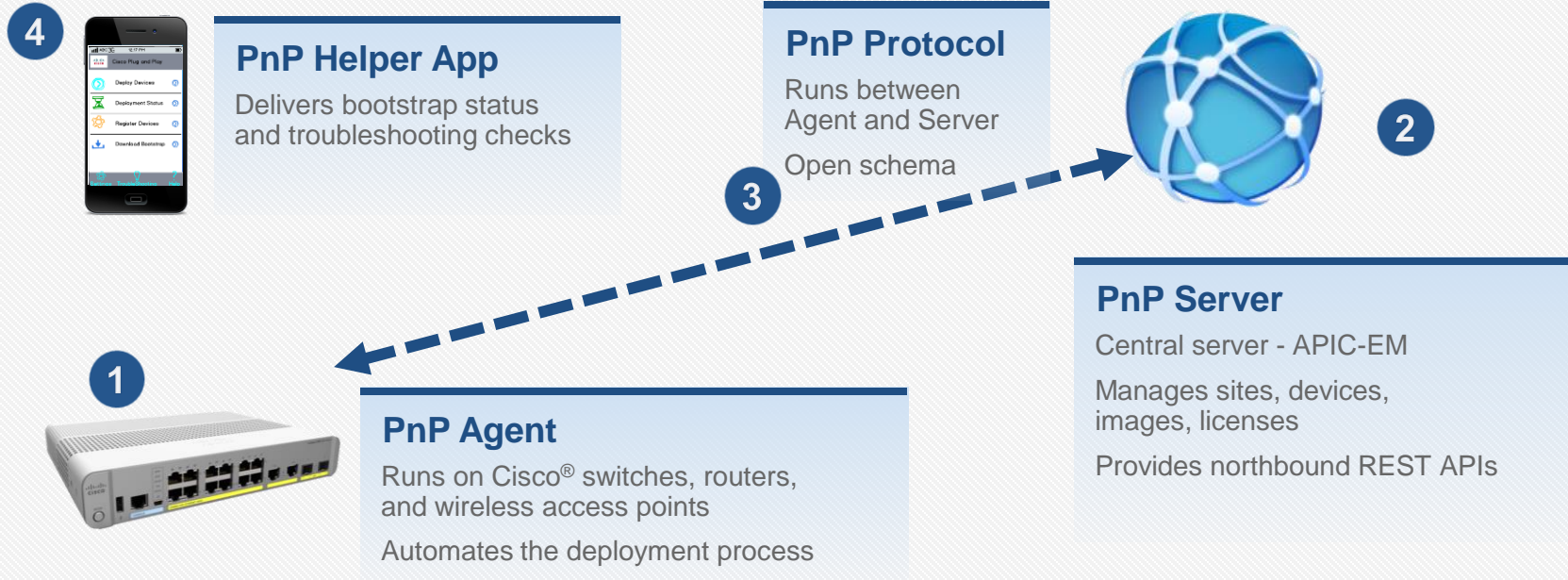
Consistent for Devices and Pin (Campus, Branch)

Highly Secure

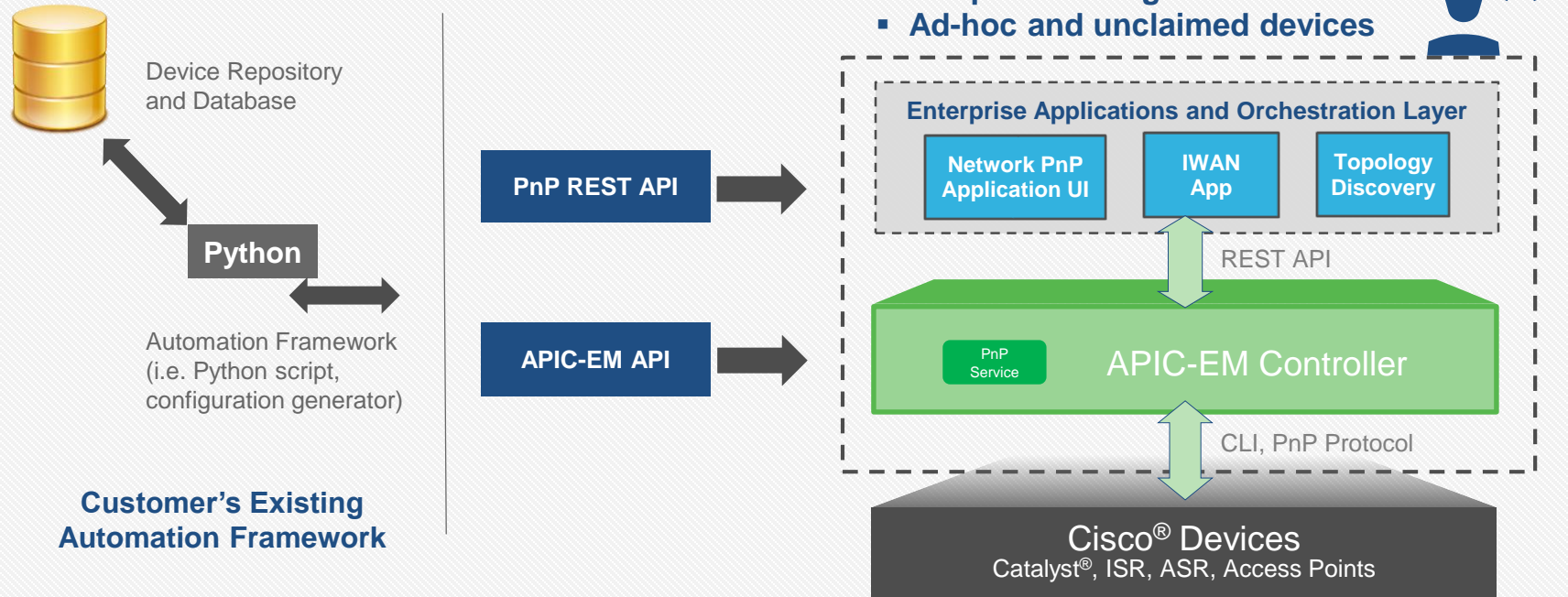
End to End

Greenfield and Brownfield

# Network Plug and Play - Components



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



# Cisco PnP Agent Device Capabilities

---

# PnP Server Discovery Options



Switches (Catalyst®)



Routers (ISR, ASR)



Wireless Access Points

1

DHCP  
Server

**DHCP with options 60 and 43**

PnP string: 5A1D;B2;K4;|[172.19.45.222](http://172.19.45.222);J80

2

DNS  
Server

**DNS lookup**

pnpserver.localdomain ---- 172.19.45.222 (PnP Server)

3



**Cloud re-direction - roadmap (Q3CY2016)**

<https://devicehelper.cisco.com/device-helper> re-directs to 172.19.45.22 (PnP Server)

4



**USB-based bootstrapping**

5



**Manual - using the Cisco® Installer App**

iPhone, iPad, Android, (roadmap - Windows mobile and PC)

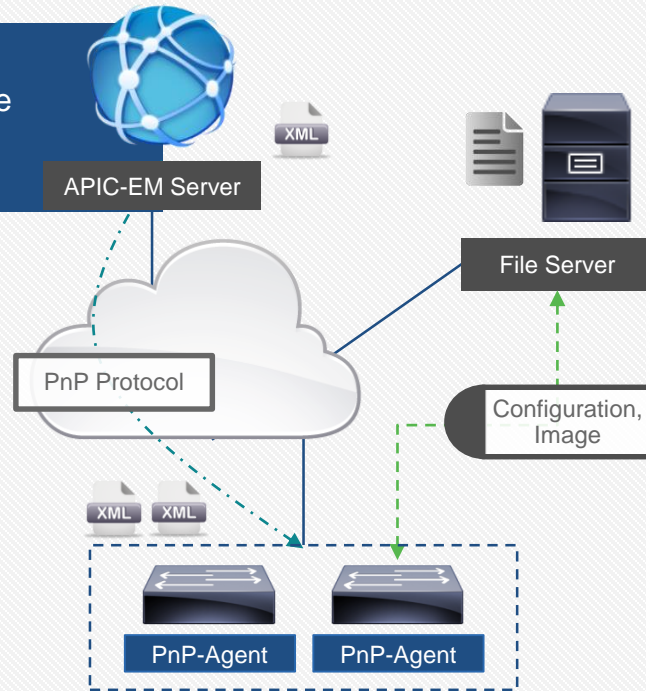






# Agent Services

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

Customer Reqts for Day 1 Provisioning	Auto Install (all ENG)	Smart Install (Cat 2k/3k,4k*)	CNS/CE (Routers, switches)	PnP Solution PI 2.0 (Routers, Switches)	Network PnP Solution
Support unskilled installers (NO CLI)	✓	✓	Partial	✓	✓
Secure deployment	✗	✗	Partial	✗	✓
Support any Place-in-Network (Campus/Branch)	Partial	Partial	✓	Partial	✓
GUI based	✗	✗	Partial	✓	✓
Consistent for all IOS devices	Partial	✗	Partial	Partial	✓
RMA Use Case	✗	✓	✗	✗	✓
Complete automation for branch deployments	✗	✗	✗	✗	✓

# 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;
```

DHCP Server



Network Admin

Pre-provision the DHCP server with:

- IP address
- Option 43

```
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

```
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"
!
```

Cisco® IOS  
DHCP Server



Network Admin

Pre-provision  
DHCP Server

- IP address
- Option 43

- 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)

```
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";
```

DNS Server

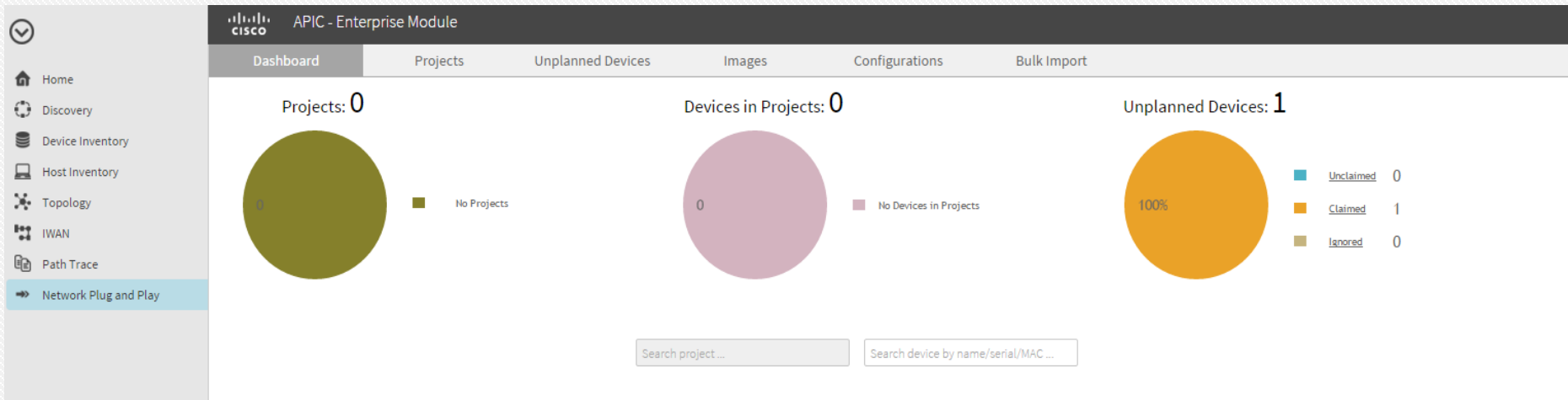


Network Admin

Network admin  
configures the  
DHCP server to a  
server domain name

```
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

APIC - Enterprise Module

Dashboard Projects Unplanned Devices Images Configurations Bulk Import

Projects: 0

Devices in Projects: 0

Unplanned Devices: 1

100%

Unclaimed 0

Claimed 1

Ignored 0

No Projects

No Devices in Projects

Search project ...

Search device by name/serial/MAC ...





# Workflow on APIC-EM

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

The screenshot shows the APIC-EM PnP app interface. The top navigation bar includes the Cisco logo, the text 'APIC - Enterprise Module', and user information 'API 2 admin' with a notification bell icon. Below the navigation bar, the 'Projects' tab is selected. The main content area displays a 'Project:' label followed by a text input field containing 'SRDL-SPOKE'. To the right of the input field are three buttons: 'Create', 'Clone', and 'Delete'. A blue callout bubble points to the 'Create' button with the text 'Name the site and click "Create"'. The 'Unplanned Devices' tab is also visible in the navigation bar.



# Workflow on APIC-EM

Step 2a. The network admin uploads the needed images

“Upload” allows to 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

API 2 admin

Unplanned Devices **Images** Configurations Bulk Import

Upload Delete Refresh

Filter

<input type="checkbox"/>	Image Name	Size (MB)	Platform	Product ID
<input type="checkbox"/>	isr4300-universalk9.BLD_V155_3_S_XE316_THROTTLE_LATEST_20150929_120036-ext.SSA.bin	447.34		

10

All available images, previous uploads, and new uploads will be listed here.

First Previous 1 Next Last



# Workflow on APIC-EM

Step 2b. The network admin uploads the needed configurations

“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.

API 2 admin

Unplanned Devices Images **Configurations** Bulk Import

**Upload** Delete Refresh

Filter

<input type="checkbox"/>	Name	Size (Bytes)
<input type="checkbox"/>	<u>config</u>	446
<input type="checkbox"/>	FLM1923W0LQSRDL-SPOKE.txt	14540

10 Displaying 1 to 2 of 2 configs First Previous 1 Next Last



# 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.

Deploy configuration/image files from external TFTP sever

Notes

ISR-4THFLOOR

WS-C4510R-E

21390989

Add Device

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

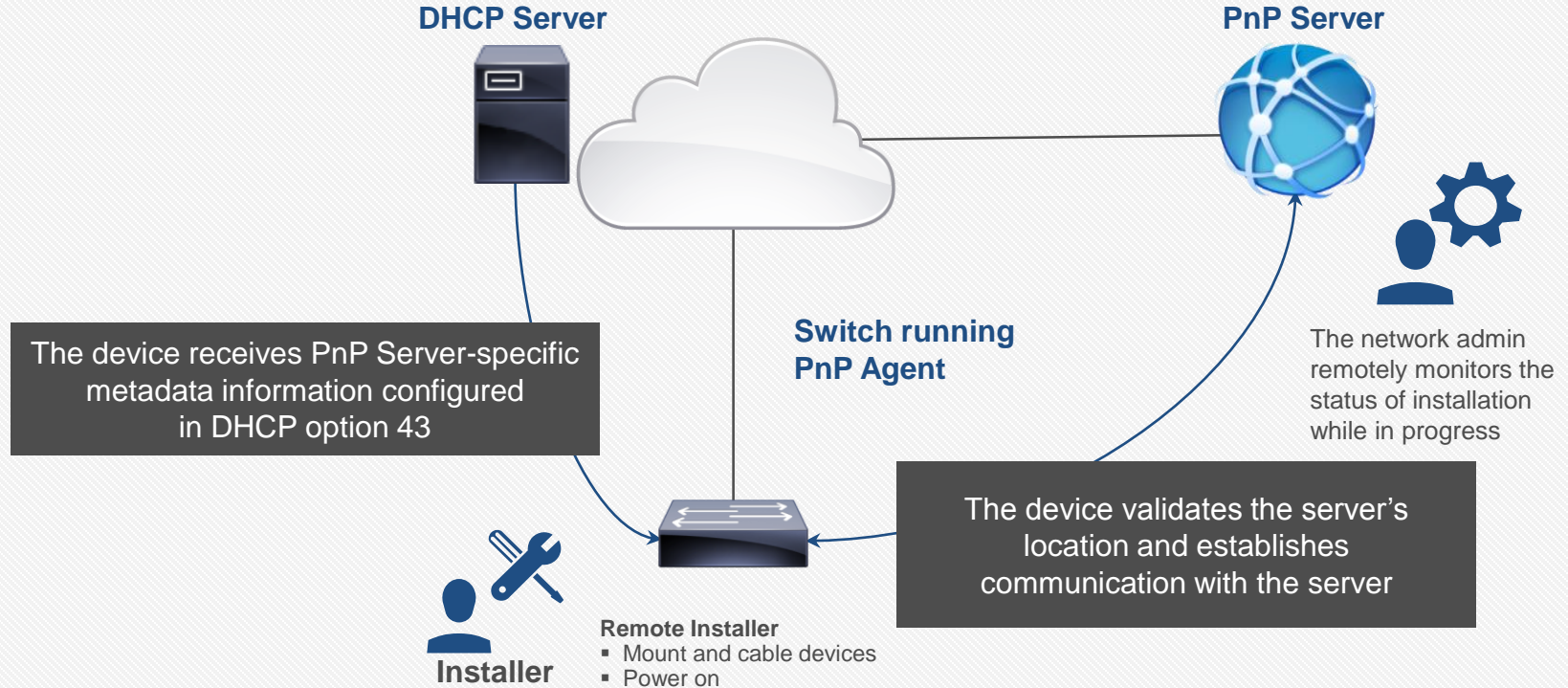
Name of device	Device type	Serial Number of device								
SRDL-SPOKE		FLM1923W0LQ			isr4300-universalk9.BLD_V155_3_S_XE...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2015-10-27 01:05:18	<a href="#">Deploying Image</a>	

Displaying 1 to 1 of 1 device

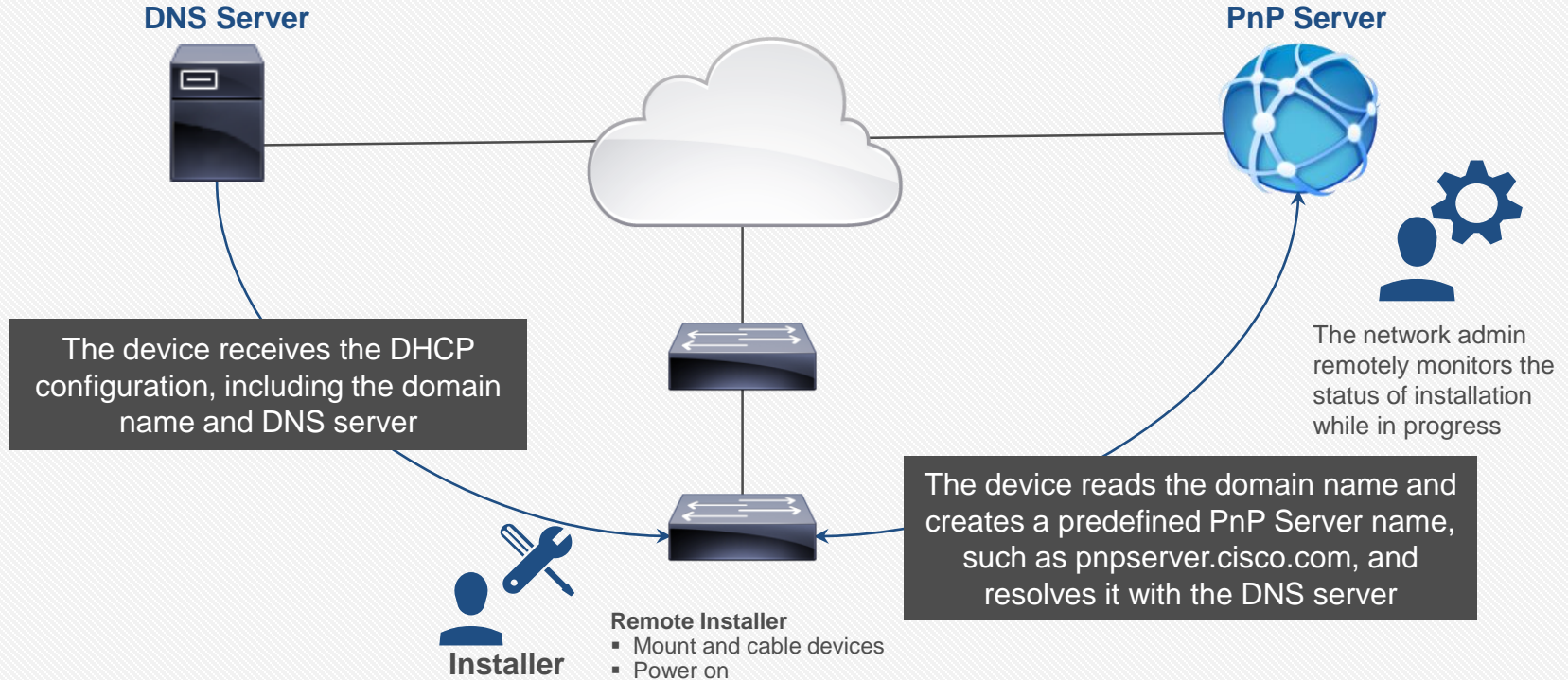
First Previous 1 Next Last

Drag and drop the device configuration here as a txt file or select from uploaded configurations

# Device Deployment - DHCP-Based Server Discovery



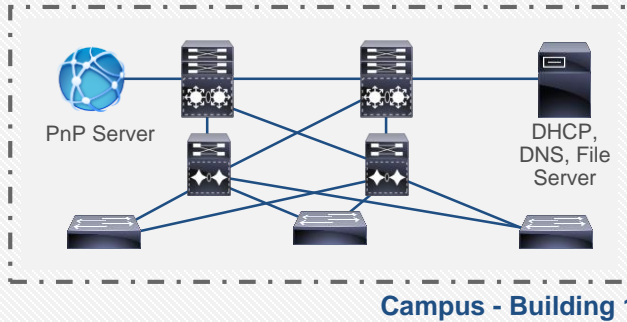
# Device Deployment - DNS-Based Server Discovery



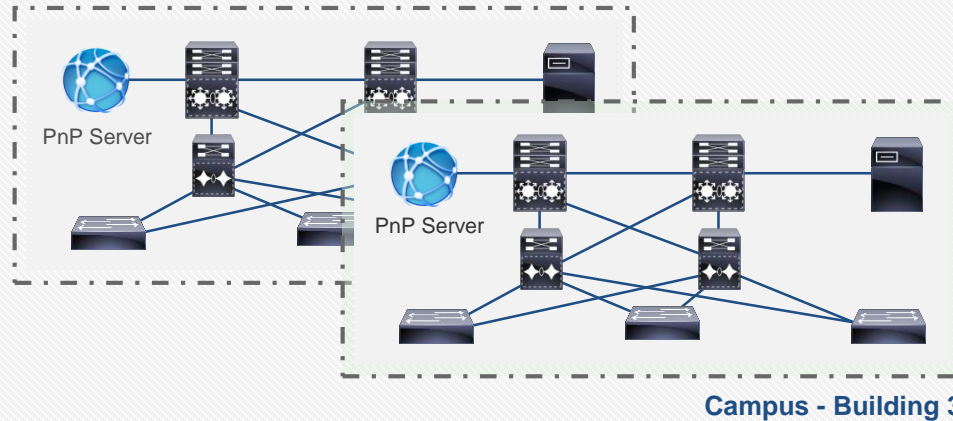
# Campus - Site Bring-Up



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



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





# Campus - Site Bring-Up

Step 4. Verify installation of devices

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

The screenshot shows the APIC-EM interface with a modal window open for device FLM1923W0LQ. The modal displays the following information:

Device Info	
Device Name	SRDL-SPOKE
Product ID	ISR4331/K9
Serial Number	FLM1923W0LQ
Site	SRDL-SPOKE
Last Contact Time	2015-10-27 01:17:23.000817

SUDI Authentication Status	
Status	Authenticated
Timestamp	2015-10-27 01:15:22

SUDI Certificate Information	
Issuer DN	CN=ACT2 SUDI CA, O=Cisco
Subject DN	CN=ISR4331/K9, OU=ACT-2 Lite SUDI, O=Cisco, SERIALNUMBER=FLM1923W0LQ, CN=FLM1923W0LQ

The background interface shows a table of devices with columns for Device Certificate, SUDI Required, Last Contact Time, and Status. The device FLM1923W0LQ is listed with a status of 'Provisioned'.

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.

The screenshot shows the Cisco Unplanned Devices interface. At the top, there are navigation tabs: Projects, Unplanned Devices (selected), Images, Configurations, and Bulk Import. On the right, there are user controls for API, a notification bell with a '2' badge, and the user name 'admin'. Below the navigation, there are three buttons: Claim, Ignore, and Delete. A 'Filter' section is visible. The main table lists unclaimed devices with columns for Serial Number, Product ID, Device IP, Config, Image, Device Certificate, Last Contact Time, and Status. One device is listed with Serial Number FTX150408VV, Product ID 891, and Status Error. The last contact time is 2015-10-27 01:58:27. At the bottom, it says 'Displaying 1 of 1 Unclaimed Device'.

Claim, ignore, or delete the device once selected

“Unplanned Devices” tab allows admin to take action on unclaimed/unplanned devices

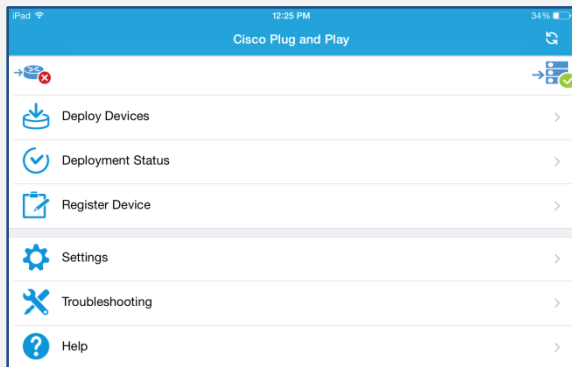
Time and current status will be shown here. Unclaimed devices will always appear in “Error”

Device information - click to get all information about the device

# Mobile Application-Based Bootstrapping



# Network PnP: Installer App



Apple

Android

## Redpark



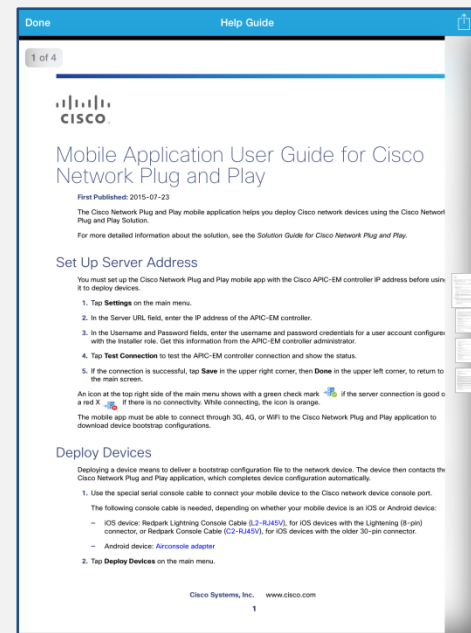
RJ45 to  
Apple 8pin

RJ45 to  
Apple 30pin

## Get Console



Airconsole 2.0  
Bluetooth Adapter



\* Tested with Network-PnP Solution

# Installer App - Workflow



## PnP Server - Sites and Devices

Filter	Device Name	Product ID	Serial Number	Config	Bootstrap
<input type="checkbox"/>	ASR1004-Bridge-Condui	ASR1004	00110		
<input type="checkbox"/>	3850-Level1	WS-C3850-12S	0123		
<input type="checkbox"/>	3850-Level 2	WS-C3850-48P	0321		
<input type="checkbox"/>	3850-Level3	WS-C3850-48P	091231		

10 | Displaying 1 to 4 of 4 devices

- WAN link up
- VPN up (Internet)

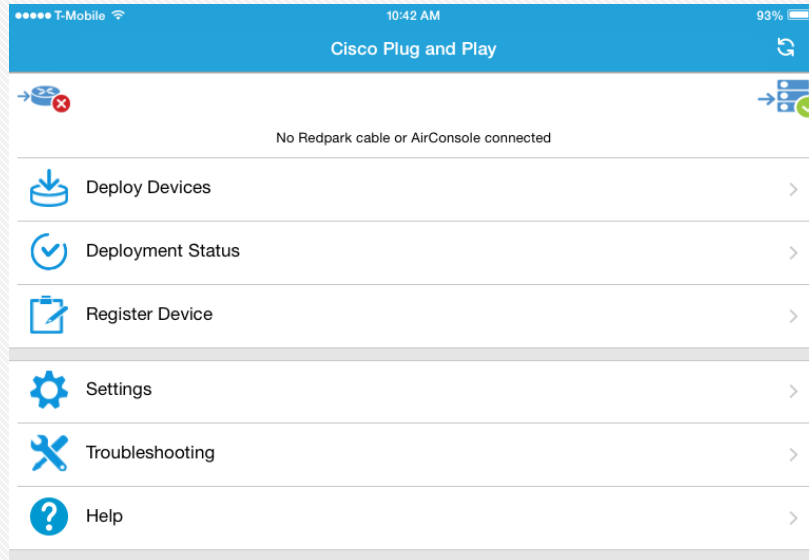
```
!
interface GigabitEthernet0/0
description To Corp Network
ip address 171.71.223.88 255.255.254.0
no shutdown
!
! PnP Server Config
pnp profile pnp-wan
transport https ipv4 172.19.45.222 port 443
```

**Custom WAN Configuration**

# 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



# Installer App: Connecting to the APIC-EM and the Device

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.

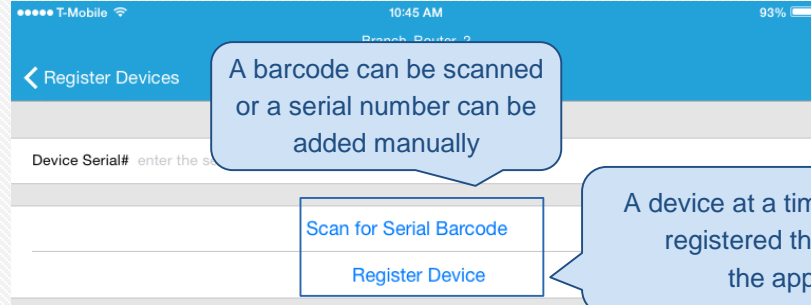
Similarly, device credentials can be added for the app to connect to the console, without sharing information with installers, if that security is required.

The screenshot shows the 'Settings' screen of the installer app. The top bar is blue with 'Done' on the left, 'Settings' in the center, and 'Saved' on the right. Below the bar, there are two main sections. The first section is for APIC-EM configuration, with fields for 'Server URL: 172.19.162.23', 'Username: installer', and 'Password: ●●●●●●'. Below this is a 'Test Connection' button. The second section is titled 'CISCO DEVICE DEFAULTS' and contains fields for 'Username: cisco', 'Password: cisco', and 'Enable: ●●●●'. At the bottom of the screen, the version '0.9 (1.36)' is displayed.

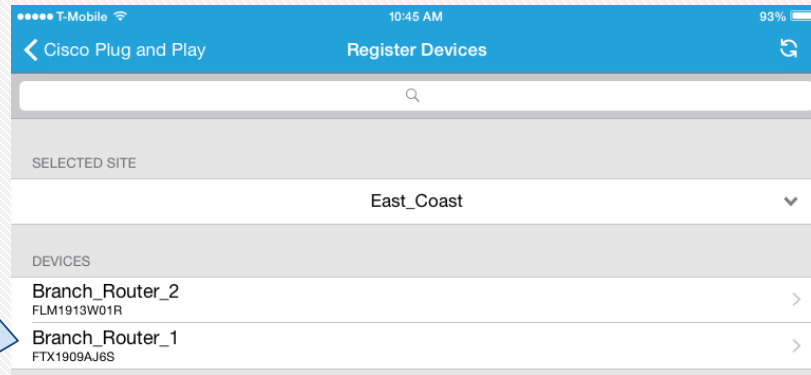
# Installer App: Registering a Device



The installer can help install and provision new devices that are unplanned



If the registration is successful, the device will show in the APIC-EM and can be provisioned accordingly



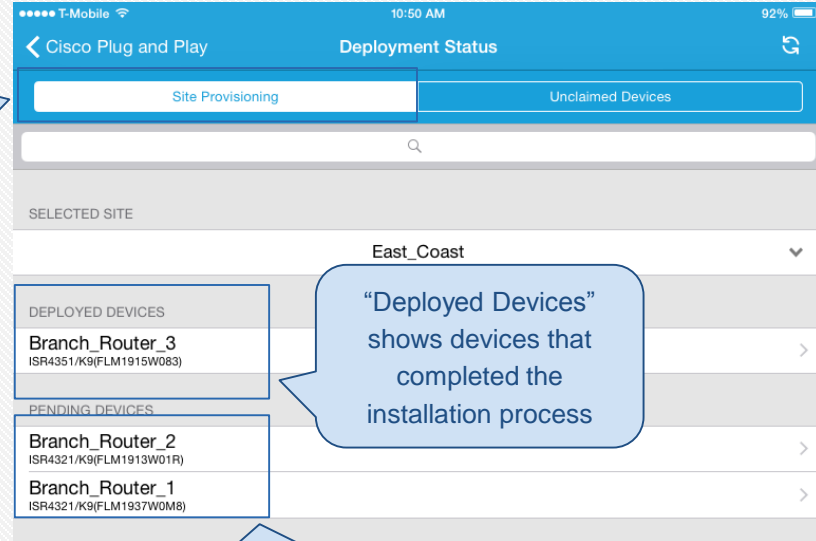


# Installer App: Site Status



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

# Installer App: Install Status



The installer get 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.

See information on the device being provisioned

Done	Device Details
	Device Name Branch_Router_1
	Serial Number FLM1937W0M8
	Platform Number ISR4321/K9
	Site East_Coast
	Bootstrap Config bootstrap.4321.server22.txt
	State Pending

See whether the provisioning has been successfully completed

Branch\_Router\_1

Cancel Deploying

Logging

```
Router(config-if)#negotiation auto
Router(config-if)#
Router(config-if)#interface GigabitEthernet0/0/1
Router(config-if)#no ip address
Router(config-if)#shutdown
Router(config-if)#negotiation auto
Router(config-if)#
Router(config-if)#interface GigabitEthernet0
Router(config-if)#vrf forwarding Mgmt-intf
Router(config-if)#no
Router(config-if)#sh
Router(config-if)#ne
Router(config-if)#
Router(config-if)#ip
Router(config)#no ip
Router(config)#no ip
Router(config)#ip ro
Router(config)#
Router(config)#pnp
Router(config-pnp-init)#transport https ipv4 172.19.162.22 port 443
Router(config-pnp-init)#end
Router#
Router#
Router#
```

**Deployment Completed**

The deployment of the certificate and bootstrap was successful. Return home now?

No Yes

# Installer App: Troubleshooting



The installer can perform more troubleshooting steps after checking physical connections and power

The screenshot shows the 'Troubleshooting' screen in the Installer App. The status bar at the top indicates 'T-Mobile' and '10:41'. The screen is divided into sections for 'AGENT STATUS' and 'PING SERVER STATUS'. Under 'AGENT STATUS', there are buttons for 'View Current Status' and 'Check Agent Status'. Under 'PING SERVER STATUS', there is a 'Check Ping Server Status' button. Below these, there are options for 'Advanced', 'View Logs', and 'Email Logs'. At the bottom, it says 'Waiting for device...'. Three callout boxes provide additional information: one for 'View Current Status' and 'Check Agent Status', one for 'Check Ping Server Status', and one for 'View Logs'.

Check and view if the PnP Agent on the device is executing correctly

Check and view if the PnP Server on the APIC-EM is reachable and can be authenticated using the credentials provided in settings

Verbose logs are available for debugging by the admin to check failure symptoms

# Installer App: Logs



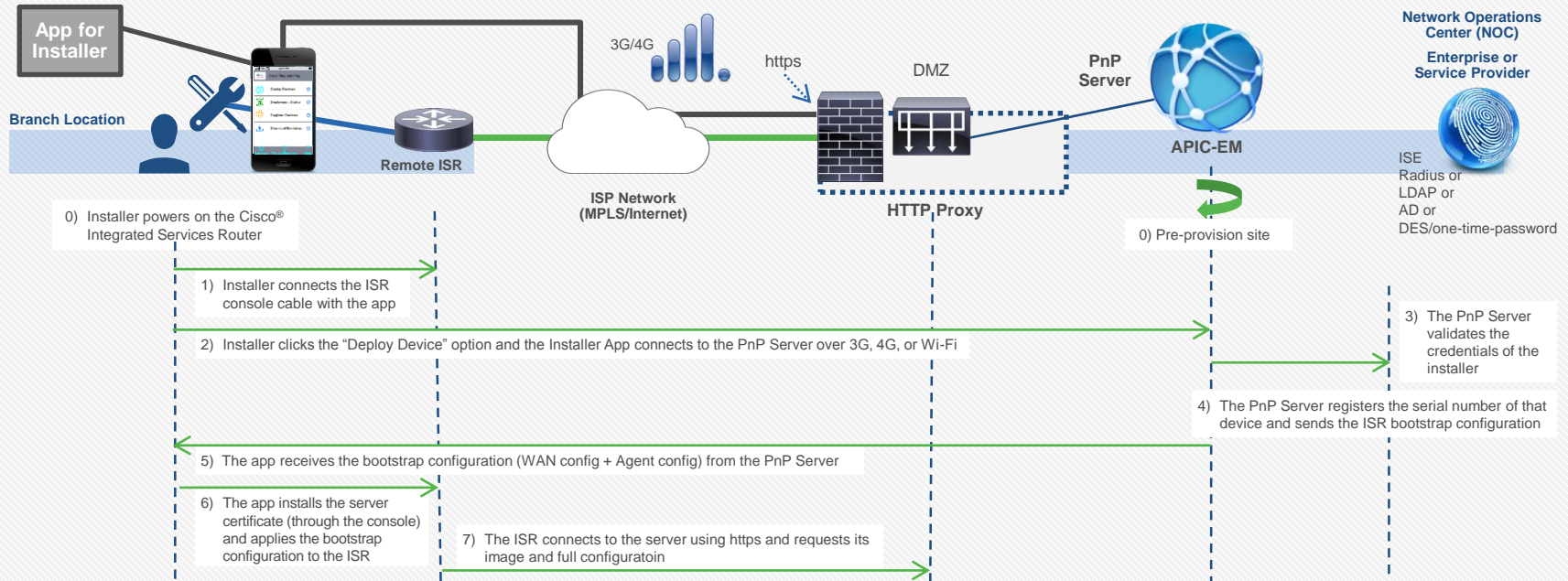
Logs can be emailed by the installer to the admin for instant troubleshooting. The per-device per-provisioning instance is saved.

SESSION	
08-20-2015 - 1.log created on: 8/20/15	>
08-20-2015.log created on: 8/20/15	>
09-22-2015 - 1.log created on: 9/22/15	>
09-22-2015.log created on: 9/22/15	>
09-24-2015 - 1.log created on: 9/24/15	>
09-24-2015 - 2.log created on: 9/24/15	>
09-24-2015 - 3.log created on: 9/24/15	>
09-24-2015.log created on: 9/24/15	>

```
09-22-2015 15:23:15] Session received challenge
[09-22-2015 15:23:15] User handled certificate
[09-22-2015 15:23:15] Preparing to fetch all Locations
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Session task completed: <NSHTTPURLResponse: 0x155cad50> [ URL: https://172.27.34.39/
api/v1/ticket ] [ status code: 200, headers {
  Connection = close;
  "Content-Type" = "application/json";
  Server = "Jetty(9.0.z-SNAPSHOT)";
} ] error: (null)
[09-22-2015 15:23:15] Request for all locations is: https://172.27.34.39/api/v1/ztd-site?offset=1&limit=500
[09-22-2015 15:23:15] Session task downloaded with response: <NSHTTPURLResponse: 0x155ab9e0> [ URL:
https://172.27.34.39/api/v1/ztd-site?offset=1&limit=500 ] [ status code: 200, headers {
  Connection = close;
  "Content-Type" = "application/json";
  Expires = "Thu, 01 Jan 1970 00:00:00 GMT";
  Server = "Jetty(9.0.z-SNAPSHOT)";
  "Set-Cookie" = "JSESSIONID=q0q4g5lwf1xeao0kg4fqwtsh;Path=";
} ]
[09-22-2015 15:23:15] Received all Locations from server
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Request for device history is: https://172.27.34.39/api/v1/ztd-device/history?pid=891W&serial-
num=FTX150408VV
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Request for all devices at location is: https://172.27.34.39/api/v1/ztd-site/device?
site_id=d33039b1-4e1c-4301-975e-f8124813910&offset=1&limit=1
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Request for all devices at location is: https://172.27.34.39/api/v1/ztd-site/device?
site_id=4a6c69fb-77d9-4850-a333-3f41d4b7462&offset=1&limit=4
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Request for all devices at location is: https://172.27.34.39/api/v1/ztd-site/device?
site_id=1f41a6b2-b1be-4e16-953c-dc47d11ba8d0&offset=1&limit=1
[09-22-2015 15:23:15] Request for all devices at location is: https://172.27.34.39/api/v1/ztd-site/device?
site_id=fe09bef1-cc68-4054-94ae-fedfb98ac712&offset=1&limit=3
[09-22-2015 15:23:15] Caching new resource: 2
[09-22-2015 15:23:15] Session task downloaded with response: <NSHTTPURLResponse: 0x15685670> [ URL:
https://172.27.34.39/api/v1/ztd-device/history?pid=891W&serial-num=FTX150408VV ] [ status code: 200, headers {
  Connection = close;
  "Content-Type" = "application/json";
  Server = "Jetty(9.0.z-SNAPSHOT)";
} ]
[09-22-2015 15:23:15] Caching new resource: 5
[09-22-2015 15:23:15] Session task downloaded with response: <NSHTTPURLResponse: 0x1557f250> [ URL:
https://172.27.34.39/api/v1/ztd-site/device?site_id=d33039b1-4e1c-4301-975e-f8124813910&offset=1&limit=1 ]
[ status code: 200, headers {
  Connection = close;
  "Content-Type" = "application/json";
  Server = "Jetty(9.0.z-SNAPSHOT)";
} ]
[09-22-2015 15:23:15] checking connection...
[09-22-2015 15:23:15] Request for device history is: https://172.27.34.39/api/v1/ztd-device/history?
pid=ISR4400&serial-num=FXA34523
[09-22-2015 15:23:15] Caching new resource: 4
```

# Installer App-Based Automated Installation with PnP Server

## Zero-Touch Configuration for the Installer



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.

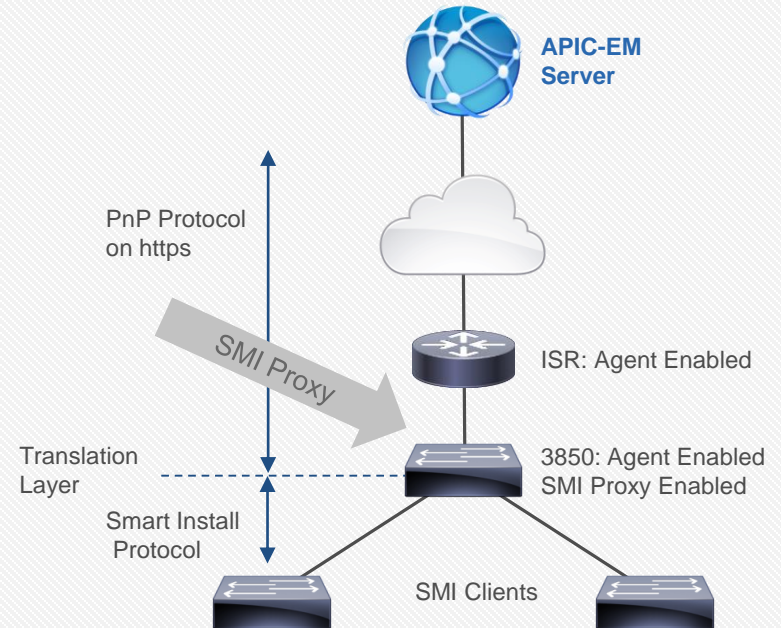
# Smart Install Proxy



# PnP Support with SMI Proxy



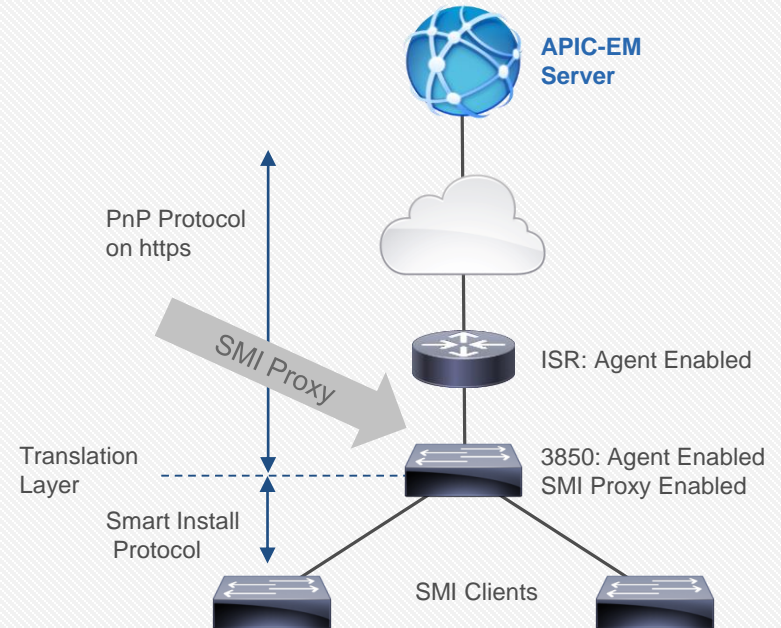
- Smart Install Proxy (SMI Proxy) runs on the device with the PnP Agent
- SMI Proxy translates the SMI to PnP
  - Represents SMI client to the PnP Server
- SMI Proxy must be explicitly enabled
- The PnP Server can manage legacy Cisco IOS® Software images on Cisco Catalyst® switches
- Catalyst 3000 and 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
    - 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
config 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

```
<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>
```

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

# Bulk Import and Export





# Bulk Import

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.

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

Date	User	Filename	Status	Import Task status						Report
				Project Added	Project Failed	Project Skipped	Device Added	Device Failed	Device Skipped	
2015-10-26 18:54	admin	pnp-service-bulk-template.csv	importing: 20%	1	0	0	0	0	0	

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.



New slide

# Bulk Import

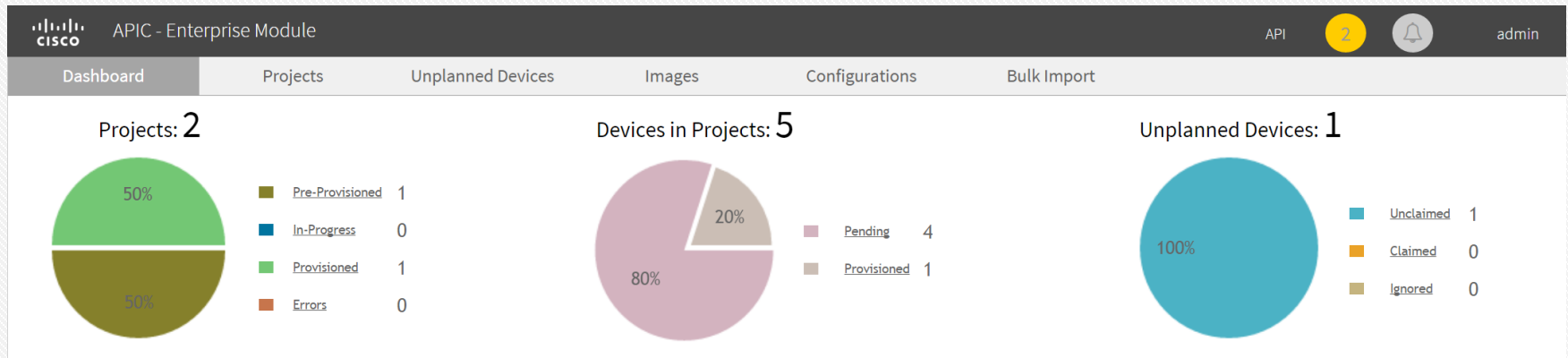
APIC - Enterprise Module

Dashboard Projects Unplanned Devices Images Configurations **Bulk Import**

Import Task status

Date	User	Filename	Status	Project Added	Project Failed	Project Skipped	Device Added	Device Failed	Device Skipped	Report
2015-10-26 18:54	admin	ppp-service-bulk-template.csv	Completed	1	0	0	4	0	0	<a href="#">Download</a>

Displaying the latest 1 of 1 Import task





# Sample Bulk Import File

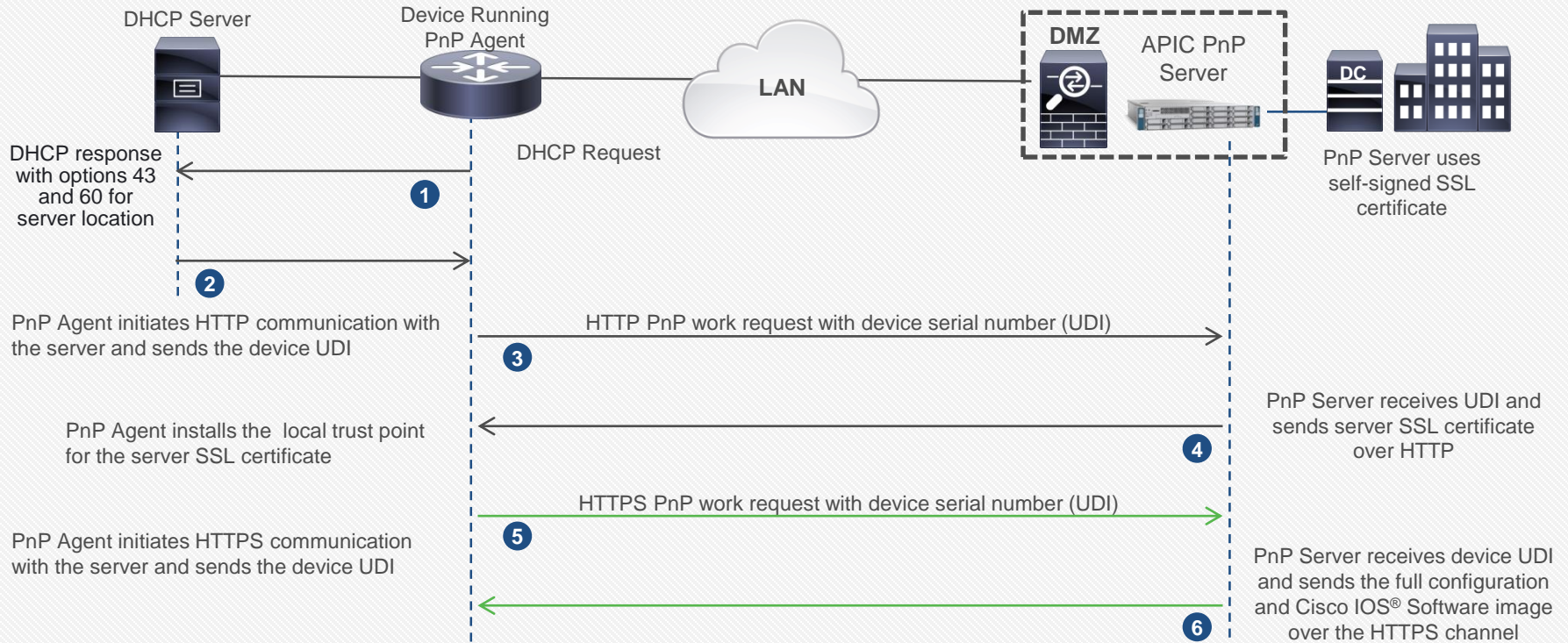
Excel interface showing a sample bulk import file for APIC-EM. The file contains a header row and several data rows. A callout box explains that all information about devices to be added can be filled in here, including the TFTP server address and path, and that the system assumes the configuration and image are available in the APIC-EM system. The file is then added using the import button in the APIC-EM Bulk Import screen.

Site Name*	Tftp server address	Tftp server Path	Serial Number	Device Name*	Product ID*	Config Name	Bootstrap	Image Name	Device Certificate*
NCC-1701-Navigation	0.0.0.0	/	FOC18492ZJL	example_switch	WS-C2960C	demo	demo	demo	FALSE
			AAA1111K3MX	example_router	C891F-K9	demo	demo	demo	TRUE
NCC-1701-Navigation	0.0.0.0	/	DOC18492ZJL	example_router23	C891F-K9	demo	demo	demo	FALSE
			BBB2222K4DN	example_switch_2	WS-C3560-12PC	demo	demo	demo	FALSE

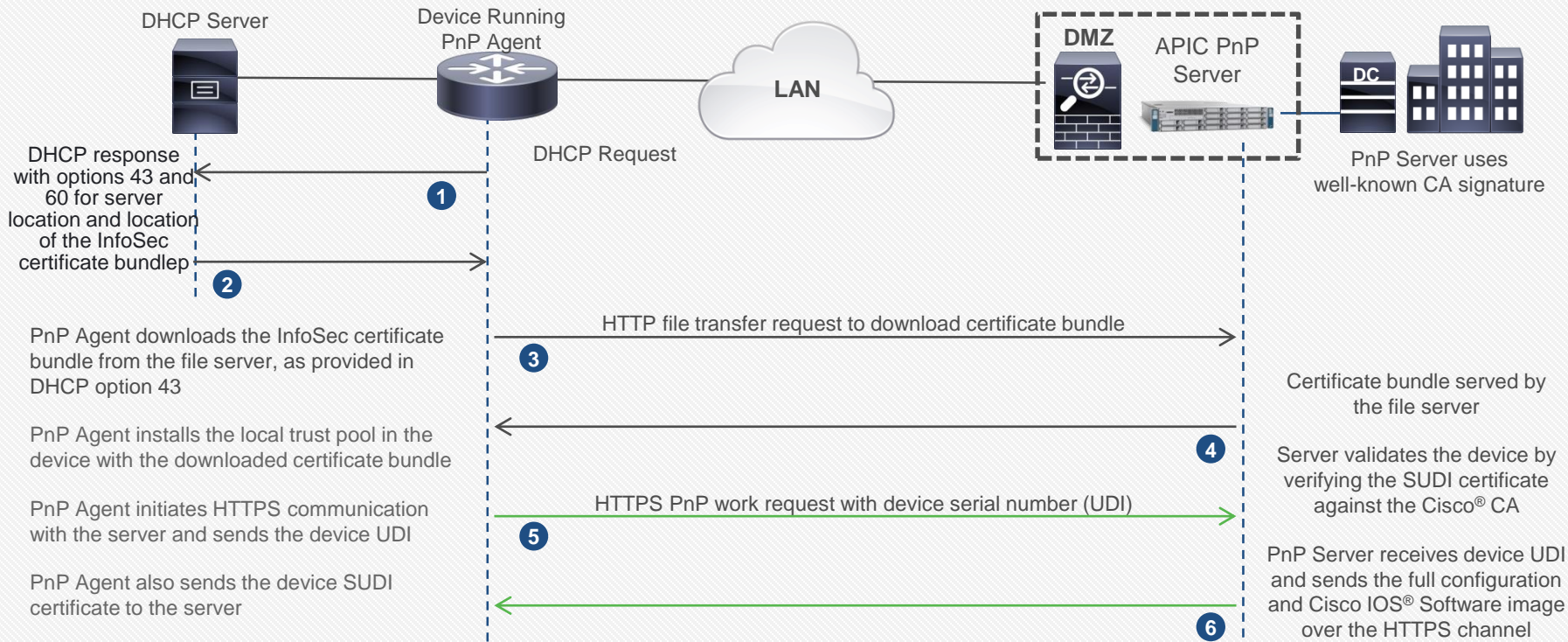
# PnP Security Workflow



# PnP Deployment for Campus - Self-Signed Certificate Method

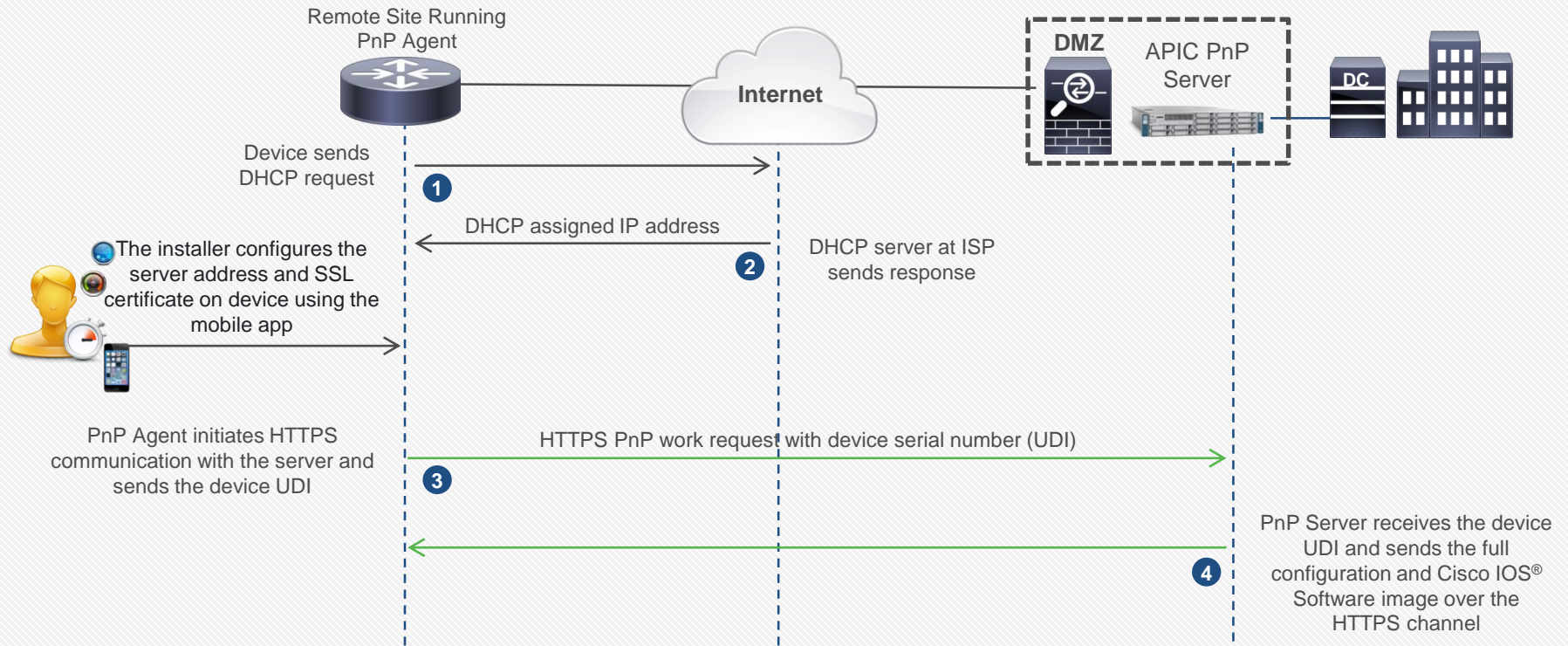


# Secured PnP Deployment for Campus - Trust Pool Method





# Secured PnP Deployment for a Branch with the Mobile App



# PnP Security - Secure Connection Enablement



## Phase 1

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

- HTTPS is always used

## Phase 2

Phase 2: 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

IOS-XE

IOS

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

