

*TOMORROW starts here.*



Cisco *live!*

# Configuration Management and Zero Touch Deployment with Prime Infrastructure

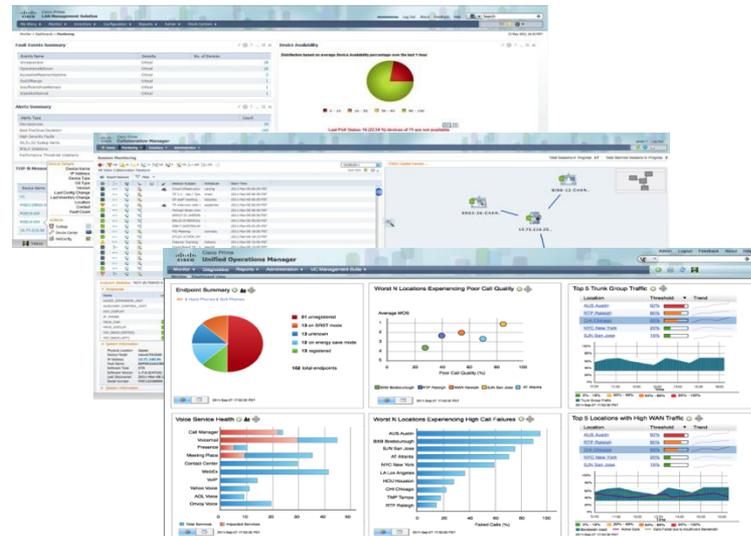
BRKNMS-2661

Scott Williamson

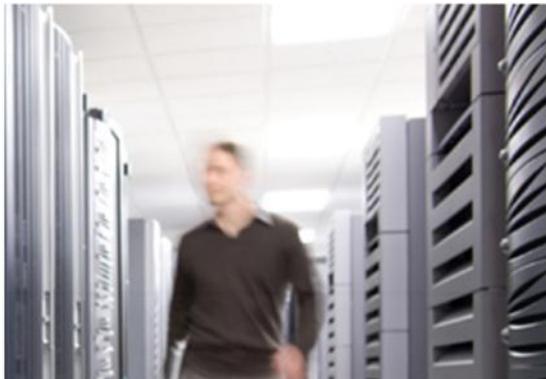
Systems Engineer

# Agenda

- What is Cisco Prime for IT
- Creating Configuration Templates
- Prime PnP Gateway
- Tips and Tricks



Cisco Prime for Enterprise Product Portfolio



What is Prime for IT

# Achieve Operation Excellence with Cisco Prime

## The Old Way

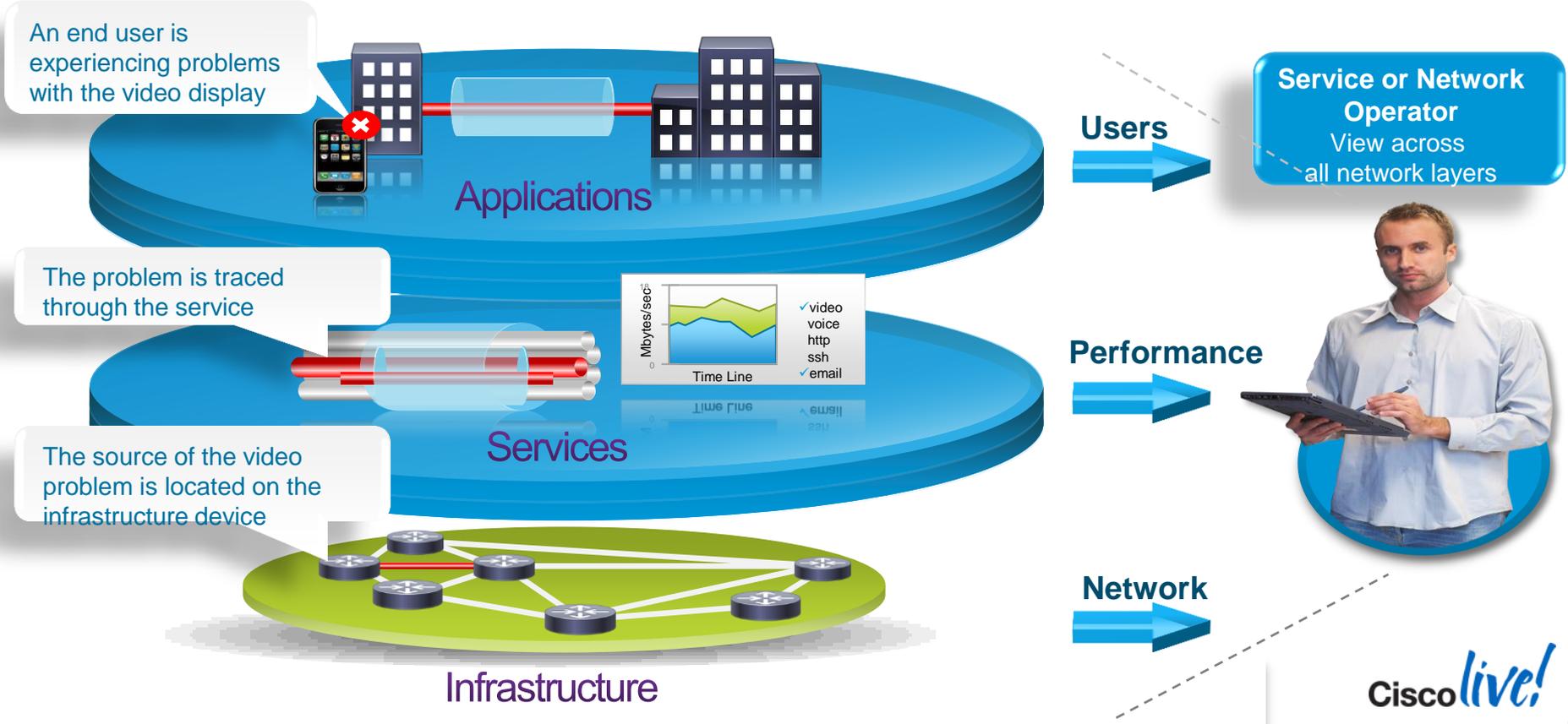
- Independent "point" products
- Untimely device and technology support
- Reliance on highly skilled staff
- Inconsistent user experience
- Difficult to install, administer, and maintain



## The Cisco Prime™ Way

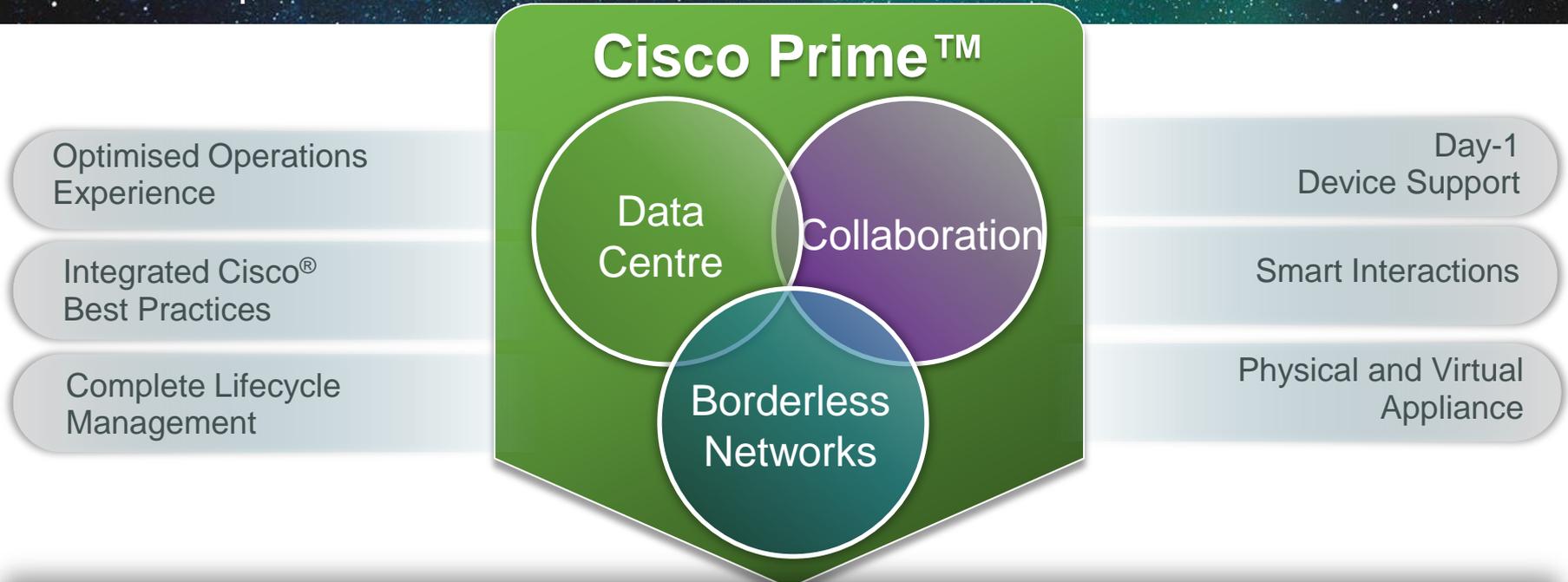
- Integrated solutions that align with major transitions
- Day-one device support for the Cisco® Advantage
- Use of Cisco best practices and knowledgebase
- Integrated workflows and user experience
- Single solution and virtual appliance

# Network Services Management Foundation



# Cisco Prime for IT

## Common Operational Attributes



Simple and Efficient Management Across Architectures, Networks, and Services

# Cisco Prime for IT

## Common Attributes

### Optimised Operations Experience

- Common user interface
- Intuitive user experience
- Optimised operator workflows

### Integrated Cisco Best Practices

- Guided deployment of Cisco-validated best practices
- Automated troubleshooting and diagnostics

### Complete Lifecycle Management

- End-to-end lifecycle
- ITIL-aligned operations
- Northbound integration to customer back office

### Day-One Device Support

- Support for new devices and technologies upon shipment
- Non-disruptive support upgrades

### Smart Interactions

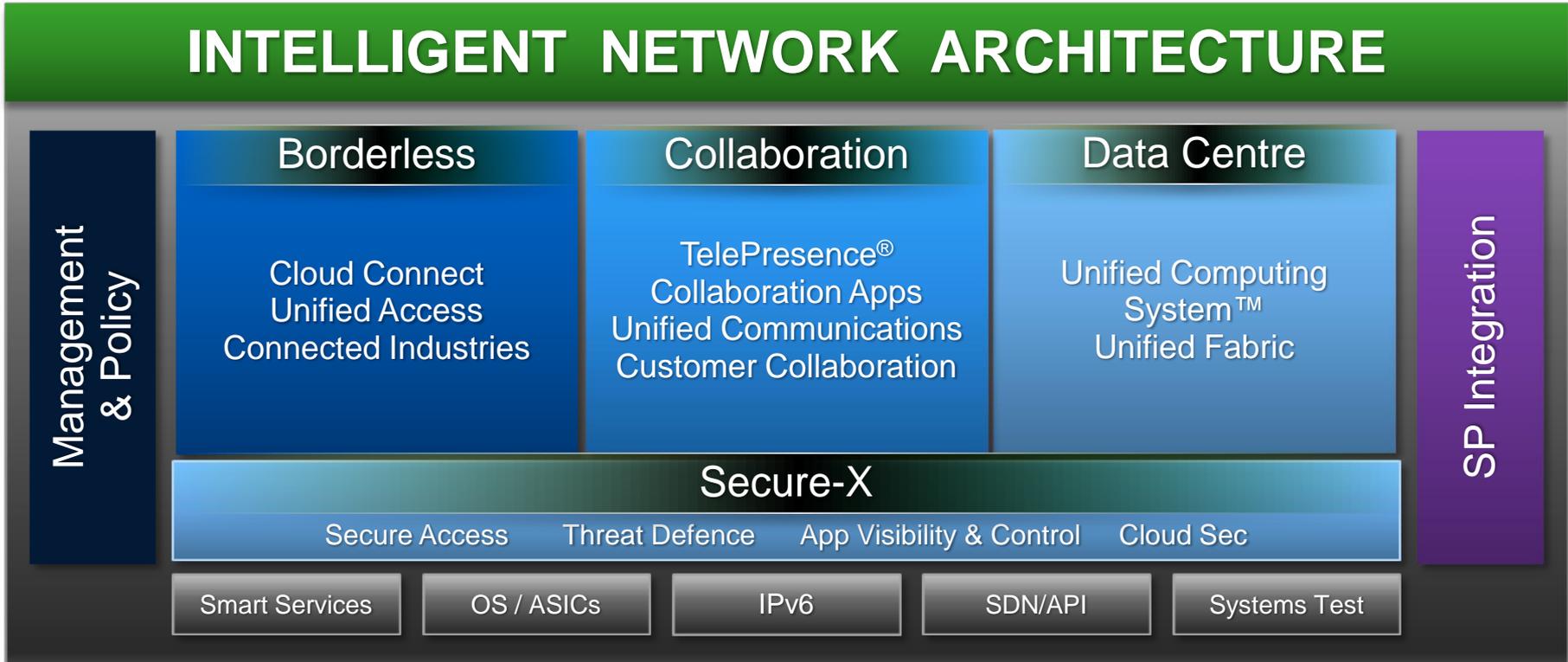
- Context-based help tool
- Real-time access to Cisco support community
- Automated Cisco TAC case creation and management

### Physical and/or Virtual Appliance

- Two delivery options
- Both options fully self-contained
- Includes operating system, software application, database, and CLI

# Enterprise Architecture

## INTELLIGENT NETWORK ARCHITECTURE



# Cisco Prime for IT Portfolio

## INTELLIGENT NETWORK ARCHITECTURE

Identity Services Engine

### Prime Infrastructure

#### Lifecycle

End-to-end lifecycle management

#### Assurance

Unified network and user-experience monitoring

#### Compliance

Regulatory and best practices

### Prime Collaboration

#### Provisioning

Deployment of services and phones

#### Assurance

Voice/video visibility and troubleshooting

#### Advanced Reporting

Service and usage reports

### Data Centre

#### Data Centre Network Manager

Management of virtual resources (network, compute, storage)

#### Netflow Generation Appliance

Unified, cross-device flow generation and export

Prime Fulfillment

#### Network Analysis Module

Rich instrumentation for application-aware troubleshooting

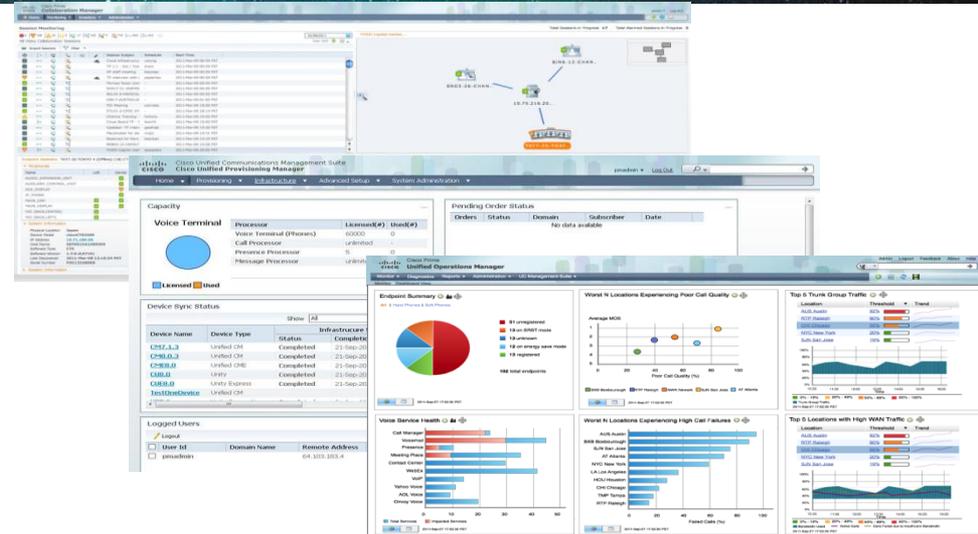
#### Network Registrar

Scalable DNS/DHCP and IP address management

# Cisco Prime Collaboration

## Improves Quality of Experience with Robust Voice and Video Management

- Gain real-time access to actionable information for quick and easy troubleshooting
- Quickly isolate the root cause of service degradation
- Solve problems pro-actively prior to impacting quality of service

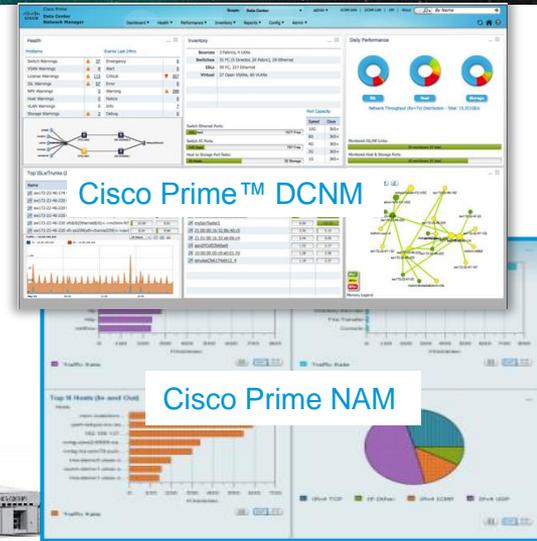


- ✓ Improve quality of experience with intuitive troubleshooting workflows
- ✓ Reduce training costs with common user experience
- ✓ Quickly isolate and fix problems, improving service availability

# Data Centre

## Application Visibility, Troubleshooting, and Resource Management

- **NAM:** Deep, application-aware network visibility and granular analytics to rapidly isolate and remediate problems and improve the user experience
- **NetFlow Generation Appliance:** Delivers NetFlow visibility to support performance, planning, and security monitoring requirements in high-throughput environments
- **Data Centre Network Manager:** Provides detailed management of data centre resources

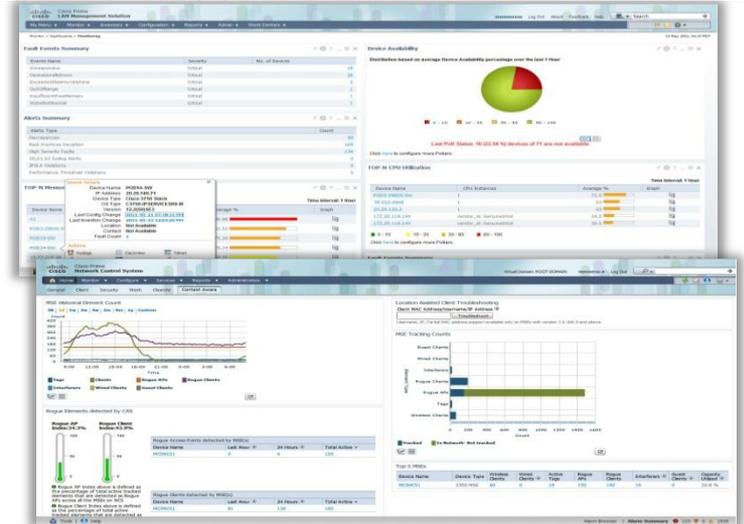


- ✓ Improve service levels with complete end-to-end network visibility
- ✓ Simplify troubleshooting with normalised data from multiple sources
- ✓ Reduce end-user and application downtime with lower TCO

# Cisco Prime Infrastructure

## Integrated Wired and Wireless Lifecycle and Assurance Management

- Complete wired and wireless lifecycle management
- Converged user and access management
- Configuration, change and compliance management
- Monitoring, troubleshooting and reporting



- ✓ Single pane of glass for wired and wireless management
- ✓ Lower TCO with intuitive user experience and workflows
- ✓ Speeds troubleshooting, improves network availability

# Access to Cisco Knowledgebase

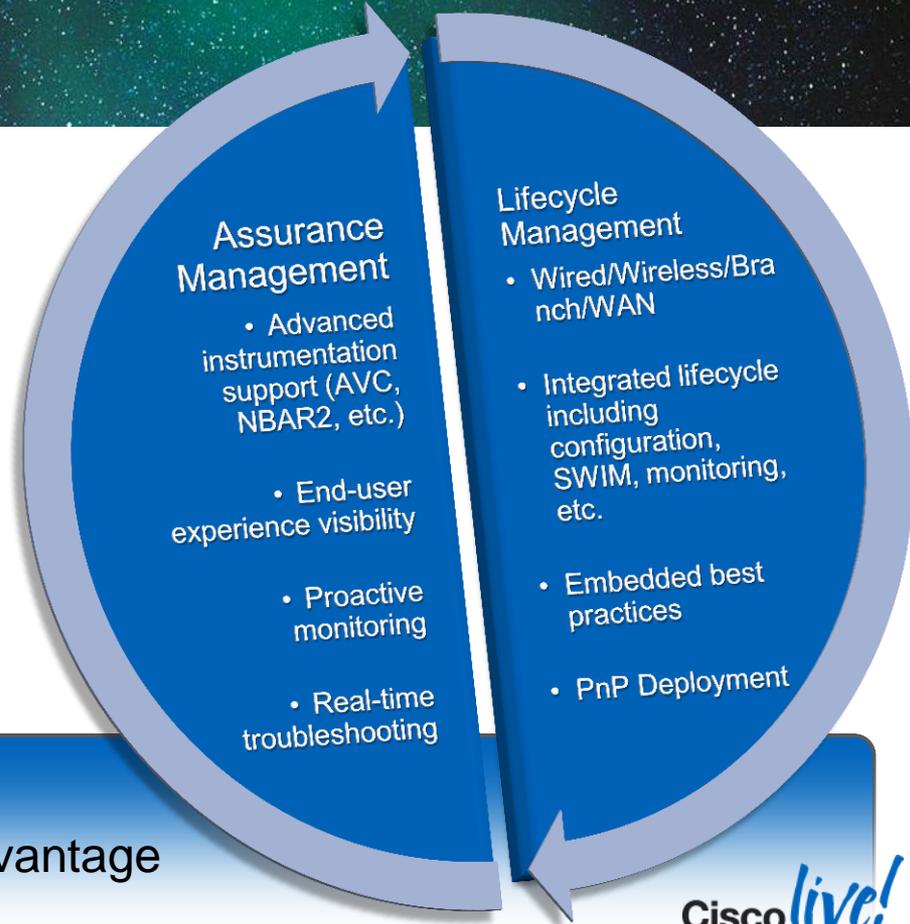
- Prime Infrastructure integrates with Cisco backend systems for increased visibility into impact analysis
- PSIRT (Security Advisories) reports provide an analysis on which devices are impacted based on:
  - IOS version running on the device
  - How the device is configured
- EoX reports provide a lifecycle management analysis on the devices
  - Shows devices that are or will be 'End-of-Sales' or 'End-of-Support'
  - Allows customers to budget for upcoming refresh
- One-Click access to related posts and discussions on Cisco Forums
- One-Click creation of TAC Case
  - Device and SmartNet Contract # automatically populated
  - Common supporting documents automatically forwarded to TAC

Software Version	Incident Description	Based on Version	Based on Configuration
12.2(52)SE	Hard-Coded SNMP Community Names in Cisco Industrial Ethernet 3000 Series Switches Vulnerability - 111895( <a href="http://www.cisco.com/en/US/products/products_security_advisory09186a0080b3f12f.shtml">http://www.cisco.com/en/US/products/products_security_advisory09186a0080b3f12f.shtml</a> )	Failed	Failed
12.2(25)SEE2	IOS Software NAT H.323 Vulnerability - 112253( <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat</a> )	Failed	Passed
12.2(25)SEE2	IOS Software NAT LDAP Vulnerability - 112253( <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat</a> )	Failed	Passed
12.2(25)SEE2	IOS Software NAT SIP Vulnerability - 112253( <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat</a> )	Failed	Passed
12.2(25)SEE2	Authentication Proxy Vulnerability - 110478( <a href="http://www.cisco.com/en/US/products/products_security_advisory09186a0080af0132.shtml">http://www.cisco.com/en/US/products/products_security_advisory09186a0080af0132.shtml</a> )	Failed	Passed
12.2(25)SEE2	TCP State Manipulation DoS Vulnerability -	Failed	Passed

# Cisco Prime Infrastructure

## One Management for Unified Access

- A single integrated solution that offers comprehensive lifecycle management of wired and wireless access, campus, and branch networks
- Utilises rich performance data for end-to-end network visibility to assure application delivery and optimal end-user experience



- Single Pane of Glass
- Consolidation, convergence, Cisco® Advantage

# Lifecycle Management

## End-to-End Lifecycle Management

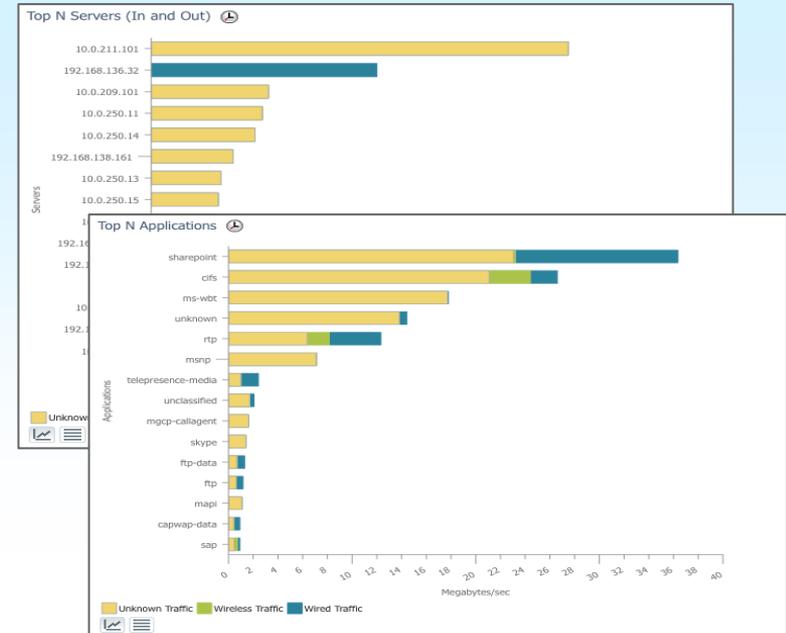
- Centralised Discovery, Inventory, Configuration Management, SWIM, and Proactive/Reactive Monitoring
- Accelerated Troubleshooting of Wired/Wireless Infrastructure Issues
- Greater device coverage: 3850/5760 (including templates and guided workflows), ASAs, IOS-XR and IDU
- Customisable out-of-the-box Cisco best practices and validated design configuration templates for wired/wireless devices
- Unified Access Management and Client Tracking
- Infrastructure lifecycle reports
- Plug & Play for Automated Deployment
- 3rd party device support

The screenshot displays the Cisco Prime Infrastructure Device Work Center interface. At the top, there's a navigation bar with tabs for Home, Design, Deploy, Operate, Report, and Administration. Below this, the 'Device Work Center' section is visible, showing a 'Device Group' dropdown set to 'ALL'. A table lists various devices with columns for Device Name, Reachability, IP Address, Device Type, Collection Status, Collection Time, and Software Version. The table includes entries like IFM-2900-Hub, IFM-3560-1, IFM-3560-2-test, IFM-8500E, IFM-CONTROLLER2, IFM-CONTROLLER3, IFM-Controller1, and IFM\_2921\_yourdo. Below the table, there are tabs for Device Details, Configuration, Configuration Archive, and Image. The 'Device Details' tab is active, showing a 'Summary' section with fields for IP Address (172.20.110.71), Device Name (IFM-3560-1), Device Type (Cisco Catalyst 3560-24PS Switch), Up Time (7 days 7 hrs 20 mins 15 secs), System Time (2012-Aug-29, 19:53:46 UTC), Reachability Status (Reachable), Location (S3CN, floor 2, Row 10), Contact, and NMSIP and Location (Cisco Identity Capable: No). A 'Unique Device Identifier (UDI)' section is also visible, listing Name (1), Description (WS-C3560-24PS), Product ID (WS-C3560-24PS-E), Version ID (F0011387200), Serial Number (F0011387200), Software Version (12.2(33)SE5), and Model No. (WS-C3560-24PS-E). At the bottom right, there are status indicators for Support Cases, Alarm Browser, Alarm Summary, and a user profile for 3077.

# Assurance Management

## Application Visibility and End User Experience

- End-to-End Visibility for Service-Aware Networking
  - By applications, services and end-users
- Out-of-the-Box Support for Cisco Advanced Instrumentation
  - Netflow, Flexible Netflow, AVC, NBAR, PA, Medianet, etc.
- Simplified End-to-End Visibility for Faster Troubleshooting
  - Normalises, correlates and aggregates data sources
- Automated Baselining with Dynamic Thresholds
- NBAR2 Custom Application Support
- Multi-NAM Management
- Service Health Dashboard



# So Why Network Management

- Improved Operational Efficiency
- Simplify Technology Deployment
- Troubleshooting and Visibility (Single View)
- Automate Lifecycle Processes
- Be Proactive and Delegate
- Speed up Problem Resolution
- **AND if you Don't**

# When Control Systems Fail



# When Control Systems Fail





## Prime Plug and Play Gateway

# What is Automation?

- Automation is the use of **control systems** and **information technologies** to reduce the need for human work in the production of goods and services

# Why Automation?

- Efficient use of resources
- Reduction in errors
- Faster deployment
- Consistency
- Security

# Why Zero-touch Provisioning?

- Estimation that 80% of network downtime can be attributed to human error
- Networks are getting more complex
- Manual configuration is slow
- People are expensive
- Travel is expensive

# When to Zero-touch?

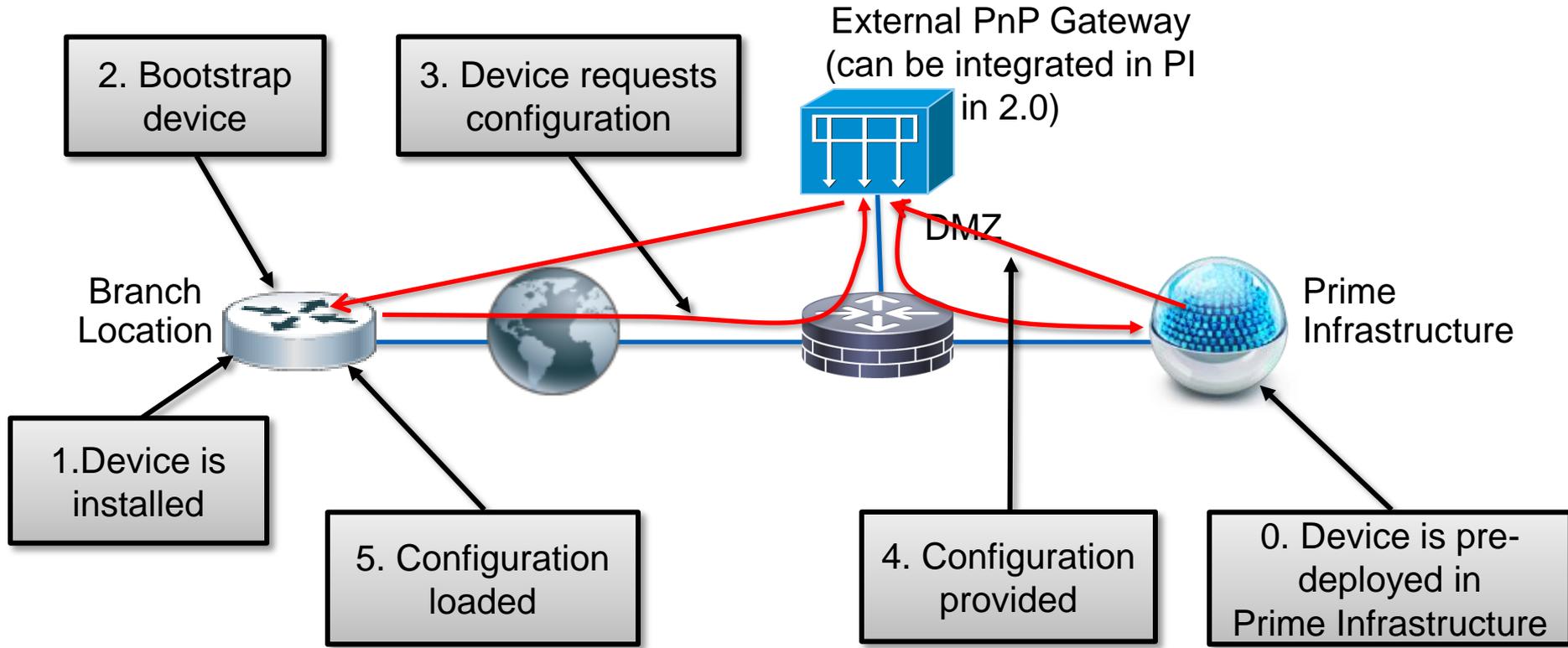
- Reduce Onsite Skilled Support
- Consistent Configuration
- Reduce Deployment Time
- Reduce Deployment Cost
- To Keep Your Job
- Allow for Innovation

# What are the Options?

## For Zero or Single Touch Deployments

- DHCP/TFTP Boot (Switches Only)
- Auto Smart Install
- Cisco Configuration Engine
- Cisco or Partner Customisation Services
- Plug and Play Gateway

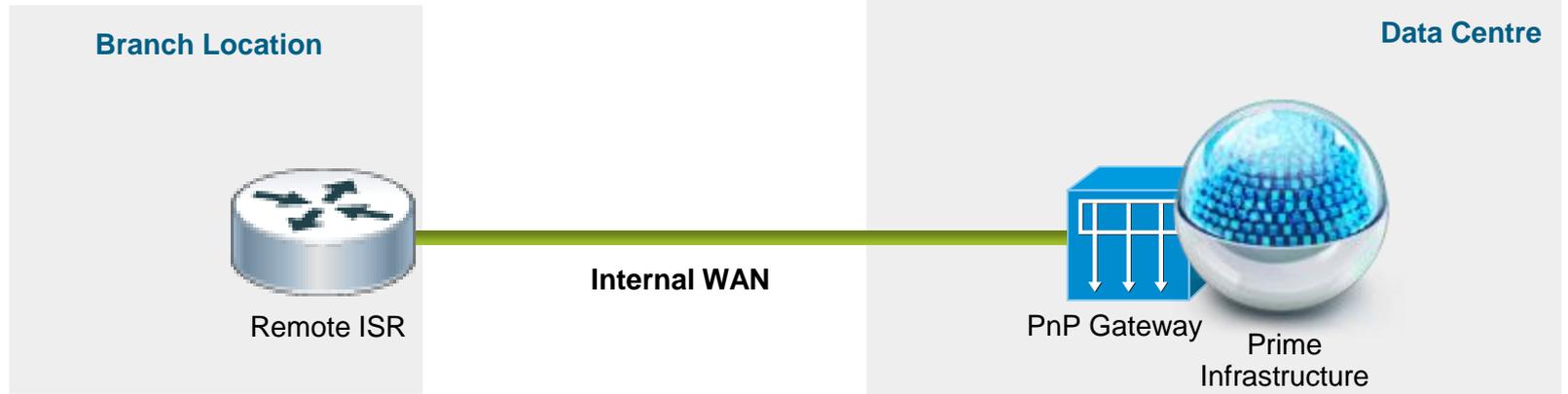
# Plug and Play Overview



# PnP Gateway for Internal Deployments

## PnP Gateway in Prime Infrastructure

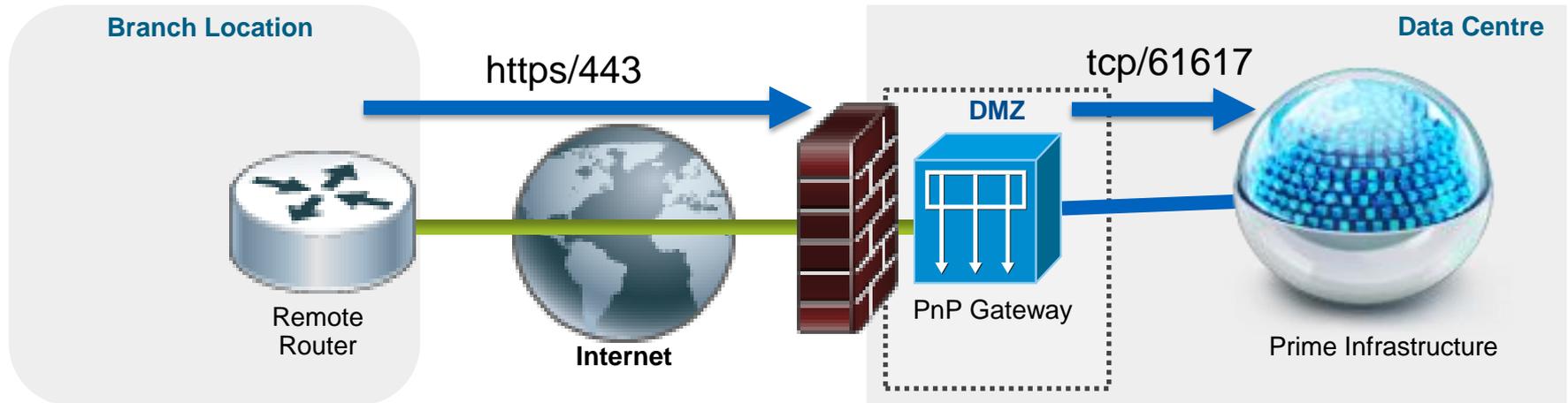
- PnP Gateway integrated into Prime Infrastructure 2.x onwards



# PnP Gateway for Internet Deployments

## PnP Gateway in a DMZ

- PnP Gateway in a DMZ for Prime Infrastructure 1.3 onwards
- A separate PnP gateway Server can be deployed on DMZ
- This allows Prime Infrastructure to now be exposed to the Internet



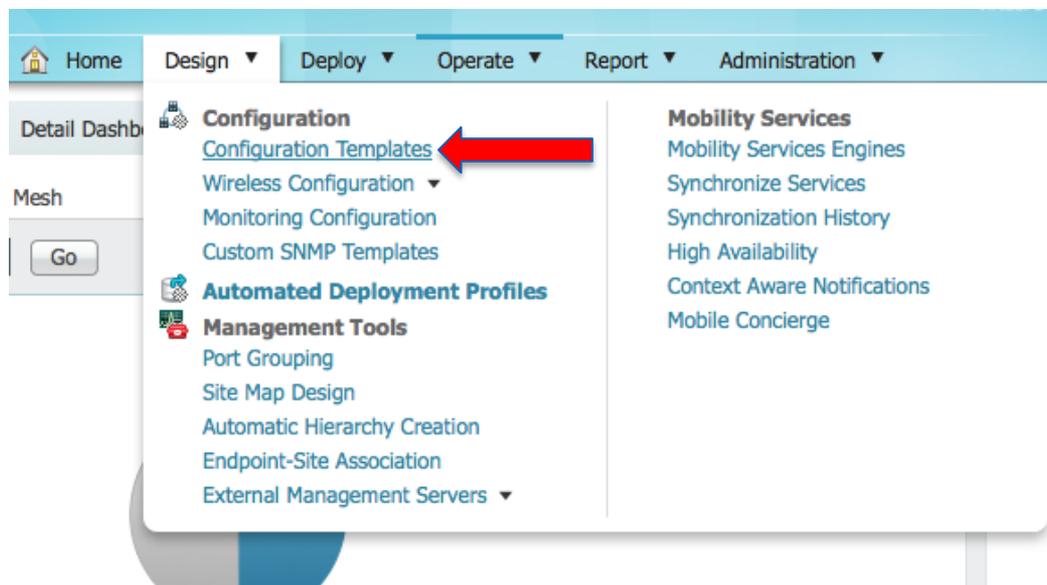
# Steps to Get This Working

- Design
  - Create Bootstrap Configuration Template
  - Create Device Configuration Template
  - Create Automated Deployment Profile
  - Publish Automated Deployment Profile
- Deploy
  - Deploy Automated Deployment Profile
- Operate
  - Monitoring the Deployment Status
  - Confirming the Device is being Managed

# Steps to Get This Working

## Create Configuration and Bootstrap Templates

- Create Templates
  - Bootstrap
  - Configuration



# Bootstrap Template

## Design – Create Bootstrap Configuration Template

### Configuration Templates

My templates > PnP

#### PnP Bootstrap

**Template Basic**

\*Name: PnP Bootstrap Author: scotwill  
Description: Feature Category: CLI

**Validation Criteria**

\*Device Type: Routers OS Version:

**Template Detail**

CLI Content Form View

```
ip host ${PnP_Gateway}.bnelab.cisco.com $PnP_IP
ip host ${PnP_Gateway}.bnelab.cisco.com $PnP_IP
cns trusted-server all-agents ${PnP_Gateway}.bnelab.cisco.com
cns trusted-server all-agents $PnP_Gateway
cns trusted-server all-agents $PnP_IP
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns config partial ${PnP_Gateway}.bnelab.cisco.com 80
cns event ${PnP_Gateway}.bnelab.cisco.com keepalive 120 2 reconnect-time 60
cns config initial ${PnP_Gateway}.bnelab.cisco.com 80
cns exec 80
cns image server http://${PnP_Gateway}.bnelab.cisco.com/cns/HttpMsgDispatcher status http://${PnP_Gateway}.bnelab.cisco.com/cns/HttpMsgDispatcher
```

BRKNMS-2661

# Bootstrap Template

## Design – The Commands to Create Bootstrap Configuration

- CNS “call-home” configuration that is required for PnP
  - Device ID is per device based on serial number
  - Device TYPE is per device type unique identifier

```
ip host <PnP Gateway server fully qualified host name> <IP address>
ip host <PnP Gateway server short hostname> <PnP Gateway IP address>
cns trusted-server all-agents <PnP Gateway server fully qualified host name>
cns trusted-server all-agents <PnP Gateway server short host name>
cns trusted-server all-agents <PnP Gateway IP address>
<The Device ID or Device Type commands go here>
cns config partial <PnP Gateway server fully qualified host name> 80
cns event <PnP Gateway server fully qualified host name> keepalive 120 2 reconnect-time 60
cns config initial <PnP Gateway server fully qualified host name> 80
cns exec 80
cns image server http://<PnP Gateway server fully qualified host name>/cns/HttpMsgDispatcher
status http://<PnP Gateway server fully qualified host name>/cns/HttpMsgDispatcher
```

### Device ID-based commands

```
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
```

### Device Type-based commands

```
cns id udi
cns id udi event
cns id udi image
```

# Device Template

## Design – Create Device Configuration Template

**Template Basic**

\*Name  Author

Description

Feature Category **CLI**

**Validation Criteria**

\*Device Type  OS Version

**Template Detail**

CLI Content  Form View

```
hostname This is now Mine - PI is taking over
username admin privilege 15 secret cisco,123
clock timezone +AEST 10
no ip domain-lookup
ip domain-name bnelab.cisco.com
spanning-tree mode rapid-pvst
logging trap debugging
logging 10.66.236.49
snmp-server community public RO
snmp-server community private RW
snmp-server host 10.66.236.49 public
ntp server 10.66.236.1
line vty 0 4
 login local
line vty 5 15
 login local
```

**Templates**

- Features and Technologies
  - Security
  - Controller
  - Network Analysis Module
- CLI Template
  - Composite Templates**
- My Templates
  - Devices
  - Discovered Templates
  - OOTB
  - PnP
    - PnP Bootstrap Device Type
    - PnP Bootstrap
    - Boot\_test
    - Org\_1\_TACACS\_Server
    - QoS 2900 ISR
    - Switch Basic Config
    - conf\_g01

# Plug and Play Profile

## Design – Create Plug and Play Profile

The screenshot displays the Cisco Prime Design interface for creating a Plug and Play Profile. The left navigation pane shows the 'Design' tab selected, with 'Plug and Play Profiles' highlighted in blue and indicated by a red arrow. The main content area is titled 'Automated Deployment Profiles' and shows a tree view where 'PnP Profile' is selected, also indicated by a blue arrow. The right-hand pane, titled 'PnP Profile', contains the following configuration fields:

- Profile Basic:** \*Name (2951 Router) and Description (empty). A blue arrow points to the Name field.
- Validation Criteria:** Device Type (Cisco 2951 Integrated Servi...). A blue arrow points to the Device Type dropdown.
- Profile Detail:** Bootstrap Template (PnP Bootstrap Device Type), Software Image (c2951-universalk9-mz.SPA...), Image Location (flash0:), and Configuration Template (conf\_g01). Blue arrows point to each of these dropdown menus.

At the bottom of the form, there are two buttons: 'Save as New PnP Profile' (highlighted with a blue arrow) and 'Cancel'.

# Plug and Play Profile

## Design – Publish and Deploy the Automated Deployment Profile

**PnP Profiles**  
**2951 Router**

▼ **Profile Basic**

\*Name   
Description

▼ **Validation Criteria**

Device Type

▼ **Profile Detail**

Bootstrap Template

Software Image

Image Location  ⓘ

Configuration Template

**PnP Profiles**  
**2951 Router**

▼ **Profile Basic**

\*Name   
Description

▼ **Validation Criteria**

Device Type

▼ **Profile Detail**

Bootstrap Template

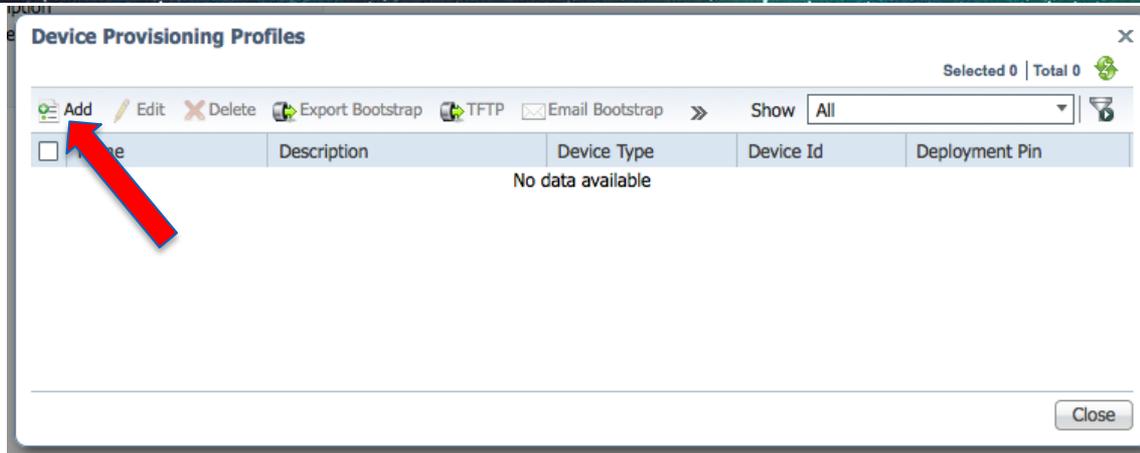
Software Image

Image Location  ⓘ

Configuration Template

# Plug and Play Profile

## Deploy – Create Device Provisioning Profiles



- Add a new device to be provisioned

# Plug and Play Profile

## Deploy – Create Device Provisioning Profiles

The image shows a screenshot of the Cisco PnP PreProvisioning Details form. The form is divided into several sections: Name, Device Selection Parameters, Profile Parameters, Configuration Template Properties, and Image Properties. A second window, titled 'Device Management Parameters', is overlaid on the right side of the main form. Blue arrows point from the 'Device Management Parameters' window to the 'Profile Parameters' and 'Configuration Template Properties' sections of the main form. The 'Device Management Parameters' window contains sections for Device Management Parameters, SNMP Parameters, and CLI Parameters.

**PnP PreProvisioning Details**

\*Name  Description

**Device Selection Parameters**

Device Id  Type

**Profile Parameters**

**Bootstrap Template Properties**

\*PnP Gateway Host Name

\*PnP Gateway IP Address

**Configuration Template Properties**

\*desc

\*g01ipadd

**Image Properties**

Image Location   
Erase Flash   
Continue On Image Failure   
Activate Image

**Device Management Parameters**

**Device Management Parameters**

IP Address

**SNMP Parameters**

Version  Timeout  (sec) Retries

\*Community

**CLI Parameters**

Protocol

UserName  Password  Confirm Password

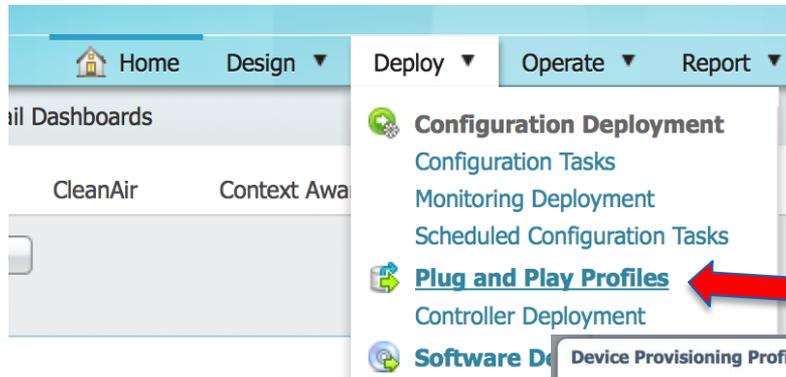
Enable Password  Confirm Enable Password  Timeout  (sec)

**Template Variables**

**Management Information**

# Plug and Play Profile

## Deploy – Plug and Play Profiles



ability: 4 Total Unreachable Device Count: 0

- Export Bootstrap
- TFTP Bootstrap
- Email Bootstrap
- Email PIN

The screenshot shows the 'Device Provisioning Profiles' window. It has a title bar with 'Selected 0 | Total 2' and a close button. Below the title bar are action buttons: 'Add', 'Edit', 'Delete', 'Bootstrap Configuration', and 'Email Pin'. There is also a 'Show' dropdown menu set to 'All'. The main content is a table with the following data:

<input type="checkbox"/>	Name	Description	Device Type	Device Id	Deployment Pin	Pre-provisioned on
<input type="checkbox"/>	3945PNP		Routers/Cisco 2900 S...	FGL12345678	1391753524238	2014-Feb-07 16:12:04 EST
<input type="checkbox"/>	2951_PnP		Routers/Cisco 2900 S...	FGL150412JX	1390191558639	2014-Jan-20 14:19:18 EST

At the bottom right of the window is a 'Close' button.

# Monitoring the Deployment

Operate – Monitoring the Status of Devices being Deployed

The screenshot shows the Cisco Manage Network interface. The top navigation bar includes Home, Design, Deploy, Operate, Report, Administration, and Workflows. The 'Operate' menu is expanded, showing options like Monitoring Dashboards, Device Work Center, Alarms & Events, and Clients and Users. A red arrow points to the 'Plug and Play Status' link. Below the menu, the 'Device Work Center | Plug and Play Status' page is visible, showing a table of device deployment status.

Device Id	Device Type	Matched Profile Name	Pre-provisioning Name	Current Status
<input type="checkbox"/> FGL150412JX	N/A	Test_2951	2951_PnP	Bootstrap response sent
<input type="checkbox"/> FGL12345678	N/A	Test_2951	3945PNP	Bootstrap response sent

# Monitoring the Deployment

## Operate – Confirming the Device is being Managed

- Device added to Work Centre
- Collection Status

The screenshot shows the Cisco Manage Network interface. The top navigation bar includes Home, Design, Deploy, Operate, Report, Administration, and Workflows. The 'Operate' dropdown menu is open, showing options like Monitoring Dashboards, Device Work Center (highlighted with a red arrow), and Operational Tools. The background shows a dashboard with various charts and data points.

Device Group > ALL

ALL

The screenshot shows a table of device collection status. A blue arrow points from the 'Device Work Center' menu item to the table. The table has columns for Device Name, Reachability, IP Address/DNS, Device Type, Admin Status, Inventory Collection Status, Last Successful Col..., and Software Version. Two devices are listed: 2951-Branch and 2951-HQ, both with a green checkmark in the Reachability column and 'Completed' in the Inventory Collection Status column.

Device Name	Reachability	IP Address/DNS	Device Type	Admin Status	Inventory Collection Status	Last Successful Col...	Software Version
2951-Branch	✓	10.66.236.243	Cisco 2951 Integrated ...	Managed	Synchronizing	February 6, 2014 1...	15.3(2)T
2951-HQ	✓	10.66.236.242	Cisco 2951 Integrated ...	Managed	Completed	February 6, 2014 1...	15.3(2)T

# Plug-n-Play Options with Prime

No CLI skills are needed for these options

**PnP**  
**1**

Cisco Integrated Customised Services (CICS) which loads a custom factory config in the ISR and is available for all ISRs

**PnP**  
**2**

USB stick to bootstrap the ISR

**PnP**  
**3**

Cisco Prime PnP Application (*PC and for iPhone/iPad*)

**PnP**  
**4**

CCP Express (GUI that optionally comes with the ISR)

# Plug-n-Play with CICS

## Cisco Integrated Customisation Services

CISCO1921/K9

Configuration Summary [View Full Summary](#)

Option Search

Region/ Country specification

Select Country (Optional) [Clear All](#)

Click links below to configure.

Software

- Software and Technology Package
- CICS Option**
- IOS Technology Package Licenses
- ADSL Firmware Options

Click CICS Option.

1 When ordering with CCW, select the CICS options

Order 12345 [Change](#)

Purchase Order #\* 98765 [Change](#)

Web Order ID #: 60264490

Export Share Delete Print Email

Items Discounts Shipping and Install Billing Review and Submit

Federal Government

Service Preferences

Add Product Item

Part #: Qty: Add Find Products Add Services/Subscriptions

Import a Saved Configuration **Attach Template** Click Attach Template.

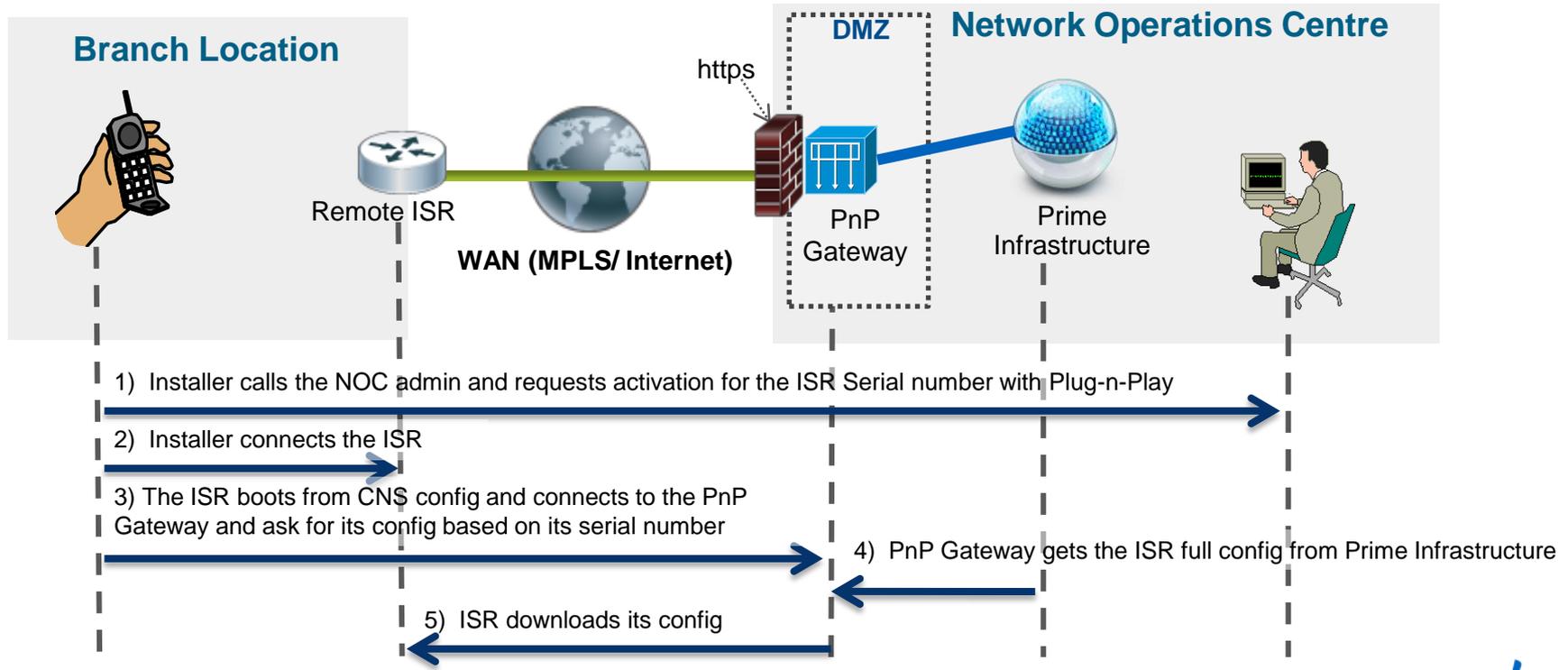
<input checked="" type="checkbox"/>	Hardware, Software and Services	P.O. Line Reference	Lead Time
<input checked="" type="checkbox"/>	1.0 CISCO1921/K9 C1921 Modular Router, 2 GE, 2 EHWIC slots, S12DRAM, IP Base	98765	21 days

2 Attach a template to this ISR (or to multiples ISRs) This template would include the CNS commands, for example:

```
Router # ip host PnP 10.1.3.99
Router # cns config initial 10.1.3.99 443
Router # cns config partial 10.1.3.99 443
Router # cns id hardware-serial
Router # cns id hardware-serial event
Router # cns id hardware-serial image
Router # cns event PnP keepalive 60 3
Router # cns exec 80
```

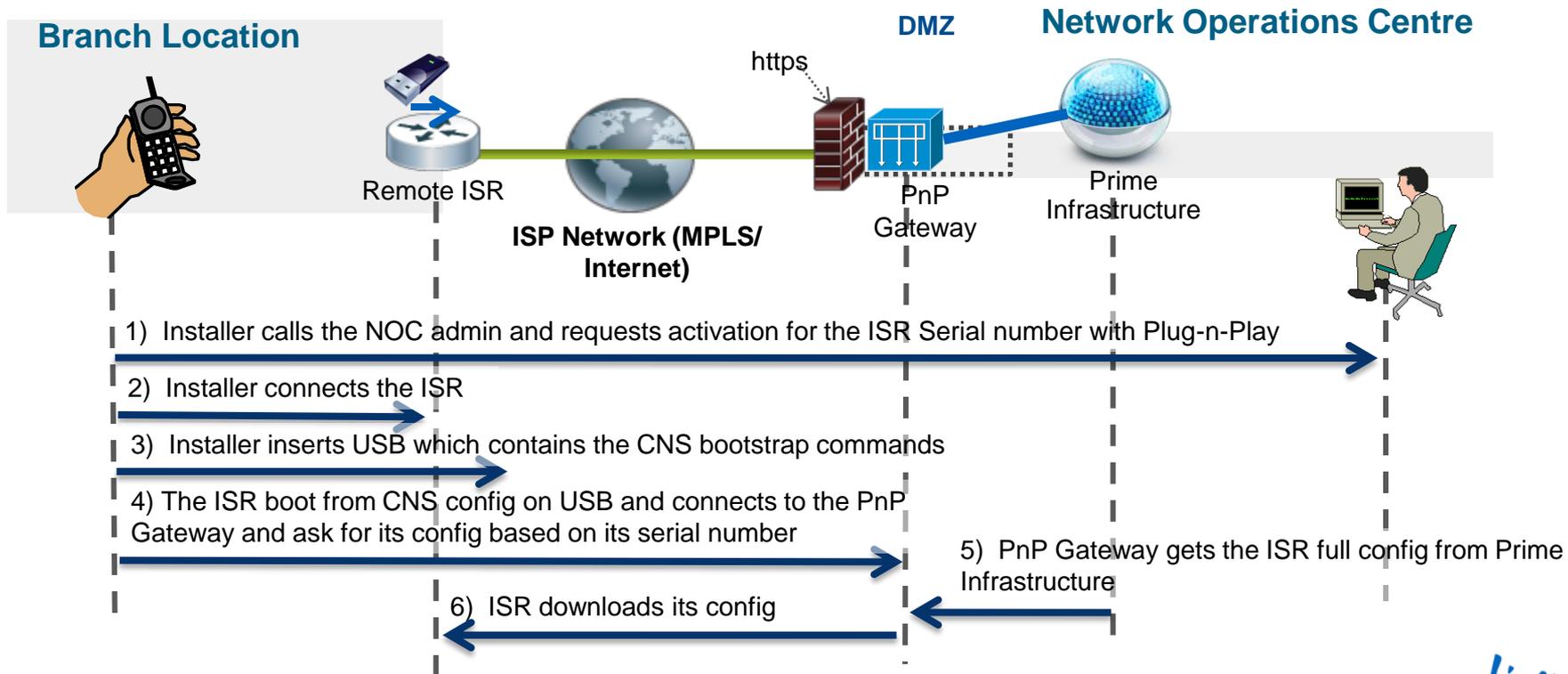
# CICS Based Plug-n-Play

Zero-touch configuration for the installer (Cisco Integrated Customisation Services)

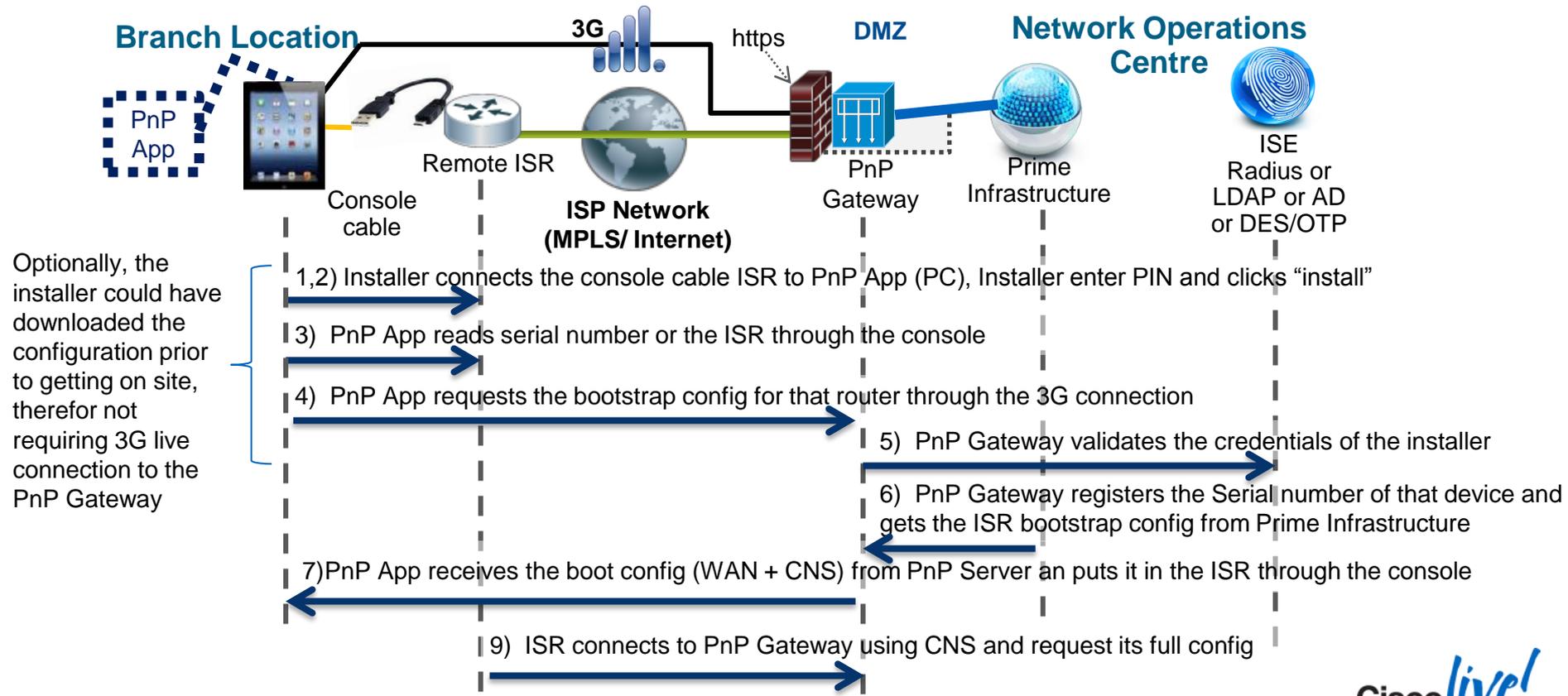


# USB Based Plug-n-Play

This option requires the CVO or ZTD factory configuration when ordering.

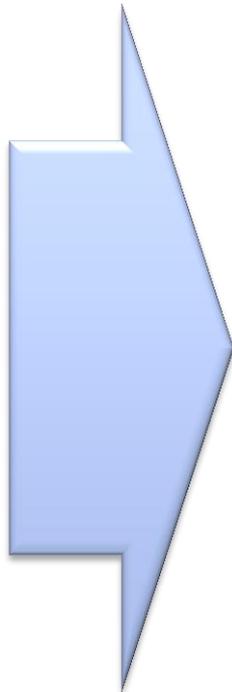


# Console Application Based Plug-n-Play



## Pre-Provisioning

- Network administrator creates the device PNP automated deployment template in Prime Infrastructure
- Administrator specifies the name of the device, desired configuration and image, and optionally the device serial number and a bootstrap configuration
- A deployment PIN number is generated and emailed to the installer



## Installation

- Installer connects the device in its final location
- Installer starts the provisioning by entering the device PIN. PnP App will register the device serial number using the deployment PIN with PnP Gateway
- PnP App bootstraps the device
- Installer monitors the deployment status

# Deployment Applications

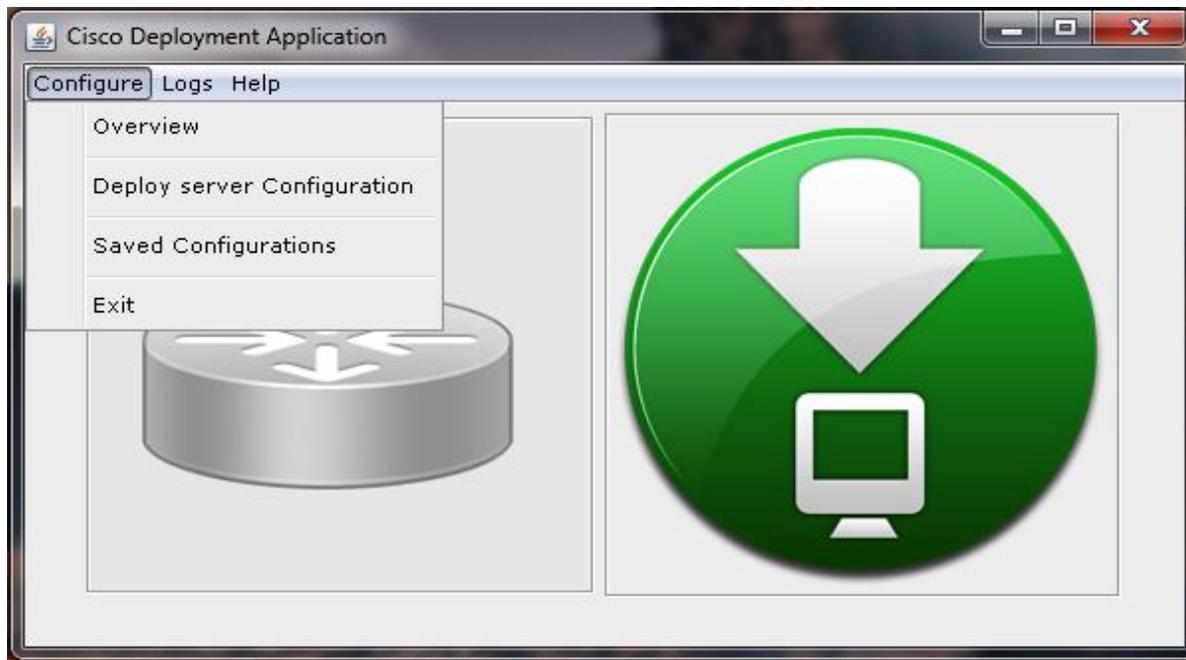
Windows PC, iPad or iPhone. Android (future)

- PC Application
  - Works with micro USB console port or a regular console port with a serial-to-USB adaptor.
  - Works with any IOS device with a console port
- iPad and iPhone Application
  - Requires a special cable (<http://www.redpark.com/c2rj45.html>)
  - Works with any IOS device with a console port



# Deployment Application - Windows

- The PnP Deployment application screen shot showing the different configuration option.



# Deployment Application - PI Configuration

- The Configure → "Deploy Server Configuration" is used to configure the PnP Gateway Server (Standalone or PI Integrated) and PI User credentials

The screenshot displays the Cisco Deployment Application interface. The main window is titled "Cisco Deployment Application" and shows a "Configure" tab. On the left, there is a green checkmark icon above a router icon, with a blue callout box pointing to it that says "Device is Connected." On the right, there is a large green circular icon with a white download arrow and a computer monitor icon. The "Cisco Prime Infrastructure and PnP Gateway Configuration" window is open, showing the following configuration options:

- Cisco Prime PnP Gateway**: Configure the Cisco Prime PnP Gateway server. The server address could be Cisco Prime server or Cisco Prime Gateway (In case the gateway is deployed as standalone server) address; Make sure to use the address on which the SSL certificate is obtained.
  - Server Address \*:
- PNP HTTPS Port**:
- Cisco Prime Infrastructure**: Configure the Cisco Prime Infrastructure server authentication details. Cisco Prime Infrastructure authenticates the Cisco PnP Gateway using these credentials when downloading a bootstrap configuration.
  - Username \*:
  - Password \*:
- Save the configurations**:  Save the login credentials and settings.

\* Indicates a mandatory field.

Buttons: Test Connection, Save, Reset

# Deployment Application - Saved Configuration

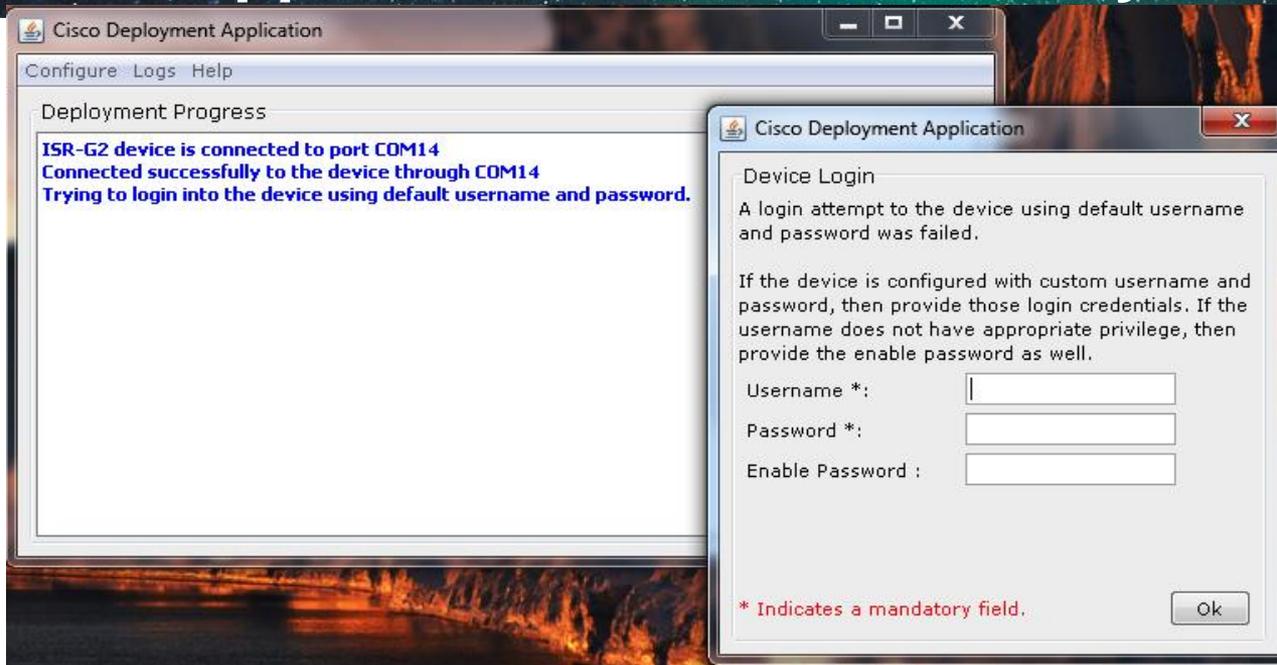
- The Configure → "Saved Configuration" is used to view all the downloaded bootstrap configuration in the Deployment Application.

The screenshot displays the Cisco Deployment Application interface. The main window shows a 'Configure' menu and a central area with a green checkmark icon and a large green download arrow icon. A 'Download Configuration' dialog box is open, showing a table of downloaded/imported configurations.

Device name	Device SID
PNP 182	FGL162426EB

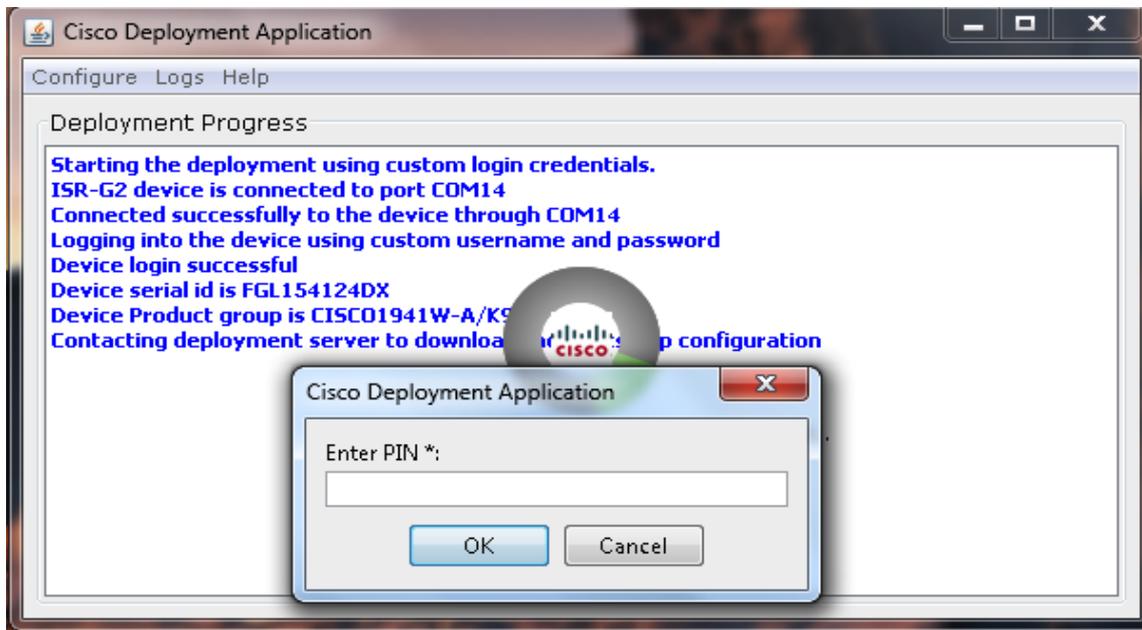
The dialog box also includes a 'Delete' button and an 'Import Configuration' section.

# Deployment Application - Password Entry



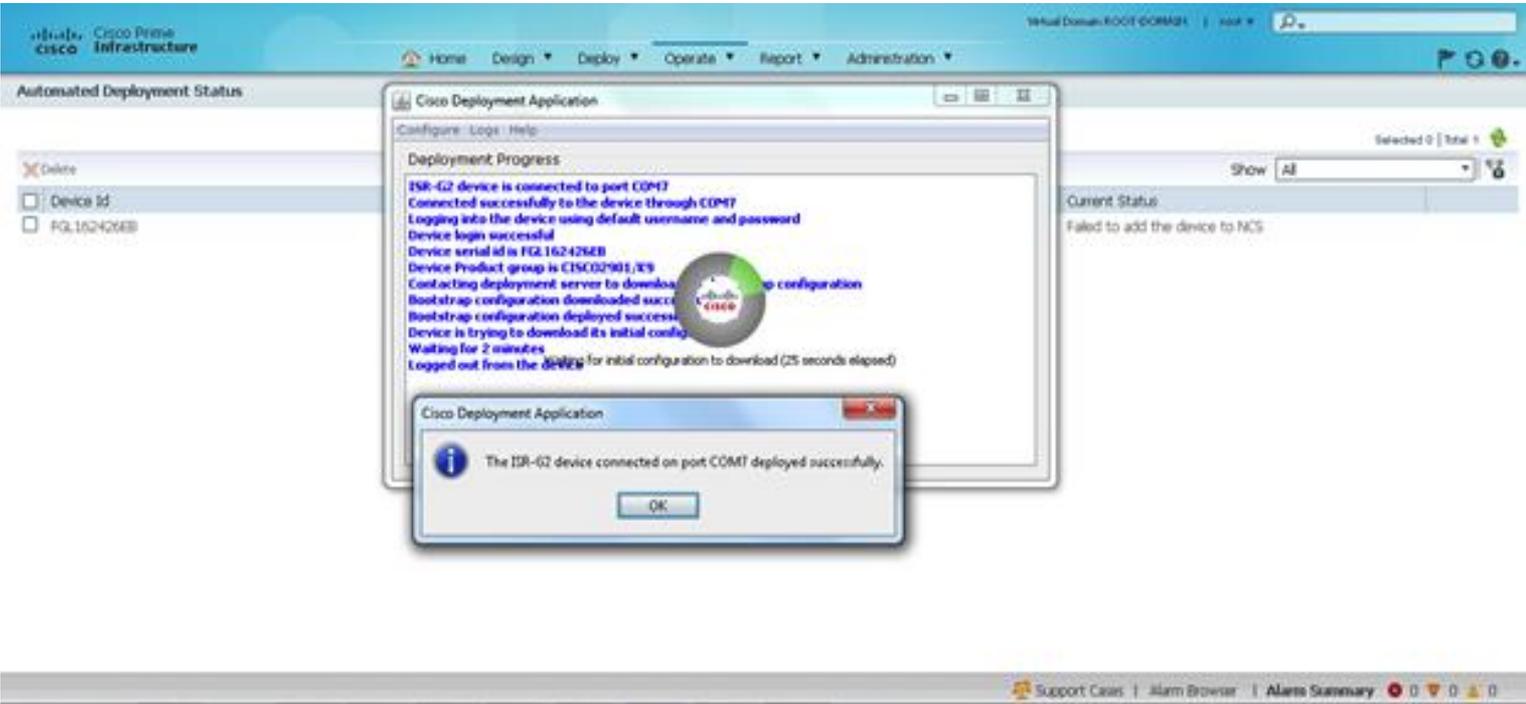
- The Deployment App tries to login with default user and password for factory default devices
- If defaults denied then it prompts the user to these details

# Deployment Application - PIN Entry



- The Screen shows the screen shot for entering the PIN for deployment.

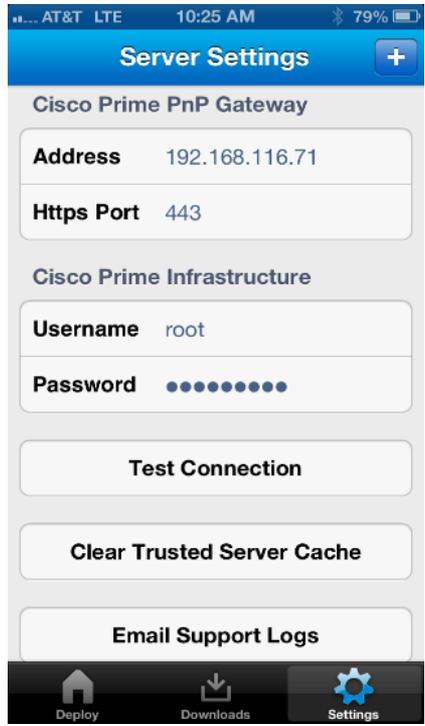
# Deployment Application - Device Deployment



- The Screen shot shows the device deployment successfully completed

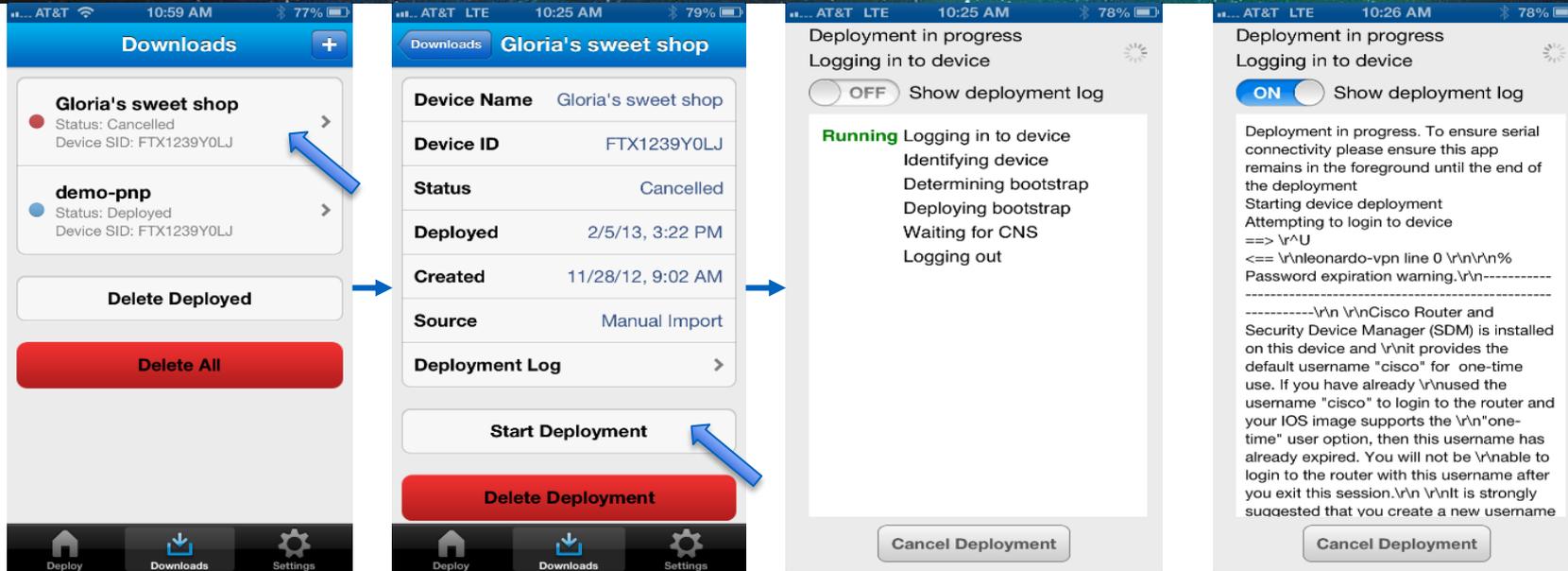
# Deployment Application – iPhone

- Configuration
- Two Deployment Options
  1. Pre-specified
  2. PIN onsite



# Deployment Application – iPhone

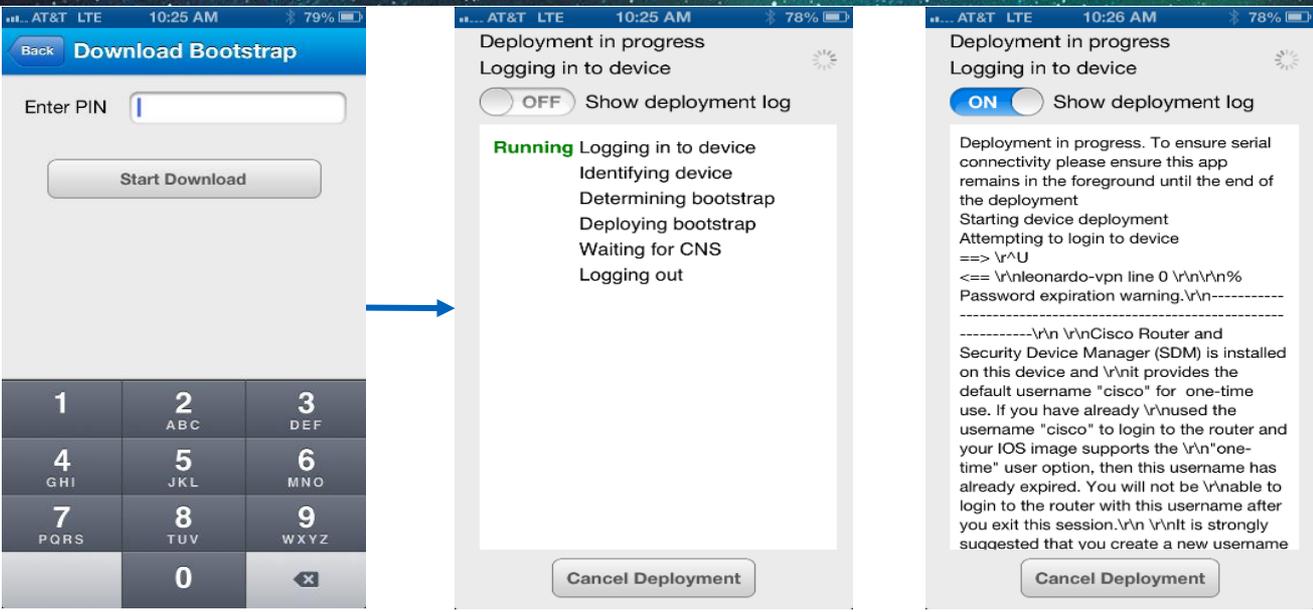
## Option 1 – Device Pre-specified in PI



1. Device Serial Number pre-specified in Prime Infrastructure
2. Bootstrap Configuration downloaded to iPhone application

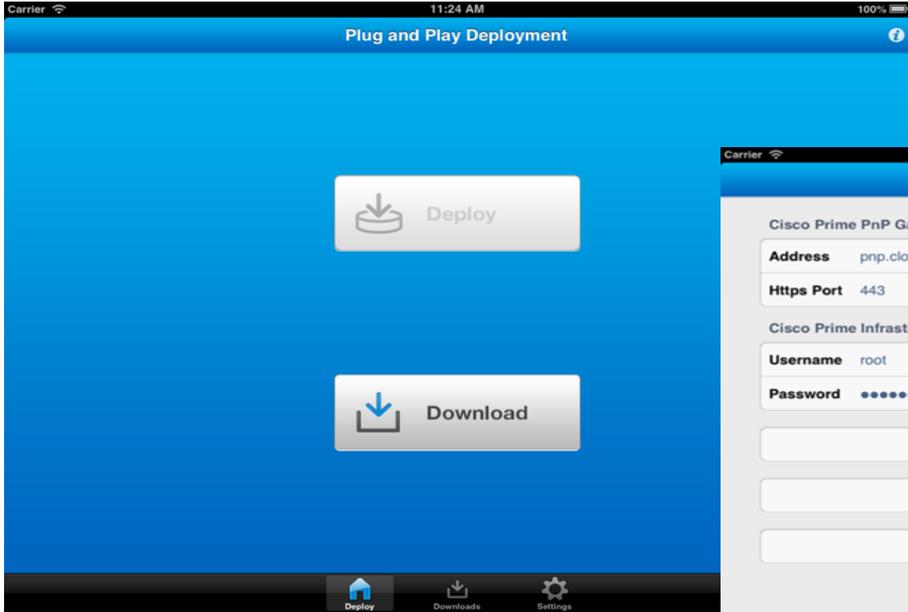
# Deployment Application – iPhone

## Option 2 – Deploy via PIN onsite

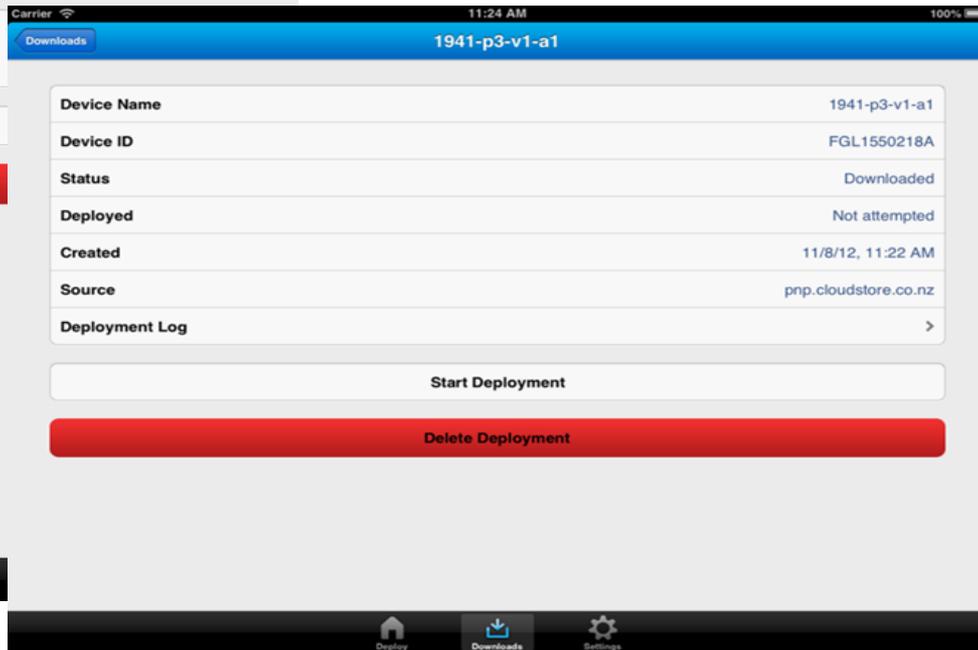
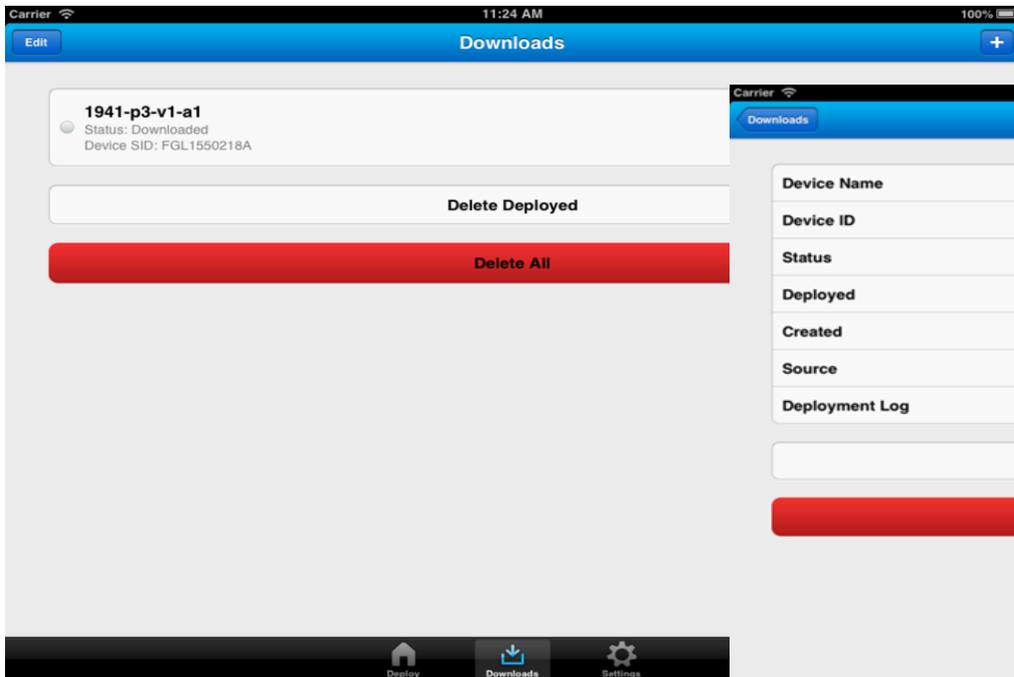


1. User is prompted for PIN for that location/device site
2. PnP App reads the Device Serial Number through the console cable and registers it in Prime Infrastructure via 3G, VPN or other

# Deployment Application – iPad

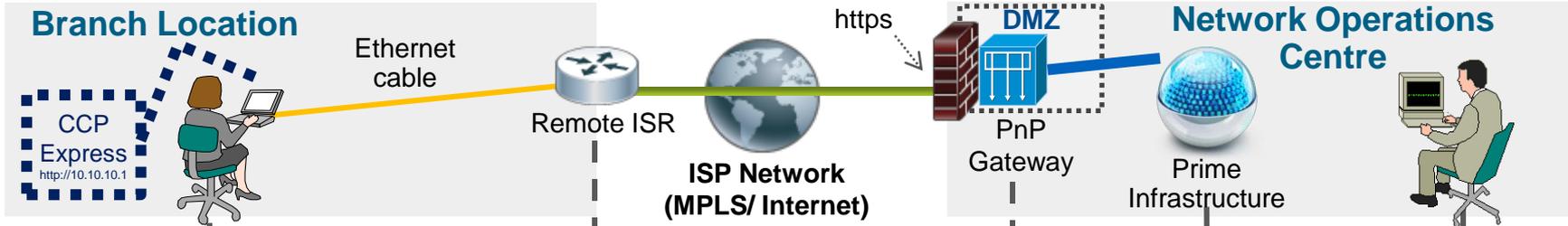


# Deployment Application – iPad



# Plug-n-Play with CCP Express

GUI that optionally comes with the ISR



- 1) Installer calls the NOC admin and requests activation for the ISR Serial number with Plug-n-Play
- 2) Installer connects the PC to the ISR's LAN port
- 3) Installer goes to <http://10.10.10.1> on the PC
- 4) Installer enters WAN config (Eth, DSL, 3G, etc)
- 5) Installer enters CNS server (PnP Gateway) IP address in the respective tab
- 6) ISR connects to PnP Gateway and requests its config based on its serial number
- 7) PnP Gateway gets the ISR full config from Prime
- 8) ISR downloads its config

# Plug-n-Play with CCP Express

GUI that optionally comes with the ISR

- Configure Interface
- Configure CNS



ADD Loopback   ADD VLAN   EDIT   DELETE

Interface	IPv4 Address	IPv6 Address	Admin Status	Operational Status
FastEthernet0	unassigned			
FastEthernet1	unassigned			
FastEthernet2	unassigned			
FastEthernet3	unassigned			
FastEthernet4	192.168.1.100			

**Edit FastEthernet4 Interface**

**IPv4 address**

Type:

HostName:

Enable NAT:

**IPv6 address**



**CNS Server**

CNS Server Hostname:

CNS Server IP Address:

Enable Image Update Service

Apply   Remove CNS Configuration

NOTE: If the server IP Address is not specified, CNS Server requires the fully qualified hostname and the hostname to be resolvable in DNS.

# Summary

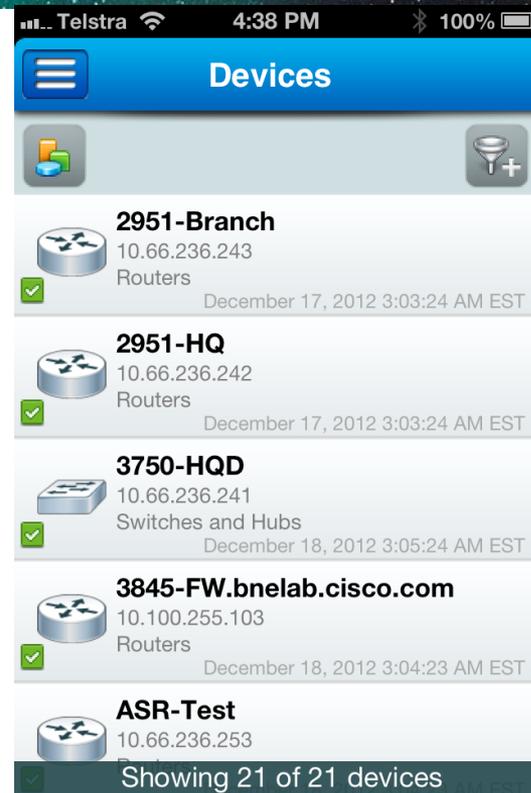
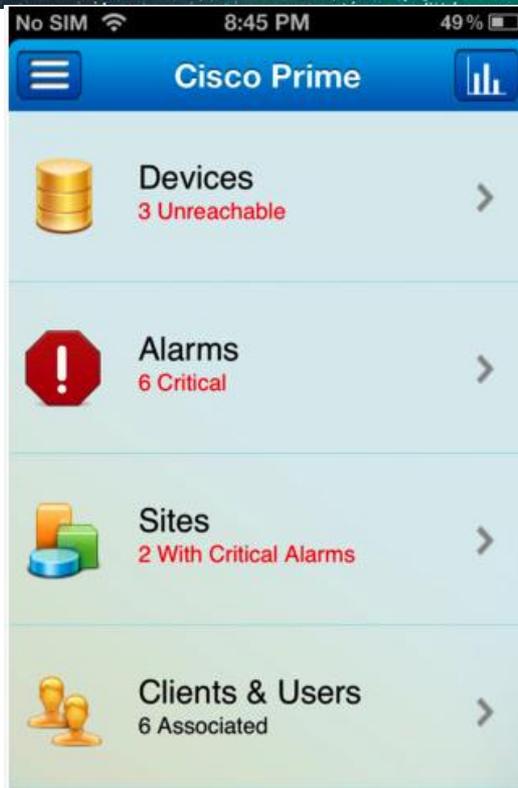
- PnP Gateway server embedded in PI server (2.x and above)
- Standalone PnP Gateway server available (1.2.x and above)
- A Windows based application for Bootstrap/Config
- A iPhone/iPad application for Bootstrap



## Tip 1 – iPhone App and Toolbar

# Prime Infrastructure iPhone App

- Free application on Apple iTunes
- Provides network management summary
- Home screen displays top-level view including alarms
- List view of device inventory
- Device list filtering capability



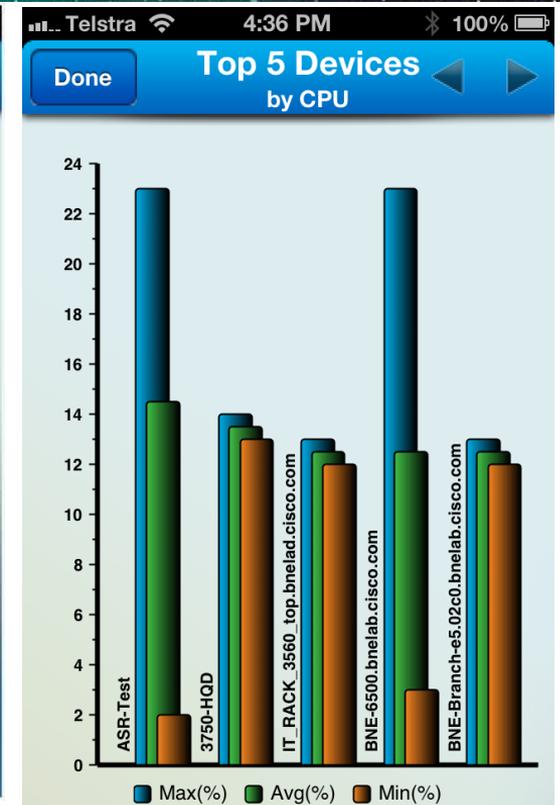
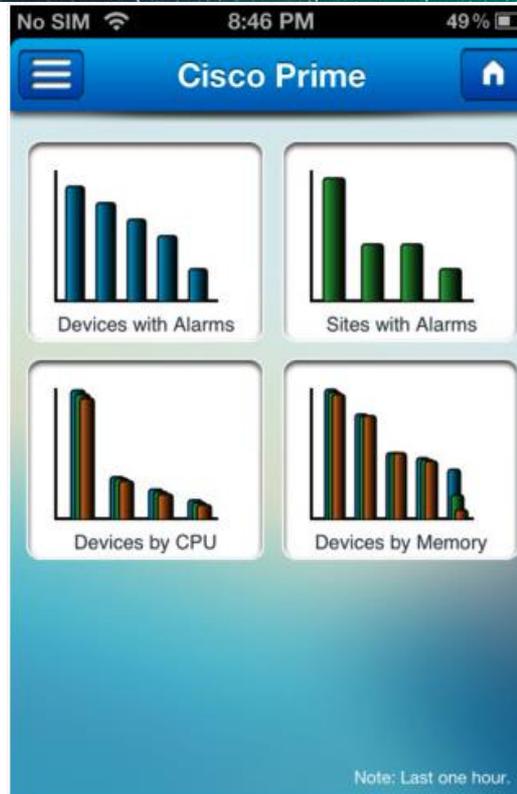
# Prime Infrastructure iPhone App

- Alarm browser
- Annotate Alarms
- Acknowledge Alarms
- Assign Alarm Owner
- Notify others of Alarm



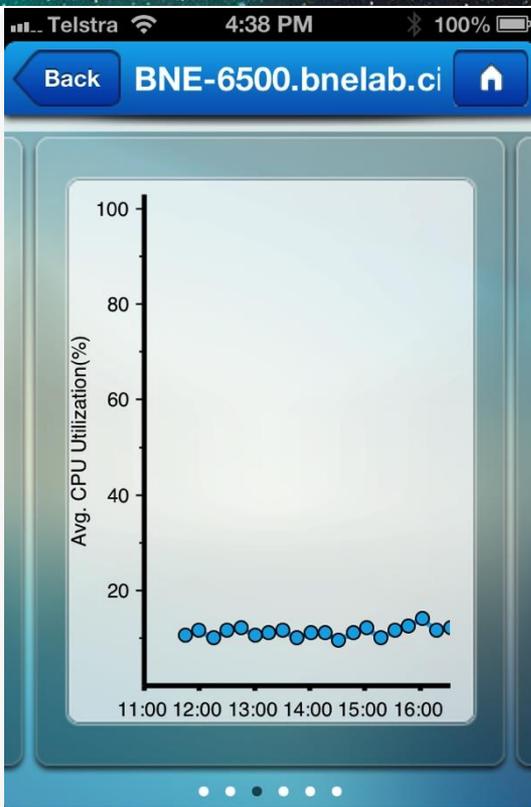
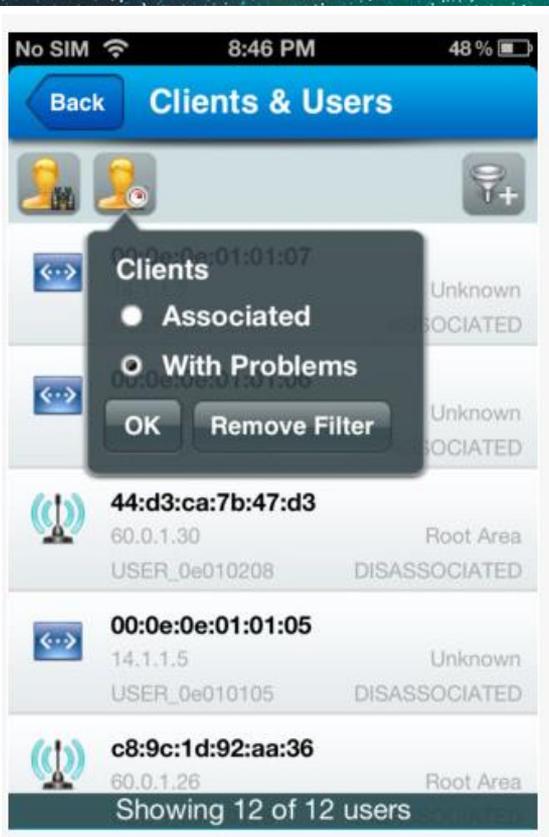
# Prime Infrastructure iPhone App

- Limited Reporting
- Alarm Report
- Alarms by Site
- CPU Utilisation
- Memory Utilisation

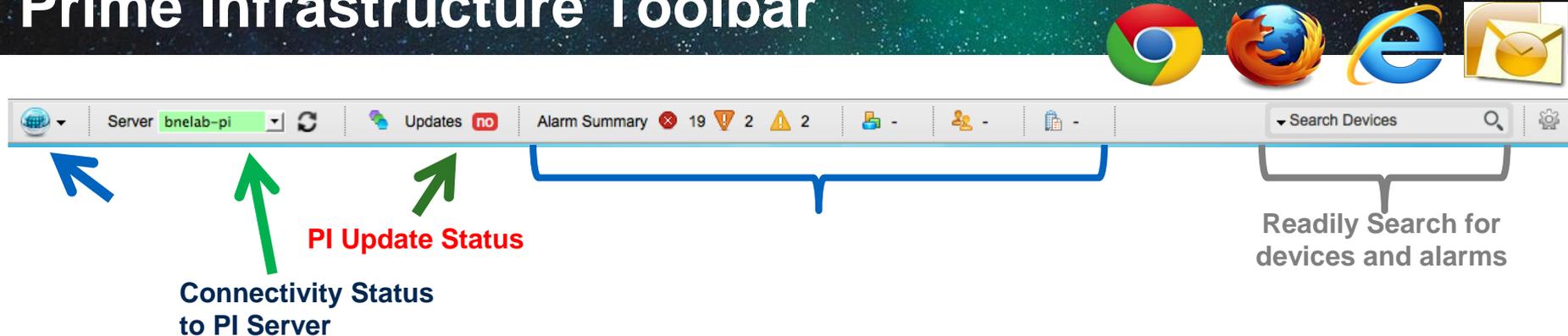


# Prime Infrastructure iPhone App

- Can view list of clients on the network
- Client list filtering capability
- Filter based on user-defined criteria
- Device specific reports



# Prime Infrastructure Toolbar



- At-a-glance, exception-based status – Devices unreachable, clients and sites with issues, active alarms
- Instant search for devices or alarms
- Contextual quick launch directly into Prime Infrastructure
- Live software update notifications – new device support, configuration templates, compliance rules, upgrades, etc.



## Tip 2 – Performing Disk Cleanup

# Performing Disk Cleanup

## Error Message

*The system is running low on disk space, please refer to online help to perform disk cleanup.*

- Run “ncs cleanup”



**The system is running low on disk space,  
please refer to online help to perform disk  
cleanup.**

OK

```
ssh admin@10.66.236.49
admin@10.66.236.49's password:
Last login: Thu Dec 20 07:37:04 2012 from mycomputer
bnelab-pi/admin# ncs cleanup
```

# Performing Disk Cleanup

```
*****
!!!!!!          WARNING          !!!!!!!
*****
The clean up can remove all files located in the backup staging directory.
Older log files will be removed and other types of older debug information
will be removed
*****
Do you wish to continue? ([NO]/yes) yes
*****
!!!!!!          DATABASE CLEANUP WARNING          !!!!!!!
*****
Cleaning up database will stop the server while the cleanup is performed.
The operation can take several minutes to complete
*****
Do you wish to cleanup database? ([NO]/yes) yes
*****
!!!!!!          USER LOCAL DISK WARNING          !!!!!!!
*****
Cleaning user local disk will remove all locally saved reports, locally
backed up device configurations. All files in the local FTP and TFTP
directories will be removed.
*****
Do you wish to cleanup user local disk? ([NO]/yes) yes
*****
=====
Starting Cleanup: Thu Dec 20 12:18:06 EST 2012
=====
(Thu Dec 20 12:20:31 EST 2012) Removing all files in backup staging directory
(Thu Dec 20 12:20:31 EST 2012) Removing all Matlab core related files
(Thu Dec 20 12:20:31 EST 2012) Removing all older log files
(Thu Dec 20 12:20:40 EST 2012) Cleaning older archive logs
(Thu Dec 20 12:20:43 EST 2012) Cleaning database backup and all archive logs
(Thu Dec 20 12:20:43 EST 2012) Removing all user local disk files
(Thu Dec 20 12:21:26 EST 2012) Cleaning database
(Thu Dec 20 12:21:56 EST 2012) Stopping server
(Thu Dec 20 12:24:50 EST 2012) Not all server processes stop. Attempting to stop remaining
(Thu Dec 20 12:24:50 EST 2012) Stopping database
(Thu Dec 20 12:24:53 EST 2012) Starting database
(Thu Dec 20 12:25:21 EST 2012) Starting database clean
(Thu Dec 20 12:42:00 EST 2012) Completed database clean
(Thu Dec 20 12:42:00 EST 2012) Stopping database
(Thu Dec 20 12:43:00 EST 2012) Starting server
=====
Completed Cleanup
Start Time: Thu Dec 20 12:18:06 EST 2012
Completed Time: Thu Dec 20 12:57:10 EST 2012
```

- Warning
- Selective Cleanup
  - Database only
  - User Local only
  - Both



## Tip 3 – Troubleshooting PnP Gateway

# PNP Gateway Troubleshooting Tips

## Integrated PnP Gateway

- PNP Gateway Start, Stop and Status are automatically done as part of the “ncs start”, “ncs stop” or “ncs status” from the admin user
- PNP Enable and Disable used for enabling and disabling of PnP on PI Server is available in “ncs pnp-gateway enable” and “ncs pnp-gateway disable”. By default PnP is enabled on PI Integrated server. Enabling and disabling of PnP would require a restart of PI Server for the changes to take effect.
- PnP Image properties can be obtained by using the “ncs pnp-gateway property image” from the Admin user.
- Modification of image properties can done using the “ncs pnp-gateway modify image <timeout\_type> <timeout value>” command.
- The PnP Log level can be modified from “Administration > Logging > General Logging Options” and modify the level for “pnpgateway”.
- The PnP logs will be generated in /opt/CSColumos/logs directory (shell)
  - pnp\_gateway\_cns.log :- CNS Gateway logs
  - pnp\_gateway\_image.log :- Image update logs
  - pnp\_gateway.log :- Config, Resource and common logs.

# PNP Gateway General Troubleshooting Tips

## Check the PnP Gateway is Working

- Check that PnP Gateway is functioning from Web Browser:
  - Using the Url `https://<PNP IP>/cns/ResourceInit?name=port`
  - Eg `https://10.66.236.26/cns/ResourceInit?name=port`
  - The URL shows The list of ports that are up(plain text and SSL ports) and Number of devices connected to each ports with device id PNP and Device Connection status

```
----- cnsGateway Resource -----  
Total plain-text connection : 2  
  
Port number : 11013 Total connection : 0 Connected Device list :  
  
Port number : 11015 Total connection : 2 Connected Device list :  
CAT0943R27H, FGL150412JU,   
  
Port number : 11017 Total connection : 0 Connected Device list :
```

# PNP Gateway General Troubleshooting Tips

## Check the Device is Working

- Execute “show cns event connections” on Device in exec mode.

```
Router#show cns event connections
The currently configured primary event gateway:
  hostname is bne-pi-pnp.bnelab.cisco.com.
  port number is 11015.
  encryption is disabled.
Event-Id is FGL150412JU ←
Keepalive setting:
  keepalive timeout is 120.
  keepalive retry count is 2.
Connection status:
  Connection Established. ←
The currently configured backup event gateway:
  none.

The currently connected event gateway:
  hostname is bne-pi-pnp.bnelab.cisco.com.
  port number is 11015. ←
  encryption is disabled.
```

# PNP Gateway General Troubleshooting Tips

## Check the Device is Working

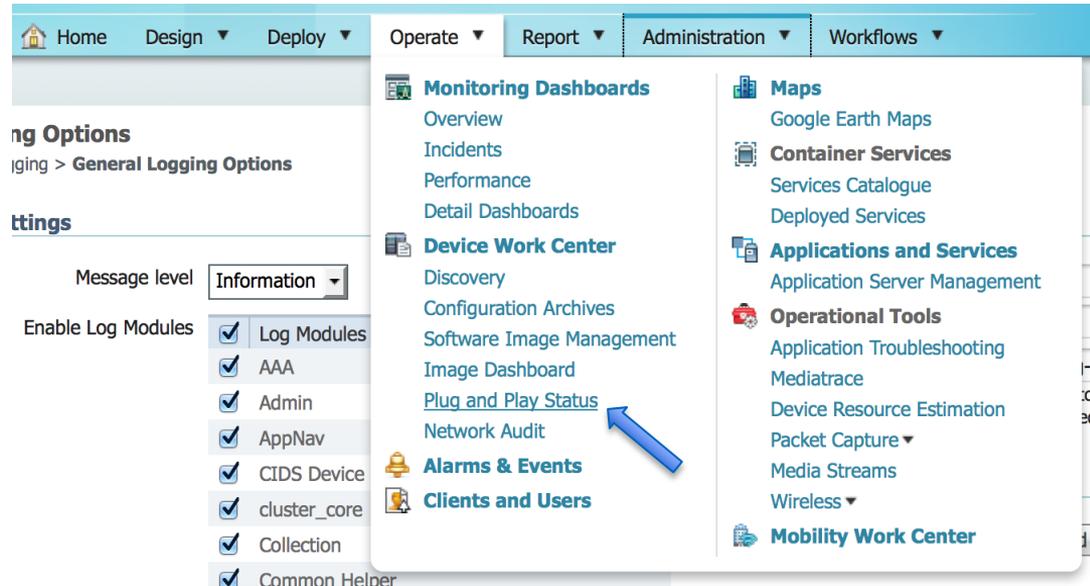
- To debug further on device enable the cns debug logs

```
Router# debug cns all
```

```
Router# sh log
*Mar 6 18:59:17.526: CNS-Trans: _ctwr.ok=2881A14
*Mar 6 18:59:17.526: CNS Event Connection: msg=0x0 17 bytes from gateway
*Mar 6 18:59:17.526: CNS Event Connection: total_len=17 nbytes=17
02912150: 00000011 .....
02912160: 000B0006 00020008 00020001 00 .....
*Mar 6 19:00:34.197: CNS Config Initial: connection timer event
*Mar 6 19:00:34.197: CNS http 1.0: http request-URI length=0x36, http request-
URI=/cns/config.asp?DeviceID=FGL150412JU&cnsPassword=
*Mar 6 19:00:34.197: CNS http 1.0: Attempting http connection to bne-pi-
pnp.bnelab.cisco.com, encrypt = 0
*Mar 6 19:00:34.197: CNS-Trans: _ctop.184.host=bne-pi-pnp.bnelab.cisco.com
*Mar 6 19:00:34.197: CNS-Trans: _ctop.184.v4.fd=0
*Mar 6 19:00:34.197: CNS-Trans: _ctop.184.ok=144CFD5C
*Mar 6 19:00:34.197: CNS-Trans: _ctco.ok=144CFD5C
*Mar 6 19:00:34.197: CNS message: Curdata not at end of blk
*Mar 6 19:00:34.197: CNS-Trans: _ctwr.ok=144CFD5C
*Mar 6 19:00:34.197: CNS-Trans: _ctre.ok=144CFD5C
*Mar 6 19:01:24.237: CNS I/O: socket 0 EOF
*Mar 6 19:01:24.237: CNS Agent Framework: cns_agent_msg_queue_drain function called
*Mar 6 19:01:24.237: CNS Agent Framework: cns_agent_msg_process_internal called
```

# PNP Gateway General Troubleshooting Tips

- To check if the matching profile triggered status on the Prime Infrastructure server: go to Operate→Plug and Play Status
  - This will show the complete details regarding the triggered profile
  - If you want to trigger the same profile again. You need to remove the existing entry from call Home deployment status.



The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar includes tabs for Home, Design, Deploy, Operate, Report, Administration, and Workflows. The 'Operate' tab is selected, and a dropdown menu is open, showing various monitoring and management options. A blue arrow points to the 'Plug and Play Status' link under the 'Device Work Center' section. The left sidebar shows 'Logging Options' with 'General Logging Options' selected, and a list of log modules with checkboxes, all of which are checked. The right sidebar shows a list of services and tools, including Maps, Container Services, Applications and Services, Operational Tools, and Mobility Work Center.

# PNP Gateway Troubleshooting Tips

## External PnP - Certificate issue

- The get the external PnP gateway communicating with the Prime Infrastructure server certificates are required

On a linux host or the Prime Server generate the required certificates:

1. Generate private pnp key 'openssl genrsa -out pnpprivkey.pem 2048'
2. Generate selfsigned pnp key 'openssl req -new -x509 -key pnpprivkey.pem -out pnpcert.pem -days 1095'
3. Get the CPI certificate 'openssl s\_client -showcerts -connect [cpi\_hostname]:443 > cpicert.pem'
4. I then copy all 3 files to the PnP Gateway server
5. Run the 'pnp setup' command and enter the correct path to these certificates

# PNP Gateway Troubleshooting Tips

## External PnP - Managing the External PnP Gateway

- Ensure PnP Gateway is started after Prime Infrastructure server
- To restart PnP Gateway software
  - SSH to PnP Gateway
  - pnp stop
  - pnp start
  - pnp status

```
bne-p1-pnp/admin# pnp status
```

SERVICE	(core/aggregation) portfolio	MODE	STATUS	ADDITIONAL INFO
System	Catalyst 6500 based Innovative Hub Platform		UP	
Event Messaging Bus	40/100G Roadmap through the next decade.	PLAIN TEXT	UP	pid: 4179
CNS Gateway Dispatcher	Prime Core	PLAIN TEXT	UP	pid: 4839, port: 11011
CNS Gateway	Network Virtualization	PLAIN TEXT	UP	pid: 4865, port: 11013
CNS Gateway	Catalyst Intelligent Satellite (PEX) "Slash OnEx" Productive Di	PLAIN TEXT	UP	pid: 4897, port: 11015
CNS Gateway	TrustSec and IPv6	PLAIN TEXT	UP	pid: 4936, port: 11017
CNS Gateway	AVC (Application Visibility Control) and Net	PLAIN TEXT	UP	pid: 4975, port: 11019
CNS Gateway	Fixed Backbone	PLAIN TEXT	UP	pid: 5004, port: 11021
CNS Gateway Dispatcher	Catalyst 4500X	SSL	UP	pid: 5039, port: 11012
CNS Gateway		SSL	UP	pid: 5076, port: 11014
CNS Gateway		SSL	UP	pid: 5124, port: 11016
CNS Gateway	new D'Alton (anddallo -	SSL	UP	pid: 5236, port: 11018
CNS Gateway		SSL	UP	pid: 5438, port: 11020
CNS Gateway		SSL	UP	pid: 5548, port: 11022
HTTPD			UP	
Image Web Service	Alton (anddallo -	SSL	UP	
Config Web Service		SSL	UP	
Resource Web Service		SSL	UP	SW 20121106
Image Web Service		PLAIN TEXT	UP	
Config Web Service		PLAIN TEXT	UP	MR 20120412
Resource Web Service		PLAIN TEXT	UP	

# PNP Gateway Troubleshooting Tips

Ensure the External PnP Gateway is communicating with the Prime Server

- Check PnP Gateway communication with Prime Infrastructure Server
  - and look for the ESTABLISHED connection to the CPI host

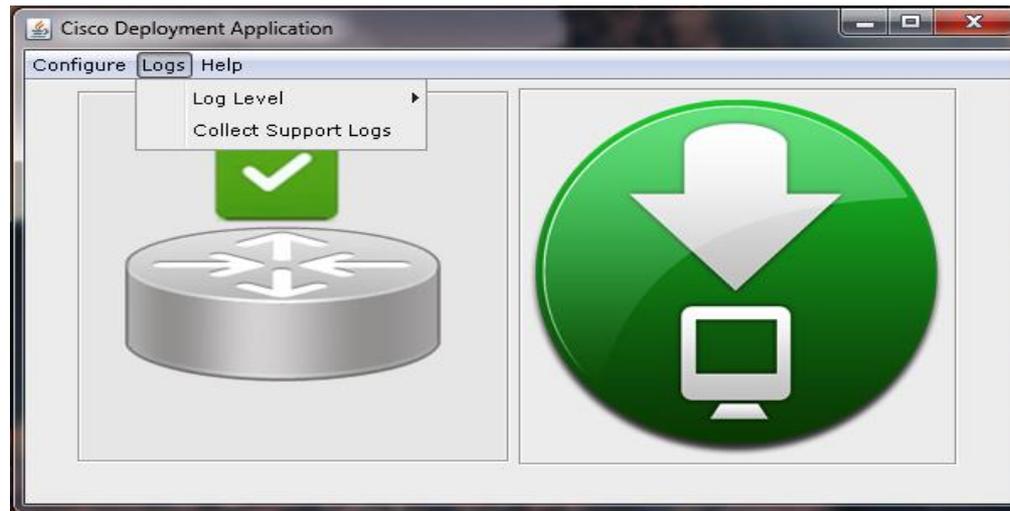
```
sh tech-support | inc 61617  
tcp 0 0 bne-pi-pnp:41741 bnelab-pi.bnelab.cisco.com:61617 ESTABLISHED
```

- On the Prime Infrastructure server in the linux shell check the reverse connection

```
ade # netstat -a | grep 61617  
tcp 0 0 bnelab-pi:61617 :::ffff:10.66.200.38:41741 ESTABLISHED
```

# Deployment Application - Troubleshooting Tips

- In case of any issues the logs are available through the "Logs→Collect Support Logs".
- To change the log level for debugging use the "Logs→Log Level" option



# Useful Documentation

- Cisco Prime Infrastructure Site

<http://www.cisco.com/go/primeinfrastructure>

- Deploying Plug and Play

[http://www.cisco.com/en/US/docs/net\\_mgmt/prime/infrastructure/2.0/user/guide/Cisco\\_Plug-n-Play-Solution-Guide.pdf](http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/2.0/user/guide/Cisco_Plug-n-Play-Solution-Guide.pdf)

- Support Forums

<https://supportforums.cisco.com/community/netpro/network-infrastructure/network-management>

## Americas Edition

Every Week*	Prime Demo Series Topic	Same Time	Same Place
Every Tuesday	Cisco Prime Collaboration Assurance & Provisioning	11:00 AM PST San Jose Time (90 Min)	<a href="http://www.tinyurl.com/primedemo">www.tinyurl.com/primedemo</a>  No Registration Required
Every Wednesday	Cisco Prime NAM & NGA		
Every Thursday	Cisco Prime Infrastructure		

\* Exceptions: US Public Holidays and Cisco Shutdown

## APJC Edition

Every Week*	Prime Demo Series Topic	Same Time	Same Place
Every Thursday	Cisco Prime Infrastructure	12:00 PM Singapore Time (90 Min)	<a href="http://www.tinyurl.com/prime-APJC">www.tinyurl.com/prime-APJC</a>  No Registration Required
Every Tuesday	Cisco Prime Collaboration		

\* Exceptions: Indian Public Holidays and Cisco Shutdown

## EMEAR Edition

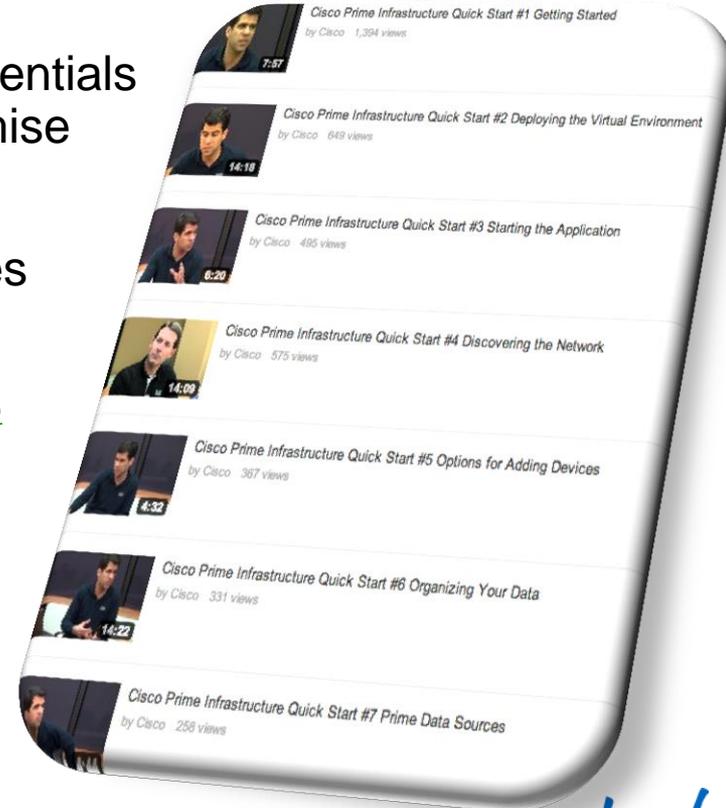
Day	Prime Demo Series Topic	Same Time	Same Place
Every Thursday	Cisco Prime Infrastructure	9:30 AM GMT (90 Min)	<a href="http://www.tinyurl.com/prime-emear">www.tinyurl.com/prime-emear</a>  Registration Required
Every Tuesday	Cisco Prime Collaboration		

**Free Trial Software**

[www.cisco.com/go/nmsevals](http://www.cisco.com/go/nmsevals)

# Prime Infrastructure Quick Start VoD Series

- Detailed, 18-segment Quick Start VoDs cover essentials of how to download, deploy, configure and customise Prime Infrastructure.
- Available on Cisco's YouTube Channel VoD Series available here:
  - <http://www.youtube.com/playlist?list=PL7406F0EF2BC7DED8>



# For More Information

Cisco Prime

[www.cisco.com/go/prime](http://www.cisco.com/go/prime)

Cisco Prime Infrastructure

[www.cisco.com/go/primeinfrastructure](http://www.cisco.com/go/primeinfrastructure)

Cisco Prime Collaboration

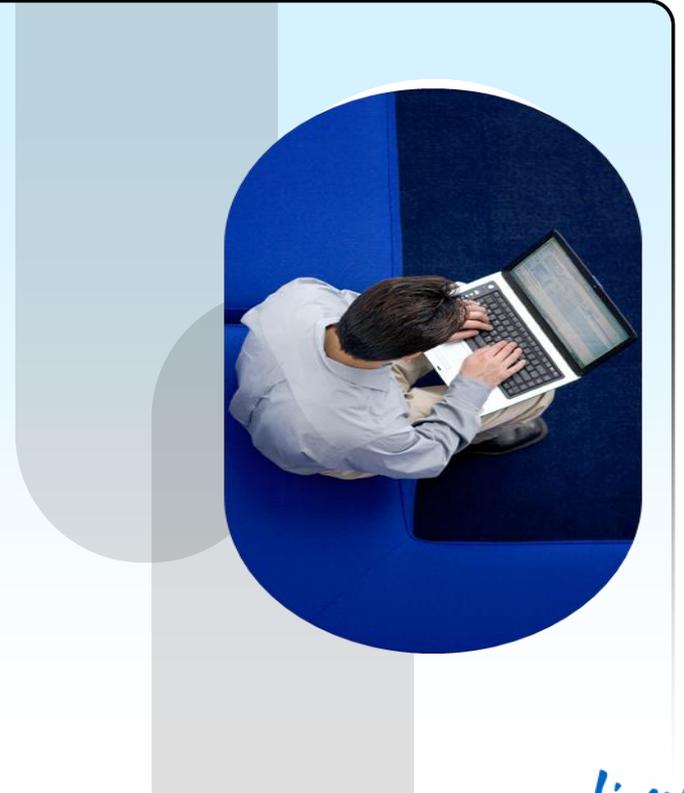
[www.cisco.com/go/primecollaboration](http://www.cisco.com/go/primecollaboration)

Cisco Prime NAM

[www.cisco.com/go/nam](http://www.cisco.com/go/nam)

Prime Demos, VoDs, Online Training, Evaluations

[www.cisco.com/go/prime-demo](http://www.cisco.com/go/prime-demo)



# Summary

- Monitor Everything
- Automate repetitive boring tasks
- If it squeaks you should know about it



Q & A

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



## Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)



**CISCO**™